



WI-FI JARRAIPENENKO TEKNIKAK:

Tratamenduaren arduradunentzako orientabideak



Bertsioa:
2024ko apirila

LABURPEN BETEARAZLEA

Wi-Fi jarraipena edo Wi-Fi trackinga, gailu mugikorrak identifikatzeko eta haien jarraipena egiteko modua ematen duen teknologia da. Gailu mugikor horiek emititzen dituzten Wi-Fi seinaleak erabiltzen ditu, eremu jakin batean gailu horien presentzia detektatzeko eta mugimendu-ereduak identifikatzeko.

Hori dela eta, leku baten edukierak kalkulatzeko, pertsonen fluxuak aztertzeko edo pertsonak leku batean egoten diren denborak neurtzeko erabiltzen da.

Modu praktikoan aplikatu ahal da merkataritza-zentroetan, museoetan, interes handiko lekuetan, lantokietan, gune publikoetan, garraio publikoan edo gertakari publiko handietan. Hala ere, jardunbide horrek pribatutasunarako arrisku handiak dakartza; izan ere, baliteke pertsonen mugimenduen jarraipena egitea pertsona horiek ezer egin gabe eta ezer jakin gabe, eta behar bezalako lege-oinarririk gabe.

Ezinbestekoa da konturatzeari Wi-Fi trackingaren erabilera horietako askotan datu pertsonalak biltzen direla eta datu pertsonal horien

beste hainbat tratamendu egiten direla eta, beraz, DBEOn ezarritako printzipioen, pertsona fisikoen eskubideen eta tratamenduaren arduradunentzako eginbeharren mende egon behar dutela.

Orientabide horietan, teknologia hori erabiltzeak dakartzan ondorioak aztertzen dira, arlo teknikoan zein arlo juridikoan, teknologia horrekin lotutako arrisku nagusiak identifikatzen dira eta gomendio zehatz batzuk ematen dira teknologia hori arduraz erabiltzeko eta datuen babesari buruzko araudiarekin bateragarri egiteko.

Datuak Babesteko Espainiako Agentziak, Datuak Babesteko Kataluniako Agintaritzak, Datuak Babesteko Euskal Agintaritzak eta Gardentasunaren eta Datu Babesaren Andaluziako Kontseiluak orientabide hauek prestatu dituzte, lau kontrol-agintaritzak horien arteko elkarlanari esker, gogoan hartuta «Wi-Fi tracking» teknologia behar ez bezala erabiltzeak ondorio txarrak ekar ditzakeela pribatutasunean eta pertsona fisikoen datuen babesean.



AURKIBIDEA

1. HITZAURREA	8
2. ESPARRU TEKNOLOGIKOAREN AZALPENA	10
A. MAC HELBIDE FINKOEN ETA AUSAZKOEN ERABILERA	10
B. WI-FI TRACKINGEAN ERABILTZEN DIREN DATUAK	11
C. GAILUAK IDENTIFIKATZEA	13
3. TARTEAN DAUDEN DATU PERTSONALAK ETA TRATAMENDUAK	14
A. “DATU PERTSONALA” TERMINOAREN NORAINOKOA	14
B. WI-FI TRACKINGA ETA “FINGERPRINTING” IZENEOA, DATU PERTSONAL GISA	16
C. WI-FI TRACKINGA ETA LOKALIZAZIOAREN ETA IBILBIDEEN DATUAK	17
D. DATU PERTSONALEN TRATAMENDUA	17
4. DATU PERTSONALEN TRATAMENDUAREN OINARRI LEGITIMATZAILEAK	18
A. ADOSTASUNA (DBEOREN 6.1.A ARTIKULUA)	19
B. KONTRATU BAT GAUZATZEA (DBEOREN 6.1.B ARTIKULUA)	20
C. LEGE-EGINBEHAR BAT BETETZEA (DBEOREN 6.1.C ARTIKULUA)	20
D. BIZI-INTERESAK BABESTEA (DBEOREN 6.1.D ARTIKULUA)	20
E. INTERES PUBLIKOA EDO BOTERE PUBLIKOAK EGIKARITZEA (DBEOREN 6.1.E ARTIKULUA)	21
F. INTERES LEGITIMOAK (DBEOREN 6.1.F ARTIKULUA)	21

5. PERTSONA FISIKOEN ESKUBIDE ETA ASKATASUNETARAKO ARRISKUAK	23
A. PERTSONEN INTIMITATEAREN GAINEKO ERAGINA	24
B. BIZILEKUAN EDO GUNE PUBLIKOETAN ESKUA SARTZEA	25
C. TRATAMENDUAREN ESKALA ETA ZIRKULATZEKO ASKATASUNAREN MUGAKETA	25
D. EZ-EGITEZKO JARRAIPENA: ERLIJO-ASKATASUNEAN EDO DATU-KATEGORIA BEREZIEN TRATAMENDUAN BIDEGABE SARTZEA	26
E. ASKATASUN PERTSONALA ETA AUTOZENTSURA	27
F. BERRIDENTIFIKAZIOAREN ERAGINA	27
G. LOKALIZAZIO-DATUEI LOTUTAKO ARRISKUAK	29
H. BITARTEKOEN «ACCOUNTABILITY» DELAKOA EZ EGOTEA	30
I. DATU PERTSONALEN ARRAKALEN EGOERAK	31
J. NAZIOARTEKO TRANSFERENTZIAK ETA NAZIOARTEKO ARAU-TESTUINGURUA	32
K. ARRISKUAREN KUDEAKETARI BURUZKO ONDORIOA	33
6. DATU-BABESAREN GAINEKO ERAGINAREN EBALUAZIOA NAHITAEZ EGIN BEHARRA	33
7. TRATAMENDUAREN BEHARRIZANAREN ETA PROPORTZIONALTASUNAREN EBALUAZIOA	35
A. TRATAMENDUAREN EGOKITASUNAREN EBALUAZIO OBJEKTIBOA	36
B. DATU PERTSONALEN TRATAMENDUA EGITEKO BEHARRIZANAREN EBALUAZIO OBJEKTIBOA	36

