



DIA DE PROTECCIÓ
DE DADES 2020

Biometria:

AFFECTACIÓ EN MATÈRIA DE PROTECCIÓ
DE DADES



ap
da

Agència Andorrana
de Protecció de Dades



TAULA DE CONTINGUTS

1. INTRODUCCIÓ

2. LA BIOMETRIA

- a. *Què entenem per biometria?*
- b. *Tipus de tècniques.*
- c. *Estatus en protecció de dades: riscos, principis, obligacions i drets dels interessats.*

3. BIOMETRIA I ÀMBIT PARTICULAR

- a. *Smartphones*
- b. *Apps*
- c. *Comerç*

4. BIOMETRIA I ÀMBIT LABORAL

- a. *Finalitat i justificació*
- b. *Dades tractables*
- c. *Tipus d'emmagatzematge*
- d. *Conservació*
- e. *Consentiment dels treballadors*

5. BIOMETRIA I ÀMBIT PÚBLIC I LAW ENFORCEMENT (L.A)

- a. *Base*
- b. *Necessarietat*
- c. *Futur del reconeixement facial.*

6. CONCLUSIONS

INTRODUCCIÓ



La biometria forma part de l'avantguarda de les novetats que dia a dia la tecnologia aporta.

Planerament, la biometria **és la mètrica relacionada amb característiques humanes**. Malgrat pugui sonar a matèries pròpies de la ciència ficció, cada cop que desbloquegem la pantalla del nostre smartphone amb l'empremta digital o amb un mètode de reconeixement facial o quan li preguntem a assistents de veu com la Siri o l'Alexa quin temps farà demà estem utilitzant tecnologies biomètriques. Aquests usos poden semblar més innocus però la realitat és que **les possibilitats que ofereix la biometria sobre els àmbits d'aplicació d'aquests mètodes són incalculables**.

Les formes d'identificació biomètrica **actuen tant com una forma d'identificar als interessats com una forma d'autenticar la seva identitat**, donant així l'aparença de ser mètodes que garanteixen la seguretat de matèries sensibles o confidencials. El seu àmbit d'aplicació creix dia a dia i ja podem veure com **el seu ús s'expandeix en múltiples disciplines**: seguretat pública i supòsits penals, militars, l'àmbit transfronterer, l'àmbit civil, medicina i prestacions socials, àmbit laboral, aplicacions comercials, etc.

Alhora, les dades emprades per aquestes tècniques aporten moltes avantatges per als responsables de tractament ja que **es tracta de dades universals a totes les persones úniques, permanents, mesurables, emmagatzemables, i difícilment falsificables**.

Tots aquests valors fan que les tecnologies i les dades biomètriques siguin un **actiu econòmic** cada vegada més rellevant.

INTRODUCCIÓ

Malgrat el caràcter especial d'aquest tipus de tecnologies, que es basen en aspectes tan íntims com pot ser el propi cos de l'interessat, resulta curiós que **les provisions legals que en regulen l'ús no són molt nombroses i les que existeixen, fan una remissió genèrica a les normes en protecció de dades** sense conferir un estatus específic a aquest tipus de tractaments.

Per tal de reconèixer aquestes particularitats, el Reglament General Europeu en matèria de Protecció de Dades (en endavant RGPD), text legal de la Unió Europea amb voluntat clara d'harmonitzar els estàndards de protecció a nivell internacional, **va descriure les dades biomètriques com a «dades sensibles»** i en prohibeix el tractament a no ser que es provi que l'interessat va consentir expressament al mateix o que es tracta d'una matèria d'interès i seguretat pública (entre d'altres excepcions).

Amb la present guia, l'Agència andorrana de protecció de dades vol aportar una visió genèrica sobre **què entenem per dades biomètriques i els impactes que el tractaments de les mateixes poden tenir sobre els particulars en diferents àmbits del seu dia a dia.**



2. QUÈ ENTENEM PER BIOMETRIA?

La Biometria és un grup de **tècniques** que permeten que una persona sigui identificada o autenticada en base a una sèrie de **dades reconeixibles i verificables que li son úniques i específiques**.

D'acord amb el RGPD es defineixen les dades biomètriques com les dades que resulten de l'aplicació de tècniques específiques de tractament de **dades físiques, psicològiques i de comportament** d'una persona física que en permet la seva identificació (art. 4) que mereixen de **protecció especial** (art. 9).

Així doncs, podem afirmar que per a que siguin efectives les dades biomètriques han de ser **úniques, permanents i que puguin recollir-se**.

Exemple de tractament de dades biomètriques:

Una empresa introdueix un sistema d'escaneig d'empremtes digitals per a regular els horaris dels treballadors i l'accés a les instal·lacions. Aquest sistema tracta dades biomètriques amb l'objectiu d'identificar a una persona física així que l'empresa necessita d'una justificació vàlida per a aquest tractament.

L'ús de tècniques biomètriques respon a **dos objectius**:

- **La identificació biomètrica:** és el procediment de determinar la identitat de la persona. L'objectiu doncs és recollir un element concret de dades biomètriques d'una persona (una fotografia de la seva cara, un enregistrament de veu, una imatge de la seva empremta digital, etc). aquest element es compara amb el d'altres persones i s'emmagatzema en una base de dades. Aquest objectiu busca respondre a la pregunta «Qui és vostè?».
- **Autenticació biomètrica:** és el procediment de comparar les característiques de la persona amb l'arxiu de dades emmagatzemat per a trobar-hi semblances. Existeix doncs un mode de referència en una base de dades que es compara amb les dades recollides en aquell moment per autenticar que la identitat de la persona es correspon amb aquella emmagatzemada. Podríem dir doncs que aquest objectiu respon a la pregunta: «És vostè el sr./la sra. X?».

QUINS TIPUS DE TÈCNIQUES BIOMÈTRIQUES EXISTEIXEN ACTUALMENT?



