TECNOLOGIES DE SEGUIMENT WIFI:

Orientacions per a responsables del tractament

aepd agencia española protección datos

apdcat Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

Consejo de Transparencia y Protección de Datos de Andalucía

Guia publicada el maig de 2024

RESUM EXECUTIU

El seguiment wifi o *wifi tracking* és una tecnologia que permet identificar i rastrejar dispositius mòbils a través dels senyals wifi que emeten, per detectar la presència del dispositiu en una zona específica i identificar patrons de moviment. Per això s'empra, per exemple, en l'estimació d'aforaments, l'anàlisi de fluxos de persones o el mesurament de temps de permanència.

Pot tenir aplicacions pràctiques en centres comercials, museus, llocs d'especial interès, centres de treball, àrees públiques, transport públic o grans esdeveniments públics. Tanmateix, aquesta pràctica planteja seriosos riscos per a la privacitat, ja que pot permetre el seguiment dels moviments de les persones sense que facin cap acció ni assabentar-se'n, i sense una base jurídica apropiada.

És crucial prendre consciència que molts d'aquests usos de seguiment wifi suposen la recollida i altres tractaments de dades personals. Per tant, s'han de sotmetre al conjunt de principis, drets de les persones físiques i obligacions per als responsables del tractament que estableix l'RGPD.

Les orientacions analitzen tant tècnicament com jurídicament les implicacions de l'ús d'aquesta tecnologia, identifiquen els principals riscos que porten associats i, també, ofereixen una sèrie de recomanacions concretes per fer-ne un ús responsable i compatible amb la normativa de protecció de dades.

Aquestes orientacions han estat elaborades conjuntament per l'Agència Espanyola de Protecció de Dades, l'Autoritat Catalana de Protecció de Dades, l'Autoritat Basca de Protecció de Dades i el Consell de Transparència i Protecció de Dades d'Andalusia. Sorgeixen fruit de la col·laboració de les quatre autoritats de control, davant l'impacte que un ús inadequat de la tecnologia de seguiment wifi pot tenir en la privacitat i la protecció de dades de les persones físiques.

ÍNDEX

ACRÒNIMS

AP: *Access Point*. Punt d'accés wifi

CEPD: Comitè Europeu de Protecció de Dades

CNIL: Comissió Nacional d'Informàtica i Llibertat de França

DPD: Delegat de protecció de dades

EEE: Espai Econòmic Europeu

AIPD: Avaluació d'impacte relativa a la protecció de dades

ENS: Esquema Nacional de Seguretat

GT29: Grup de treball de l'article 29

IA: Intel·ligència artificial

IEEE: Institute of Electrical and Electronics Engineers

IOT: *Internet of things*. Internet de les coses

LOPDGDD: Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals

MAC: *Media Access Control*

RGPD: Reglament general de protecció de dades

RIA: Reglament d'intel·ligència artificial

RSSI: *Received Signal Strength Indicator*. Indicador de força del senyal rebut

WPS: *Wifi Protected Setup*

1. INTRODUCCIÓ DE LA GUIA

Actualment, el telèfon mòbil és un dispositiu personal omnipresent equipat amb diverses tecnologies sense fil, com ara wifi i Bluetooth, que a més admet generacions presents i passades de tecnologies de xarxes mòbils (és a dir, 2G–5G).

Per dur a terme les comunicacions, totes aquestes tecnologies es basen en l'intercanvi de missatges entre aquests dispositius i altres equips de xarxa, com ara estacions base i punts d'accés.

En particular, la tecnologia wifi és una tecnologia sense fil basada en protocols de comunicació estandarditzats (família de protocols IEEE802.11), caracteritzada per un conjunt de terminals (mòbils o no) que es connecten a un punt d'accés (AP, per les seves sigles en anglès). Un conjunt d'AP administrat sota una mateixa entitat conforma una xarxa wifi.

La comunicació wifi s'efectua per mitjà de missatges anomenats *trames*, un conjunt de bytes que sempre conté una capçalera que inclou l'identificador del dispositiu d'origen, anomenat adreça MAC (Media Access Control). Algunes d'aquestes trames no estan xifrades i s'emeten des del dispositiu periòdicament, fins i tot quan no s'ha connectat a cap xarxa wifi.

Emprant diverses tecnologies disponibles actualment, les dades que contenen aquestes trames poden ser capturades, analitzades i processades, per determinar un identificador que permeti singularitzar el terminal origen d'aquestes trames. Igual com passa en el món d'internet, aquest conjunt de tecnologies es coneix com a *device fingerprinting*, o simplement *fingerprinting*; en català, empremta digital del dispositiu o marcatge del dispositiu. Al llarg del text s'utilitzaran indistintament aquestes denominacions.

La informació emprada per determinar aquesta empremta digital és enviada pel dispositiu sense que hi hagi acció ni coneixement de la persona que el porta. Això fa que aquestes tecnologies siguin especialment delicades des de la perspectiva de la privacitat i la protecció de dades.

> Mitjançant la construcció, emmagatzematge i anàlisi d'aquesta empremta, es pot detectar la presència del dispositiu en una determinada zona i identificar-ne els patrons de moviment i, per tant, també els de la persona que el porta.

Aquest tipus de tecnologies que recullen dades dels missatges wifi intercanviats entre terminals i AP, per processar-les i analitzar-les posteriorment, s'anomenen *seguiment wifi*.

Els dos tipus principals d'analítiques ofertes per aquestes tecnologies són la de presència i la de localització. L'analítica de presència se centra a estudiar si hi ha terminals en una determinada zona, i durant quant de temps hi són, mentre que la de localització té com a objectiu traçar el recorregut seguit pel terminal dins d'una zona d'estudi.

Entre els seus usos principals es poden esmentar l'estimació d'aforaments; l'anàlisi de fluxos de persones; el càlcul d'estadístiques d'assistència i de temps mitjans de permanència en ubicacions concretes o d'espera en una cua; la determinació dels recorreguts més habituals; o el càlcul de la taxa de repetició de visites.

S'hi poden trobar aplicacions pràctiques en **centres comercials, museus, llocs d'especial interès, centres de treball, àrees públiques, transport públic, grans esdeveniments públics, escenaris d'emergències, etc**.

Depenent de les característiques de l'empremta digital generada per aquestes tecnologies, del temps d'emmagatzematge i del seu processament, l'ús de seguiment wifi pot suposar un tractament de dades personals; en ocasions, un tractament que no només és desconegut per a l'usuari del terminal, sinó també per al mateix responsable del tractament, si considera que no es tracta d'una dada personal. Cosa que pot ser errònia, tal com s'explica a l'**apartat 3**.

A l'hora de plantejar-se desplegar aquest tipus de tecnologies, **la privacitat de les persones ha de ser el primer**.

Totes les persones han de tenir dret a moure's lliurement sense "sentir-se espiats", sense que un tercer, ja sigui Administració pública o empresa privada, pugui observar o portar un registre del que estan fent.

Ningú hauria de poder rastrejar quines botigues, centres sanitaris o llocs de culte visita una persona. Aquestes dades han de romandre en la seva esfera privada, perquè pugui ser ella mateixa, sense sentir-se cohibida per un possible registre o utilització d'aquesta informació.[1]

Aquestes orientacions analitzen tant tècnicament com legalment les implicacions de l'ús d'aquesta tecnologia, n'identifiquen els principals riscos associats i ofereixen una sèrie de recomanacions concretes, per fer-ne un ús responsable i compatible amb la normativa de protecció de dades.

[1] https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wifi-tracking_en.

2 DESCRIPCIÓ DEL MARC TECNOLÒGIC

A. L'ÚS D'ADRECES MAC FIXES I ALEATÒRIES

L'adreça MAC és un identificador generalment fix i unívoc de qualsevol dispositiu, emprat en les comunicacions entre els diferents elements d'una xarxa.

Quan un dispositiu es connecta a un AP d'una xarxa wifi, tots els seus missatges s'inicien identificant l'adreça MAC del dispositiu. D'aquesta manera, l'AP pot llegir el contingut de les trames i, mitjançant l'adreça MAC, identificar unívocament el terminal.

La cobertura de les xarxes wifi la proporcionen els AP que la conformen. Aquests AP poden estar ubicats en espais públics oberts o a l'interior d'edificis o instal·lacions.

No obstant això, la majoria dels terminals mòbils que entren a la zona de cobertura de les xarxes wifi no s'hi connecten. Tot i així, els dispositius que tenen capacitat wifi fan una recerca periòdica de les xarxes que poden estar disponibles en el seu radi de cobertura. Aquesta recerca es fa enviant periòdicament trames anomenades *Probe Request*, que el dispositiu transmet encara que no estigui connectat a una xarxa wifi i, en ocasions, sense ni tan sols tenir activada la funcionalitat wifi. La finalitat principal d'aquest tipus de trames és enviar una "sol·licitud de sondeig" a les diferents xarxes wifi que hi pugui haver a la zona. Els AP estan preparats per respondre aquests missatges, enviant al terminal informació que li permetrà connectar-s'hi, si així ho tria l'usuari.

Fa uns anys, en les trames Probe Request, a més de determinada informació tècnica s'hi enviava l'adreça MAC fixa i única del terminal. Per tant, mitjançant la recol·lecció en el temps d'aquestes trames, juntament amb tecnologies de localització, era possible identificar unívocament el terminal i registrar-ne el recorregut dins de la zona de cobertura de la xarxa wifi, fins i tot sense estar-hi connectat.

A causa dels problemes de privacitat que plantejava aquesta situació, els fabricants de terminals mòbils van incorporar l'ús de l'adreça MAC aleatòria de manera generalitzada. Aquest procés es va iniciar als Apple iOS8 i va ser seguit i estès per Android.

L'adreça MAC aleatòria és una adreça "virtual" emprada en les trames Probe Request. D'aquesta manera, diferents missatges enviats des d'un terminal no comparteixen el mateix identificador únic (adreça MAC fixa). Per tant, ja no resulta possible conèixer l'adreça MAC real del dispositiu capturant mitjançant l'anàlisi de les trames Probe Request. D'altra banda, atès que l'adreça MAC aleatòria es modifica amb freqüència i les mateixes trames s'envien aleatòriament, tampoc resulta senzill identificar el dispositiu utilitzant directament les adreces MAC aleatòries.

Aquesta mesura **va enfortir la privacitat de les persones**. No obstant això, cal **tenir en compte els factors següents**:

- El procediment de generació de MAC aleatòries no està estandarditzat, cosa que implica comportaments dispars entre els terminals.
- Un cop s'ha efectuat la connexió del terminal a un determinat AP, l'adreça MAC emprada es manté constant durant tota la connexió, encara que s'hagi generat aleatòriament. Per tant, permet vincular les accions realitzades pel dispositiu durant tota la connexió, com ara la seva localització absoluta i relativa amb la localització d'altres terminals.
- S'estima que actualment entre un 5% i 10% dels dispositius no utilitza adreces MAC aleatòries.
- Hi ha multitud de tècniques que, en un elevat percentatge de casos, són capaces d'identificar unívocament els dispositius mòbils, encara que utilitzin una adreça MAC aleatòria canviant. Són les tècniques actuals emprades en el seguiment wifi, basades en la diversa informació continguda en (o deduïda a partir de) les trames Probe Request, combinada amb la detecció de patrons estadístics de les adreces MAC aleatòries. Les tècniques més avançades per vincular la informació de diferents trames a un mateix dispositiu empren algoritmes d'aprenentatge automàtic i analítica de dades basada en big data.

B. DADES EMPRADES EN EL SEGUIMENT WIFI

Les diverses tècniques de seguiment wifi tenen com a objectiu identificar i rastrejar terminals de manera única i precisa en entorns wifi.
Aquest mètode es basa en l'ús d'una gran varietat de paràmetres i característiques físiques, tant dels dispositius com de les mateixes condicions de la transmissió, per generar una empremta digital individualitzada per a cada dispositiu.

L'ús de tècniques de reconeixement de patrons i l'analítica de dades en general, unit a una contínua evolució de les tècniques emprades pels fabricants de dispositius en defensa de la privacitat, porta a una situació de canvi permanent. Com a resultat, algunes tècniques plenament eficaces fa pocs anys han perdut la seva utilitat avui dia. A continuació, es descriuen els principals mètodes emprats en l'actualitat.

La trama Probe Request és un tipus de trama de gestió previst per l'estàndard wifi i es fa servir quan el dispositiu (per exemple, un *smartphone*) no està connectat a un AP wifi. En cadascun dels canals disponibles de la wifi, el dispositiu fa un sondeig "preguntant" per AP disponibles en el seu radi de cobertura, als quals pugui connectar-se.

Quan un determinat AP rep la trama Probe Request, respon amb una trama anomenada Probe Response. Amb aquesta trama, el dispositiu coneix l'existència i les característiques d'aquest AP, en cas que s'hi vulgui connectar.

Aquest tipus de trames s'emet per tots els dispositius en comunicacions wifi automàticament, sense control de l'usuari i sense xifrar. Així, pot ser rebut i descodificat no només per qualsevol AP, sinó també per qualsevol dispositiu de baix cost a l'escolta del canal wifi.

Les característiques concretes de l'emissió d'aquest tipus de trames depenen de moltes circumstàncies, com ara el fabricant, el model i el sistema operatiu del dispositiu. En alguns casos, les dades enviades (per exemple, el SSID)

poden oferir directament informació relacionada amb la persona.[2]

Les tecnologies de seguiment wifi aprofiten aquestes característiques de les trames Probe Request (enviament per tots els dispositius, enviament sense xifrar i amb gran quantitat de dades) per generar una empremta digital única, que permet identificar el dispositiu.

A més de la informació directament tramesa en les trames Probe Request, és possible obtenir informació mitjançant mesuraments indirectes, combinant-los o mitjançant tècniques heurístiques.

A la pràctica, qualsevol mesura o dada que assisteixi en la tasca d'identificar el dispositiu pot ser utilitzada. Entre les mesures físiques o dades addicionals que poden emprar aquest tipus de tecnologies hi ha la força del senyal rebut (RSSI, per les sigles de l'anglès Received Signal Strength Indicator), que a més pot ser emprada per determinar la ubicació aproximada del dispositiu; l'interval de temps entre l'enviament de les trames Probe Request; la distribució estadística, tant del nombre de seqüència de les trames com de les MAC aleatòries; o les desviacions inherents dels rellotges dels dispositius. En resum, totes elles poden acabar permetent la generació d'una empremta digital.

L'objectiu de la recollida i anàlisi de dades com les descrites anteriorment (i d'altres, depenent de la solució concreta del fabricant) és generar una empremta digital única, que permeti identificar cada dispositiu. En termes generals, el **procés de generació de l'empremta digital** dels terminals mòbils en una xarxa wifi **comporta** les fases següents:

- **Captura de trames Probe Request:** es recopilen massivament les trames Probe Request rebudes en els diferents AP de la xarxa wifi en observació. A més de la informació de les trames, es poden recollir dades relacionades amb les condicions físiques de la transmissió, com el RSSI i altres. Per dur a terme aquesta captura, es pot utilitzar equipament especialitzat, o fins i tot equipament de xarxa wifi convencional que proporcioni aquestes capacitats addicionals.