8. NEURRI TEKNIKO ETA ANTOLAKUNTZAKO NEURRI EGOKIAK	37
A. ANONIMIZAZIOA	39
B. MAC HELBIDEAK ETA METADATUAK MASKARATZEA	40
C. DESLOTZEA	41
D. AGREGATZEA	41
E. DATUAK MINIMIZATZEA	41
F. DATUEN KONTSERBAZIO EPEA	42
G. SEGURTASUN-NEURRIAK ETA HIRUGARRENEK EGIN BEHARREKO AUDITORETZA	42
H. ANTOLAKUNTZAKO NEURRIAK	43
I. ARRISKUAREN ETENGABEKO KUDEAKETA	44
9. GARDENTASUNA ETA INFORMAZIOA	44
A. INFORMAZIOA HAINBAT GERUZATAN	45
10. DBEO-N ONARTUTAKO ESKUBIDEAK EGIKARITZEA	46
A. IRISPIDE-ESKUBIDEA (DBEOREN 15. ARTIKULUA)	47
B. EZEREZTEKO ESKUBIDEA (DBEOREN 17. ARTIKULUA)	47
C. TRATAMENDUA MUGATZEKO ESKUBIDEA (DBEOREN 18. ARTIKULUA)	48
D. DATUEN ERAMANGARRITASUN-ESKUBIDEA (DBEOREN 20. ARTIKULUA)	49
E. AURKA EGITEKO ESKUBIDEA (DBEOREN 21. ARTIKULUA)	49
F. BANAKAKO ERABAKI AUTOMATIZATUAK, PROFILAK EGITEA BARNE (DBEOREN 22. ARTIKULUA)	49
11. ADIMEN ARTIFIZIALAREN ERREGELAMENDUA	50

AKRONIMOAK

AP: «Access Point». Wi-Fi sarbide-puntua

EDPB: Datuak Babesteko Europako Lantaldea

CNIL: Frantziako Informatika eta Askatasunerako Batzordea

DPD: Datuak babesteko ordezkaria

EEE: Europako Esparru Ekonomikoa

DBGEB: Datu-babesaren gaineko eraginaren ebaluazioa

SEN: Segurtasun Eskema Nazionalea

29LT: 29. artikuluko Lantaldea

AI: Adimen artifiziala

IEEE: “Institute of Electrical and Electronics Engineers”

IOT: “Internet of things”. Gauzen Internet

DPBEDBLO: 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa eta Eskubide Digitalak Bermatzekoa

MAC: “Media Access Control”

DBEO: Datuak Babesteko Erregelamendu Orokorra

AAE: Adimen Artifizialaren Erregelamendua

RSSI: “Received Signal Strength Indicator”. Jasotako seinalearen indarraren adierazlea

WPS: “Wifi Protected Setup”

1. HITZAURREA

Gaur egun, telefono mugikorra edonon agertzen den gailu pertsonala da. Haririk gabeko hainbat teknologiaz hornituta dago, adibidez Wi-Fi eta Bluetooth-ek eta, gainera, sare mugikorren oraingo eta lehengo belaunaldiak onartzen ditu (hau da, 2G–5G).

Komunikazioak burutzeko, teknologia horien guztien oinarria da gailu horien eta sareko beste ekipamendu batzuen –esate baterako, oinarri-estazioen eta sarbide-puntuen– arteko mezu-elkartrukea.

Bereziki, Wi-Fi teknologia, komunikazio-protokolo estandarizatuetan (IEEE802.11 protokolo-familia) oinarritutako haririk gabeko teknologia da. Bere ezaugarria da «sarbide-puntu» batera (AP, ingelesezko sigletan) konektatzen diren terminal multzo bat (terminal mugikorrak edo ez). Entitate baten mendearen administratutako AP multzo batek Wi-Fi sare bat osatzen du.

Wi-Fi komunikazioa «trama» izeneko mezuen bitartez egiten da. Mezu horiek byte multzoak dira, multzo horren barruan goiburuko bat doa, zeinak era berean barnean hartzen baitu jatorriko gailuaren identifikatzailea, MAC izeneko (Media Access Control). Trama horietako batzuk ez daude zifratuta eta gailuak aldiro emititzen ditu, baita Wi-Fi sare batera konektatuta ez dagoenean ere.

Gaur egun erabilgarri dauden teknologia batzuk erabiliz, trama horiek biltzen dituzten datuak atzitu, analizatu eta prozesatu ahal dira eta, hala, trama horien jatorrizko terminala singularizatu ahal izateko identifikatzaile bat zehaztu ahal da. Interneteko munduan gertatzen den bezala, teknologien multzo horri «device fingerprinting» deitzen zaio, edo besterik gabe «fingerprinting», hau da, gailuaren hatz-marka edo aztarna. Testu honetan izen bat zein bestea erabiliko da.