El reconeixement facial o les empremtes digitals són només dos exemples de tècniques biomètriques però no és un llistat exhaustiu. Dins de les tècniques **podem distingir tres tipus: les físiques/sensorials, les de comportament i les biològiques.**

TÈCNIQUES FÍSQUES / SENSORIALS

El processament d'aquest tipus de dades biomètriques es fa a través de la digitalització d'imatges, enregistraments o mostres per tal de crear una plantilla o un perfil que s'emprarà per trobar coincidències i ajudar a la identificació.



Reconeixement empremtes digitals: captura de la imatge i establiment de patrons. El seu ús és comú en tota mena d'àmbits: policial, de seguretat, tràmits, comerç, etc.



Reconeixement facial: captura de la imatge i establiment de patrons i trets distintius. S'empra habitual en àmbits de seguretat i de law-enforcement, malgrat ja és comú el seu ús per desbloquejar dispositius com smartphones o ordinadors portàtils.



Reconeixement d'iris i retina: captura de la imatge i establiment de patrons. S'empra habitualment a l'àmbit de la seguretat.



Geometria de l'orella, de la mà o dels dits: captura de la imatge i establiment de patrons.



Reconeixement d'olor: captura d'una mostra i establiment de patrons que la facin identificable.



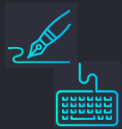
Reconeixement de veu: enregistraments d'audio emprats per analitzar les ondes sonores de la veu del particular. S'empra per verificar la identitat o per donar instruccions assistents de veu.

QUINS TIPUS DE TÈCNIQUES BIOMÈTRIQUES EXISTEIXEN ACTUALMENT?



TÈCNIQUES DE COMPORTAMENT

El processament d'aquest tipus de dades es basa en analitzar la forma amb la que l'interessat interactua amb un sistema informàtic per tal d'analitzar la fluïdesa, la velocitat, etc.



Reconeixement de la signatura o de la velocitat d'escriure amb teclats: existeixen dues formes d'anàlisi la estàtica (captura d'una imatge de la signatura) i dinàmica (analitza els moviments de l'interessat per tal de produir la signatura).. En el cas de la velocitat de teclejar s'emprarà per considerar si l'interessat està familiaritzat amb el que escriu.



Reconeixement de mirada: anàlisi de la forma i els patrons que segueix l'interessat amb la seva mirada.



Reconeixement de la forma de caminar: la forma de caminar o la velocitat també es poden capturar mitjançant imatges per tal d'identificar als particulars.

TÈCNIQUES BIOLÒGIQUES

El processament d'aquest tipus de dades es basa en analitzar aspectes relatius a la biologia de l'interessat per tal d'identificar-lo.



Identificació d'ADN: identificar al particular a través de l'anàlisi de segments concrets del seu ADN.



Reconeixement de venes: anàlisi dels patrons que crea el sistema circulatori de cada particular en un punt concret del seu cos (mans, dits, etc).



LA BIOMETRIA I LA PROTECCIÓ DE DADES.

RISCS INHERENTS AL TRACTAMENT DE DADES BIOMÈTRIQUES

Tal i com hem vist, les dades biomètriques tenen la consideració de dades personals ja que permeten identificar a particulars i a més a més, tenen la consideració de dades sensibles. Aquest darrer punt implica doncs que **la llei confereix a aquest tipus de dades una protecció especial i per tant, convindrà analitzar per una banda els riscos que presenten per tal de dissenyar un sistema de seguretat adient per a protegir-les.**

Podem veure com fàcilment existeixen riscos inherents al tractament de dades biomètriques com pot ser la **irreversibilitat** de subsanar filtracions o de ciberatacs.

Com hem dit, en el cas de dades biomètriques cal tenir en compte que **les mateixes són permanents per tant, no es poden modificar.** Per exemple, en el cas de la filtració d'una contrasenya, aquesta pot canviar-se ràpidament. Ara bé, les dades biomètriques d'un particular es mantenen inalterables així que si es veuen compromeses no es pot recuperar el control sobre les mateixes.

Un altre dels riscos inherents al tractament de dades biomètriques és **la impossibilitat de la normativa de mantenir-se al dia de les constants novetats que apareixen i dels nous mètodes** per tal de tractar nou tipus de dades. Per aquest motiu és convenient que les mesures de seguretat adoptades pels responsables de tractament siguin flexibles i permetin la seva constant actualització.

LA BIOMETRIA I LA PROTECCIÓ DE DADES.

PRINCIPIS RECTORS

Conscients d'aquests riscos, els responsables de tractament han d'aplicar una sèrie de principis rectors a la seva actuació amb dades personals de tipus biomètric.

Aquests principis són 5:

- **Objectiu concret i legítim.** Quan es recullen dades biomètriques convé informar extensament i clarament de les finalitats per les quals es fa aquesta recollida. Alhora, qualsevol tractament o ús d'aquestes dades més enllà de les previstes i informades a l'interessat, es considerarà il·legítim de ple dret.
- **Proporcionalitat.** En el moment d'optar per un sistema de tractament de dades biomètrics cal dur a terme una ponderació per tal de veure si aquests sistemes són els adequats i adients per complir amb l'objectiu concret i legítim anteriorment citat. Cal valorar doncs criteris com la necessitat i la proporcionalitat de les mesures en base a la ingerència a la intimitat dels particulars que provoquen.
Així doncs convindria que els responsables valoressin si existeixen mitjans menys invasius que permetin complir amb el mateix objectiu i, de així existir, optar per aquests últims.
- **Precisió.** Les dades biomètriques hauran de ser pertinents a la finalitat per la qual es recolliren i exactes. Aquesta exactitud és de vital importància per tal d'evitar casos d'usurpació d'identitat.
- **Minimització de dades.** Només podran tractar-se, cedir-se i emmagatzemar-se dades personals biomètriques necessàries i no tota la informació que estigui disponible al responsable.
- **Termini de conservació adequat.** Ja en el moment de la recollida convindrà determinar un període de conservació que mai podrà ser superior al necessari per a dur a terme la finalitat concreta i legítima. Alhora convindrà garantir que un cop hagi transcorregut aquest període les dades es suprimiran de qualsevol sistema d'emmagatzematge i no es tractaran en cap cas.