- **Extracció i enviament d'informació:** s'extreu la informació rellevant de les trames capturades i de les característiques de la transmissió. Aquesta informació s'envia a un servidor centralitzat per processar-la i analitzar-la. Les dades específiques enviades dependran del model de seguiment wifi implementat a la xarxa.

- **Anàlisi de patrons i generació de l'empremta digital:** després d'extreure la informació, s'analitzen els patrons de les dades recopilades. L'objectiu és combinar característiques específiques de les dades recollides que permetin distingir un dispositiu d'un altre. Aquesta anàlisi variarà segons el sistema utilitzat i és fonamental per aconseguir identificar unívocament els terminals mòbils a la zona monitoritzada, i ja és habitual l'ús de tècniques avançades, com ara l'aprenentatge automàtic (*machine learning*) i el modelatge probabilístic.

  Els algoritmes d'aprenentatge automàtic són capaços d'aprendre patrons i establir correlacions entre els diferents paràmetres de les trames, per determinar la probabilitat que una trama pertanyi a un dispositiu prèviament identificat o sigui d'un de nou. En combinar aquestes característiques en un model probabilístic, es genera una empremta digital única per a cada dispositiu. Aquests models poden integrar diferents fonts d'informació, com ara dades històriques de dispositius prèvia-

[2] https://svs.informatik.uni-hamburg.de/publications/2022/2022-06-08_Probing_for_Passwords.pdf

ment identificats, informació contextual i patrons de comportament, per generar empremtes digitals més robustes i precises.

En resum, es crea una empremta digital (*fingerprint*), que representa el dispositiu mitjançant una combinació de múltiples atributs que permeten singularitzar-lo.

- **Comparació i reconeixement:** un cop s'han construït les empremtes digitals de diferents dispositius, es fa una comparació i reconeixement per identificar dispositius i determinar si han estat detectats prèviament pel sistema.

C. IDENTIFICACIÓ DE DISPOSITIUS

Després de generar-ne l'empremta digital, el dispositiu queda identificat. Si se'n fa un seguiment a través de la seva empremta digital, serà possible obtenir el tipus d'informació següent:

- **Presència a la zona de cobertura de l'AP:** l'empremta digital permet determinar si el dispositiu és present o no a la zona on hi ha l'AP. Això resulta especialment útil per comptar el nombre de dispositius presents en un lloc, o per obtenir dades sobre l'afluència de visitants en diferents dies.

- **Temps aproximat de permanència:** a més d'indicar la presència del dispositiu, l'empremta digital permet estimar el temps aproximat que el terminal mòbil passa a la zona de cobertura. Aquesta dada pot ser útil per comprendre els hàbits dels usuaris i obtenir informació sobre la durada i freqüència de les visites.

- **Seguiment de trajectòria:** l'empremta digital del dispositiu possibilita el seguiment de la seva trajectòria al llarg del temps. Això implica registrar els moviments del dispositiu a la zona de cobertura de la xarxa wifi i obtenir informació sobre els llocs que ha visitat.

Per millorar la precisió en el seguiment de la trajectòria d'un terminal mòbil, es poden emprar tècniques de triangulació basades en la potència del senyal rebut de tres o més AP de la xarxa.

En combinar la informació d'aquests AP, és possible aconseguir una alta precisió en la ubicació del dispositiu, que pot arribar fins i tot a nivells de 0,5 metres, segons estudis realitzats. Aquesta major precisió facilita el seguiment i l'anàlisi de la trajectòria del dispositiu i proporciona, així, més detall dels patrons de desplaçament dels usuaris.

És important destacar que la retenció de l'empremta digital d'un mateix terminal durant diversos dies permetria fer un seguiment més intens i ampli. Així, en emmagatzemar i reconèixer l'empremta digital d'un dispositiu al llarg del temps, seria possible identificar patrons de comportament, descobrir preferències o rutines, activitats diàries i llocs freqüentats, entre altres aspectes íntims de la vida de les persones.

3 DADES PERSONALS I TRACTAMENTS INVOLUCRATS

La tecnologia de seguiment wifi ha evolucionat significativament fins a permetre recollir i analitzar múltiples característiques dels dispositius.

Aquesta capacitat no es limita a la identificació per mitjà de l'adreça MAC, sinó que també abasta la creació d'empremtes digitals úniques. Aquestes empremtes, creades amb la combinació de múltiples característiques, permeten identificar dispositius de manera contínua, superant les mesures d'anonimització com ara l'aleatorització d'adreces MAC.

Al seu torn, el telèfon mòbil, convertit en un element quotidià i inseparable, actua com un vincle directe amb el seu usuari i, així, genera una identificabilitat tant directa com indirecta.[3] Aquests dispositius formen part de l'esfera privada dels usuaris, que s'ha de protegir de conformitat amb el Conveni Europeu per a la Protecció dels Drets Humans i de les Llibertats Fonamentals[4] i la normativa reguladora de la protecció de dades personals. Per això, en aquest context tecnològic, és crucial analitzar si s'efectuen tractaments de dades personals i, si escau, quin és el seu contingut.

A. ABAST DEL TERME "DADA PERSONAL"

El concepte "dada personal", tal com s'estableix a l'RGPD, té un abast molt extens. A l'article 4.1 es defineix "dada personal" com "qualsevol informació sobre una persona física identificada o identificable."

La referència a "qualsevol informació" en aquesta definició ressalta la intenció del legislador d'atorgar a aquest concepte un significat molt ampli, que no se cenyeix a les dades confidencials o relacionades amb la intimitat sinó que pot abastar qualsevol mena d'informació, tant objectiva com subjectiva, sempre que sigui *sobre* la persona en qüestió. Per a això, n'hi ha prou que la informació estigui relacionada amb una persona concreta a causa del seu contingut, finalitat o efectes.[5]

Sobre el concepte "identificable", el mateix article 4.1 disposa que es considera persona física identificable "qualsevol persona la identitat de la qual es pugui determinar, directament o indirectament; en particular mitjançant un identificador, com ara un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona."

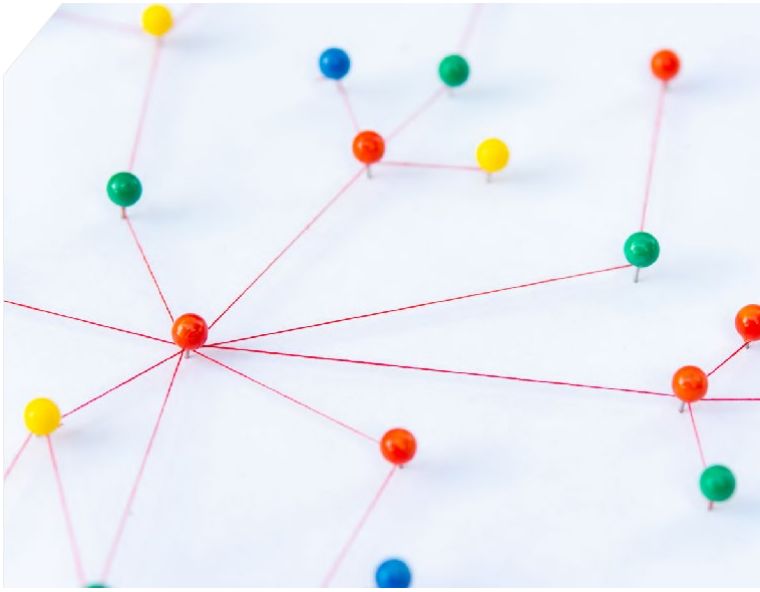
Per tant, per qualificar una informació de dada personal no cal que aquesta informació permeti, per si sola, identificar l'interessat.

[3] Ap. 4.2.2. Dictamen 13/2011 sobre els serveis de geolocalització en els dispositius mòbils intel·ligents (GT29,WP185).
[4] Considerant 24 Directiva 2002/58/CE de 12 de juliol de 2002 relativa al tractament de les dades personals i a la protecció de intimitat en el sector de les comunicacions electròniques.
[5] Paràgrafs 34 i 35 STJUE de 20 de desembre de 2017, cas C 434/16.

És més, una persona física és identificable des del moment en què el posseïdor de les dades és capaç de distingir-la i tractar-la de manera diferent, fins i tot quan per fer-ho no n'hi hagi prou amb aquestes dades per si soles.

En aquest sentit, resulta útil diferenciar entre dades identificadores úniques, que permeten identificar la persona de manera inequívoca, i "quasi identificadors." Aquests últims, a primera vista, no permeten identificar una persona determinada. No obstant això, en combinar-los entre si o amb d'altres permeten identificar la persona a causa de les "combinacions úniques." Aquest fenomen, conegut com a "efecte mosaic", il·lustra com l'acumulació de dades "quasi-identificadores" pot portar a identificar una persona, un procés que les tecnologies d'anàlisi de dades massives faciliten. És perfectament possible parlar de l'existència de dades personals fins i tot en supòsits en què no té una identificació directa o expressa de l'interessat.

Exemple:
Es disposa d'informació d'un mòbil que ha visitat (se'n coneix la data, hora i temps de permanència) en 2 ocasions el comerç A, en 3 ocasions l'establiment B, ha pernoctat a l'establiment hoteler C durant 16 dies i està qualificat com a turista amb estada superior a 15 dies i menor d'1 mes. Aquesta informació per si mateixa ja és tan detallada que amb molt poca informació addicional es podria identificar la persona portadora d'aquest terminal mòbil.



Pel que fa a la capacitat de ser "identificable" com a persona, el considerant 26 de l'RGPD subratlla que s'han de considerar "tots els mitjans, com ara la singularització, que raonablement pugui utilitzar el responsable del tractament o qualsevol altra persona per identificar directament o indirectament la persona física."

És a dir, no cal que tota la informació que permeti identificar l'interessat s'hagi de trobar en poder d'una sola persona o dins d'un únic tractament.

El que s'ha d'analitzar és si hi ha una possibilitat raonable que utilitzant altres mitjans addicionals es pugui identificar la persona. D'altra bada, es tracta d'una anàlisi dinàmica, per la qual cosa cal tenir en compte el grau d'avenç tecnològic en el moment del tractament, així com el seu possible desenvolupament en el període durant el qual es tractaran les dades.

En definitiva, aquesta identificabilitat també es relaciona amb el fet que no requereixi esforços desproporcionats i, com s'acaba d'indicar, la constant evolució tecnològica la facilita.

B. SEGUIMENT WIFI I *FINGERPRINTING* COM A DADES PERSONALS

Aquesta definició àmplia del concepte de dades personals establerta per l'RGPD pren una rellevància especial en el context del seguiment wifi. Aquesta tecnologia afecta tots els dispositius amb funcionalitat wifi, sense que necessàriament estiguin connectats a cap xarxa concreta, i en ocasions fins i tot si no aquesta funcionalitat no està activada. Entre aquests dispositius s'hi inclouen mòbils, tauletes, portàtils, ordinadors fixos, routers, impressores, electrodomèstics, joguines, dispositius corporals (els anomenats *wearables*, inclosos marcapassos, sistemes d'oxigen portàtils, dispositius per a diabètics, implants neuronals, etc.) i fins i tot automò-bils.[8]

L'RGPD, al seu considerant 30, **adverteix** de la **capacitat d'identificar les persones a través de les empremtes dels dispositius**:

"Les persones físiques poden ser associades a identificadors en línia facilitats pels seus dispositius [...]. Això pot deixar empremtes que, en particular, en ser combinades amb identificadors únics i altres dades rebudes pels servidors, poden ser utilitzades per elaborar perfils de les persones físiques i identificar-les."

D'acord amb l'anterior, les dades transmeses pels senyals wifi utilitzats en aquest tipus de processos poden ser considerades com a dades personals, ja que estan relacionades amb persones identificables i són susceptibles de ser utilitzades per identificar-les directament o indirectament. En particular, d'acord amb el que estableix l'RGPD, el *fingerprinting* o empremta digital en el context del seguiment wifi pot suposar un tractament de dades personals.

El concepte d'empremta digital es defineix com "un conjunt d'elements d'informació que identifica un dispositiu o instància d'aplicació." Per tant, abasta qualsevol informació que pugui ser emprada per individualitzar, vincular o inferir un usuari o dispositiu al llarg del temps.[9]

Això pot incloure, entre d'altres, dades derivades de:

- La configuració d'un agent d'usuari/dispositiu.
- Dades exposades per l'ús de protocols de comunicació de xarxa.

Per tant, l'empremta digital proporciona la capacitat de distingir un dispositiu d'un altre i es podria utilitzar per rastrejar la ubicació o el comportament d'un usuari en el temps, fins i tot si no es compta amb una identificació directa o expressa de la persona.

[8] Algunes autoritats de control, com Unabhängige Landeszentrum für Datenschutz (Schlewig Holstein, Alemanya), han expressat la seva preocupació per l'aplicació d'aquestes tecnologies sobre els automòbils que incorporin punts d'accés wifi que permetin el seguiment de persones. Location Services can Systematically Track Vehicles with WiFi Access Points at Large Scale.

[9] Ap. 3 Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting.

C. SEGUIMENT WIFI I DADES DE LOCALITZACIÓ I DE TRAJECTÒRIES

Es pot conèixer la posició d'un dispositiu de forma aproximada, per "presència" (proximitat al sensor), o bé més precisament, mitjançant triangulació. En mantenir la identificació o individualització del dispositiu i determinarne la posició al llarg del temps, és possible establir una trajectòria durant el temps en què el dispositiu estigui dins de la zona de cobertura dels sensors.

Aquestes dades de localització representen una tipologia de dades personals d'alt risc per a la privacitat de les persones, tal com es detalla a l'apartat de riscos per als drets i llibertats de les persones físiques.

Quan es mantingui l'àmbit espacial i temporal de les dades recollides mitjançant seguiment wifi, aquestes dades poden ser suficients per si soles, o en combinació amb d'altres, per permetre la identificació de les persones, i el responsable del tractament hauria de considerar aquest tipus de dades com a dades personals.

D. TRACTAMENT DE DADES PERSONALS

La tecnologia de seguiment wifi no és en si mateixa un tractament de dades personals, però podria formar-ne part. De fet, en la decisió sobre com desenvolupar un tractament o assolir una finalitat, el responsable pot optar per solucions diferents del seguiment wifi o per opcions que no impliquin un tractament de dades personals.

La tecnologia seguiment wifi pot aparèixer en operacions de tractament de dades personales derivades de dos tipus d'analítiques principalment: la de presència i la de localització. L'analítica de presència se centra en l'estudi de l'existència i la permanència dels terminals en una determinada zona, mentre que la de localització té com a objectiu traçar el recorregut seguit pel terminal dins d'una determinada zona d'estudi, fins i tot per temps indefinit.

En moltes ocasions, la seva finalitat és detectar i analitzar comportaments col·lectius. Tanmateix, no es pot oblidar que es parteix de la detecció de dades individuals.

A títol il·lustratiu, s'assenyalen alguns tractaments en els quals s'han emprat tecnologies de seguiment wifi:[10]

- Servei de geolocalització del dispositiu, amb conformitat o no del mateix usuari.
- Seguiment de persones als centres de treball.
- Serveis d'emergències, mitjançant la cerca o localització com a part de la prestació d'auxili vital a les persones. Es tracta d'un mecanisme pel qual els centres d'atenció a trucades d'emergència poden rebre automàticament informació sobre la ubicació de qui truca, enriquida per les dades de localització wifi.
- Vigilància de persones, emprant seguiment wifi per detectar si hi ha persones en certs recintes o llocs, i control individual de l'accés a aquestes zones.