Aztarna digital hori zehazteko erabiltzen den informazioa gailuak igortzen du, gailua eramaten duenak ezer egin gabe eta ezer jakin gabe; hori dela eta, teknologia horiek kontu bereziaz hartu behar dira pribatutasunaren eta datuen babesaren ikuspegitik.

Aztarna hori eratuz, biltegiratzuz eta analizatzuz posible da gailu bat zona jakin batean dagoen detektatzea eta gailu horren mugimendu-ereduak identifikatzea eta, beraz, gailua eramaten duen pertsonaren mugimendu-ereduak ere identifikatzea.

Gailuen eta APen artean elkartrukutzen diren Wi-Fi mezuen datuak jasotzen dituzten teknologia horiei «Wi-Fi tracking» deitzen zaie”.

Teknologia horiek eskura jartzen dituzten bi analitika-motak presentziarena eta lokalizazioarena dira. Presentzia-analitikaren ardatza da zona batean terminalik dagoen eta bertan zenbat geratu diren aztertzea; lokalizazio-analitikaren helburua, aldiz, terminalak aztergai den zonan egindako ibilbidea trazatzea da.

Analitika horien erabilera nagusien artean aipa daitezke leku baten edukierak kalkulatzeko, pertsonen fluxuak aztertzea, asistentziaren estatistikak kalkulatzeko edo pertsonak leku batean edo ilara batean egoten diren denborak neurtzea, ohikoenak diren ibilbideak zehaztea edo bisiten errepikapenaren tasa kalkulatzeko.



Modu praktikoan aplikatu ahal dira **merkataritza-zentroetan, museoetan, interes handiko lekuetan, lantokietan, gune publikoetan, garraio publikoan, gertakari publiko handietan, larrialdiak gertatzen diren lekuetan eta abar.**

Kontuan hartuta teknologia horiek sortzen duten azterna digitalaren ezaugarriak, bilte-giratzeko denbora eta prozesatzeko modua, baliteke Wi-Fi trackingaren erabilerak datu pertsonalen tratamendua ekartzea. Eta, batzuetan, baliteke terminalaren erabiltzaileak tratamendu horren berririk ez izatea edo, areago, tratamenduaren arduradunak berak horren berririk ez izatea, datu pertsonalik ez dagoela uste izanez gero; hain zuzen ere, uste hori okerra izan daiteke, **3. apartatuan** azaltzen denez.

Mota horretako teknologia hedatzea pentsatzerakoan, **lehenik eta behin pertsonen pribatutasuna izan behar da gogoan.**

Pertsona guztiek aske eta inor «zelatan» dutela sentitu gabe mugitzeko eskubidea izan behar dute, eta hirugarren batek, administrazio publikoa edo enpresa pribatua izan, ez du zertan behatu edo erregistratu zer egiten ari diren.

Inork ere ez luke pertsona baten aztarnari jarraitu behar zein denda, osasun-zentro edo gurtza-leku bisitatzen dituen jakiteko. Datu horiek pertsona horren eremu pribatuan geratu behar dute pertsona horrek bere izaerari euts diezaion, informazio hori erregistratu edo erabiltzeko ote den pentsatzeagatik kikildu gabe¹.

Orientabide hauetan, teknologia hori erabiltzeak dakartzan ondorioak aztertzen dira, arlo teknikoan zein arlo juridikoan, teknologia horrekin lotutako arrisku nagusiak identifikatzen dira eta gomendio zehatz batzuk ematen dira teknologia hori arduraz erabiltzeko eta datuen babesari buruzko araudiarekin bateragarri egiteko.

¹ https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en

2. ESPARRU TEKNOLOGIKOAREN AZALPENA

A. MAC HELBIDE FINKOEN ETA AUSAZKOEN ERABILERA

MAC helbidea gailu ororen identifikatzaile bat da, orokorrean finkoa eta unibokoa izaten dena, eta sare bateko elementu batzuen eta besteen arteko komunikazioetan erabiltzen da.

Gailu bat Wi-Fi sare baten APra konektatzen denean, bere mezu guztiak hasten direnean gailuaren beraren MAC helbidea identifikatzen da. Hala, APak tramen edukia irakur dezake eta, MAC helbidearen bitartez, terminala modu unibokoan identifikatu ere bai.

Wi-Fi sareen estaldura, sare hori osatzen duten APeK ematen dute. AP horiek guneko publiko irekietan edo eraikin edo instalazioen barrualdean egon daitezke.

Dena dela, Wi-Fi sareen estaldura-zonan sartzen diren terminal mugikor gehienak ez dira sare horietara konektatzen. Hala eta guztiz ere, Wi-Fi gaitasuna duten gailuek, aldiro, beren estaldura-eremuan erabilgarri egon daitezkeen sareen bilaketa egiten dute. Bilaketa hori egiteko, aldiro «Probe Request» izeneko tramak igortzen dituzte. Trama horiek Wi-Fi sare batera konektatuta egon gabe transmititzen ditu gailuak eta, batzuetan, Wi-Fi funtzioa aktibatuta eduki gabe ere. Halako tramen helburu nagusia da zonan egon daitezkeen Wi-Fi sareei «galdeketa-eskaria» egitea. APak mezu horiei erantzuteko prestatuta daude: terminalari informazioa bidaltzen diote, erabiltzaileak hala erabakiz gero AP horretara konektatzeko.