LA BIOMETRIA I LA PROTECCIÓ DE DADES.

OBLIGACIONS DEL RESPONSABLE I DRETS DELS INTERESSATS

Tal i com hem vist fins ara, **la seguretat** en la recollida de dades biomètriques ha de ser la preocupació principal de responsables de tractament i dels interessats arran de la naturalesa irrevocable d'aquest tipus de dades.

Els drets dels interessats en dades biomètriques són els mateixos que en qualsevol recollida de dades (a consentir lliurement, drets ARSO, etc). És en el **dret a la informació en el que trobem especificitats** ja que la persona interessada haurà de ser informada del tipus de dades biomètriques recollides, la finalitat de la mateixa, la base legal per al tractament de dades, la font d'obtenció, la forma de control sobre les mateixes (*serà el propi usuari qui emmagatzemarà les dades o una base de dades encriptada?*), possibles destinataris d'aquestes dades, etc. De no complir amb aquest deure d'informació, qualsevol cessió de dades de l'interessat es considerarà nul·la ja que no fou consentida plenament.

Obligacions específiques dels responsables de tractament en dades biomètriques:

- Informar degudament a l'interessat i obtenir-ne un consentiment exprés i informat.
- Establir un sistema de recollida i tractament de dades biomètriques basat en la protecció de la intimitat by design i by default: tant en el seu disseny com en la implantació el mecanisme emprat ha de tenir en compte i garantir en tot moment la intimitat i la confidencialitat de les dades recollides i la seva configuració ha de ser d'entrada la més restrictiva a possibles afectacions d'aquests drets.
- Avaluar l'impacte sobre la intimitat que pot tenir aquest mecanisme. Aquestes no només hauran d'identificar els riscos inherents al tractament sinó també haurà de proporcionar les mesures adequades de protecció i buscar les solucions més adients per atenuar aquests riscos.
- Establir mesures tècniques i organitzatives que assegurin la confidencialitat i la seguretat de les dades tractades.



EL CONSENTIMENT

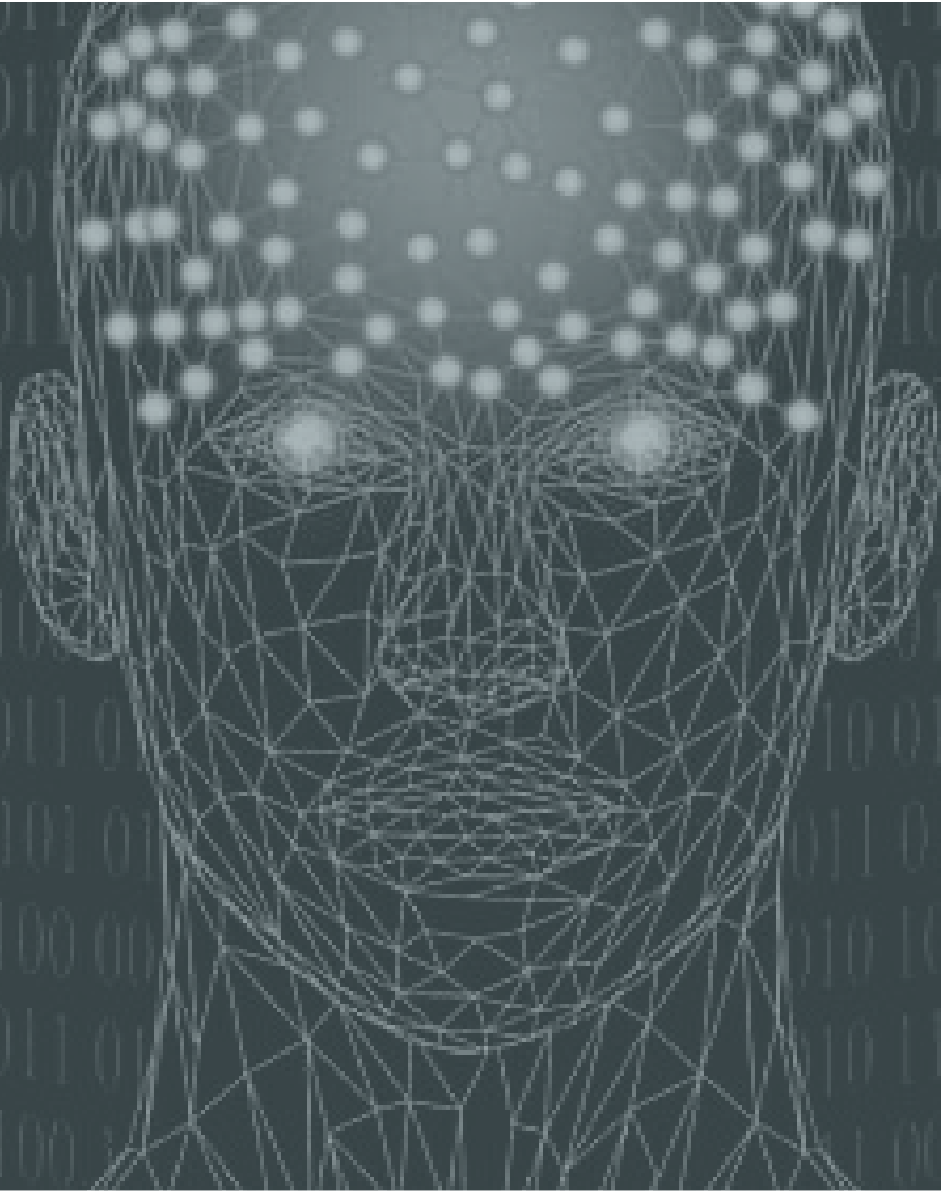
Tal i com s'ha mantingut tant en la normativa andorrana com a l'europea es defineix al consentiment com una **manifestació de voluntat, expressa, lliure, específica i informada, mitjançant el qual l'interessat consenteix al tractament de les seves dades personals**. Així doncs, entenent que el fet de condicionar l'acceptació de les condicions generals la oferta o la prestació d'un servei no serà un consentiment lliure.