[10] El llistat ofert no suposa un posicionament de les autoritats de control de protecció de dades ni a favor ni en contra.

- Vinculació entre persones, per determinar si dues o més han compartit el mateix espai, s'han aproximat, s'han aturat en el mateix punt, etc.

- Anàlisi del flux de persones en instal·lacions privades (per exemple, centres de treball o centres comercials), per optimitzar el disseny de l'espai físic o de la dotació de personal.

- Gestió de multituds en llocs d'accés públic: en àrees concorregudes, com ara aeroports, transport públic, estadis, vies públiques, etc., per controlar aforaments màxims, gestionar el trànsit de persones o rodat de manera eficient, optimitzar rutes o proporcionar informació en temps real, per millorar la seguretat i la comoditat. És habitual trobar aquests usos dins de projectes de ciutats intel·ligents (*smart cities*).

- Màrqueting i publicitat dirigida, per enviar promocions o anuncis als dispositius dels usuaris, quan accedeixen o s'acosten a una ubicació específica o en funció del comportament o patrons de moviment.

- Creació de perfils d'usuari, en funció dels patrons de moviment i el comportament.

En resum, és important tenir en compte que molts d'aquests usos impliquen la recopilació i el tractament de dades personals. Per tant, s'han de sotmetre al conjunt de principis, drets de les persones físiques i obligacions per als responsables del tractament establerts a l'RGPD i l'LOPDGDD.

4 BASES LEGITIMADORES DE TRACTAMENTS DE DADES PERSONALS

Qualsevol tractament de dades personals s'ha d'adequar als principis establerts a l'article 5 de l'RGPD i ha de complir alguna de les condicions de licitud enumerades a l'article 6 de l'RGPD. Això és aplicable al seguiment wifi, en els casos en què el responsable del tractament opti per una tecnologia que faci possible aquest tractament.

El tractament ha de ser lleial i transparent i ha de quedar totalment clar per a les persones quines dades s'estan tractant mitjançant seguiment wifi, i com. Aquesta informació s'ha de proporcionar de manera fàcilment accessible i senzilla d'entendre, amb independència de les dificultats tècniques o pràctiques que el seguiment wifi pugui suposar per al responsable del tractament complir aquests principis.

Els fins del tractament mitjançant seguiment wifi han de ser explícits; és a dir, s'han d'indicar clarament, han de ser legítims i s'han de comunicar a les persones interessades, com a molt tard, en el moment de la recollida. Addicionalment, les dades recollides per a una finalitat concreta mitjançant seguiment wifi no es poden utilitzar per a una finalitat posterior que sigui incompatible. Per això, és fonamental assegurar-se que el tractament posterior no s'aparta de les finalitats ja establertes, i de les quals cal informar les persones interessades. Per exemple, si s'efectués un tractament de dades dels desplaçaments de les persones dins d'un local comercial per optimitzar la ubicació física d'uns determinats productes, basat en un interès legítim del responsable, possiblement resultaria difícil de justificar la compati-

bilitat d'un tractament que impliqués que aquestes persones rebessin notificacions relatives a ofertes comercials d'aquests productes.

Igualment, és essencial que les dades personals tractades siguin adients i pertinents i es limitin a l'estrictament necessari per a la seva finalitat. Cal recordar que la finalitat del tractament no és fer seguiment wifi, per la qual cosa si la finalitat última es pot aconseguir amb una tècnica menys intrusiva s'estaria incomplint el principi de minimització de dades. Si no fos possible cap altra tècnica que el seguiment wifi, per complir el principi de minimització les dades tractades s'haurien d'ajustar a l'estrictament necessari, pel que fa a les seves categories, freqüència, granularitat, etc. També, que el termini de conservació sigui el mínim indispensable i eliminar-les o fer-ne una anonimització efectiva, sempre que sigui possible mitjançant processos automatitzats.

També cal complir el principi d'exactitud, en particular si s'estan utilitzant tècniques probabilístiques per vincular accions a un individu, rectificant o suprimint les dades que siguin inexactes, quan escaigui, i garantint la seguretat i confidencialitat de les dades personals, com s'analitzarà amb detall posteriorment.

El responsable del tractament, a més de complir els principis exposats anteriorment i ser capaç de demostrar-ho, s'ha d'assegurar que el tractament compleix alguna de les condicions de licitud establertes a l'article 6.1 de l'RGPD.

No obstant això, abans de determinar o considerar l'aplicació de qualsevol condició de licitud, és important recordar que les dades personals només s'han de tractar si la finalitat del tractament no es pot aconseguir raonablement per altres mitjans.

La base legitimadora aplicable a cada tractament requereix que el responsable del tractament faci una anàlisi detallada del cas concret, en virtut del principi de responsabilitat proactiva (article 5.2 RGPD), que ha de tenir en compte la naturalesa, l'àmbit, el context i els fins del tractament. No obstant això, és possible proporcionar orientacions generals als responsables, que els guiïn a l'hora d'identificar si es dona alguna de les condicions que legitimaria un tractament concret que empri tecnologies de seguiment wifi.

A. CONSENTIMENT (ARTICLE 6.1.*A* RGPD)

D'acord amb l'analitzat prèviament, la majoria de les tècniques de seguiment wifi operen sense necessitat que el dispositiu estigui connectat a la xarxa wifi i sense que la persona que n'és propietària se n'assabenti. És a dir, no hi ha una via de comunicació entre l'interessat i el responsable del tractament. Per això, resultaria materialment impossible sol·licitar el consentiment a l'interessat i, per tant, s'hauria de descartar com a base legitimadora.

Això no obstant, es podria plantejar algun escenari concret on l'usuari es connectés a la xarxa wifi voluntàriament i, després d'aquesta connexió, se l'informés i sol·licités el consentiment per tractar les seves dades mitjançant seguiment wifi. No podem oblidar que, en aquests supòsits, aquest consentiment hauria de ser lliure, específic, informat i inequívoc.

Un exemple pràctic:
Podria donar-se en escenaris on, mitjançant una aplicació, es convidés els usuaris a permetre el seguiment de la seva localització a canvi d'ofertes comercials.[11]

En aquests casos, s'haurien d'articular sistemes que garantissin el compliment del principi de transparència i permetre que la informació sigui concisa, fàcilment accessible i senzilla d'entendre, que s'utilitzi un llenguatge clar i senzill i a més, si escau, es visualitzi, tal com s'analitza a l'**apartat 9**.

En determinats casos, com ara l'àmbit laboral, educatiu o també el sector públic, cal analitzar si es podria produir un clar desequilibri de poder en la relació entre el responsable del tractament i l'interessat. Per tant, l'avaluació de la llibertat del consentiment s'ha de fer curosament.

B. EXECUCIÓ D'UN CONTRACTE (ARTICLE 6.1.*B* RGPD)

L'execució d'un contracte o de mesures precontractuals podria legitimar el tractament de dades únicament si estigués relacionat amb la prestació d'un servei específic, en el context de seguiment wifi.

En aquest cas, és essencial poder demostrar que el tractament és necessari per complir les obligacions contractuals, cosa que no serà habitual tret de certs casos de serveis de geolocalització sol·licitats per l'usuari.

C. COMPLIMENT D'UNA OBLIGACIÓ LEGAL (ARTICLE 6.1.*C* RGPD)

Aquesta base només seria aplicable quan hi hagués una obligació legal que exigís al responsable el compliment d'una finalitat per a la qual calgui utilitzar les tècniques de seguiment wifi. Addicionalment, de conformitat amb l'LOPDGDD, aquesta obligació hauria d'estar prevista en una norma de dret de la Unió Europea o una norma amb rang de llei.

De conformitat amb la jurisprudència del TJUE, aquesta base jurídica o mesura legislativa ha de ser clara i precisa i la seva aplicació previsible per als seus destinataris, incloses les mesures per garantir un tractament lícit i equitatiu i complint un objectiu d'interès públic i proporcional al fi legítim perseguit.

D. PROTECCIÓ D'INTERESSOS VITALS (ARTICLE 6.1.*D* RGPD)

Aquesta condició de licitud només podria aplicar-se quan el tractament fos necessari per protegir la vida o la integritat física d'una persona. En principi, el tractament de dades personals en el context de seguiment wifi difícilment podria justificar-se per aquestes raons.

No obstant això, no se'n pot descartar per complet l'aplicació, en situacions en què els interessos vitals estiguessin realment en perill, com ara emergències, auxili o recerca i rescat de persones desaparegudes. Això requeriria una rigorosa anàlisi del cas concret que en justifiqués l'aplicació.[12]

[11] Considerant 17. Dictamen 01/2017 sobre la proposta de Reglament sobre la privacitat i les comunicacions electròniques (2002/58/CE) (GT29,WP247).

[12] Informe 39/2019 del Gabinet Jurídic de l'AEPD.

E. INTERÈS PÚBLIC O EXERCICI DE PODERS PÚBLICS (ARTICLE 6.1.*E* RGPD)

Fonamentar un tractament de dades d'aquestes característiques en aquesta base legitimadora implica fer una anàlisi acurada de les exigències establertes en la normativa de protecció de dades. Així, el responsable del tractament haurà d'identificar la norma amb rang de llei que li atribueixi una competència concreta que li permeti demostrar que aquest tractament mitjançant seguiment wifi és necessari i proporcionat per complir una missió d'interès públic o per exercir poders públics. De conformitat amb la jurisprudència del TJUE, aquesta base jurídica o mesura legislativa ha de ser clara i precisa i la seva aplicació previsible per als seus destinataris, incloses les mesures per garantir un tractament lícit i equitatiu i complint un objectiu d'interès públic i proporcional al fi legítim perseguit.

Cal advertir en contra de l'ús de preceptes legals excessivament genèrics com a base de legitimitat. Atès que no hi ha legislació expressa respecte d'aquest tractament, seria recomanable desenvolupar mesures legislatives que, d'acord amb l'indicat anteriorment, preveiessin i regulessin aquest tipus de tractaments.

Cal tenir en compte que l'actuació de l'Administració se centrarà principalment en espais públics i que les persones tenen una expectativa legítima de gaudir de llibertat de moviments, sense ser monitoritzats. En aquests escenaris, la intromissió sobre la privacitat de les persones pot ser molt alta, si el responsable del tractament no extrema les garanties.[13]

F. INTERESSOS LEGÍTIMS (ARTICLE 6.1.*F* RGPD)

En el sector privat, l'interès legítim es pot considerar una condició de licitud vàlida, sempre que calgui per satisfer aquests interessos i no hi prevalguin els interessos o els drets i llibertats dels interessats, tenint en compte les seves expectatives raonables.

En tot cas, es requereix una avaluació meticulosa de si es pot dur a terme el tractament i prova de sospesament, fins i tot si un interessat pot preveure'l de forma raonable en el moment i en el context de la recollida de dades personals.[14]

Correspon al responsable acreditar la prova de "sospesament." Al Dictamen 6/2014, de 9 d'abril, sobre el concepte d'interès legítim del responsable del tractament, del grup de treball de l'article 29 de la Directiva 95/46/CE -WP 217, s'incorporen diverses directrius i orientacions per analitzar l'existència de l'interès legítim, així com els elements de salvaguarda necessaris en atenció al respecte i garantia dels drets dels afectats per aquest tipus de tractaments.

[13] Vegeu decisió Autoritat de Protecció de Dades dels Països Baixos sobre el tractament de dades personals d'usuaris d'aquests mòbils, als quals es va engegar el wifi al centre de la ciutat d'Enschede sense una base legal apropiada.

[14] Considerant 47 RGPD: "En particular, els interessos i els drets fonamentals de l'interessat podrien prevaler sobre els interessos del responsable del tractament, quan es procedeixi al tractament de les dades personals en circumstàncies en què l'interessat no esperi raonablement que es realitzi un tractament posterior."

En una primera aproximació, s'han de ponderar els interessos i drets de l'interessat i els tractaments que el responsable pretengui dur a terme, valorant l'afectació a la privacitat. No s'ha d'oblidar que el considerant 47 de l'RGPD indica que, als efectes de l'interès legítim, "els interessos i els drets fonamentals de l'interessat podrien prevaler sobre els interessos del responsable del tractament, quan les dades personals es tractin en circumstàncies en les quals l'interessat no esperi raonablement que es realitzi un tractament posterior." I, en el cas del seguiment wifi, tal com s'ha indicat a l'inici, en moltes ocasions el titular del terminal desconeix que s'estan captant les dades.

En definitiva, en aquests casos s'hauria de poder demostrar clarament que l'interès legítim del responsable és prevalent.

Només en els casos en què, com a resultat de la ponderació efectuada, no prevalguin els interessos i els drets fonamentals dels afectats, es podrà dur a terme el tractament de dades personals justificat en un interès legítim. Això, a més, exigiria que s'incorporessin al tractament les salvaguardes, garanties i mesures tècniques i organitzatives, incloses les relatives a la seguretat de la informació, necessàries per protegir les dades personals tractades.

És a dir, la licitud del tractament emparada en aquesta base també queda supeditada a l'existència i intensitat de garanties adequades. Sens dubte, aquestes garanties dependran de la naturalesa més o menys invasiva del tractament proposat i, en gran mesura, de com i quan es realitzi la dissociació irreversible de les dades personals.

En termes generals, el tractament serà considerat menys intrusiu quan les dades s'anonimitzin més a prop del moment en què es van generar o es van rebre les dades de trànsit a través del dispositiu amb wifi activat.

Sense perjudici de la necessitat d'una anàlisi cas per cas i sempre amb ple respecte a totes les exigències de l'RGPD, mesures com una prompta anonimització de les dades recollides, obtenir exclusivament informació agregada sobre el nombre de visitants i les zones més o menys visitades (mapes de calor) de l'interior d'un establiment, garantir que no es prenen dades a l'exterior, ni en zones comunes de pas ni a la via pública, i garantir que no és possible el seguiment de les persones, podrien acostar a un sospesament favorable. Això, sense perjudici del resultat de l'avaluació d'impacte relativa a la protecció de dades.

Altres escenaris que prevegin la recollida de més dades personals en l'espai (àrees de cobertura més grans), en el temps (períodes de temps superiors) o en l'àmbit (dades de mobilitat, de repetició de visites, etc.) allunyen la possibilitat del sospesament favorable, atesa la dificultat de mecanismes efectius i pràctics que permetin a les persones oposar-se al tractament (mecanismes d'*opt-out*) en el seguiment wifi.

5 RISCOS PER ALS DRETS I LLIBERTATS DE LES PERSONES FÍSIQUES

L'article 24.1 de l'RGPD estableix l'obligació de gestionar el risc que un tractament de dades personals suposa per als drets i llibertats de les persones, tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament. Per tant, qualsevol organització que prengui la decisió de posar en marxa un tractament de dades personals ha de gestionar aquests riscos.

En aquest apartat, es presenten els principals riscos que podrien associar-se a tractaments de dades personals que s'implementin utilitzant tecnologia de seguiment wifi. No és una llista exhaustiva, sinó una panoràmica dels principals riscos a considerar. En qualsevol cas, d'acord amb les particulars del tractament concret, els responsables del tractament han de determinar quins riscos hi són aplicables i si n'hi ha d'altres possibles no identificats en aquesta guia.