Duela urte batzuk, Probe Request trametan, informazio tekniko jakin batez gain, terminalaren MAC helbide finkoa eta bakarra bidaltzen zen. Beraz, denboran zehar trama horiek batuz eta lokalizazio-teknologiak erabiliz, posible zen identifikatzaile horren bidez terminala modu unibokoan identifikatzea eta terminal horrek Wi-Fi sarearen estaldura-zonan egindako ibilbidea erregistratzea, sare horretara konektatuta egon gabe.

Egoera horren ondorioz pribatutasunaren arloan arazoak gertatzen zirenez, terminal mugikorraren fabrikatzaileek orokorrean ausazko MAC helbidea erabiltzen hasi ziren. Prozesu hori Apple iOS8 bertsioan hasi zen, eta geroago Androidek egin zuen, baita zabaldu ere.

Ausazko MAC helbidea Probe Request trametan erabiltzen den helbide «birtuala» da. Modu horretan, terminal batetik bidaltzen diren mezu batzuek eta besteek ez dute identifikatzaile bera (MAC helbide finkoa) konpartitzen eta, beraz, ez dago jakiterik zein den Probe Request tramen analisiaren bidez atzitutako gailuaren benetako MAC helbidea. Bestalde, ausazko MAC helbidea sarritan aldatzen denez eta tramak eurak ausaz bidaltzen direnez, ausazko MAC helbideak zuzenean erabilia ere ez da erraza gailua identifikatzea.

Neurri horrek pertsonen pribatutasuna indartu zuen; hala ere, honako faktore hauek kontuan hartu behar dira:

- Ausazko MAC helbideak sortzeko prozedura ez dago estandarizatuta; horregatik, terminal batzuek eta besteek portaera desberdinak izaten dituzte.
- Terminala AP jakin batera konektatutakoan, erabilitako MAC helbidea konexio osoan konstantea da, nahiz eta ausaz sortu; beraz, gailuak konexio osoan egindako ekintza guztiak –adibidez, bere lokalizazio absolutua eta erlatiboa– beste terminal batzuen lokalizazioarekin lotu ahal da.

- Kalkuluen arabera, gutxienez gailuen % 5ek eta gehienez % 10ek ez du ausazko MAC helbiderik erabiltzen.
- Teknika ugari daude kasuen ehuneko handi batean gailu mugikorrek modu unibokoan identifikatu ahal izateko, nahiz eta ausazko MAC helbide aldakor bat erabili. Halakoak dira Wi-Fi trackingean gaur egun erabiltzen diren teknikak. Teknika horien oinarria da Probe Request trametan bildutako askotariko informazioa (edo trama horietatik ateratakoa), ausazko MAC helbideen eredu estatistikoen atzipenarekin konbinatuta. Trama batzuen eta besteen informazioa gailu bakar batekin lotzeko teknikarik aurreratuenetan ikasketa automatikoko algoritmoak eta Big Data oinarritutako datu-analitika erabiltzen dituzte.

B. WI-FI TRACKINGEAN ERABILTZEN DIREN DATUAK

Wi-Fi trackingeko tekniken helburua da Wi-Fi inguruneetan terminalak modu bakar eta zehatzean identifikatzea eta haien aztarnari jarraitzea. Metodo horretan askotariko parametroak eta askotariko ezaugarri fisikoak erabiltzen dira, bai gailuei bai transmisioaren baldintzei dagoenikenez, gailu bakoitzarentzat aztarna digital indibidualizatua sortzeko.

Ereduak ezagutzeko teknikak eta, orokorrean, datu-analitika erabiltzen dira. Horrekin batera, gailuen fabrikatzaileek pribatutasuna babesteko erabilitako tekniken bilakaera etengabea da; horrek guztiak etengabeko aldaketako egoera batera eraman gaitu. Emaizta gisa, duela urte batzuk erabat efikazak diren teknika batzuek, gaur, erabilgarritasuna galdu dute. Jarraian, gaur egun erabiltzen diren metodo nagusiak azalduko dira.

«Probe Request» trama Wi-Fi estandarrak erabiltzen duen kudeaketa-trama mota bat da. Gailua (adibidez, smartphone bat) Wi-Fi AP batera konektatuta ez dagoenean erabiltzen da. Gailuak, Wi-Fian erabilgarri dagoen kanal

bakoitzean, ikerketa bat egiten du eta bere estaldura-eremuan erabilgarri dauden APez «galde egiten du», horietara konektatu ahal izateko.

AP jakin batek Probe Request trama jasotzen duenean, «Probe Response» izeneko trama batekin erantzuten du. Trama horrekin, gailuak jakiten du AP hori badagoela, eta haren ezaugarrien berri izaten du, konektatu nahi badu ere.

Halako tramak gailu guztiek automatikoki emititzen dituzte Wi-Fi komunikazioetan, erabiltzailearen kontrolik gabe eta zifratu gabe; hala, edozein APk jaso eta deskodetu dezake trama hori, eta hala egin dezake AP batek ez ezik Wi-Fi kanalean entzuten ari den kostu txikiko edozein gailuk ere. Halako tramen emisioaren ezaugarri zehatzak inguruabar askoren mende daude, adibidez gailuaren fabrikatzailearen, modeloaren eta sistema eragilearen beraren mende. Kasu batzuetan, baliteke trama horietan bidaltzen diren datuek (adibidez, SSIDak) zuzenean pertsonari buruzko informazioa ematea.²

Wi-Fi trackingeko teknologiek Probe Request tramen ezaugarri horiek baliatzen dituzte (gailu guztiek bidaltzea, zifratu gabe eta datu-kopuru handiarekin bidaltzea) azterna digital bakarra sortzeko; hala, gailua identifikatzeko aukera ematen da.