Concretament en el cas de dades biomètriques fins i tot es considera que el fet de **no proporcionar una alternativa vàlida a l'autenticació per biometria suposarà un vici en el consentiment donat** ja que el mateix no haurà estat donat amb totes les garanties.

Alhora, cal recordar que el consentiment **ha de poder-se revocar en qualsevol moment** i per tant, els responsables de tractament hauran d'adoptar les mesures tècniques necessàries que puguin esborrar les dades biomètriques del seu sistema.



3. LA BIOMETRIA EN L'ÀMBIT PERSONAL



Cada dia podem veure com més **tècniques biomètriques es posen al servei de la vida quotidiana dels particulars i consumidors** per funcions més senzilles (com podria ser l'ús del reconeixement facial com a mètode de desbloqueig del nostre smartphone) i convé doncs **conscienciar dels riscos i dels drets garantits als interessats** que tenen aquest tipus de tècniques en diferents àmbits.

A. LA BIOMETRIA I ELS SMARTPHONES.

En els darrers anys hem vist com els smartphones han anat **incorporant mètodes de recollida de dades biomètriques per tal d'autenticar la identitat de l'usuari** per a determinades funcions: desbloquejar l'aparell, realitzar pagaments segurs, etc.

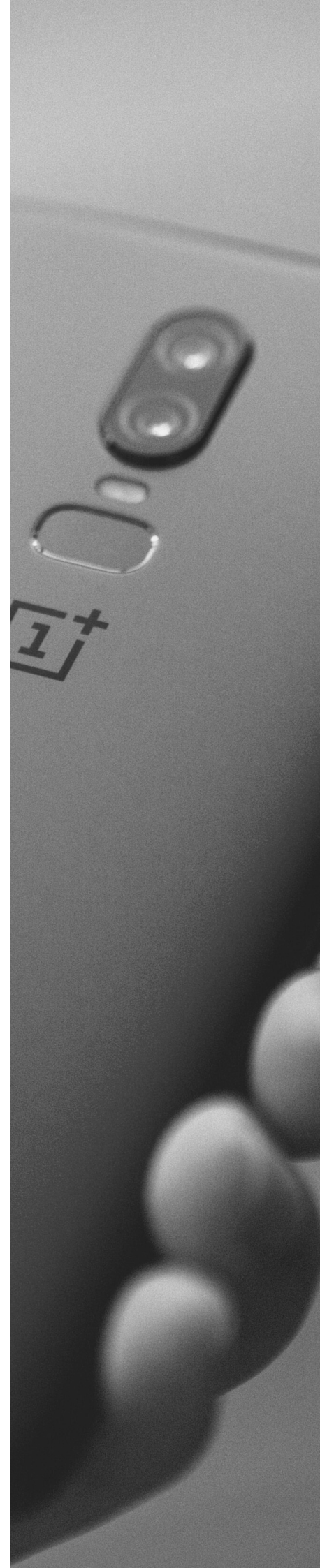
Aquests mètodes s'incorporen de forma automàtica al nostre dispositiu i moltes vegades **l'usuari desconeix que pot optar per altres formes** d'autenticació.

Així doncs podem distingir **dos tipus de dispositius**: aquells que emmagatzemen les dades biomètriques al propi aparell i aquells que ho fan en servidors o núvols.

La primera configuració és habitual en aquest tipus d'aparells i permet que les **dades biomètriques no surtin més enllà del dispositiu** i que estiguin sota el control de l'interessat.

- En aquests casos, serà necessari que el dispositiu garanteixi la seguretat de les dades i la impossibilitat d'accedir-hi de forma extern i ofereixi una alternativa que no impliqui una recollida de dades,

Els dispositius biomètrics que emmagatzemen les dades en servidors externs en canvi presenten més problemes ja que l'interessat en perd el control que passa a ser exclusivament del responsable de tractament. En aquests casos, l'empresa a qui pertanyi aquest dispositiu haurà d'analitzar de forma prèvia els riscos inherents a aquest tipus de tractaments de dades per a les llibertats i els drets dels interessats.





B. LA BIOMETRIA EN APPS.

Des de filtres graciosos a transformacions radicals del nostre aspecte, Cada vegada veiem com més **aplicatius gratuïts demanen que l'usuari cedeixi a la companyia responsable** d'aquestes aplicacions una imatge del nostre rostre. Altres fins i tot ens demanen que portem un dispositiu extern que mesurarà aspectes tan variats com la nostra freqüència cardíaca, les nostres hores de descans o la quantitat de passes que fem en un dia.

Però perquè? Com hem dit la majoria d'aquestes apps son gratuïtes però el que desconeix l'interessat que **el preu que paga per emprar-les és la cessió de les seves dades personals.**

Aquestes sovint es cedeixen a tots els col·laboradors de l'empresa responsable de l'aplicatiu i **l'interessat en perd qualsevol tipus de control.** Les dades recollides doncs **es posen a disposició de virtualment qualsevol empresa** per tal que configuri perfils, ens envii publicitat dirigida en base al nostre estil de vida, es creeïn perfils falsos a les xarxes o en altres àmbits.

En la majoria d'aplicatius a més a més es condiona l'ús del **mateix a l'acceptació d'unes condicions i polítiques de privacitat** que l'interessat no arriba a llegir mai.

