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

La biometria dactilar

20-03-2023

En el món digital i tecnològic en què vivim, la biometria s'utilitza com un mètode efectiu, ràpid i senzill per identificar una persona.

D'acord amb l'article 4.14 del Reglament Europeu de Protecció de Dades (RGPD), les dades biomètriques són les dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física, que permeten o confirmen la identificació única d'aquesta persona, com ara imatges facials o dades dactiloscòpiques.

En aquest sentit, les tecnologies biomètriques són mètodes automàtics que s'utilitzen per reconèixer persones sobre la base de l'anàlisi de les seves característiques físiques o de comportament. En funció de la tècnica biomètrica que es fa servir els paràmetres a considerar són diferents.

Per tant, hi ha diferents dades biomètriques. Així, per exemple, podem pensar en l'empremta dactilar, el reconeixement facial, el reconeixement d'iris, el reconeixement de geometria de la mà, el reconeixement de retina, però també en el reconeixement d'escriptura, de signatura i de veu i, fins i tot, en el reconeixement de la forma de caminar.

D'entrada, cal tenir en compte que, amb l'entrada en vigor del RGPD, les dades biomètriques adreçades a identificar de manera unívoca una persona física es consideren una categoria especial de dades personals (art. 9.1), de manera que el tractament requereix que, a més d'una base jurídica de l'article 6.1, concorri també alguna de les excepcions que estableix l'article 9.2.

Encara més, el Comitè Europeu de Protecció de Dades i l'Autoritat Catalana de Protecció de Dades han considerat que les dades biomètriques, tant en la vessant d'identificació com en la d'autenticació, sempre són categories especials de dades si s'adrecen a la identificació unívoca d'una persona física, amb independència de la tècnica que s'ha utilitzat per captar-la.

Ens centrarem aquí en l'empremta dactilar.

La biometria dactilar és el procés que s'utilitza per identificar una persona a través de les seves empremtes dactilars. El sistema escaneja les empremtes per verificar la identitat d'una persona i concedir-li un permís o accés.

La biometria dactilar té molts avantatges, entre els quals la seguretat, la precisió i la fiabilitat que proporciona, atès que les empremtes dactilars són úniques perquè identifiquen directament la persona (patró únic), són inalterables, ja que no canvien durant la seva vida i, a més, són difícils de falsificar.

Per contra, la fiabilitat com a sistema d'identificació està condicionada per l'envergadura amb què es puguin utilitzar aquests sistemes d'identificació. Com més gran sigui el nombre de sistemes d'identificació que es basen en dades biomètriques o en una plantilla obtinguda a partir de dades biomètriques, més elevat és el risc que la dada biomètrica es pugui utilitzar de manera inadequada i donar lloc a un risc de suplantació d'identitat.

A banda d'això, també cal tenir en compte que l'ús de l'empremta dactilar pot tenir punts febles associats a les condicions del dit i de la pell en el moment d'agafar la mostra (moll/a, sec/a, brut/a, etc.), a les condicions de l'empremta (talls, ferides, inflamacions, etc.), a les condicions climatològiques que afecten el lector (humitat, temperatura, etc.) i, fins i tot, vulnerabilitats relacionades amb l'àmbit laboral, ja que hi ha activitats que poden afectar l'empremta, com són totes les relacionades amb productes químics, que la poden deteriorar.

Entre els usos de la biometria dactilar, destaquem, a tall d'exemple, el control d'accessos físics i lògics, el control de presència, el control d'accés a un servei digital o el control d'accés a aparells com els dispositius mòbils i portàtils i a aplicacions informàtiques.

Per això, és habitual veure que l'empremta dactilar s'utilitza per accedir a complexos esportius i gimnasos o al lloc de treball, per fitxar a la feina (control de presència) i fins i tot per accedir als centres educatius o als menjadors escolars en què, a més a més, també es recullen dades de menors, considerats pel RGPD un col·lectiu vulnerable.

Ara bé, això no significa que l'ús de l'empremta dactilar hagi de ser el sistema més eficient o el mitjà preferent per dur a terme aquestes finalitats, atesa l'especial naturalesa d'aquestes dades i el grau d'intrusió i impacte en els drets i les llibertats de les persones afectades i en la seva privacitat.