Probe Request trametan zuzenean bidalitako informazioaz gain, informazioa jasotzea dago tramen konbinazioetatik abiatutako zeharkako neurketen bidez edo teknika heuristikoen bidez.

Praktikan, gailua identifikatzeko zereginen lagun dezakeen edozein neurri edo datu erabiltzea dago. Teknologia horiek erabili ahal dituzten neurri fisikoen edo datu gehigarrien artean honako hauek daude: jasotako seinalearen indarra (RSSI, ingelesezko sigletan: Received Signal Strength Indicator), zeina gailuaren gutxi gorabeherako kokalekua zehazteko erabil daitekeen; Probe Request tramen bidalketen arteko denbora-tartea, tramen sekuentzia-zenbakiaren nahiz ausazko MAC helbideen banaketa estatistikoa edo gailuen erlojuek berez dauzkaten desbideratzeak. Laburbilduta, horrekin guztiarekin, azkenean azterna digitala sor daiteke.

Azaldu diren datuak (eta beste batzuk, fabrikatzaileak erabiltzen duen soluzioaren arabera) biltzearen eta aztertzearen helburua gailu bakoitza identifikatu ahal izateko azterna digital bat sortzea da.

Wi-Fi sare batean terminal mugikorren azterna digitala sortzeko prozesuak, orokorrean, honako fase hauek dauzka:

➤ **Probe Request tramak atzitzea:** Behatzen ari den Wi-Fi sareko APetan jasotzen diren Probe Request tramak masiboki biltzen dira. Tramen informazioaz gain, transmisioaren baldintza fisikoei buruzko datuak ere jaso daitezke, adibidez RSSI eta beste

batzuk. Atzipen hori burutzeko, ekipamendu espezializatua erabil daiteke, edo gaitasun gehigarri horiek dauzkan Wi-Fi sareko ekipamendu arrunta ere bai.

➤ **Informazioa erauzi eta bidaltzea:** Atzitutako tramen informazio garrantzitsua erauzten da, baita transmisioaren ezaugarri fisikoen informazio garrantzitsua ere. Informazio hori zerbitzari zentralizatu batera bidaltzen da, prozesatzeko eta analizatzeko. Bidalitako datu espezifikoak era batekoak edo bestekoak izango dira, sarean inplementatuta dagoen Wi-Fi tracking ereduaren arabera.

➤ **Ereduak analizatzea eta azterna digitala sortzea:** Informazioa erauzi ondoren, bildutako datuen ereduaren analisia egiten da. Helburua da bildutako datuen ezaugarri espezifikoak konbinatzea, gailu bat beste batetik bereizi ahal izateko. Analisi hori era batekoa edo bestekoa izango da erabiltako sistema-aren arabera. Funtsezkoa da monitorizatutako zonan terminal mugikorrak modu unibokoan identifikatzea lortzeko, eta dagoeneko ohikoa da teknika aurreratuak erabiltzea, adibidez ikasketa automatikoa (machine learning) eta modelatze probabilistikoa.

Ikasketa automatikoko algoritmoak gai dira ereduak ikasteko eta tramen parametroen artean korrelazioak ezartzeko eta hala, trama bat aurretiaz identifikatutako gailu batena edo gailu berri batena izateko zein probabilitate dagoen ezartzeko. Ezaugarri horiek eredu probabilistikoa batean konbinatuz, gailu bakoitzarentzat azterna digital bakarra sortzen da. Eredu horien barruan informazio-iturri diferenteak sartu ahal dira, esate baterako lehenago identifikatutako gailuen datu historikoak, informazio kontestuala eta portaera-ereduak, azterna digital sendoagoak eta zehatzagoak sortzeko.

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

Laburbilduta, gailua atributu anitzen konbinazio baten bidez adierazten duen aztarna digital bat (fingerprint) sortzen da; hala, gailu hori singularizatzeko bidea ematen da.

➤ **Konparatzea eta ezagutzea:** Hainbat gailuren aztarnak taxutu direnean, konparatu eta ezagutu egiten dira, gailuak identifikatzeko eta sistemak gailu horiek lehenago detektatu dituen ala ez zehazteko.

C. GAILUAK IDENTIFIKATZEA

Gailuaren aztarna digitala sortu ostean, gailu hori identifikatuta geratzen da. Aztarna digitalaren bidez gailu horren jarraipena egiten bada, posible izango da honelako informazio hau lortzea:

➤ **APren estaldura-zonako presentzia:**

Aztarna digitalari esker zehaztu ahal da gailua AP dagoen zonan agertzen den ala ez. Hori erabilgarria da bereziki leku batean dauden gailuen kopurua zenbateko edo hainbat egunetan bildu diren bisitarien kopuruari buruzko datuak lortzeko.

➤ **Egonaldiaren gutxi gorabeherako denbora:**

Aztarna digitalak, gailua dagoen ala ez adierazteaz gain, terminal mugikorra estaldura-zonan egoten den denbora gutxi gorabehera kalkulatzeko bidea ematen du. Datu hori erabilgarria izan daiteke erabiltzaileen ohiturak ulertzeko eta bisiten iraupenari eta maiztasunari buruzko informazioa lortzeko.

