EAPC - Gestió de la informació: transparència i protecció de dades

El reconeixement facial i la protecció de dades

19-06-2023

Cada cop se sent més a parlar del reconeixement facial. Però exactament, què és? Quines repercussions pot tenir respecte del dret fonamental a la protecció de dades personals? Captar imatges a través de càmeres de videovigilància implica que s'està aplicant el reconeixement facial? En aquest apunt intentaré resoldre aquestes i altres preguntes que ens podem fer sobre aquesta qüestió.

El reconeixement facial és el tractament automàtic d'imatges digitals que contenen les cares de persones amb fins d'identificació, autenticació i verificació o categorització (per edat, sexe, etc.) d'aquestes persones (Dictamen 02/2012 del Grup de Treball de l'Article 29, WP 192).

La diferència entre la identificació i l'autenticació rau que la primera és un procediment per reconèixer la identitat d'una persona, és a dir, qui és aquella persona. I l'autenticació es refereix al procediment per comprovar aquella identitat i determinar que aquella persona és realment qui diu que és. Es veu més clara la diferència en un procediment d'identificació i autenticació basat en el codi d'usuari i contrasenya: a través del codi d'usuari t'identifiques i mitjançant la contrasenya t'autentiques.

Aquesta definició del Grup de Treball de l'Article 29 ha estat actualitzada recentment pel Comitè Europeu de Protecció de Dades (CEPD) en les Directrius 05/2022 sobre l'ús de la tecnologia de reconeixement facial en l'àmbit de l'aplicació de la llei, aprovades el 26 d'abril de 2023, en què exposa que el reconeixement facial és una tecnologia probabilística que permet reconèixer automàticament individus a partir de la seva cara per autenticar-los o identificar-los.

Així, el reconeixement facial és una característica d'un programari que es pot implementar en sistemes existents (càmeres, bases de dades d'imatges, etc.); és a dir, que la captació d'imatges mitjançant càmeres de videovigilància no comporta necessàriament el reconeixement facial, el qual només tindrà lloc si s'utilitza un programari que permeti autenticar i identificar persones físiques.

A grans trets, el reconeixement facial es duu a terme en dues etapes: la primera consisteix a recollir una mostra biomètrica de la cara, de la qual s'extreu una representació digital de diferents característiques anomenada "plantilla". Aquesta plantilla és única i específica per a cada persona i, en principi, permanent en el temps. La segona etapa té per objecte reconèixer la cara mitjançant la comparació de la plantilla corresponent amb una plantilla emmagatzemada o més.

Què podem fer mitjançant el reconeixement facial?

En primer lloc, autenticar una persona, és a dir, verificar que aquella persona és qui diu que és. En aquest cas, el sistema es limita a comparar dues plantilles: la plantilla generada que s'ha enregistrat prèviament i la plantilla que es genera en aquell moment a partir del rostre de la persona que es vol autenticar.

En segon lloc, identificar una persona dins un grup d'individus. Aquest procés es fonamenta en la comparació de la plantilla de la persona que es vol identificar en aquell moment amb altres plantilles que consten en una base de dades i que s'han enregistrat prèviament.

Tant en l'autenticació com en la identificació, el reconeixement facial es basa a deduir una probabilitat que aquella persona sigui la que es vol autenticar o identificar. Si se supera un determinat llindar predefinit, el sistema pressuposa que hi ha coincidència o correspondència i que, per tant, hi ha una probabilitat molt alta que efectivament es tracti de la persona a autenticar o a identificar.

Hi ha una tercera funció que és categoritzar les persones. Consisteix a extreure unes determinades característiques de la imatge d'una persona per classificar-la en una o diverses categories generals (edat, sexe, color de la roba, etc.).

Hi ha tractament de categories especials de dades?

Una de les principals repercussions del reconeixement facial és dirimir si comporta el tractament de categories especials de dades. Respecte de la funció de categorització de les persones és evident que no implica el tractament de categories especials de dades, perquè no s'identifica ni s'autentica cap persona. En canvi, les autoritats de protecció de dades afirmen que el reconeixement facial amb fins d'identificació pressuposa el tractament de categories especials de dades.