En altres paraules, abans d'implementar un sistema biomètric, cal analitzar les característiques de l'entitat, la naturalesa, l'àmbit, el context i les finalitats del tractament, els riscos majors que se'n poden derivar per a les persones afectades, el cost, etc., perquè el que pot ser adequat per a una entitat amb tractaments complexos que involucren moltes persones i tipus de dades pot no ser-ho per a una organització més petita i amb tractaments més senzills.

Un altre punt és que, a banda que el tractament sigui lícit (art. 6 i 9), també s'han d'aplicar els altres principis de protecció de dades (art. 5). i el tractament de l'empremta dactilar ha de complir, entre d'altres, els principis de limitació de la finalitat i de minimització de dades, de manera que el tractament ha de ser necessari, proporcional, adequat i pertinent en relació amb la finalitat del tractament per tal de no vulnerar el dret fonamental a la protecció de dades de les persones afectades.

En particular, vull destacar el **principi de minimització**, que no només comporta que si cal tractar dades únicament es poden recollir les mínimes indispensables i necessàries per assolir la finalitat pretesa, sinó que exigeix també que si la finalitat es pot aconseguir sense tractar dades de categories especials (en aquest cas, dades biomètriques destinades a identificar de manera unívoca una persona física), aquesta opció ha de prevaler davant les altres opcions que puguin comportar el tractament d'aquests tipus de dades.

Això vol dir que cal escollir la tecnologia que resulti menys intrusiva des del punt de vista de la protecció de dades i en aplicació de la protecció de dades des del disseny i per defecte (art. 25).

L'objectiu és evitar tractar dades de categories especials si no és estrictament necessari. Així, com a mostra, en el cas del control horari es poden utilitzar altres mitjans com les targetes personals i, per exemple, en el cas del control d'accés a un servei digital es pot emprar una contrasenya en lloc de l'empremta dactilar.

A més, pel que fa a la **proporcionalitat** en el tractament, d'acord amb la jurisprudència (STC 186/2000), per comprovar si una mesura restrictiva d'un dret fonamental respecta el principi de proporcionalitat, cal que compleixi tres requisits: que sigui susceptible d'aconseguir l'objectiu proposat (judici d'idoneïtat); que sigui necessària, en el sentit que no hi hagi una altra mesura més moderada per aconseguir aquest propòsit amb la mateixa eficàcia (judici de necessitat), i que sigui ponderada o equilibrada, en derivar-se més beneficis o avantatges per l'interès general que perjudicis sobre altres béns o valors en conflicte (judici de proporcionalitat en sentit estricte).

En concret, cal determinar si tractar l'empremta dactilar és una mesura idònia per aconseguir la finalitat pretesa (control d'accés, control horari, etc.) o aquesta es pot aconseguir amb mitjans que envaeixin menys l'esfera íntima de les persones amb la mateixa eficàcia.

Per tant, la implementació d'aquesta tècnica biomètrica ha de ser avaluada d'acord amb criteris de proporcionalitat, necessitat i impacte en els drets i llibertats de les persones físiques afectades en relació amb la finalitat del tractament.

En tot cas, amb caràcter previ al tractament, a la posada en marxa d'un sistema de control d'aquest tipus, és necessari fer una avaluació de l'impacte relativa a la protecció de dades, ateses les implicacions tecnològiques del sistema emprat, el tractament de dades d'una categoria especial (biomètriques) i l'alt risc que implica l'ús d'aquestes dades biomètriques adreçades a identificar de manera unívoca una persona física, en la qual cal avaluar tant la legitimitat del tractament i la seva proporcionalitat, com la determinació dels riscos existents i les mesures per mitigar-los (CNS 63/2018).

Així mateix, cal fer una anàlisi de riscos per establir les mesures tècniques i organitzatives adients per garantir un nivell de seguretat adequat, atenent la naturalesa especialment protegida d'aquest tipus de dades, de manera que potser és necessari adoptar mesures de seguretat reforçada en la recollida, l'emmagatzematge i la conservació de les dades com, per exemple, el xifrat, no tractar l'empremta en brut o, fins i tot, extreure una plantilla o patró específic per al sistema d'identificació i la seva conversió mitjançant un algoritme.

Tot això, és clar, sense obviar el compliment de la resta d'obligacions establertes a la normativa de protecció de dades.

Si us interessa aquest tema, podeu consultar, entre d'altres, els dictàmens següents: CNS 21/2020, CNS 63/2018 i CNS 38/2017, que trobareu al web de l'APDCAT.

Montserrat Rof Bertrans

Consultora sènior de l'Autoritat Catalana de Protecció de Dades