➤ **Ibilbidearen jarraipena:**

Gailuaren aztarna digitalak aukera ematen du denboran izan duen ibilbidearen jarraipena egiteko. Horrek esan nahi du gailuak Wi-Fi sarearen estaldura-zonan egin dituen mugimenduak erregistratzen direla eta bisitatu dituen lekuei buruzko informazioa lortzen dela.

Terminal mugikor baten ibilbidean jarraipenaren zehaztasuna hobetzeko, sareko hiru APtatik edo gehiagotatik jasotako seinalearen potentzian oinarritutako triangelukatzeteknikak erabil daitezke.

AP horien informazioa konbinatuz, gailua zehaztasun handiz kokatzea lortzen da. Azterlan batzuen arabera, 0.5 metrora arteko zehaztasuna ere lortzen da. Zehaztasun horri esker, gailuaren ibilbidearen jarraipena eta analisisa errazago egiten da eta, hala, erabiltzaileen joan-etorrien ereduen xehetasun handiagoa lortzen da.

Nabarmendu behar da terminal baten aztarna digitala zenbait egunez gordez gero jarraipen intentsoagoa eta zabalagoa egin ahalko litzatekeela. Hala, gailu baten aztarna digitala denboran zehar gorde eta ezagutuz, posible izango litzateke portaera-ereduak identifikatzea eta pertsonen bizimoduko alderdi intimo batzuk deskubritzea, esate baterako zaletasunak edo errutinak, eguneroko jarduerak, maiz bisitatzen diren lekuak.

3. TARTEAN DAUDEN DATU PERTSONALAK ETA TRATAMENDUAK

Wi-Fi tracking teknologiak eboluzio nabarmena izan du, eta gailuen askotariko ezaugarriak biltzeko eta analizatzeko bidea ematen du

Gaitasun horri esker MAC helbidearen bidezko identifikazioa egitea lor daiteke baina, hori ez ezik, aztarna digital bakarrak ere sor daitezke. Ezaugarri anitzen konbinazioaren bitartez sortutako aztarna horiei esker, gailuak modu etengabearen identifikatu ahal dira, anonimizazioarako neurriak (MAC helbideak ausazkotzea, kasu) egon arren.

Era berean, telefono mugikorra eguneroko eta ezin bananduzko elementua izanik, erabiltzailearekiko zuzeneko lotura da eta, hala, zuzeneko nahiz zeharkako identifikagarritasuna sortzen da.³ Gailu horiek erabiltzaileen esparru pribatuaren zati dira, eta esparru pribatu hori babestu egin behar da Giza Eskubideak eta Oinarriko Askatasunak Babesteko Hitzarmenaren⁴ eta datu pertsonalen babesari buruzko araudia- ren arabera. Horregatik, teknologiaren testu- ingurua halakoa izanik, funtsezkoa da aztertzea datu pertsonalen tratamendurik dagoen ala ez eta, hala izanez gero, tratamendu horien edukia aztertzea.

A. “DATU PERTSONALA” TERMINOAREN NORAINOKOA

«Datu pertsonala» kontzeptua, DBEOn ezarrita dagoen moduan, oso hedadura handikoa da. DBEOren 4.1 artikulua dio zer den datu pertsonala: «Pertsona fisiko identifikatu edo identifikagarri bati buruzko informazio guztia».

Definizio horretan «informazio guztia» esaten da. Hala, nabarmendu egiten da legegilearen asmoa izan dela kontzeptu horri esanahi oso zabala ematea, ez mugatzea datu konfidentzial- etara edo intimitateari buruzkoetara, baizik eta mota guztietako informazioa barnean hartzea, informazio objektiboa nahiz subjektiboa, baldin eta dena delako pertsonari «buruzkoa» bada.

Horretarako, nahikoa izango da informazioak lotura izatea pertsona zehatz batekin, infor-

mazio horren edukia, helburua edo ondorioak direla eta.⁵

Gainera, zehazten da pertsona bat identifikagarria dela bere identitatea zuzenean edo zeharka zehaztu ahal denean. Hortaz, datu pertsona- lei buruzko informazio bat kalifikatzeko, ez da beharrezkoa informazio horrek berez interesdu- na identifikatzeko bidea ematea.⁶

Are gehiago, pertsona fisiko bat identifikagarria da datuen edukitzaileak pertsona hori bereizte- ko eta modu diferente batean tratatzeko gai den unetik, baita datu horiek hala egiteko nahikoak ez direnean ere.

³ 13/2011 irizpena, gailu mugikor adimentsuen geolokalizazio-zerbitzuei buruzkoa. 4.2.2 apartatua (29LT, WP185).

⁴ 2002/58/EE Zuzentaraua, 2002ko uztailaren 12koa, Komunikazio Elektronikoen Sektoreko Datu Pertsonalak Tratatzeari eta Inti- mitatea Babesteari buruzkoa. 24. kontuan hartuzkoa.

⁵ EBJAren Epaia, 2017ko abenduaren 20koa, C 434/16 kasua. 34. eta 35. paragrafoak.