En canvi, s'han mantingut criteris dispars pel que fa a l'ús del reconeixement facial amb finalitats d'autenticació. L'Autoritat Catalana de Protecció de Dades (APDCAT) esgrimeix que les dades biomètriques amb fins d'autenticació tenen la consideració de categories especials de dades (Dictamen CNS 21/2020). Per contra, l'Agència Espanyola de Protecció de Dades (AEPD) defensa que no se li pot atorgar aquesta consideració, tot i que en l'informe del seu Gabinet Jurídic núm. 0036/2020 ja advertia que es tractava d'una qüestió complexa, de manera que caldria estar atents als pronunciaments dels òrgans judicials i del CEPD.

L'article 9.1 del RGPD inclou, com a dades de categoria especial, les "dades biomètriques destinades a identificar de manera unívoca una persona física", de manera que es podria interpretar que les dades destinades a autenticar una persona no tenen la consideració de categoria especial, tal com argumenta l'AEPD.

D'altra banda, l'APDCAT incideix que el considerant 51 del RGPD determina que el "tractament de fotografies no s'ha de considerar sistemàticament tractament de categories especials de dades personals, ja que únicament s'inclouen en la definició de dades biomètriques si, quan es tracten amb mitjans tècnics específics, permeten la identificació o l'autenticació unívoques d'una persona física". I afegeix que quan l'article 4.14 del RGPD defineix les dades biomètriques, inclou les que "permeten o confirmen la identificació única" de la persona i, per tant, l'autenticació (que consisteix a confirmar la identificació). El posicionament de l'APDCAT expressat en el dictamen esmentat se sostè finalment en el fet que l'autenticació implica haver identificat abans la persona.

Aquesta disparitat de criteris entre autoritats de protecció de dades, que també afecta altres dades biomètriques com ara l'empremta dactilar, que es pot utilitzar per al control horari de les persones treballadores, ha estat clarificada pel CEPD en les directrius esmentades. El CEPD es posiciona clarament a favor d'atorgar la qualificació de categoria especial de dades a les dades biomètriques emprades amb fins d'autenticació. Per tant, tal com avançava en l'Informe 0098/2022, que es feia ressò de la versió provisional de les Directrius 5/2022 del CEPD sotmesa a consulta pública, previsiblement l'AEPD revisarà el seu criteri per adequar-lo al que manté el CEPD.

Altres repercussions

Seguidament, repassaré breument altres implicacions en el dret fonamental a la protecció de dades personals que pot presentar un sistema de reconeixement facial, d'acord amb el que indica el CEPD en les Directrius 5/2022:

- Altres drets fonamentals: el reconeixement facial pot afectar l'exercici d'altres drets fonamentals com el dret a la intimitat i el dret a la llibertat ideològica, religiosa i de culte; el dret a la llibertat d'expressió; el dret de reunió, o el dret d'associació.

- Licitud: atès que el reconeixement facial determina el tractament de categories especials de dades, és necessari que el responsable fonamenti el tractament de les dades biomètriques en alguna de les bases jurídiques recollides a l'article 6.1 del RGPD, però també esdevé imprescindible que concorri una de les circumstàncies establertes a l'article 9.2 del RGPD que permeten el tractament de categories especials de dades.

- Minimització: només s'haurien de tractar categories especials de dades si és estrictament necessari, és a dir, si és indispensable.

- Lleialtat i transparència: el fet que el reconeixement facial sigui una funció que es pot implementar en un sistema de videovigilància ja existent o que tingui lloc remotament o a distància, implica el risc que les persones afectades desconeguin que s'està duent a terme un tractament de les seves dades de categoria especial si no se les informa adequadament (principi de transparència), la qual cosa també podria vulnerar el principi de lleialtat.