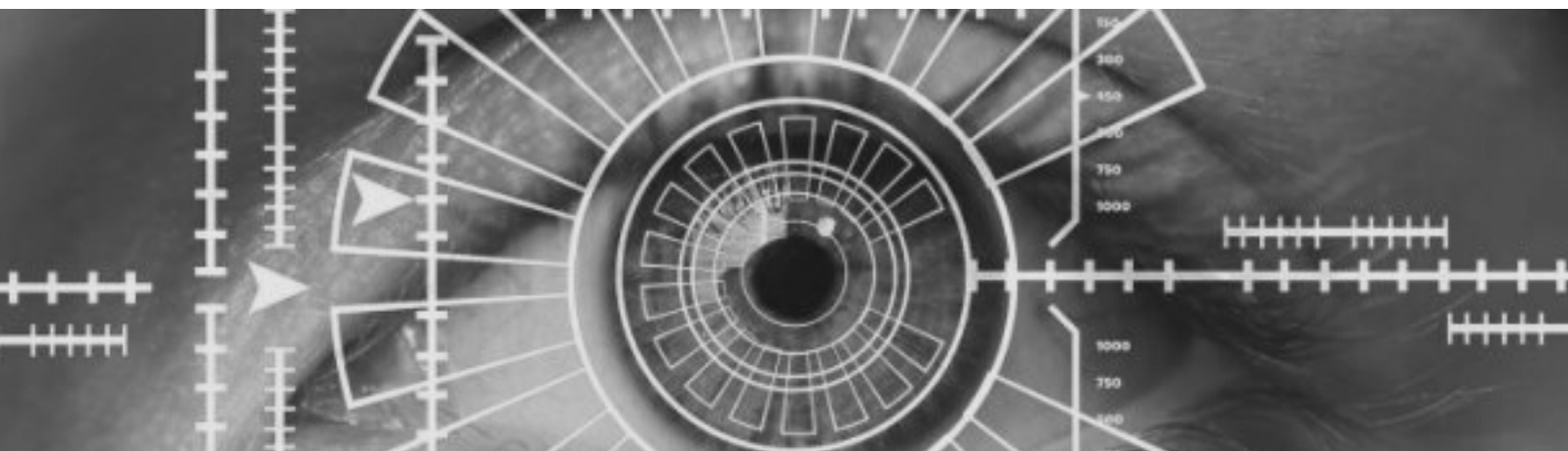
L'ús d'aplicatius que recullen dades personals, i especialment dades biomètriques, ha de condicionar-se sempre a que **l'interessat en conegui les conseqüències.** Aquestes només apareixeràn en aquestes condicions i polítiques d'ús per tant resulta vital que els interessats se les llegeixin abans d'utilitzar-les.

C. BIOMETRIA I COMERÇ

En el comerç online els responsables han de fer front a diferents reptes de seguretat arran de la vulnerabilitat que suposa per al client exposar-se a pràctiques tan habituals com el frau, els hackeigs, spams o el robatori de dades confidencials. Així, veiem que **els responsables de tractament busquen constantment millorar el seu apartat de seguretat online** no només per a que les transaccions siguin més fluides sinó per generar en el client una confiança que garantirà que torni a optar pels seus serveis.

Amb aquesta idea en ment podem veure com la biometria com a mètode per tal d'aprovar o dur a terme pagaments o transaccions proporciona un sistema fluït, ràpid i segur que dona per una banda **aparença de seguretat** i de l'altra, permet en molts casos que l'interessat mantingui el **control sobre les seves dades biomètriques**. Cal remarcar però que en el cas d'optar per mètodes biomètrics per a la autenticació d'usuaris serà responsabilitat del venedor o del proveïdor dels serveis de que, en cas de detectar algun tipus d'accés indegut o divulgació de dades, canviar els mecanismes d'autenticació; ja que, com hem vist, la informació basada en qualitat físiques o sensorials de l'interessat és immutable en el temps.

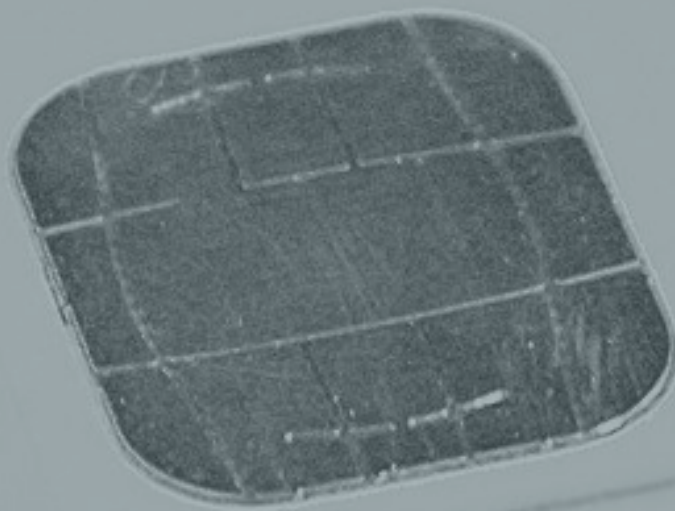
A part de l'exemple comentat de transaccions comercials online podem veure com aquest tipus de tècniques són adoptades cada vegada més sovint per altres àmbits com ara les entitats bancàries. En el cas de transaccions bancàries **on sigui obligatòria la autenticació de l'usuari, mètodes com el reconeixement facial o de veu poden ajudar a agilitzar aquestes verificacions**. Ara bé, per tal d'assegurar que l'interessat no perdi el control sobre aquestes dades, la informació biomètrica recollida ha d'emmagatzemar-se o bé en un dispositiu en possessió de l'interessat o en una base de dades centralitzada i encriptada a la que només podrà accedir a les dades biomètriques la persona afectada.



4. LA BIOMETRIA EN L'ÀMBIT LABORAL

L'amenaça dels atacs cibernètics, on les dades personals de milers de persones es poden veure compromesos, ha fet que **moltes empreses recorrin a nous mètodes de seguretat** per tal d'evitar aquests hackeigs.

La biometria sol presentar-se com la solució a aquests problemes ja que suposa una nova capa en el **marc de l'autenticació dels treballadors i alhora permet establir un control dels accessos del mateixos** combinant tant claus personals amb aspectes biomètrics.



4. LA BIOMETRIA EN L'ÀMBIT LABORAL

L'amenaça dels atacs cibernètics, on les dades personals de milers de persones es poden veure compromesos, ha fet que moltes empreses recorrin a nous mètodes de seguretat per tal d'evitar aquests hackeigs.

La biometria sol presentar-se com la solució a aquests problemes ja que suposa una nova capa en el marc de l'autenticació dels treballadors i alhora permet establir un control dels accessos del mateixos combinant tant claus personals amb aspectes biomètrics.