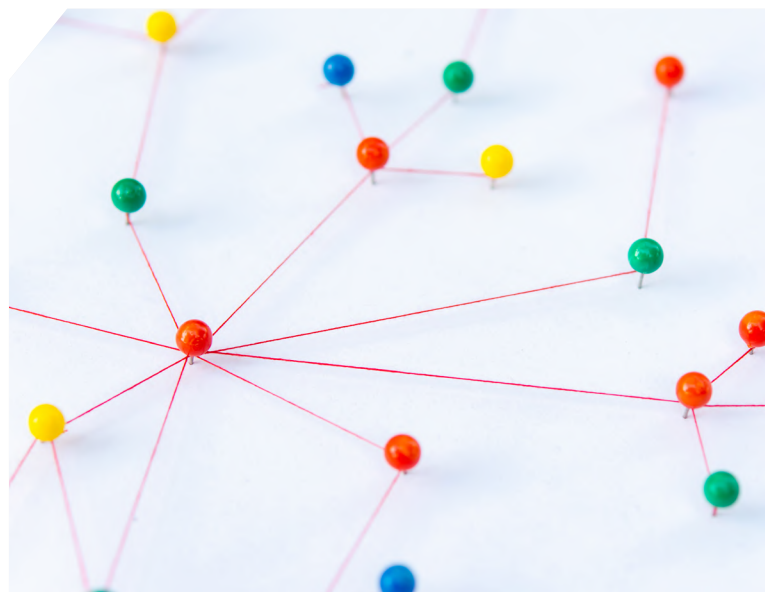
⁶ EBJAren Epaia, 2016ko urriaren 19koa, C-582/14.a kasua.

Horren haritik, baliagarria da pertsona bat argi identifikatzeko modua ematen duten datu identifikatzaile bakarrak eta «kuasi-identifikatzaileak» bereiztea. Azken horiek, lehenengo begiratuan, ez dute modua ematen pertsona jakin bat identifikatzeko. Hala ere, elkarren artean edo beste batzuekin konbinatuz gero, pertsona bat identifikatzeko modua ematen dute «konbinazio bakarren-gatik». «Mosaiko efektua» izeneko fenomeno horrek agerian jartzen du datu «kuasi-identifikatzaileen» metaketaren bidez pertsona bat identifikatzea dagoela; bada,⁷ prozesu hori datu masiboen analisirako teknologiek erraztu egiten dute. Arazorik gabe esan daiteke datu pertsonalak daudela nahiz eta interesdunaren zuzeneko edo esanbidezko identifikaziorik ez egon.

Adibidea:

Mugikor baten informazioa eskura dago (egonaldiaren data, ordua eta denbora jakinak dira), A saltokian birritan egon da, B saltokian 3 aldiz, C hotelean 16 egunez egon da eta turista gisa dago kalifikatuta, 15 egunetik gorako eta hilabete batetik beherako egonaldia izanik. Informazio hori, berez, oso xehatua da, eta informazio gehigarri gutxi izanik ere terminal mugikor hori daraman pertsona identifikatu ahalko litzateke.

Pertsona gisa «identifikagarri» izateko gaitasunari buruz, DBEOren 26. kontuan hartuzkoak dioenez, kontuan hartu behar dira «tratamenduaren arduradunak edo beste edozeinek pertsona fisiko hori zuzenean edo zeharka identifikatzeko erabil ditzakeen baliabide guztiak».



Hau da, interesduna identifikatu ahal izateko informazioa ez du zertan pertsona bakar batek eduki, edo ez da zertan egon tratamendu bakar baten barruan. Aztertu behar da ea arrazoizko posibilitaterik dagoen beste bitarteko gehigarri batzuk erabiliz pertsona hori identifikatzeko.

Bestalde, analisi dinamikoa da; beraz, kontuan izan behar da tratamenduaren unean teknologiaren aurrerapena nolakoa den, eta datuak tratatzeko epealdian teknologia horrek zein garapen izan dezakeen ere.

Azken batean identifikagarritasunarekin zerikusia du zeregin horretarako ahalegin neurrigaberi behar ez izateak eta, arestian esan dugunez, teknologiaren garapen etengabeak identifikagarritasunerako erraztasuna ematen du.

⁷ 5/2014 irizpena, anonimizazio-teknikei buruzkoa (29LT, WP216).

B. WI-FI TRACKINGA ETA “FINGERPRINTING” IZENEOA, DATU PERTSONAL GISA

Definizio horrek DBEOn datu pertsonalen kontzeptuari buruz ezarritako definizioa zabaltzen du, eta bereziki garrantzitsu bilakatzen da Wi-Fi trackingaren testuinguruan. Teknologia horrek Wi-Fi funtzioa daukaten gailu guztiak ukitzen ditu, sare jakin batera konektatuta egon behar izan gabe eta, batzuetan, funtzio hori aktibatuta izan gabe ere bai. Gailu horietako batzuk dira mugikorrak, tabletak, ordenagailu eramangarriak, ordenagailu finkoak, routerrak, inprimagailuak, etxetresna elektrikoak, jostailuak, gorputzeko gailuak («wearable» izenekoak, barnean direla taupada-markagailuak, oxigeno-sistema eramangarriak, diabetikoentzako gailuak, inplante neuronalak eta abar) eta automobilak ere bai⁸.

DBEOren 30. kontuan hartuzkoan ohartarazten da pertsonak identifikatzea dagoela gailuen aztarnen bidez:

“Pertsona fisikoak onlineko identifikatzaileekin lotu daitezke, zeinak ematen baitituzte haien gailuek,[...]Horiek utzitako aztarnak, batez ere identifikatzaile bakarrekin eta zerbitzariak jasotako beste datu batzuekin konbinatzen direnean, erabil daitezke pertsona fisikoen profilak sortzeko eta beraiek identifikatzeko”.