La gestió del risc per als drets i llibertats de les persones és diferent d'una gestió del risc de compliment dels principis establerts a l'RGPD i la normativa de protecció de dades aplicable. La gestió de riscos de compliment normatiu, com altres gestions del risc amb altres objectius (legal, financer, negoci, frau, projecte, etc.), pot resultar necessària per assolir certs objectius de l'organització, però no dona resposta a les obligacions de gestió de riscos per als drets i llibertats de les persones físiques que imposa l'RGPD. Si el tractament que es pretén iniciar no compleix els principis de l'RGPD, per exemple perquè hi manca una base legal jurídica adequada o no compleix el principi de necessitat i proporcionalitat, el tractament seria il·lícit i estaria prohibit. L'ús de seguiment wifi s'emmarca en un tractament de dades personals i l'organització que l'implementi està obligada a complir els requisits i obligacions que estableix l'RGPD i, entre d'altres, gestionar els riscos per a les persones que es veuran afectades pel tractament en el seu conjunt.

Exemple:
Amb el propòsit de preservar la seguretat de les persones en els accessos a un esdeveniment massiu, és possible voler determinar si algunes de les vies d'accés s'estan congestionant. Per mesurar aquesta congestió, es podria plantejar l'ús de tecnologia de seguiment wifi per fer-ne un compte aproximat, i això serà un mitjà per implementar una de les operacions del tractament, el mesurament de la congestió. La finalitat de preservar la seguretat de les persones no s'assolirà únicament mesurant la congestió, ja que el tractament ha de disposar d'altres operacions, com la presa de decisió de reduir la congestió en un moment donat, la capacitat de fer-ho de forma efectiva i accions perquè això es produeixi de manera eficient i ordenada. Si aquestes operacions que donen sentit a la fi última del tractament no estan implementades correctament, el tractament no està complint una finalitat que tingui una base legal. Així mateix, si ja hi ha mitjans amb els quals s'estan assolint aquests objectius (vídeovigilància, comptadors de persones, etc.), el tractament tampoc seria necessari. Alhora podria resultar no idoni, atès que aquesta mesura comporta un risc addicional, perquè hi ha mitjans menys lesius per assolir la possible finalitat d'aquest sistema.

La gestió de riscos s'ha de fer considerant el tractament de dades personals en el seu conjunt. Una mera anàlisi aïllada dels possibles riscos de la tecnologia de seguiment wifi no tindria sentit i seria insuficient, d'acord amb l'RGPD, ja que aquesta tecnologia és un mitjà que es pot utilitzar en tractaments de diversa complexitat que impliquin l'ús combinat d'altres tecnologies (núvol, *blockchain*, IA, IOT, etc.).

Exemple:
No implica els mateixos riscos un tracta ment que tingui com a finalitat exclusiva controlar l'aforament per garantir la seguretat d'una botiga física individual d'una PIME que es decideixi implementar seguiment wifi, que un tractament amb la mateixa finalitat però en totes les botigues físiques d'una cadena d'àmbit nacional, o un tractament que tingui com a finalitat oferir publicitat en línia adreçada a les persones, segons els establiments o seccions visitades dins d'un establiment.

Utilitzar la mateixa tecnologia a nivell provincial o autonòmic per determinar fluxos habituals de turistes, o obtenir taxes de repetició de visites turístiques de les quals és responsable una autoritat o organisme públic, implicarà més risc que utilitzar-la en una única botiga física, per estimar aforaments. Utilitzant en essència la mateixa tecnologia, els tractaments són diferents i els riscos també ho són.

A. IMPACTE SOBRE LA INTIMITAT DE LES PERSONES

L'ús de la tecnologia seguiment wifi implica que en determinades circumstàncies sigui possible singularitzar les persones, localitzar-les en una ubicació precisa i inferir[16] dades relatives a les persones, en funció del context de la ubicació.

Exemple:
La implementació d'aquesta tècnica en l'àmbit laboral, per exemple en un edifici, pot proporcionar informació sobre part de l'activitat que actualment està protegida per la normativa laboral, com ara el control del temps que es transcorre en zones comunes, amb qui es dialoga i durant quant de temps, l'assistència als lavabos o la localització fora de l'horari estrictament laboral (biblioteca, zones d'esbarjo), etc.

[15] La singularització fa referència a la possibilitat d'individualitzar una persona en un conjunt de dades, ressaltant certs registres. La singularització pot ocórrer fins i tot sense necessitat que la persona sigui identificada.
[16] La inferència s'esdevé quan és possible deduir el valor d'una característica personal amb un alt grau de probabilitat, a partir dels valors d'una sèrie d'altres atributs com ara la localització en determinades ubicacions, el context d'aquestes ubicacions o altres.

B. INTROMISSIÓ AL DOMICILI O ZONES PÚBLIQUES

La tecnologia de seguiment wifi fa difícil establir límits físics clars i definits sobre on sí que es recull el senyal del dispositiu i on no es pot recollir.

En una videocàmera es poden establir certes màscares i orientar les lents, però aquest tipus de límits costa més d'implementar en un sistema basat en radiofreqüència.

Exemple:
La instal·lació d'un sistema de seguiment wifi en un edifici pot estar recollint el senyal de dispositius ubicats en llars o domicilis privats que estiguin darrere d'un mur, de treballadors d'altres entitats o de la mateixa entitat que no haurien de ser subjectes de dades del tractament o, fins i tot, de persones que transiten per la via pública. Aquesta intrusió no seria un risc, sinó un incompliment del principi de legitimació del tractament.

C. ESCALA DEL TRACTAMENT I LIMITACIÓ DE LA LLIBERTAT DE CIRCULACIÓ

Analitzar l'impacte de determinats sistemes tecnològics només segons l'àmbit d'una entitat proporciona una visió limitada de la possible intromissió en la privacitat de les persones.

Actualment, les tecnologies s'implementen a gran escala i cal analitzar-ne l'impacte quan s'implementen massivament, ja que de manera conjunta poden produir un efecte limitador dels drets i llibertats dels ciutadans.

Exemple:
Una empresa de seguretat ofereix, a més dels habituals, un servei de seguiment wifi per al petit comerç, de manera que un 30% dels locals comercials d'una ciutat implementen aquest servei, que permet registrar els identificadors dels transeünts propers al local comercial. D'aquesta manera, seria possible tenir-registrat i controlat el deambular per la ciutat de qualsevol ciutadà, en un determinat moment.

D. SEGUIMENT PER OMISSIÓ: INTROMISSIÓ EN LA LLIBERTAT RELIGIOSA O EL TRACTAMENT DE CATEGORIES ESPECIALS DE DADES

El registre de quins llocs visita una persona permet inferir hàbits de vida i gustos o interessos amb temàtiques relacionades amb els punts en què se la pot localitzar.

Tanmateix, cal tenir en compte que les àrees que una persona no visita també proporcionen molta informació, o fins i tot més, i poden permetre un perfilat basat en categories especials de dades.

A més, és independent del fet que la informació que reveli el tractament en qüestió sigui o no exacta i que el responsable del tractament actuï per obtenir informació inclosa en alguna de les categories especials.[17]

Exemple:
En el marc d'un tractament que incorpori seguiment wifi en l'àmbit d'un centre comercial, que permeti singularitzar una persona, aquesta persona podria ser rastrejada mentre visita botigues d'esport, restaurants de menjar tradicional d'algun país concret, amb pauses en els horaris habituals de culte d'una determinada religió. També se'n podria perfilar l'edat, sexe, religió i procedència estimada, amb o sense prou fonament, quan no accedeix a establiments vinculats amb altres religions ni s'atura mai als exhibidors d'alcohol. De la mateixa manera, un centre comercial que té un determinat centre religiós al seus voltants podria obtenir informació de les persones que habitualment hi assisteixen per exercir el culte religiós segons les seves creences, inclosos menors o persones en risc d'exclusió social o altres situacions de risc.

En essència, quan aquests tractaments es duguin a terme en llocs relacionats amb categories especials de dades, com podria ser un centre hospitalari, una clínica d'una especialitat mèdica o la seu d'un partit polític, el responsable podria estar incorrent en un tractament de categories especials de dades, cosa que incrementa el risc per als drets i llibertats de les persones.

Exemple:
La possibilitat d'atribuir a una persona individual visites a una clínica oncològica en un hospital en el qual s'utilitza la tecnologia de seguiment wifi pot comportar que s'infereixi la malaltia de la persona i que, en el futur, pugui trobar dificultats per contractar una assegurança de salut.

[17] El TJUE (sentència TJUE C-252/21 Meta vs. Oficina Defensa de la Competència Alemanya) considera com a tractament de dades de categories especials la recollida de visites a pàgines o app relacionades amb una o més categories especials de dades, encara que no es recullin dades sensibles en si. Extrapolant aquesta decisió al cas de tractaments que incorporin seguiment wifi, implicaria que en els casos en què aquests tractaments tinguin lloc en recintes o establiments relacionats amb categories especials de dades, el responsable podria estar tractant dades de categories especials.

E. LLIBERTAT PERSONAL I AUTOCENSURA

El coneixement per part d'una persona que serà rastrejada mentre transita per zones públiques, per un edifici o per un centre comercial pot fer que exerceixi l'autocensura per preservar el seu interès per determinades associacions polítiques o religioses, centres culturals o activitats de lleure. Pot condicionar la seva llibertat personal, la seva llibertat de moviments i produir situacions d' autocensura.

Això pot succeir fins i tot en els casos en què s'informi adequadament l'interessat sobre el tractament de les seves dades personals, a causa de les expectatives pròpies sobre el tractament que s'aplicarà a les dades capturades del seu terminal mòbil.

Exemple:
Una persona que tingui curiositat per algun tipus de producte, de servei o de lleure que s'ofereixi en un centre comercial, però que contravingui algun precepte ètic del seu ambient social, o pugui tenir una repercussió mediàtica o ser mal interpretat en qualsevol altra circumstància, pot canviar el seu comportament, si sap que el seu deambular pot ser registrat.

F. L'IMPACTE DE LA REIDENTIFICACIÓ

Fins i tot quan el que es persegueix sigui obtenir dades col·lectives o estadístiques agregades, i no es pretengui singularitzar les persones, l'origen de les dades partirà d'operacions de tractament sobre identificadors únics, com ara adreces MAC o una empremta digital dels dispositius, o d'altres als quals, en el millor dels casos, se'ls aplicarà algun tractament de dades personals de pseudonimització o d'anonimització.[18]

La pseudonimització és un tractament de dades que, a partir d'un conjunt de dades personals, genera un nou conjunt d'informació pseudònima i, també, la informació que permet reidentificar les persones. L'RGPD continua essent aplicable a un conjunt de dades, ja que les persones són identificables.

Per exemple
Substituir les adreces MAC d'un conjunt de dades per un *hash* de l'adreça MAC podria ser una operació de tractament de pseudonimització.

L'anonimització és un tractament de dades que, a partir d'un conjunt de dades personals, genera un nou conjunt d'informació anònima. Per tant, des que es recopilen les dades fins que s'anonimitzen sempre hi ha una fase en què hi ha un tractament de dades personals.

En qualsevol tractament d'anonimització de dades hi ha una certa probabilitat que es produeixi una reidentificació dels interessats.[19]

[18] La pseudonimització i l'anonimització són operacions de tractament diferents i no s'han de confondre. Vegeu **Anonimització i pseudonimització**.

[19] **Anonimització (III); el risc de la reidentificació.**

És a dir, un conjunt de dades suposadament anònim deixa de ser-ho[20] perquè els interessats han estat identificats o poden ser-ho.

Quan això succeeix, es materialitza el risc per als drets i llibertats de les persones perquè possibilita la singularitat, vinculació o inferència, entre altres conseqüències.

Fins i tot aplicant estratègies d'anonimització, cal avaluar la probabilitat de reidentificació i de violació de dades personals, així com l'impacte que pot tenir sobre els drets i llibertats dels interessats.

Per a això cal considerar les condicions del pitjor cas, com ara intents de reidentificació per persones internes o externes a l'organització, amb accés a dades auxiliars, incloses les disponibles per mitjans il·legals, per ordres judicials o per agències d'informació. Això, a més de considerar que es compta amb els recursos adequats i tenint en compte tant la tecnologia disponible en el moment del tractament com els avenços tecnològics.

Exemple:

En algunes aplicacions, es pretén garantir que sigui impossible reutilitzar la informació de seguiment wifi, amb l'ús d'un mètode de *hash* específic a l'ús de *salts* o claus per a cada propietari. Si bé és un mètode per augmentar la seguretat, cal tenir en compte que s'està seguint una tècnica de "seguretat a través de la foscor", que qualsevol principi de seguretat estableix que no ha de ser el pilar de les garanties, per la seva debilitat intrínseca. En qualsevol cas, pot ser una de les moltes mesures a adoptar, sense garantia d'eficàcia absoluta.

Aquesta probabilitat existeix a causa del tipus de dades que es recullen; d'una possible absència de mecanisme robust d'anonimització; del moment o fase del tractament en què s'aplica l'anonimització; del fet que l'anonimització pugui no ser-ho realment; o de l'existència de la tecnologia que permetria dur a terme aquesta reidentificació.

Exemple:

En una base de dades suposadament anonimitzada amb dades de més de 8 milions de trames Probe Request, a través d'un dels camps (WPS) contingut en aquest tipus de trames va ser possible reidentificar més del 90% de dades identificatives dels terminals que transmetien aquest camp.[21]

[20] A. Di Luzio, A. Mei and J. Stefa, "Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests," IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco , CA, USA, 2016, p. 1-9, doi: 10.1109/INFOCOM.2016.7524459.

[21] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo Cardoso, Frank Piessens. Why MAC Address Randomization is not Enough: An Analysis of wifi Network Discovery Mechanisms. ACM AsiaCCS, May 2016, Xi'an, Xina. ff10.1145/2897845.2897883ff. ffhal-01282900

G. RISCOS ASSOCIATS A LES DADES DE LOCALITZACIÓ

Cal incidir en l'especial dificultat d'anonimitzar conjunts de dades, quan inclouen diverses dades de localització d'una mateixa persona o dades de trajectòries,[22] a causa de la facilitat de reidentificació que presenten.

Exemple:

Es van publicar les carreres de 173 milions de taxis a Nova York, anonimitzant (suposadament) el número de llicència de cada taxi amb un *hash*. Les dades incloïen *hash* del número de llicència, inici, final, durada, temps, cost i propina. En molt poc temps, el número de llicència dels taxis es va reidentificar i, amb cerques a Google, es van obtenir imatges de persones amb rellevància pública que agafaven els taxis reidentificats.[23]

El Comitè Europeu de Protecció de Dades (CEPD) i anteriorment el Grup de treball de l'article 29 han advertit en diverses ocasions sobre la naturalesa especialment sensible de les dades de localització.[24] Els desplaçaments d'una persona poden proporcionar informació reveladora, com ara el seu lloc de treball, el lloc de residència i centres d'interès, inclosos llocs de culte o activitats relacionades amb la seva orientació sexual. Això podria permetre crear un perfil detallat dels seus comportaments.