La biometria en l'àmbit laboral permet implementar un sistema mitjançant el qual el treballador registra alguna dada biomètrica tant com a mecanisme de fitxar com per tal d'accedir a dades confidencials de l'empresa. Així podem veure com aquests mètodes resulten especialment atractius per a empreses que vulguin dur a terme aquest tipus de controls o vulguin optar per aquests mètodes de seguretat.

Ara bé, les empreses que vulguin implantar aquests sistemes hauran de tenir en compte que els mecanismes emprats hauran de respectar una sèrie d'exigències legals i concretament de la normativa de protecció de dades, donant èmfasi a la necessitat de complir amb els principis rectors de tractament de dades, els drets dels interessats o qualsevol altre precepte d'aplicació.

Així doncs hem de distingir, entre d'altres diferents aspectes com ara les finalitats permeses per a aquestes tècniques i la seva justificació, el tipus de dades que podem recollir, les tècniques més adients a emprar en cada cas, la conservació de les dades, la recollida del consentiment del treballador i les avaluacions d'impacte a dur a terme abans de la instal·lació.

4. LA BIOMETRIA EN L'ÀMBIT LABORAL

FINALITAT I JUSTIFICACIÓ

Recórrer a dispositius biomètrics en l'àmbit laboral ha de respondre a una finalitat legítima i concreta. Al tractar-se d'un mecanisme molt intrusiu en la intimitat dels treballadors, l'ús de dades biomètriques només es podrà restringir a:

- controlar l'accés a les instal·lacions o a locals o zones identificades pel propi empresari com a zones de circulació restringida.
- controlar l'accés a aplicatius o dispositius informàtics professionals especificats pel responsable de tractament.

Alhora convindrà justificar l'ús d'aquestes tècniques per sobre de mecanismes tradicionals d'organització o de control. Així doncs, el responsable haurà d'especificar en un document:

- el context específic que fa necessària l'adopció d'un sistema de protecció més elevat;
- les raons que justifiquen l'ús d'una tècnica biomètrica per sobre d'una tradicional.

DADES PERSONALS TRACTABLES:

DADES IDENTIFICATIVES

Són dades recollides pel responsables basades en **identificar als treballadors**. Poden referir-se a:

- Identitat: *nom, cognom, fotografies, enregistraments en brut de dades biomètriques, número d'autenticació o de suport individual, contrassenyes, etc.*
- Vida professional: *número de registre intern, lloc de treball.*
- Accessos: *zones permeses, zones restringides, dispositius permesos i horaris autoritzats.*

DADES DERIVADES

Són dades **generades pels dispositius de tractament de dades biomètriques** com és el registre d'accessos a zones o dispositius i el seu control.

4. LA BIOMETRIA EN L'ÀMBIT LABORAL

TIPUS D'EMMAGATZEMATGE DE DADES BIOMÈTRIQUES

TIPUS A

Les dades biomètriques recollides i emmagatzemades en **dispositius en possessió i control exclusiu de la persona interessada** (els treballadors). Ex: una targeta identificativa.

TIPUS B

Les dades biomètriques **són emmagatzemades en un sistema controlat pel responsable** (l'empresari) però són conservades en una forma que les fa inservible a no ser que **s'introdueixi una clau o un suport controlat per l'interessat**. Ex: Base de dades protegides amb múltiples contrassenyes.

TIPUS C

Les dades són **emmagatzemades i controlades pel responsable de tractament de forma exclusiva**. Ex. Sistema biomètric per a fitxar amb dades biomètriques.

En el supòsit que els responsables vulguin optar per mesures d'emmagatzematge de tipus B o C hauran de **justificar de forma profusa i per escrit la necessarietat** d'aquestes mesures.

Cal tenir en compte també que les mesures de seguretat a adoptar per part dels responsables de tractament **s'establiran en base al risc previsible** inherent al tractament de dades biomètriques.



4. LA BIOMETRIA EN L'ÀMBIT LABORAL

CONSERVACIÓ DE DADES BIOMÈTRIQUES

En el cas de la conservació de dades biomètriques en l'àmbit laboral cal distingir segons el tipus de dades de que es tractin.

Dades en brut.

Es tracta de les imatges, els àudios, que capturen la dada biomètrica a tractar. Aquestes dades només es podran conservar durant el temps necessari per a la seva digitalització o transformació en càlculs o plantilles. Un cop feta aquesta transformació, han de destruir-se.

- Les dades biomètriques que es generin hauran d'encriptar-se de forma que no es pugui recalculer les característiques biomètriques d'origen i hauran de conservar-se durant el temps d'habilitació del treballador.

Dades derivades.

Les dades generades pels dispositius de tractaments de dades biomètriques hauran de conservar-se en el propi dispositiu durant un termini màxim de 6 mesos des del seu enregistrament. Si aquestes dades es traslladen a un dispositiu diferent, es podran conservar durant més temps sempre que aquesta pròrroga es justifiqui en un imperatiu legal o una necessitat del responsable per a complir amb les seves funcions.

Dades identificatives.

Les dades diferents a les dades biomètriques que es vinculin a les mateixes (nom del treballador, càrrec professional, etc) hauran de suprimir-se en un termini màxim de 6 mesos a comptar des de la inhabilitació del treballador en qüestió. Aquesta supressió no afecta a dades similars o idèntiques que el responsable de tractament tracti per a finalitats diferents a les finalitats que justifiquen la recollida de dades biomètriques.

4. LA BIOMETRIA EN L'ÀMBIT LABORAL

CONSENTIMENT DELS TREBALLADORS

Tal i com s'ha especificat en el primer apartat d'aquesta guia, **la obligació d'informar és un dels pilars que legitimen el tractament** de dades biomètriques.

Així doncs, el responsable de tractament haurà d'informar als seus treballadors, per escrit, del **tipus** de dades biomètriques recollides, la **finalitat** de la mateixa, la **base legal** per al tractament de dades, la font d'obtenció, la **forma de control** sobre les mateixes, possibles **destinataris** d'aquestes dades, etc. Davant aquesta informació, l'interessat (treballador) haurà de **consentir**.

