Anàlisi de casos i novetats en l'àmbit de Protecció de Dades

Consorci de Salut i Social de Catalunya

DESMUNTEM MITES I ELS EQUÍVOCS MÉS COMUNS ENTORNA LA IDENTIFICACIÓ I AUTENTIFICACIÓ BIOMÈTRIQUES

L'Agència Espanyola de Protecció de Dades Personals (AEPD), davant l'increment en l'ús de sistemes de identificació i autentificació d'usuaris mitjançant l'ús de dades biomètriques (com l'empremta o el reconeixement facial), ha publicat recentment un comunicat per tal de refutar certes creences àmpliament esteses entorn al tractament de dades biomètriques per part de sistemes que validen la identitat o bé identifiquen als usuaris. És a dir, el tractament de dades biomètriques a mode de claus d'accés, entre d'altres funcionalitats.

D'acord amb el criteri de l'AEPD, **identificació** és el procediment pel qual es reconeix a una persona a dins d'un grup d'individus comparant les dades de qui es vol identificar amb les dades dels qui es trobin dins el grup d'individus. En canvi, la **autentificació** és el procediment mitjançant el qual es pretén provar que la identitat que una persona reclama com seva és certa. És a dir, es comparen només les dades de la persona amb les dades associades prèviament a aquesta persona dins la base de dades, i així validar la identitat reclamada.

Festes aquestes precisions inicials i necessàries, passem a exposar les diferents creences imperants en aquesta matèria que, com veurem, no són certes del tot.

1. La informació biomètrica s'emmagatzema en un algoritme.

D'acord amb la seva definició (RAE) un algoritme és un mètode, un conjunt ordenat d'operacions però no un suport o mitjà d'emmagatzematge de dades.

Així doncs, la informació recollida, per exemple, la imatge de l'empremta dactilar, es processa i el resultat d'aquest procés de digitalització s'emmagatzema en registres de dades denominats firmes/patrons. Són aquests patrons els que registren numèricament les característiques físiques de la dada biomètrica que permeten diferenciar o identificar a persones.

2. L'ús de dades biomètriques és igual d'intrusiu que altres mecanismes de identificació o autentificació.

Novament, aquesta afirmació no és certa. Donat que l'ús de dades biomètriques en els processos de identificació o autentificació revelen més informació de l'individu que la pròpia identitat d'aquests. Depenent de les dades biomètriques que es tractin, també es podria conèixer la raça, gèneres, estat emocional, malalties, consum de substàncies...etc. De fet, tots aquesta informació vinculada a la dada biomètrica, al estar subjecta a aquesta, fa que l'individu no pugui impedir la seva recollida.

3. La identificació/autentificació és precisa.

La identificació i autentificació mitjançant el tractament de dades biomètriques es basa en probabilitats, que tot i ser elevades no són 100% precises com si ho és una contrasenya o certificació (és correcta, o no ho és). Per exemple, una empremta digitalitzada proporciona entorn a un 96% de correspondència. Així doncs, amb l'ús d'aquestes dades com a mitjà de validació, existeix una número de falsos positius (casos en que es permet un accés no autoritzat) i de falsos negatius (casos en que es restringeix un accés autoritzat). Llavors, serà rellevant la precisió de l'equip que captura les dades.

4. La identificació/autentificació biomètrica és suficientment precisa per a diferenciar dues persones.

Ha sigut provat que el semblant biomètric entre germans o familiars pot portar a error als dispositius de tractament de dades biomètriques. També, és rellevant el fet de que les condicions físiques com l'ús de maquillatge, mascareta, lluminositat poden augmentar la probabilitat de confusió del dispositiu que processa les dades.

5. La identificació/autentificació és adequada per a totes les persones.

Certes persones, donades les seves peculiaritats físiques, no poden fer ús de determinats tipus de biometria. Donades les seves característiques, alguns sistemes poden no reconèixer les seves dades biomètriques (lesions, accidents, paràlisis). És més, en aquests casos els sistemes de tractament de dades biomètriques poden donar lloc a exclusió social.