La capacitat d'identificació de les dades de localització és ben coneguda i sovint n'hi ha prou amb pocs punts espacials per singularitzar una persona dins d'una població amb alta precisió, considerant els patrons habituals de mobilitat. Això significa que, fins i tot quan se suprimeixen identificadors únics, com l'adreça MAC, com que el dispositiu està singularitzat les dades de localització poden portar a la identificació d'una persona. Lògicament, com més gran sigui l'àmbit temporal i espacial de la localització més factible serà la identificació.

Un patró de dades que conté la localització d'una persona al llarg del temps no es pot anonimitzar completament, fins i tot si es redueix la precisió de les coordenades geogràfiques registrades o s'eliminen detalls de l'itinerari.

A més, això també s'aplica a dades de localització agregades de forma incompleta. És a dir, simplement anonimitzant dades no es garanteix la protecció de la privacitat, ja que si els patrons de mobilitat són prou únics es pot utilitzar informació externa per vincular novament les dades amb un individu específic.

Així, es poden donar circumstàncies específiques, com ara l'existència d'àrees poc concorregudes a certes hores, on seria senzill identificar la persona i els seus comportaments; o, fins i tot, combinar la captació d'un indicador amb les imatges d'un sistema de videovigilància, cosa que donaria lloc a la identificació automàtica de la persona.

[22] de Montjoye, YA., Hidalgo, C., Verleysen, M. et al. Unique in the Crowd: The privacy bounds of human mobility. Sci Rep 3, 1376 (2013).
[23] On Taxis and Rainbow Tables: Lessons for researchers and governments from NYC's improperly anonymized taxi logs.
[24] Veure Dictamen 13/2011 i 01/2017 del GT29, i les Directrius 04/2020 del CEPD.

H. MANCA DE CAPACITAT D'*ACCOUNTABILITY* DELS MITJANS

L'habitual és que els responsables de tractaments que incorporin als seus tractaments tecnologies d'aquest tipus ho facin mitjançant encarregats del tractament o proveïdors que ofereixen serveis de seguiment wifi, fins i tot en combinació amb altres tecnologies.

En aquest tipus de projectes, sovint s'observa un control insuficient del responsable del tractament dels mitjans que s'estan emprant per implementar el tractament. Molts responsables, en lloc d'una assessoria professional independent, prenen decisions basades en informació purament comercial, amb desconeixement de les implicacions que té això per als drets i llibertats, els possibles tractaments col·laterals i la pèrdua de control del tractament.

Habitualment, les dades es troben en l'entorn tecnològic d'encarregats de tractament amb relacions molt complexes, amb múltiples cessions de dades, en què solen intervenir infraestructures al núvol, sotmesos a l'entorn de dades i que en molts escenaris inclouen tècniques d'aprenentatge automàtic i tractaments per compte dels encarregats de tractament.

Davant d'una eventual generalització d'aquest tipus de serveis, i davant de la competitivitat de les economies d'escala, la situació probablement serà que un mateix encarregat de tractament, o uns quants, prestin els seus serveis a gairebé tots o molts dels responsables. Per tant, aquests encarregats tractaran dades de múltiples orígens diferents i de diversos responsables, amb l'impacte multiplicador que ja estan tenint les violacions de dades personals en encarregats que presten servei a múltiples entitats i que podrien utilitzar-les per a finalitats pròpies,[25] com ara millores en el seu servei, oferir publicitat en línia personalitzada o obtenir rendibilitat de les dades, posant-les a disposició de tercers. Això implica un risc per als drets i llibertats de les persones que el responsable del tractament ha gestionar.

Exemple:

Un proveïdor de serveis de seguiment wifi proporciona gratuïtament a tots els establiments d'un carrer, galeria o centre comercial la possibilitat d'oferir un servei de connectivitat wifi als seus clients, que inclou tecnologia de seguiment wifi de la qual se'n podran aprofitar tots els responsables de manera independent. Cada responsable únicament obtindrà dades estadístiques i suposadament anonimitzades dels clients que entrin al seu establiment. No obstant això, l'encarregat del tractament rebrà les dades de tots els establiments. L'encarregat pot mantenir les dades sense anonimitzar o, fins i tot, haver-les vinculat amb altres bases de dades pròpies o de tercers per mantenir singularitzades o identificades les persones i basar el seu model de negoci en la venda d'aquestes dades personals. En aquest cas, podria estar utilitzant dades al marge del seu rol d'encarregat i convertir-se en responsable d'un tractament per al qual no estaria legitimat.

De fet, encara que el responsable no tingui la intenció d'identificar els interessats ni de realitzar tractaments amb altres finalitats, algun encarregat de tractament o tercer sí que podria tenir la intenció de dur a terme altres

[25] En aquest cas, l'encarregat esdevé responsable per a aquests tractaments propis i no els pot dur a terme sense informar-ne el responsable inicial, obtenir-ne el vistiplau i que les noves finalitats siguin compatibles amb les inicials.

tractaments, aprofitar les dades per a finalitats pròpies, vincular-les[26] amb altres bases de dades que permetin identificar les persones i aconseguir que l'anonimització de les dades no sigui realment efectiva.

Tot i que aquests tractaments seran manifestament il·lícits, en molts casos l'entorn d'aquest tipus de tractaments impedeix tenir garanties o control sobre si s'estan produint.

I. ESCENARIS DE VIOLACIONS DE DADES PERSONALS

El fet que ni el responsable ni els encarregats pretenguin singularitzar, ni identificar, ni perfilar els interessats no implica que això no pugui succeir.[27] En particular, aquest risc es materialitza quan es produeixen violacions de dades personals tant per part d'elements interns com externs a la mateixa organització. Qualsevol tractament de dades personals és susceptible de patir una violació de dades personals, independentment de les mesures tècniques i organitzatives implantades en el tractament.

Quan una violació de dades personals es produeix no només en un responsable, sinó en algun dels encarregats o sotsencarregats de tractament que donen servei a múltiples responsables, l'impacte pot ser molt més gran, tant pel volum de dades com pels diferents àmbits de la vida personal dels interessats afectats.

En general, en tractaments de dades personales que utilitzin seguiment wifi és especialment important considerar la probabilitat que es produeixi una violació de la confidencialitat, bé perquè hi hagi una exfiltració de dades, bé perquè es pugui revertir l'anonimització aplicada al conjunt de dades.

Exemple:
Una empresa de seguretat ofereix, a més dels serveis habituals, un de seguiment wifi per al petit comerç. Un 30% dels locals comercials d'una ciutat implementen aquest servei, que permet registrar els identificadors dels transeünts propers al local comercial. Les dades són anonimitzades per l'empresa de seguretat, de manera que els petits comerços únicament tenen accés a dades anonimitzades. L'empresa de seguretat pateix un ciberincident i s'exfiltren dades, que inclouen logs del sistema de seguiment wifi dels últims 5 anys d'una fase del tractament en la qual les dades encara no estan anonimitzades. Aquestes dades permeten singularitzar les persones, en alguns casos identificar-les, obtenir-ne la ubicació i seguir els seus recorreguts per la ciutat durant els últims 5 anys.

La realitat de les violacions de seguretat de dades personals fa evident que la materialització de les amenaces sobre conjunts de dades és qüestió de temps, i que l'única incògnita és la dimensió que assolirà la violació.

[26] Es parla de vinculabilitat quan és possible vincular almenys dos registres sobre el mateix subjecte de dades o grup de subjectes de dades (a la mateixa base de dades o en dues bases de dades diferents).

[27] Vegeu la decisió de l'Autoritat de Protecció de Dades de Països Baixos sobre el tractament de dades personals d'usuaris de dispositius mòbils en els quals es va connectar el wifi al centre de la ciutat d'Enschede sense una base legal apropiada. "El fet que no utilitzin aquests recursos a la pràctica per identificar les persones al centre de la ciutat no resta valor al fet que podrien fer-ho raonablement."

En aquests casos, el problema no només és en el conjunt de dades que s'han filtrat d'un responsable, sinó en el moment que aquest conjunt es vincula amb dades de violacions anteriors, no solament en el marc de tractaments que utilitzen seguiment wifi, però d'altres serveis d'internet.

Exemple:
Una base de dades de seguiment wifi es pot filtrar a la web fosca. Cal plantejar-se que a la web fosca es poden trobar altres bases de dades que permetin vincular accions d'un mateix individu en dos entorns completament diferents. Fins i tot s'ha pogut filtrar una base de dades prèviament, que permeti vincular les dades wifi amb altres dades personals.

Per tant, abans de posar en marxa un tractament amb tecnologia de seguiment wifi, en particular a l'hora de seleccionar els proveïdors tecnològics i encarregats, és imprescindible plantejar què pot sortir malament i quines conseqüències pot tenir una violació de dades personals per als drets i llibertats de les persones físiques. D'aquesta manera, abans d'implementar el tractament, es poden dissenyar les salvaguardes de privacitat per minimitzar l'impacte de la materialització d'una violació, així com establir-ne els mecanismes de reacció per minimitzar els riscos per als drets i llibertats dels afectats.[28]

J. TRANSFERÈNCIES INTERNACIONALS I EL CONTEXT NORMATIU INTERNACIONAL

De la mà de l'ús d'infraestructures tecnològiques d'encarregats del tractament i de l'ús combinat de múltiples tecnologies, moltes vegades amb sotsencarregats del tractament i infraestructures tecnològiques al núvol, hi ha la possibilitat que el tractament comporti transferències internacionals de dades a països fora de l'Espai Econòmic Europeu (EEE).

En situacions en què es produeixin transferències internacionals de dades, el responsable ha de valorar escenaris com ara fallides de l'estat de dret, emergències nacionals o internacionals o crisis en les relacions i acords internacionals.

Exemple:
Un tractament que incorpori seguiment wifi, que permeti vincular una persona amb la seu d'un partit polític o sindicat vinculat a una ideologia determinada i que utilitzi encarregats de tractament amb tecnologies al núvol, podria implicar transferències internacionals de dades a tercers països. La possibilitat d'identificar-la podria implicar conseqüències sobre les persones, fins i tot legals (per exemple, denegació d'un visat o imputació de càrrecs penals).

[28] Considerant 83 RGPD: A l'hora d'avaluar el risc en relació amb la seguretat de les dades, cal tenir en compte els riscos que es deriven del tractament de les dades personals, com ara la destrucció, pèrdua o comunicació o accés no autoritzats a aquestes dades, susceptibles en particular d'ocasionar danys i perjudicis físics, materials o immaterials.

K. CONCLUSIÓ SOBRE LA GESTIÓ DEL RISC

El responsable ha de tenir en compte i gestionar tots els riscos per als drets i llibertats fonamentals dels interessats aplicables en el tractament. Ha de revisar cadascuna de les amenaces i com poden afectar els drets fonamentals, tenint en compte el cas concret en el seu context, àmbit, naturalesa i finalitats, i analitzant el tractament complet i no únicament algunes de les operacions de tractament.

Sovint, els riscos estan vinculats entre si i la materialització d'algunes amenaces o factors de risc implica que també se'n puguin materialitzar d'altres.

Les mesures tècniques i organitzatives per minimitzar aquests riscos s'aborden en un apartat específic posterior.

6 OBLIGACIÓ DE DUR A TERME UNA AVALUACIÓ D'IMPACTE RELATIVA A LA PROTECCIÓ DE DADES

L'RGPD estableix les obligacions relacionades amb l'avaluació d'impacte relativa a la protecció de dades (AIPD) als articles 35 i 36. No obliga a fer una AIPD a qualsevol tractament de dades personals, però sí als que sigui probable que comportin un alt risc.

L'existència d'un grau raonable de presumpció que el tractament pot comportar un alt risc fa imprescindible executar una AIPD.

L'AIPD és un procés d'avaluació d'un tractament que s'estén en el temps, al llarg de tot el seu cicle de vida, i que s'ha de revisar contínuament, com a mínim quan hi hagi un canvi del risc que representen les operacions de tractament. En cap cas s'ha de considerar un mer formalisme documental.

En termes generals, **una AIPD**:

- És exigible quan hi pugui haver alt risc per als drets i llibertats.
- És una obligació específica del responsable.
- Exigeix superar una avaluació de la necessitat i proporcionalitat del tractament en relació amb les seves finalitats.
- Exigeix que l'avaluació determini que s'ha aconseguit reduir el risc residual a un nivell tolerable, mitjançant l'aplicació de mesures i garanties.
- Exigeix que es faci abans d'iniciar les activitats de tractament.
- Exigeix l'assessorament del DPD, quan la designació sigui obligatòria o hagi estat voluntat del responsable.
- Ha de tenir en compte el compliment dels codis de conducta aprovats i les certificacions que siguin aplicables.

- Cal tenir-ne en compte el resultat, a l'hora d'avaluar la viabilitat o inviabilitat del tractament des del punt de vista de la protecció de dades. El resultat de l'AIPD és vinculant per al responsable del tractament i, segons el nivell de risc residual, obliga a fer una consulta prèvia a l'autoritat de control de protecció de dades competent o, fins i tot, a decidir no dur a terme el tractament.

Per als tractaments que incorporin la tecnologia de seguiment wifi, com per a qualsevol altre tractament, l'avaluació de riscos i l'avaluació de la necessitat de realitzar una AIPD s'ha de considerar tenint en compte el tractament en el seu conjunt; és a dir, tenint en compte el seu propòsit, naturalesa, àmbit o abast i context.

D'acord amb l'article 35.3 de l'RGPD, en els tractaments que incorporin seguiment wifi i que suposin una observació sistemàtica a gran escala[29] d'una zona d'accés públic, l'AIPD és obligatòria. Encara que el responsable del tractament no pretengui fer aquesta observació sistemàtica a gran escala, l'AIPD també serà obligatòria, ja que a la vista del risc inherent del tractament estaríem parlant d'un tractament d'alt risc i, en aquest cas, li són d'aplicació les exigències de l'RGPD per a aquests tractaments. Igualment, caldrà considerar-ho com un agreujant, a causa de la mateixa naturalesa de moltes de les operacions que formen part del seguiment wifi, que farà més difícil per als interessats exercir els seus drets.[30]

Si el tractament compleix dos o més criteris de la **llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a la protecció de dades (art 35.4)** publicada per l'AEPD, també cal fer una AIPD.

Alguns dels criteris rellevants d'aquesta llista per a **tractaments que incorporin seguiment wifi** són:

- Que impliquin l'**observació, monitorització, supervisió, geolocalització o control** de l'interessat de forma sistemàtica i exhaustiva, inclosa la recollida de dades i metadades a través de xarxes, aplicacions o en zones d'accés públic, així com el processament d'identificadors únics que permetin identificar usuaris de serveis de la societat de la informació, com ara els serveis web, TV interactiva, aplicacions mòbils, etc.

- Que impliquin l'**ús de categories especials de dades** a què es refereix l'article 9.1 de l'RGPD, dades relatives a condemnes o infraccions penals a què es refereix l'article 10 de l'RGPD o dades que permetin determinar la situació financera o de solvència patrimonial o deduir informació sobre les persones relacionada amb categories especials de dades.

- Que impliquin l'**ús de dades a gran escala**. Per determinar si un tractament es pot considerar a gran escala, es consideraran els criteris establerts a la guia WP243 "Directrius sobre els delegats de protecció de dades (DPD)" del Grup de treball de l'article 29.