- Exactitud: un dels principals problemes que planteja el reconeixement facial és la fiabilitat i eficiència en la identificació i l'autenticació de persones. Circumstàncies com la qualitat de les imatges, la llum o l'angle en què es capta la imatge poden afectar-ne els resultats. Tot i que aquests sistemes tenen un marge d'error reduït, quan s'utilitzen en llocs freqüentats per milions de persones comporta que centenars de persones poden ser identificades o autenticades incorrectament, de manera que es veu vulnerat el principi d'exactitud de les dades (art. 5.1.*d* del RGPD).

- Avaluació d'impacte relativa a la protecció de dades (AIPD): el CEPD defineix com a requisit obligatori l'execució d'una AIPD.

- Risc d'accés il·lícit: cal partir de la premissa que les característiques físiques a partir de les quals es generen les dades biomètriques són, en principi, inalterables, de manera que la persona interessada no

les pot modificar en el supòsit que la seguretat de les dades es vegi compromesa. Vinculat amb la seguretat de les dades, el CEPD recomana implementar un registre d'accessos o d'operacions.

- Protecció de dades des del disseny i per defecte: la tecnologia emprada ha de garantir els principis relatius a la protecció de dades, com ara la minimització de dades i la limitació de l'emmagatzematge.

Pronunciaments destacats de l'APDCAT

Acabo aquest apunt fent menció als pronunciaments públics de l'APDCAT sobre el reconeixement facial que considero més rellevants:

- Procediment sancionador núm. PS 49/2019. Té l'origen en les notícies publicades en els mitjans de comunicació, que relaten que un determinat institut havia instal·lat un sistema de reconeixement facial per controlar l'assistència dels alumnes a causa del grau d'absentisme. L'APDCAT va sancionar l'institut, entre d'altres, per tractar dades biomètriques de manera il·lícita.

Com a curiositat, segons consta en la resolució, el sistema de reconeixement facial va fallar amb dues persones bessones, la qual cosa es va "resoldre" mitjançant la verificació de la seva identitat a través de l'empremta dactilar, que també és una dada biomètrica de categoria especial.

- Dictamen CNS 2/2022. S'hi aborda la consulta d'un ajuntament referent a la possibilitat d'utilitzar dispositius de control de presència al lloc de treball mitjançant reconeixement facial. L'APDCAT fa una anàlisi del compliment del principi de licitud, del qual es desprèn que el consentiment explícit de l'empleat (art. 6.1.*a* i 9.2.*a* del RGPD) no serviria per legitimar-ne el tractament, atès que el consentiment no seria lliure. En canvi, considera que un conveni col·lectiu, pacte o acord sí que podrien tenir en compte el tractament de dades biomètriques amb la finalitat de controlar la jornada laboral, sempre que estableixin les garanties adequades respecte dels drets fonamentals i dels interessos de les persones interessades, de manera que aquests instruments permetrien concloure la concurrència de l'excepció establerta a l'article 9.2.*b* del RGPD.

Una altra qüestió important és que, a banda del principi de licitud, també s'ha de tenir present la resta de principis, com ara el de minimització. D'acord amb aquest principi s'hauria d'optar per altres sistemes de control que permetin assolir la finalitat pretesa sense necessitat de tractar categories especials de dades.

- Procediment sancionador PS 41/2022. L'APDCAT imposa a una universitat una sanció de 20.000 € per emprar un sistema de reconeixement facial per dur a terme proves en línia. En aquesta resolució, l'APDCAT reitera que les dades biomètriques per identificar els estudiants són categories especials de dades.

Afegeix que el consentiment explícit dels alumnes no era lliure, ja que si no acceptaven obtenien en la prova la qualificació de "no presentat". En la resolució s'argumenta que tampoc no es pot acudir a l'interès públic essencial, a l'interès legítim, i que no és un tractament necessari per a l'execució d'un contracte.

A l'hora d'analitzar les mesures correctores, escau ressaltar que l'APDCAT admet que es pugui continuar utilitzant el sistema de reconeixement facial, però condicionat que s'obtingui el consentiment explícit de les persones afectades i s'hi ofereixi una alternativa que no comporti el tractament de dades biomètriques.

Oriol València Bozal

Advocat, delegat de protecció de dades, consultor i formador al sector públic en matèries de transparència i protecció de dades