6. El procés de identificació/autentificació no es pot burlar.

Malauradament sí que existeixen mètodes capaços de burlar aquests sistemes i donar lloc a accessos no autoritzats en els mateixos. Serien els casos de ús de mascaretes o reproductors d'empremta dactilar.

7. La informació biomètrica no està exposada a vulnerabilitats.

A diferència dels processos basats en contrasenyes, la majoria de característiques biomètriques estan exposades a vista de tothom i poden capturar-se a distància (fotografies, per exemple). De manera que de no adoptar-se els mesures per a mitigar els riscos d'un ús no autoritzat, és com si féssim una contrasenya pública a tercers.

8. Tot tractament de dades biomètriques implica identificació o autentificació.

No necessàriament. Per exemple, el moviment del ratolí del PC pot ser utilitzat per a determinar si qui pretén l'accés és una persona o un robot, però no està identificant a cap persona o autentificant cap identitat tot i que el moviment sigui una dada biomètrica.

9. Els sistema de identificació/autentificació biomètrica són més segurs pels usuaris.

Des de el moment en que les nostres dades biomètriques es troben en un sistema, aquest pot patir una fuita o violació de seguretat. De manera que no és pot afirmar que aquestes dades no puguin veure's compromeses. A més, en cas de que aquestes siguin accessibles, pot donar lloc a que es produeixin accessos no autoritzats en altres sistemes on utilitzem les mateixes dades biomètriques. És a dir, l'ús d'una mateixa dada biomètrica a mode de autentificació, seria l'equivalent a l'ús d'una mateixa contrasenya per a accedir a diferents sistemes. També s'ha de tenir en compte que un cop la dada biomètrica ha estat compromesa, aquesta no és pot canviar (com sí es pot amb una contrasenya).

10. La autentificació biomètrica és forta o robusta.

Realment, com a sistema de autentificació ha de ser considerat més aviat dèbil. Ja que teòricament, un sistema de autentificació robust és aquell que reuneix dos d'aquests tres factors: alguna cosa que *sabem*, alguna cosa que *tenim* i alguna cosa que *és* (biometria). Per exemple, l'ús de una targeta i una contrasenya com a doble factor d'autentificació sí seria robust (una cosa que tenim + una cosa que sabem).

11. La identificació/autentificació biomètrica és més còmoda per a l'usuari.

Aquesta afirmació depèn molt de context, la tecnologia utilitzada, la percepció de la persona i les seves peculiaritats físiques (tal i com s'ha comentat anteriorment). En determinats casos la persona pot sentir que la seva privacitat està sent envaïda al veure's obligat a utilitzar les seves dades biomètriques en diferents sistemes.

12. La informació biomètrica convertida en un *hash* no és recuperable.

S'ha demostrat que el *hash* pot revertir-se, és a dir, a partir de *hash* obtenir el patró biomètric original. Per tant, la tècnica més segura consisteix en eliminar el patró original un cop s'ha processat el *hash* a partir d'aquell.

13. La informació biomètrica emmagatzemada no permet reconstruir la informació biomètrica original.

La informació biomètrica que es conté en el patró, sí permet obtenir en part la informació biomètrica original (per exemple, part de la empremta dactilar). A més, en funció de la precisió de reconeixement del dispositiu que verifica la dada, una informació parcial de la dada biomètrica permetrà que el sistema de autentificació ja permeti l'accés per haver reconegut la informació parcial reconstruïda com a original.

14. La informació biomètrica no és interoperable.

Novament, aquesta afirmació és refutable. Donat que els sistemes de tractament de dades biomètriques es desenvolupen seguint estàndards per a garantir la seva interoperabilitat. A mode d'exemple, els sistemes que utilitzen una funció *hash* sobre patrons biomètrics poden esdevenir interoperables en cas de que es comparteixin les claus utilitzades en el procés de *hashing* (creació del *hash*).