- Que impliquin l'**associació, combinació o enllaç de registres de bases de dades** de dos o més tractaments amb finalitats diferents o efectuats per responsables diferents.

- Que impliquin la **utilització de noves tecnologies o un ús innovador de tecnologies consolidades**, inclòs l'ús de tecnologies a una nova escala, amb un nou objectiu o combinades amb altres, de manera que suposi noves formes de recollida i utilització de dades amb risc per als drets i llibertats de les persones.

[29] **WP243** explica el terme *gran escala* i no exclusivament en termes absoluts del nombre d'interessats.
[30] Considerant 91 del Reglament general de protecció de dades.
[31] **Guia Gestió del risc i avaluació d'impacte en tractaments de dades personals - Apartat XIII. Avaluació de la necessitat i proporcionalitat del tractament.**

Aquests criteris els ha de tenir en compte tant el mateix responsable del tractament com l'encarregat o encarregats de tractament utilitzats pel responsable.

A més, convé recordar l'obligació d'encarregats i sotsencarregats d'ajudar el responsable en la realització de l'AIPD, així com la diligència deguda dels responsables en la contractació d'encarregats que ofereixin garanties adequades. Atesos els factors i elements de risc inherents a la utilització de la tecnologia seguiment wifi exposats en aquesta guia, en general es compliran les condicions perquè l'AIPD sigui obligatòria en tractaments de dades personals que emprin tecnologia de seguiment wifi. Fins i tot en els casos en què el responsable pugui no tenir clara l'obligatorietat de fer una AIPD, cosa que no exclou l'anàlisi i actualització dels riscos associats, les autoritats de control de protecció de dades recomanen fer-la, atesos els factors de risc exposats en aquesta guia.

Finalment, cal recordar que, quan escaigui, el responsable ha de recollir l'opinió dels interessats o dels seus representants en relació amb el tractament previst. En particular, en l'àmbit de les administracions públiques podria ser oportú dur a terme un procediment de participació perquè la ciutadania afectada pogués expressar la seva opinió al respecte, quan es tracti d'actuacions realitzades a l'empara de les lletres *c* i *e* de l'article 6.1 de l'RGPD.

7 AVALUACIÓ DE LA NECESSITAT I PROPORCIONALITAT DEL TRACTAMENT

La primera mesura en el procés d'una AIPD és l'obligació d'avaluar la necessitat i proporcionalitat del tractament en relació amb la finalitat que es persegueix. Això implica fer una ponderació tenint en compte tres criteris: judici d'idoneïtat, judici de necessitat i judici de proporcionalitat, en sentit estricte.[31]

Aquesta avaluació ha de finalitzar amb una decisió sobre si s'ha de dur a terme o no el tractament o, si escau, modificar-lo fins que superi l'anàlisi del triple judici assenyalat abans.

El responsable ha de triar l'opció menys intrusiva per a la privacitat i que impliqui menys riscos per a les persones.

Exemple
Un responsable pretén controlar l'aforament màxim d'un local, amb la finalitat de garantir la seguretat de les persones.

En la implementació del tractament, podria decidir utilitzar elements bàsics per comptar les persones que entren/surten del local, utilitzar mitjans humans, emprar qualsevol altre conjunt de sensors, de CO2, cèl·lules fotoelèctriques, de pressió, videovigilància amb algun grau d'anàlisi o utilitzar tecnologia de seguiment wifi. Tot i perseguir la mateixa finalitat en tots els casos, en principi algunes de les opcions no impliquen un tractament de dades personals, mentre que d'altres poden implicar tractaments de dades personals amb diferent grau d'intrusisme en la privacitat de les persones. Fins i tot podríem parlar de tractaments d'alt risc per als drets i llibertats de les persones físiques, i caldrà determinar la necessitat i la proporcionalitat de les diferents opcions disponibles.

A. AVALUACIÓ OBJECTIVA DE LA IDONEÏTAT DEL TRACTAMENT

A l'hora de definir els requisits del tractament que es podria implementar amb seguiment wifi, cal determinar si la qualitat de la dada que es pot obtenir mitjançant aquesta tecnologia és idònia per executar les accions necessàries del tractament, tenint en compte que no serà infal·lible.

Exemple:
Posem el cas d'un tractament per aplicar una obligació legal que no més de 30 persones estan en una determinada sala. Utilitzant seguiment wifi, es pot donar la situació que algunes persones no portin telèfon, siguin menors sense telèfon, el portin desactivat per no ser comptabilitzats o sense bateria, mentre que d'altres poden portar dos o més mòbils (personal, professional, etc.) i tot això pot dependre de l'edat, del tipus de servei, de l'activitat que s'hagi fet prèviament i d'altres. Per tant, aquest sistema no seria idoni.

Exemple:
Posem el cas d'un tractament per prendre decisions sobre ampliar superfície o personal en un servei d'atenció al client. Per a això, es vol obtenir una estadística d'ocupació d'un determinat local o sala d'espera. En primer lloc, cal determinar el nivell i grau de confiança de la dada que permet prendre una decisió, per exemple, d'un 90% +- 2%.

Això permetrà determinar quins mètodes o tecnologies seran adequats.

B. AVALUACIÓ OBJECTIVA DE LA NECESSITAT DEL TRACTAMENT

En funció de la finalitat del tractament, pot ser intrínsecament necessari un cert grau de singularització per complir amb les finalitats del tractament. Però, en altres ocasions, la singularització no serà necessària per a la finalitat que es persegueix.

Exemple:
Un tractament que incorpora seguiment wifi en una botiga física amb diverses sales, que té com a única finalitat determinar l'aforament de cada estada per no superar l'aforament màxim, en principi no necessitaria singularitzar les persones de cap manera. N'hi hauria prou amb determinar el nombre total de dispositius presents en cada moment. Podria ser fins i tot innecessari tractar qualsevol identificador, sinó només portar un comptatge de les trames Probe Request que s'estan generant.

No obstant això, un tractament similar en un museu en el qual es pretén obtenir els recorreguts habituals entre sales necessitarà singularitzar els individus com a mínim durant determinats períodes de temps i abans d'anonimitzar les dades, per determinar, per exemple, l'ordre de visita de les sales de cada individu o un mapa de calor dels espais més transitats.

En qualsevol cas, per a tractaments que ja s'estiguin duent a terme i es decideixi fer una actualització tecnològica que impliqui més intrusisme en la privacitat dels usuaris, caldrà plantejar-se quina necessitat s'està cobrint que abans no s'assolia dins d'uns marges d'efectivitat raonables.

Exemple:
Es pretén actualitzar el control de presència utilitzant seguiment wifi. El control de presència és un tractament que s'està fent des de fa molts anys amb un grau d'eficàcia raonable. Cal plantejar-se la necessitat de canviar a una tecnologia més intrusiva, que a més pot incorporar limitacions en la seva eficàcia i possibilitats de frau que no es coneixen.

Així mateix, al llarg del cicle de vida del tractament caldrà verificar que aquestes necessitats es continuen aconseguint i continuen essent necessàries per a les finalitats objectives del tractament, i establir caducitats per limitar l'execució d'un tractament que ja no doni resposta a les necessitats esmentades.

8 MESURES TÈCNIQUES I ORGANITZATIVES APROPIADES

Un cop identificats els factors de risc i determinat el nivell de risc del tractament, cal disminuir aquest nivell de risc fins a un valor acceptable, per mitjà de controls i mesures apropiades d'índole tècnica i organitzativa, polítiques de protecció de dades, protecció de dades i privacitat des del disseny i mesures de seguretat. Aquestes mesures han d'estar orientades a disminuir l'impacte o la probabilitat que es materialitzin un o diversos factors de risc específics. Acumular mesures i garanties sense un objectiu específic pot generar noves vulnerabilitats.

No obstant això, no s'ha de confondre la gestió de riscos per als drets i llibertats dels interessats amb el compliment estricte de la resta dels preceptes i principis imposats per la normativa de protecció de dades. La naturalesa de l'RGPD dona llibertat al responsable i l'encarregat en la manera d'implementar les garanties de compliment dels principis i la resta d'obligacions de l'RGPD, sense que això impliqui que el responsable o l'encarregat puguin triar quins preceptes cal complir i quins no. Una de les mesures de protecció de dades des del disseny a aplicar és l'anonimització. Però no és l'única opció possible, ni el responsable ha de renunciar a aplicar altres mesures addicionals, com ara la privacitat diferencial,[32] *compute-to-data* i altres.

En el seu informe jurídic 2019/017, l'AEPD posa de manifest les obligacions per a responsables del tractament que utilitzin la tecnologia de seguiment wifi. S'han d'entendre com a obligacions establertes per la normativa de protecció de dades, entre les quals també hi poden trobar algunes **mesures tècniques i organitzatives**. A continuació se'n relacionen algunes:

- Cal adoptar mesures que garanteixin la prompta anonimització[33] de les dades.

[32] Anonimització i pseudonimització (II): la privacitat diferencial.

- S'ha de valorar l'àmbit en el qual es realitza el seguiment wifi. Per exemple, en l'àmbit privat cal tenir en compte l'existència d'una relació comercial, de manera que es tracti de clients o potencials clients, i evitar en tot cas utilitzar-ho a la via pública.

- Cal limitar i delimitar les zones on es realitza. S'ha d'evitar un control dels moviments en zones molt àmplies, així com a les zones que puguin suposar una ingerència excessiva en la privacitat de la persona, com ara en el cas dels lavabos.

- No es poden utilitzar sense el consentiment dels afectats a les zones en què puguin revelar categories especials de dades, com per exemple les que tinguin productes relacionats amb la salut.

- En cap cas es poden creuar les dades de geolocalització obtingudes d'aquesta manera amb altres dades procedents d'altres fonts que puguin permetre la identificació de la persona (com ara els pagaments amb targeta de crèdit o les imatges captades pels sistemes de videovigilància).

- D'acord amb el criteri de minimització de dades, encara que la recollida de dades hagi de ser contínua, l'emmagatzematge i posteriors operacions de tractament de la posició s'ha de limitar a assenyalar les àrees indicades com d'interès i impedir una recollida detallada i contínua dels moviments dels interessats.

- No s'han de creuar les dades recollides d'un interessat en els locals de diferents responsables. Si el responsable té diversos locals, també cal recollir diferents identificadors.

- No s'ha d'assignar el mateix identificador a un mateix dispositiu mòbil en les diferents visites que realitzi en el temps a la mateixa ubicació.

- L'accés a la wifi del responsable no s'ha de condicionar al consentiment de l'interessat per tractar dades mitjançant seguiment wifi.

- Quan la base jurídica del tractament sigui l'interès legítim del responsable o el compliment d'una missió d'interès públic, s'ha de permetre als interessats exercir el dret d'oposició mitjançant una opció *d'opt-out* quan se'n recullin les dades.[34]

- Cal garantir que les persones tenen ple coneixement que s'estan tractant les seves dades personals en cada moment que produeixi el tractament, així com l'exercici dels seus drets en virtut de l'RGPD.

En la mateixa línia s'expressen la Comissió Nacional d'Informàtica i Llibertat de França (CNIL)[35] i el CEPD.[36] En concret, aquest últim indica a més les mesures següents:

- L'anonimització s'ha de realitzar just després de la recollida de les dades, de manera que tornar-les a identificar estigui tècnicament exclòs.

[33] Cal no confondre-ho amb pseudonimització de les dades.
[34] L'ús de *probe requests* amb MAC aleatòries pot dificultar seriosament la possibilitat d'oferir una opció *d'opt-out*.
[35] CNIL: Audience and attendance measurement devices in spaces accessible to the public: the CNIL recalls the rules
[36] Dictamen 01/2017, sobre la proposta de Reglament sobre la privacitat i les comunicacions electròniques (2002/58/CE) (GT29,WP247).

- Si l'anonimització immediata no és possible tenint en compte la finalitat (per exemple, perquè s'està registrant una trajectòria), les dades personals es poden tractar durant un període en què no estiguin anonimitzades únicament en les condicions següents:
  - La finalitat de la recollida de dades s'ha de limitar al mer recompte estadístic.
  - El seguiment es limita en el temps i l'espai en la mesura estrictament necessària per a aquest fi.
  - Les dades s'eliminen o anonimitzen immediatament després.
  - Hi ha la possibilitat efectiva d'exclusió voluntària.

Els responsables del tractament també han de prendre altres mesures de mitigació per garantir que no hi hagi impacte en els drets fonamentals de tercers. Per exemple, protegir la privacitat de les persones que viuen al costat d'un punt de recopilació.

A l apartat VIII. Controls per disminuir el risc de la Guia de Gestió del risc i avaluació d' impacte en tractaments de dades personals, es presenta una panoràmica completa de controls per disminuir el risc que poden ser apropiats per a qualsevol tractament de dades personals. El responsable que decideixi implementar un tractament amb tecnologia de seguiment wifi ha d'implementar totes aquelles que siguin d'aplicació al tractament concret que pretén dur a terme.

A continuació, es relacionen de manera no exhaustiva algunes mesures tècniques i organitzatives rellevants que podrien ajudar a gestionar els riscos en tractaments que incorporin tecnologia de seguiment wifi.

A. ANONIMITZACIÓ

L'anonimització és un tractament de dades personals que, a partir d'un conjunt de dades personals, genera un nou conjunt d'informació anònima.

Com qualsevol tractament, ha de complir els principis de l'RGPD, entre els quals el de responsabilitat proactiva. Això implica que el responsable ha de prendre les mesures adequades per executar el tractament d'anonimització, amb les garanties necessàries; i, en particular, s'ha de plantejar quin risc suposa per a les persones que el procés d'anonimització es pugui revertir.

L'AEPD posa a disposició dels responsables diverses eines amb àmplia informació sobre l'anonimització de dades al microlloc web d'Innovació i Tecnologia, així com el Dictamen 05/2014 sobre tècniques d'anonimització del Grup de treball de l'article 29.

El tractament d'anonimització no és un procés trivial i comporta una probabilitat de reidentificació que depèn de diversos factors, entre d'altres:

- Moment en què s'anonimitzen les dades. En general, com més aviat s'anonimitzin menor és el tractament de dades personals i menor és el risc per als interessats.[37] Tanmateix, per emprendre determinades finalitats en un tractament és possible que calgui fer l'anonimització en fases posteriors. Per exemple, quan el que es pretén és seguir trajectòries de persones en un interval de temps important, hi ha la possibilitat que les dades s'emmagatzemin sense anonimitzar durant períodes de temps prolongats. L'anonimització tardana de les dades suposa l'augment d'alguns riscos.

[37] Article 25.2 RGPD.

- Tècnica d'anonimització utilitzada: hi ha el risc d'utilitzar procediments d'anonimització febles i que puguin ser revertits.

- Independentment de l'anonimització proposada, es poden donar circumstàncies específiques, com ara l'existència d'àrees poc concorregudes a certes hores o la disponibilitat de diversos punts de localització sobre un mateix dispositiu,[38] on seria senzill identificar la persona o fins i tot els seus comportaments.

Per tot això, després d'un tractament d'anonimització, el responsable ha de determinar mitjançant anàlisis i proves pràctiques que no és possible reidentificar el conjunt de dades. El responsable ha de fer una anàlisi dels riscos de reidentificació i considerar les condicions del pitjor cas, i seria convenient que un tercer en fes una periòdicament. Si en aquestes condicions es pot reidentificar tot o part del conjunt de dades, no es pot parlar de risc de reidentificació; simplement, aquest conjunt de dades no és anònim.