Ara bé, en l'àmbit laboral convé qüestionar **fins a quin punt el treballador és lliure** de consentir arran de la dinàmica de poder entre les dues figures. Per aquest motiu, en supòsits que el responsable condicioni l'acceptació de les mesures a la continuïtat al lloc de treball o no ofereixi mesures no biomètriques alternatives, **s'entendrà que el consentiment prestat pel treballador no serà vàlid**.



5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I LAW ENFORCEMENT (L.A)



Entenem per *law enforcement* com la **prevenció, la investigació, la detecció i la persecució de delictes o l'execució de sentències penals**, incloent les accions dutes a terme per a la prevenció d'amenaques a la **seguretat pública**.



5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I L.A

El reconeixement facial o les empremtes digitals són només dos exemples de tècniques biomètriques però no és un llistat exhaustiu. Dins de les tècniques **podem distingir tres tipus: les físiques/sensorials, les de comportament i les biològiques.**

COM FUNCIONA EL SISTEMA DE RECONeixEMENT FACIAL?

Durant els darrers mesos hem vist com molts estats i administracions públiques han optat per la instal·lació de sistemes de reconeixement facial en punts estratègics i públics com són duanes, estacions de transport públic o aeroports. Aquests sistemes es basen en un **tractament de dades en temps real mitjançant el qual es capta la imatge de tota persona mitjançant càmeres de videovigilància.** Les imatges llavors es processen per un software de reconeixement facial que produeix una plantilla biomètrica de cada rostre.

Aquestes plantilles llavors **es comparen amb una base de dades** de persones d'interès creada per autoritats legitimades com el cos policial de l'Estat en qüestió i organismes policials supranacionals.

Si el software estipula que entre la imatge captada en temps real i alguna de les cares de la base de dades **hi ha semblances suficients, es procedeix a la comprovació de la identitat de la persona interessada** per part del personal de seguretat d'aquests espais públics per veure si, efectivament, es tracta d'alguna de les persones llistades per les autoritats de law enforcement.

5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I L.A

QUINA HA DE SER LA BASE PER A AQUESTS TRACTAMENTS?

En la recollida d'aquestes dades biomètriques s'afectaran els interessos tant de persones presents a les llistes de persones d'interès com de particulars que no hi constin. Així convindrà que el tractament de dades descrit haurà d'ajustar-se sempre a les limitacions de la normativa de protecció de dades.

Així les dades podran recollir-se si el tractament de dades:

- és **legítim** (d'acord amb els principis prevists a l'art. 11 de la Llei 15/2003, de 18 de desembre, qualificada de protecció de dades i a l'art. 6 del Decret del 9-6-2010, d'aprovació del Reglament de l'Agència andorrana de protecció de dades).
- Es fonamenta en una **disposició legal** que estableixi de forma prèvia uns usos clars, precisos i previsibles. Alhora, aquesta norma haurà de revisar-se de forma periòdica per tal d'adaptar-la als avenços científics i tecnològics.
 - *Pot un particular preveure de forma raonable que la seva imatge es reculli i tracti amb aquesta pràctica?*
- Es basa en el **consentiment** de l'interessat o en la **seguretat pública** (aquest últim, caldrà justificar la necessarietat de la mesura arran del seu caràcter excepcional).
 - *Consentiment?* Ha de ser una manifestació de voluntat, expressa, lliure, específica i informada, mitjançant el qual l'interessat consenteix al tractament de les seves dades personals.

Al mateix temps convindrà que el responsable de tractament conscienciï, formi i posi a l'abast dels treballadors que duren a terme la recollida d'aquestes dades biomètriques de la normativa de protecció de dades, dels riscos i les bones pràctiques d'aquestes tècniques.

5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I L.A

LA NECESSARIETAT

Al tractar-se d'un tractament de dades considerades sensibles, la justificació per l'ús d'aquestes mesures ha de ser més elevat; així que cal fixar-se en el criteri de la necessarietat. La necessarietat es basa en els principis de proporcionalitat i efectivitat.

Així, el responsable haurà de considerar si el tractament d'aquestes dades sensibles és proporcional a la finalitat perseguida i si no es pot optar per mesures alternatives al reconeixement facial o la recollida de dades biomètriques. Fàcilment podem deduir que l'ús de tecnologies com el reconeixement facial hauria de limitar-se a la persecució de crims greus i no optar per un auge d'aquest tipus de mètodes per a delictes menors o, fins i tot, infraccions administratives.

Per tant, l'ús de tècniques com el reconeixement facial serà més respectuosa amb la normativa de protecció de dades com més concreta sigui la finalitat per la qual s'empra i com menor sigui l'escala d'afectats a la que es pensa aplicar.