Quant al moment d'anonimitzar, l'anonimització primerenca és la mesura més eficaç per protegir els drets i llibertats de les persones.

Per això cal que el procés d'anonimització s'apropi al màxim possible al moment d'adquisició de les dades. Un sistema que adquireixi les dades personals i les anonimitzi en el punt d'adquisició, abans de qualsevol altre tipus de tractament i fins i tot abans d'emmagatzemar-les, en general comportarà menys riscos per als drets i llibertats de les persones que un sistema que anonimitzi les dades al cap d'unes hores, dies o mesos.

En essència, sempre que sigui possible, l'anonimització s'ha d'aplicar immediatament i el més a prop possible del punt de recollida de les dades, preferiblement de forma local en el dispositiu de captura.

En els casos en què la finalitat que es persegueix exigeixi retardar les operacions d'anonimització, cal aplicar la pseudonimització primerenca fins al moment en què l'anonimització sigui possible. Tanmateix, la pseudonimització no pot ser un substitut de l'anonimització, ni la pseudonimització de les dades justifica endarrerir o no aplicar l'anonimització de les dades.

B. EMMASCARAMENT D'ADRECES MAC I METADADES

L'emmascarament és una mesura tècnica de protecció de dades àmpliament utilitzada en tractaments de dades personals. L'emmascarament d'identificadors únics, com per exemple l'adreça MAC, en el mateix moment de la captura de les dades i per la mateixa interfície de captura, abans que s'emmagatzemin ni tan sols en logs, és una mesura que en determinats escenaris pot resultar eficaç per dificultar la singularització i identificació de persones.

Exemple

Una adreça MAC té 24 bits que identifiquen el fabricant i 24 bits per a assignació lliure del fabricant. Si es pretén controlar diferents persones en un local, és possible que no calgui utilitzar els 48 bits. És possible emmascarar des del moment de la captura de les dades i utilitzar únicament un fragment de l'adreça MAC, per exemple els últims 24 bits.

[38] de Montjoye, YA., Hidalgo, C., Verleysen, M. et al. Unique in the Crowd: The privacy bounds of human mobility. Sci Rep 3, 1376 (2013).

Si es pretén distingir 1.000 persones alhora, amb 14 bits només hi haurà un 6% de possibilitats que dues coincideixin. Si es pretén distingir entre 100 persones, amb 11 bits únicament hi haurà un 5% de possibilitats que dues coincideixin.

Tanmateix, aquesta tècnica no serà útil quan l'adreça MAC no sigui l'identificador emprat o els dispositius enviïn les trames Probe Request amb adreces MAC aleatòries. Quan el mitjà per identificar els dispositius d'usuari sigui una empremta digital, l'emmascarament de les metadades en el moment de la captura serà la mesura que cal aplicar per dificultar la singularització i identificació de persones.

C. DESVINCULACIÓ

Consisteix a aplicar mesures que permetin desvincular les dades capturades en diferents zones geogràfiques i en diferents períodes de temps.

Exemple:
Les empremtes digitals del dispositiu (o qualsevol altre identificador) se substitueixen per un *hash amb salt*, amb la particularitat que s'utilitza una *salt* diferent en cada ubicació i que canvia aleatòriament cada cert temps (cada 12/24 hores). L'històric de *salts* utilitzades no s'emmagatzema, ja que es descarten i eliminen cada vegada que se'n genera una de nova.

D. AGREGACIÓ

Consisteix a agrupar la informació relativa a diversos subjectes, utilitzant tècniques de generalització i supressió.[39] S'utilitza quan no es requereixen registres individuals i les dades agregades són suficients per al propòsit que es persegueix, com pot ser el cas d'alguns tractaments que utilitzin seguiment wifi.

Exemple:
Per obtenir mapes de calor sobre les principals trajectòries seguides per les persones en un museu, no caldrien identificadors únics; n'hi hauria prou amb un simple recompte estadístic.

E. MINIMITZACIÓ DE DADES

Consisteix a adoptar mesures destinades a garantir el compliment del principi de minimització de dades establert a l'RGPD (les dades personals han de ser "adequades, pertinents i limitades al necessari en relació amb els fins per als quals es tracten") a l'hora de dissenyar tractaments que utilitzin seguiment wifi.

[39] La k-anonimitat com a mesura de la privacitat.

Exemples pràctics d'això serien:

- Limitar el període d'activitat dels sensors al mínim imprescindible.
- Limitar l'àrea subjecta a seguiment wifi, evitant incloure-hi zones privades.
- Limitar al màxim l'àrea subjecta a monitorització de les trajectòries de les persones.[40]
- Evitar la captura i emmagatzematge de dades de les trames wifi que facilitin la identificació de les persones (per exemple, el SSID).
- Evitar la captura de dades procedents de determinats tipus de dispositius (dispositius fixos, sensors IOT, implants corporals/sanitaris, etc.)

F. TERMINI DE CONSERVACIÓ DE DADES

Com en qualsevol tractament de dades personals, la limitació efectiva del termini de conservació de les dades té especial rellevància, tant per a les no anonimitzades com per a les anonimitzades, pel risc residual de reidentificació.

G. MESURES DE SEGURETAT I AUDITORIA EXECUTADA PER TERCERS

Les mesures de seguretat s'han d'entendre en un sentit ampli. En cas de tractaments posats en marxa per administracions públiques, els sistemes d'informació utilitzats han d'estar sotmesos a l'Esquema Nacional de Seguretat (ENS),[41] en la categoria corresponent al nivell de risc per als drets i llibertats d'acord amb el resultat de l'AIPD. Aquesta obligació inclou igualment sistemes d'informació de les entitats del sector privat, quan prestin serveis o proveeixin solucions a les entitats del sector públic per a l'exercici de les seves competències i potestats administratives. Les mesures adequades de seguretat no es limiten a les enumerades a l'ENS, sinó que s'han d'estendre, si escau, a les necessàries per garantir un nivell de seguretat adequat al risc per als drets i llibertats fonamentals de cada tractament específic, d'acord amb l'article 32 de l'RGPD.

En cas de tractaments que no estiguin sotmesos a l'obligació de complir l'ENS, caldrà implementar les mesures necessàries per gestionar el nivell de risc per als drets i llibertats fonamentals de cada tractament específic, d'acord amb l' article 32 de l'RGPD.

Cal recordar que l'article 32 de l'RGPD, a l'apartat 1.*d*, exigeix un procés de verificació, avaluació i valoració regular de les mesures de seguretat.

Auditories independents fetes per tercers ajuden a demostrar el compliment de les mesures de seguretat adequades al nivell de risc per als drets fonamentals.

[40] Únicament quan sigui necessari monitoritzar trajectòries per a la finalitat que es persegueix amb el tractament.

[41] Disposició addicional primera LOPDGDD: "Mesures de seguretat en l'àmbit del sector públic: 2. Els responsables enumerats a l'article 77.1 d'aquesta llei orgànica han d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguin a les previstes en l'Esquema Nacional de Seguretat, així com impulsar un grau d'implementació de mesures equivalents en les empreses o fundacions que hi estiguin vinculades subjectes al dret privat."

H. MESURES ORGANITZATIVES I SOBRE ELS ENCARREGATS DEL TRACTAMENT

L'RGPD obliga els responsables a mantenir la diligència deguda per garantir que el tractament s'ajusta a la normativa de protecció de dades i estar en condicions de demostrar-ho. El responsable ha de seleccionar encarregats de tractament amb prou garanties per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme als requisits de l'RGPD. Aquesta previsió s'estén també als encarregats, quan subcontracten operacions de tractament amb altres sotsencarregats.

L'encàrrec de tractament s'ha de regir per un contracte o qualsevol altre vincle legal equivalent. Així mateix, l'encarregat no pot tractar les dades per a finalitats pròpies, sinó únicament seguint les instruccions documentades del responsable i evitant transferències internacionals de dades sense garanties suficients.

D'acord amb les obligacions de l'RGPD, els contractes d'encàrrec del tractament han de contenir explícitament clàusules que impedeixin recórrer a un altre encarregat, sense l'autorització prèvia per escrit del responsable i el tractament de les dades personals per part de l'encarregat del tractament per a finalitats pròpies, o si escau que limitin i condicionin quins tractaments compatibles amb la finalitat del tractament inicial pot realitzar l'encarregat per compte propi. A més, han d'establir explícitament la resposta a una violació de dades personals que pugui patir l'encarregat, tant per al tractament efectuat per compte del responsable com per a possibles tractaments propis de l'encarregat.

El responsable s'ha d'assegurar d'impedir transferències internacionals de dades sense garanties adequades.

Igualment, els responsables han d'implantar mesures de protecció de dades des del disseny i per defecte, per minimitzar els riscos sobre els drets i llibertats que podria causar una violació de dades personals. Pel que fa a les mesures de seguretat, cal recordar que, segons l'experiència i la doctrina del Tribunal Suprem, suposen una obligació de mitjans, però no de finalitats.

En general, en tractaments de dades personales que utilitzin seguiment wifi és especialment important considerar la probabilitat que es produeixi una violació de la confidencialitat. Per tant, a priori el responsable ha d'adoptar mesures per minimitzar els riscos sobre els interessats i, en el cas que succeeixin, tenir prevista la resposta del responsable i els encarregats per minimitzar-ne l'impacte sobre els drets i alliberaments de les persones.

És important identificar per endavant el grau de responsabilitat de cadascun dels intervinents en el tractament, en els diferents escenaris en els quals es pugui produir una violació de la confidencialitat, i a quines obligacions ha de fer front cadascun d'ells per gestionar adequadament la violació, incloses les obligacions de notificació a l'autoritat de control de protecció de dades competent i la comunicació als afectats, quan siguin obligatòries.

[42] C.G.P.J - Notícies Judicials (poderjudicial.es)

I. GESTIÓ CONTÍNUA DEL RISC

El responsable del tractament ha d'analitzar els riscos del tractament tenint en compte totes les seves particularitats i circumstàncies. Si en algun moment es produeix un canvi en el tractament o en factors que l'afectin, els riscos s'han de tornar a avaluar i gestionar.

L'RGPD (article 24) i la Llei orgànica 7/2021 (article 27, que transposa l'article 19 de la Directiva 680/2016) exigeixen que el responsable del tractament revisi i actualitzi les mesures implantades en el tractament, per garantir que compleix la normativa de protecció de dades. La mateixa norma estableix que aquesta revisió i actualització s'ha de dur a terme quan resulti necessari.

9. TRANSPARÈNCIA I INFORMACIÓ

Cal considerar que l'ús de la tecnologia de seguiment wifi en la qual es recull informació com a resultat de la comunicació entre un terminal (telèfon mòbil o qualsevol altre dispositiu) d'una persona física i una xarxa wifi, a fi de generar una empremta digital del dispositiu que el diferencii de la resta de terminals, pot suposar un tractament de dades personals. Per tant, el responsable i l'encarregat del tractament han de respectar els principis i drets recollits a l'RGPD.

Entre aquests principis, l'article 5.1.*a* de l'RGPD reconeix el principi de transparència, conjuntament amb els principis de licitud i lleialtat.
La particularitat que implica que aquest tractament pugui passar inadvertit a les persones titulars dels terminals fa encara més necessari complir el principi de transparència, per mitjà d'una informació clara i accessible. L'article 13 de l'RGPD detalla la informació necessària que cal facilitar a l'interessat, quan les dades personals s'obtinguin del mateix interessat.

Cal **informar prèviament les persones** sobre els aspectes següents:

- Identitat i dades de contacte del responsable del tractament i, si escau, del seu representant.
- Dades de contacte del delegat o delegada de protecció de dades.
- Fins i base jurídica del tractament.
- Interessos legítims del responsable o d'un tercer.
- Destinataris o categories de destinataris de les dades personals.
- Transferències internacionals previstes.
- Termini de conservació.
- Drets d'accés, rectificació o supressió, limitació del tractament, oposició i portabilitat.
- Possibilitat de revocació del consentiment.
- Dret a presentar una reclamació davant d'una autoritat de control.

[43] Quan cal revisar les mesures de protecció de dades.

A. INFORMACIÓ PER CAPES

La informació que es faciliti ha de ser concisa, transparent, accessible i fàcil d'entendre i s'ha de presentar en un llenguatge clar i senzill, en especial l'adreçada específicament als infants.

Així, l'article 11 de l'LOPDGDD ha previst que el responsable pugui complir el deure d'informació establert a l'article 13 de l'RGPD facilitant a l'interessat una informació bàsica, i indicant-li una adreça electrònica o un altre mitjà que li permeti accedir, de manera senzilla i immediata, a la informació restant (és el que s'anomena "informació per capes").

El **contingut mínim** que ha de tenir la informació bàsica és el següent:

- La identitat del responsable del tractament.
- La finalitat del tractament.
- La possibilitat d'exercir els drets establerts als articles 15 a 22 de l'RGPD.
- Informació sobre si les dades personals obtingudes es tractaran per a l'elaboració de perfils i, també, del seu dret a oposar-se que s'adoptin decisions individuals automatitzades que produeixin efectes jurídics sobre l'afectat o l'afectin significativament de manera similar, quan hi concorri aquest dret d'acord amb l'article 22 de l'RGPD.
- La informació s'ha de facilitar per escrit o altres mitjans, fins i tot electrònics, si escau. La informació es pot facilitar verbalment, quan ho sol·liciti l'interessat, sempre que es demostri la identitat del sol·licitant per altres mitjans.

Les Directrius del Grup de treball de l'article 29 sobre la transparència en virtut de l'RGPD, adoptades el 29 de novembre de 2017 (revisades l'11 d'abril de 2018), van recollir com **a vies possibles per transmetre la informació als interessats**, en un entorn com el de seguiment wifi, l'ús de:

- Panells clarament visibles amb informació.
- Senyalització pública en tota l'àrea de cobertura.
- Campanyes públiques d'informació.
- Icones (icones normalitzades que permetin proporcionar de manera fàcilment visible, intel·ligible i clarament llegible una adequada visió de conjunt del tractament previst, segons l'article 12.7 de l'RGPD).
- Alertes de veu.
- Detalls per escrit, inclosos en instruccions de configuració.
- Vídeos integrats en instruccions digitals de configuració.
- Informació per escrit sobre dispositius intel·ligents, missatges per SMS o correu electrònic.

En el cas concret que les administracions públiques emprin aquestes tecnologies, es recomana addicionalment el següent conjunt de **mesures de transparència**, mitjançant la publicació de:[44]

- Un registre de sensors de seguiment wifi desplegats a la via pública.
- Els objectius concrets que es persegueixen, amb indicació de les dates d'inici i de finalització del tractament.

[44] Més informació a Investigation Report on the Protection of Personal Data in the Development of Dutch Smart Cities.

- Un extracte adequat (sense informació sensible) de les avaluacions d'impacte que es realitzin.
- La informació rellevant dels algoritmes d'anonimització emprats.
- La informació accessible en diversos idiomes, si es tracta d'una zona de gran afluència turística.