5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I L'A

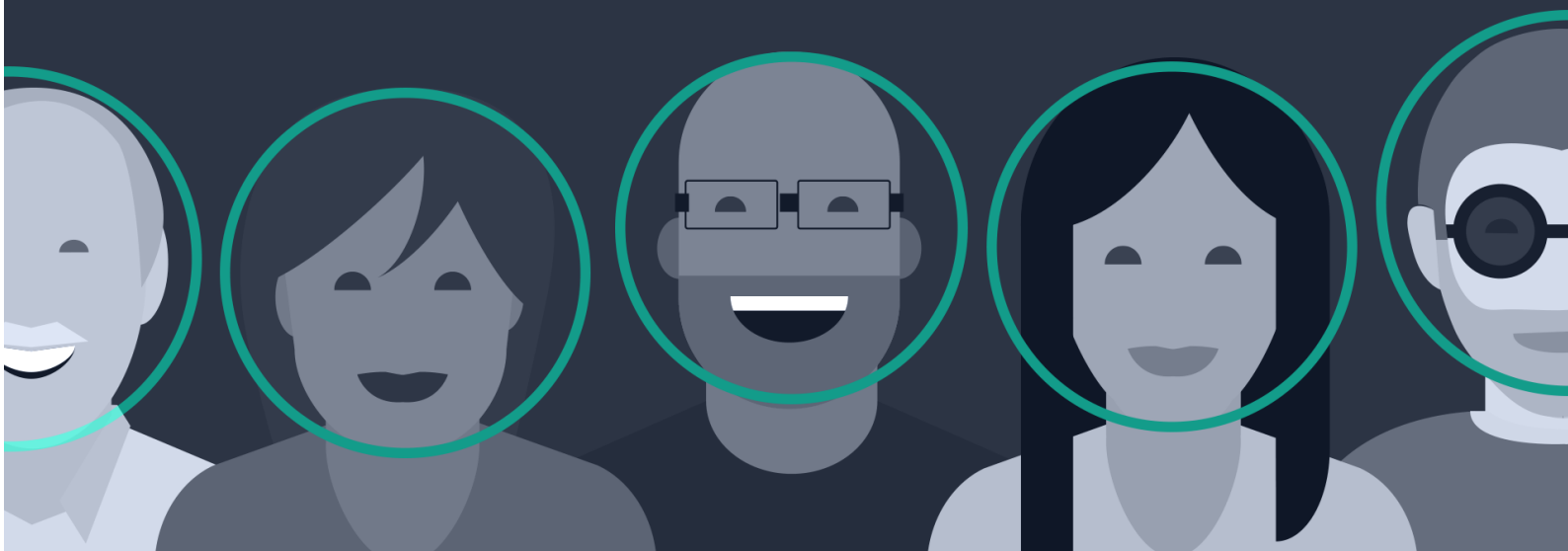
LA NECESSARIETAT

Cal considerar també que un ús indiscriminat d'aquestes tècniques provocaria que la confiança de la opinió pública en aquest tipus de mesures fes que els potencials interessats deixessin de poder preveure clarament les conseqüències esdevenint llavors el tractament il·lícit.

En aquest sentit, un exemple clar de principi afectat podria ser el de la minimització de dades. Així, les llistes de persones d'interès haurien d'incloure només aquells casos que siguin més greus.

Ens referim a efectivitat com la valoració que ha de fer el responsable de valorar si les mesures preses són les que, en relació a la intromissió a la intimitat que suposen, garanteixen al màxim els beneficis que es volen obtenir d'emprar tècniques com el reconeixent facial. En aquest cas, l'efectivitat no ha de valorar-se amb criteris com el número de coincidències i de falsos positius sinó que l'ús d'aquestes mesures es mostri útil i beneficiós per al ciutadà en la prevenció de delictes penals greus. La informació suficient i completa que cal proporcionar als potencials interessats abans de procedir al tractament de les seves dades biomètriques serveix per a que els mateixos puguin entendre de la necessarietat d'aquestes mesures i així crear una conscienciació de prevenció de delictes i de respecte a la intimitat.





5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I L.A

EL FUTUR DEL RECONeixEMENT FACIAL

Com hem vist la recollida i tractament de dades biomètriques, i més concretament, dades derivades d'un mecanisme de reconeixement facial comporta una sèrie de riscos per a la intimitat dels interessats amb conseqüències tant lesives que es comencen a sentir veus des de la Comissió Europea que parlen d'una possible prohibició d'aquest tipus de tècniques durant un futur pròxim. Malgrat això, el negoci del reconeixement facial s'estima com un negoci a l'auge que en menys de 5 anys doblarà el seu volum de negoci. Les principals crítiques versen doncs sobre l'eficàcia d'aquests mètodes ja que bàsicament presenten un risc de mal ús que es tradueixi en una vigilància generalitzada.

D'acord amb l'executiu de la Unió Europea el principal repte passa per regular aquestes tècniques per tal de garantir els drets dels ciutadans. Amb aquest objectiu en ment, s'ha preparat per part de la Unió un llibret blanc sobre consells i bones pràctiques en matèria de reconeixement facial (que es publicarà al Febrer de 2020) i ha proposat la prohibició d'aquest tipus de tècniques als espais públics durant un termini de 2 a 3 anys.

6. CONCLUSIONS

Durant els darrers anys hem vist com **tant empreses privades com les administracions públiques** han optat per la instal·lació de sistemes de recollida i tractament de dades biomètriques i alhora, com aquestes **s'han anat fent lloc en l'àmbit privat** a través de dispositius mòvils i formes d'interactuar amb el nostre entorn.

La pròpia naturalesa permanent de les dades biomètriques les converteix en un mètode aparentment segur d'identificació o autenticació però alhora, aquesta immutabilitat pot comportar greus riscos per a la intimitat dels interessats en supòsits d'accessos indeguts o il·legítim a les dades o la seva filtració o comunicació indegudes o no autoritzades.

Així doncs podem veure com la seguretat en la recollida de dades biomètriques ha de ser la preocupació principal de responsables de tractament i dels interessat arran de la naturalesa

irrevocable d'aquest tipus de dades.

Així doncs, hem cregut necessària la redacció d'aquesta guia per tal de conscienciar als responsables de les seves obligacions (Informar degudament a l'interessat i

obtenir-ne un consentiment vàlid, establir un sistema de recollida i tractament de dades biomètriques basat en la protecció de la intimitat by design i by default:

tant en el seu disseny com en la implantació, avaluar l'impacte sobre la intimitat que pot tenir aquest mecanisme, etc) i alhora informar sobre els drets dels que disposen els particulars davant d'aquest tipus de tractament de dades i les eines necessàries per tal d'impedir-ne un mal ús o possibles atacs fraudulents.

La recollida i el tractament de dades biomètriques **suposen un risc molt elevat de produir danys irreparables en la privacitat dels interessats** així que cal limitar-ne l'ús a supòsits on quedi provada la seva **necessarietat, proporcionalitat i efectivitat**.



ap
da

Agència Andorrana
de Protecció de Dades

apda@apda.ad

C. Doctor Vilanova 15, Ed. Consell General, Planta -5
(+376) 808 115