En qualsevol cas, de conformitat amb l'article 31 de l'LOPDGDD, els responsables i encarregats del tractament o, si escau, els seus representants, han de mantenir el registre d'activitats de tractament a què es refereix l'article 30 de l'RGPD, llevat que sigui d'aplicació l'excepció que preveu l'apartat 5. Els subjectes enumerats a l'article 77.1 de l'LOPDGDD han de fer públic un inventari de les seves activitats de tractament, accessible per mitjans electrònics, i la seva base legal.

10. EXERCICI DE DRETS RECONEGUTS A L'RGPD

De conformitat amb l'article 11 de l'RGPD, si els fins per als quals un responsable tracta dades personals no requereixen o ja no requereixen la identificació d'un interessat, el responsable no està obligat a mantenir, obtenir o tractar informació addicional per identificar-lo l'interessat, amb l'única finalitat de complir l'RGPD. En aquests casos, si el responsable és capaç de demostrar que no està en condicions d'identificar-lo, l'ha d'informar en conseqüència, si és possible, i no seran d'aplicació els articles 15 a 20 de l'RGPD (drets d'accés, de rectificació, de supressió, dret a la limitació del tractament, i a la portabilitat de les dades), tret que l'interessat, a l'efecte d'exercir els seus drets en virtut d'aquests articles, faciliti informació addicional que permeti identificar-lo.

Aquest serà el cas quan el responsable del tractament hagi dut a terme un procés d'anonimització de les dades personals tractades i sigui capaç de demostrar que no està en condicions d'identificar l'interessat. Els articles 15 a 20 de l'RGPD no seran d'aplicació a les dades anonimitzades, però sí que seran d'aplicació a les dades personals que el responsable estigui tractant en fases del tractament prèvies a l'anonimització.

El responsable del tractament està obligat a informar la persona afectada sobre els mitjans a la seva disposició per exercir els drets reconeguts als articles 15 a 22 de l'RGPD. Els mitjans han de ser fàcilment accessibles per a la persona afectada. El responsable ha d'establir mecanismes visibles, accessibles i senzills, inclosos mitjans electrònics, per a l'exercici de drets.

Quan es tracti de l'exercici per mitjans electrònics en particular, aquests mecanismes han d'incorporar procediments per verificar la identitat de les persones afectades que els utilitzen, així com mecanismes per a la recepció de l'exercici del dret corresponent i la resposta oportuna.

A. DRET D'ACCÉS (ARTICLE 15 RGPD)

L'interessat té dret a obtenir del responsable del tractament confirmació de si s'estan tractant o no dades personals que el concerneixen i, en aquest cas, té dret a accedir a les dades personals i a la informació que es detalla a l'article 15.1 de l'RGPD.

Es pot considerar repetitiu l'exercici del dret d'accés en més d'una ocasió durant el termini de sis mesos, llevat que n'hi hagi una causa legítima (art. 13.3 LOPDGDD). Davant d'això, el responsable del tractament pot cobrar un cànon raonable en funció dels costos administratius, o negar-se a actuar respecte de la sol·licitud. En tot cas, l'interessat té dret a conèixer i que se li comuniquin, en particular, els fins per als quals es tracten les dades personals, les categories de dades personals, els destinataris, el termini de conservació, informació sobre el seu origen, l'existència de decisions automatitzades, inclosa l'elaboració de perfils a què es refereix l'article 22 de l'RGPD i, almenys en aquests casos, informació sobre la lògica aplicada, així com la importància i les conseqüències previstes d'aquest tractament per a l' interessat.

Fins i tot quan el responsable hagi dut a terme processos d'anonimització pels quals no pugui identificar les dades de l'interessat i facilitar-li una còpia les seves dades personals objecte del tractament, sí que ha d'oferir tota la informació necessària sobre el tractament per complir amb el principi de transparència.

B. DRET DE SUPRESSIÓ (ARTICLE 17 RGPD)

L'interessat té dret a obtenir del responsable del tractament, sense dilació indeguda, la **supressió de les dades personals** que el concerneixen, **quan hi** concorri algunes de les circumstàncies següents:

- Les dades personals ja no siguin necessàries en relació amb les finalitats per a les quals es van recollir o tractar d'una altra manera.
- La persona interessada retiri el consentiment en què es basa el tractament, de conformitat amb l'article 6.1.*a* o l'article 9.2.*a* de l'RGPD, i aquest no es basi en un altre fonament jurídic.
- La persona interessada s'oposi al tractament, d'acord amb l'article 21.1 de l'RGPD, i no prevalguin altres motius legítims per al tractament, o la persona interessada s'oposi al tractament d'acord amb l'article 21.2 de l'RGPD.
- Les dades personals hagin estat tractades il·lícitament.
- Les dades personals s'hagin de suprimir per complir una obligació legal establerta en el dret de la Unió o dels estats membres que s'apliqui al responsable del tractament.
- Les dades personals s'hagin obtingut en relació amb l'oferta de serveis de la societat de la informació esmentats a l'article 8.1 de l'RGPD.

Quan el responsable del tractament hagi fet públiques les dades personals i estigui obligat a suprimir aquestes dades perquè hi concorri alguna de les circumstàncies referides, tenint en compte la tecnologia disponible i el cost de la seva aplicació ha d'adoptar mesures raonables, incloses mesures tècniques, a fi d'informar els responsables que estiguin tractant les dades

personals, de la sol·licitud de la persona interessada de supressió de qualsevol enllaç a aquestes dades personals, o de qualsevol còpia o rèplica d'aquestes dades. No escau la supressió de les dades personals en els supòsits previstos a l'article 17.3 de l'RGPD.

El responsable del tractament està obligat a bloquejar les dades, quan les suprimeixi (article 32 LOPDGDD). Les dades bloquejades quedaran a disposició exclusiva dels jutges i tribunals, del Ministeri Fiscal o les administracions públiques competents, en particular de les autoritats de protecció de dades, per a l'exigència de possibles responsabilitats derivades del tractament i fins que aquestes responsabilitats prescriguin. Transcorregut aquest termini, cal destruir les dades. Les dades bloquejades no es poden tractar per a cap finalitat diferent de les assenyalades. Les autoritats de control poden fixar excepcions a l'obligació de bloqueig.

El responsable del tractament ha de comunicar la supressió a cadascun dels destinataris als quals s'hagin comunicat les dades personals, llevat que sigui impossible o exigeixi un esforç desproporcionat, i informarà l'interessat sobre aquests destinataris, si així ho sol·licita (article 19 RGPD).

C. DRET A LA LIMITACIÓ DEL TRACTAMENT (ARTICLE 18 RGPD)

Permet a la persona afectada demanar al responsable del tractament que **suspengui el tractament de dades, quan**:

- S'impugni l'exactitud de les dades, mentre el responsable verifica aquesta exactitud.
- La persona afectada ha exercit el seu dret d'oposició al tractament de dades, mentre es verifica si els motius legítims del responsable prevalen sobre els de la persona afectada.
- Sol·licitar al responsable del tractament que conservi les seves dades personals quan:
  - El tractament sigui il·lícit i la persona afectada s'oposi a la supressió de les seves dades i en el seu lloc sol·liciti que se'n limiti l'ús.
  - El responsable ja no necessita les dades per a les finalitats del tractament, però la persona afectada sí que les necessita per formular, exercir o defensar reclamacions.

Limitat el tractament de les dades personals de la persona afectada, tret de la seva conservació aquestes dades només es poden tractar amb el consentiment de la mateixa persona afectada, o per formular, exercir o defensar reclamacions, o amb la finalitat de protegir els drets d'una altra persona física o jurídica o per raons d'interès públic important de la Unió o d'un estat membre.

El fet que el tractament de les dades personals estigui limitat ha de constar clarament en els sistemes d'informació del responsable del tractament (article 16.2 LOPDGDD).

Qualsevol persona interessada que hagi obtingut la limitació del tractament ha de ser informada pel responsable abans d'aixecar aquesta limitació. El responsable del tractament ha de comunicar la limitació a cadascun dels destinataris als quals s'hagin comunicat les dades personals, llevat que sigui impossible o exigeixi un esforç desproporcionat, i ha d'informar l'interessat sobre aquests destinataris, si així ho sol·licita (article 19 RGPD).

D. DRET A LA PORTABILITAT DE LES DADES (ARTICLE 20 RGPD)

L'interessat té dret a rebre les dades facilitades al responsable de tractament en un format estructurat, d'ús comú i lectura mecànica, així com que les dades cedides a un responsable de tractament es puguin transmetre directament a un altre responsable, sempre que el tractament estigui basat en el consentiment de l'interessat o en el marc de l'execució d'un contracte i que aquest tractament s'efectuï per mitjans automatitzats.

No obstant això, aquest dret no s'aplicarà quan el tractament sigui necessari per complir una missió realitzada en interès públic o en l'exercici de poders públics concedits al responsable del tractament.

E. DRET D'OPOSICIÓ (ARTICLE 21 RGPD)

L'interessat té dret a oposar-se en qualsevol moment, per motius relacionats amb la seva situació personal, al fet que les dades personals que el concerneixen siguin objecte d'un tractament basat en el que disposa l'article 6.1, lletres *e* i *f* de l'RGPD, inclosa l'elaboració de perfils sobre la base d'aquestes disposicions.

Davant l'exercici del dret d'oposició, el responsable del tractament ha de deixar de tractar les dades personals, llevat que acrediti motius legítims imperiosos per tractar-les que prevalguin sobre els interessos, els drets i les llibertats de l'interessat, o per formular, exercir o defensar reclamacions.

El dret d'oposició s'ha de comunicar explícitament a la persona interessada, i s'ha de presentar clarament i al marge de qualsevol altra informació.

Cal facilitar que els interessats es puguin oposar al tractament de manera senzilla.

Com una garantia addicional per reduir o mitigar l'impacte sobre els interessats dels quals es recullen les dades personals a través del seguiment wifi, el responsable podria optar per possibilitar una "exclusió voluntària" general, més enllà de la mateixa oposició, i cessar en el tractament sense necessitat de cap mena de justificació.

F. DECISIONS INDIVIDUALS AUTOMATITZADES, INCLOSA L'ELABORACIÓ DE PERFILS (ARTICLE 22 RGPD)

La mateixa naturalesa de la tecnologia de seguiment wifi fa viable dur a terme tractaments basats en aquesta tecnologia que impliquin la presa de decisions automatitzades, inclosa l'elaboració de perfils.

L'interessat té dret a no ser objecte d'una decisió realitzada pel responsable del tractament basada únicament en el tracta- ment automatitzat de la seva informació personal, inclosa l'elaboració de perfils, que produeixi efectes jurídics en aquesta persona o l'afecti significativament de manera similar.

No obstant això, **serà lícit efectuar el tractament i prendre una decisió automatitzada**:

- Quan sigui necessària per formalitzar o executar un contracte entre la persona interessada i un responsable del tractament, o quan es basa en el consentiment explícit de la persona interessada.

- Quan està autoritzada pel dret de la Unió o dels estats membres que s'apliqui al responsable del tractament i que, així mateix, estableixi mesures adequades per salvaguardar els drets i llibertats i els interessos legítims de la persona interessada.

En ambdós casos, el responsable ha d'adoptar les mesures adequades per salvaguardar els drets i llibertats i els interessos legítims de la persona interessada; com a mínim, el dret a obtenir intervenció humana per part del responsable, a expressar el seu punt de vista i a impugnar la decisió.

En aquests tractaments, no s'han d'emprar categories especials de dades personals previstes a l'article 9.1 de l'RGPD, llevat que el tractament es realitzi mitjançant el consentiment de la persona interessada o es tracti d'un interès públic essencial, imposat pel dret de la Unió o de l'estat membre. En aquests casos, s'ha d'assegurar que s'hagin pres mesures adequades per salvaguardar els drets i llibertats i els interessos legítims de la persona interessada.

11. REGLAMENT D'INTEL·LIGÈNCIA ARTIFICIAL

Atesa la situació tecnològica actual, és possible que s'efectuïn tractaments de dades personals en els quals es combini l'ús de la tecnologia de seguiment wifi i sistemes d'intel·ligència artificial (IA). Aquest tipus de tractaments està subjecte al sistema de principis, obligacions per als responsables i drets per als interessats que estableix l'RGPD. Addicionalment, l'ús de determinats sistemes d'IA estarà regulat pel Reglament d'intel·ligència artificial (RIA).

En el moment de publicar aquesta Guia, el RIA encara no s'ha publicat. Entrarà en vigor en el termini de 20 dies després de la seva publicació i en la majoria de les seves disposicions serà aplicable al cap de dos anys d'haver-se publicat.

Des de la perspectiva de la protecció de dades personals, el RIA no té per objecte afectar l'aplicació del dret fonamental a la protecció de dades. És complementari a l'RGPD i s'aplicarà sens perjudici d'aquest, amb el propòsit de permetre que els responsables i els encarregats estiguin en condicions de complir les seves obligacions en matèria de protecció de dades quan incorporen sistemes d'IA als seus tractaments (considerant 78 RGPD), per implementar la protecció de dades des del disseny del tractament.

Per això, la introducció en el mercat i la posada en servei i la utilització de sistemes d'IA han de facilitar l'aplicació efectiva i permetre l'exercici dels drets i altres vies de recurs dels interessats garantits per la normativa de protecció de dades, així com d'altres drets fonamentals.

Això inclou les obligacions de proveïdors i responsables, o d'altres intervinents i operadors quan escaigui, de desplegar sistemes d'IA en la mesura que el disseny, el desenvolupament o l'ús de sistemes d'IA impliquin el tractament de dades personals, així com les funcions i competències de les autoritats de control independents de protecció de dades. Entre d'altres, aquestes autoritats tindran la facultat de demanar qualsevol documentació creada o

conservada d'acord amb el RIA relativa a sistemes d'IA d'alt risc esmentats a l'annex III d'aquest Reglament, quan l'accés a aquesta documentació sigui necessari per al compliment efectiu de les seves competències.

També convé aclarir que els interessats continuen gaudint de tots els drets i garanties que els confereix la normativa de protecció de dades, inclosos els drets relacionats amb les decisions individuals totalment automatitzades, com l'elaboració de perfils.

En aquest sentit, com a exemple, quan partint de les dades obtingudes mitjançant la tecnologia de seguiment wifi com a informació d'entrada, s'implementin decisions que produeixin efectes jurídics en una persona o l'afectin significativament mitjançant sistemes d'intel·ligència artificial (amb independència del tipus que siguin), basades únicament en el tractament automatitzat de dades personals, s'aplicarà el que ja preveu l'RGPD (articles 13, 14, 15 i 22 i considerant 71 RGPD).

A més, per a aquest supòsit, en el cas concret que el sistema d'intel·ligència artificial en el qual es basa la decisió fos d'alt risc, d'acord amb el RIA, de manera complementària als drets previstos a l'RGPD, quan la persona considerés que la decisió té un impacte advers sobre la seva salut, seguretat o els seus drets fonamentals, serà d'aplicació el que preveu la regulació d'IA respecte que la persona afectada pugui tenir dret a rebre explicacions clares i significatives sobre el paper del sistema d'intel·ligència artificial en el procediment de presa de decisions i els principals elements de la decisió adoptada.


aepd
agencia
española
protección
datos


apdcat
Autoritat Catalana de
Protecció de Dades


Datuak Babesteko
Euskal Agintaritza
Autoridad Vasca de
Protección de Datos


Consejo de Transparencia
y Protección de Datos
de Andalucía