Aurreko horren arabera, halako prozesuetan erabilitako Wi-Fi seinaleek transmititutako datuak datu pertsonaltzat jo daitezke, pertsona identifikagarriekin lotuta daudelako eta pertsona horiek zuzenean edo zeharka identifikatzeko erabil daitezkeelako. Bereziki, Wi-Fi trackingaren testuinguruan «fingerprinting» izeneko edo aztarna digitala datu pertsonalen tratamendua izan daiteke, DBEOn ezarrita dagoenaren arabera.

Honela definitzen da «fingerprinting» kontzeptua. «Informazio-elementuen multzo bat, zeinak gailu bat edo aplikazio-instantzia bat identifikatzen baitu». Beraz, kontzeptu horren barruan sartzen dira erabiltzaile bat edo gailu bat denboran zehar indibidualizatzeko, lotzeko edo inferitzeko erabil daitekeen informazio guztiak⁹.

Horren barruan egon daitezkeen datuak honako hauetatik deribatu ahal dira:

- erabiltzaile/gailu baten agente baten ezarpenetik;
- edo sareko komunikaziorako protokoloen erabilerarengatik agerian geratzen diren datuak.

Beraz, «fingerprintingak» gaitasuna ematen du gailu bat beste batetik bereizteko, eta denbora batean erabiltzaile baten kokalekuaren edo portaeraren jarraipena egiteko erabil ahalko litzateke, nahiz eta pertsona bat zuzenean edo espresuki ez identifikatu.

⁸ Kontrol-agintaritzak batzuek, adibidez Unabhängige Landeszentrum für Datenschutz izenekoak (Schlewig Holstein, Alemania) kezkatuta ageri dira, teknologia horiek aplikatu ahal direlako Wi-Fi sarbide-puntuak daukaten automobiletan eta, hala, pertsonen jarraipena egitea dagoelako. Location Services can Systematically Track Vehicles with WiFi Access Points at Large Scale.

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

C. WI-FI TRACKINGA ETA LOKALIZAZIOAREN ETA IBILBIDEEN DATUAK

Gailu baten posizioa zein den jakitea dago, bai gutxi gorabehera «presentziagatik» (sentsorea-
rekiko hurbiltasuna), bai modu zehatzagoan,
triangelukatze bidez. Gailu baten identifikazioa
edo indibidualizazioa mantenduz eta denboran
gailu horren posizioa zehaztuz, gailua sent-
soreen estaldura-zonaren barruan dagoen
denboran ibilbide bat ezartzea dago.

Lokalizazio-datu horiek adierazten duten datu
pertsonalen tipologia arrisku handikoa da pert-

sonen pribatutasunerako, pertsona fisikoen
eskubide eta askatasunetarako arriskuen apar-
tatuaz azaltzen denez.

Wi-Fi tracking bidez bildutako datuen lekuzko
eta denborazko esparrua mantentzen denean,
datu horiek berez edo beste batzuekin konbi-
natuta nahikoak izan daitezke pertsonak iden-
tifikatu ahal izateko, eta tratamenduaren ardu-
radunak halako datuak datu pertsonaltzat jo
beharko lituzke.

D. DATU PERTSONALEN TRATAMENDUA

Wi-Fi tracking teknologia, berez, ez da datu pert-
sonalen tratamendua baina, kasuan kasu, trata-
mendu baten barruan egon liteke. Hain zuzen
ere, tratamendu bat nola garatu edo helburu
bat nola lortu erabakitzean, arduradunak Wi-Fi
Trackinga ez diren soluzio batzuk hauta ditzake
edo, bestela, datu pertsonalen tratamendurik
ekartzen ez duten aukerak.

Wi-Fi tracking teknologia, batik bat, bi motatako
analitiketarik eratorritako datu pertsonalen
tratamenduetan ager daiteke: presentzia-
analitikatik eta lokalizazio-analitikatik eratori-
takoez ari gara. Presentzia-analitikaren ardatza
da zona batean terminalik dagoen eta bertan
zenbat denboran geratzen diren aztertzea;
lokalizazio-analitikaren helburua, aldiz, termi-
nalak aztergai den zona jakin batean –denbora
zehaztugabea bada ere– egindako ibilbidea
trazatzea da.

Askotan, analitika horren helburua da portaera
kolektiboak detektatzea eta aztertzea; hala ere,
ez da ahaztu behar abiapuntua datu indibidua-
len detekzioa dela.

Argibide gisa, hona hemen tratamendu batzuk,
zeinetan Wi-Fi trackingeko teknologiak erabili
baitira¹⁰:

- Gailua geolokalizatzeko zerbitzua, erabilt-
zailea bera ados egon zein ez.
- Pertsonen jarraipena egitea, lantokietan.
- Larrialdi-zerbitzuak, pertsonen eman beha-
rreko premiazko laguntzarako bilaketa edo
lokalizazioa eginez. Mekanismo horren bitar-
tez, larrialdi-deiei arreta emateko zentroek
automatikoki jaso dezakete dei-egilearen
kokalekuari buruzko informazioa, eta Wi-Fi
lokalizazioko datuek informazio hori joriago
egin dezakete.
- Pertsonen zaintza. Wi-Fi trackinga erabiltzen
da, barruti edo leku batzuetan pertsonarik
al dagoen detektatzeko. Zona horietarako
sarbidearen kontrol indibiduala.

¹⁰ Zerrenda hori hona ekartzeak ez du esan nahi datuak babesteko kontrol-agintaritzak alde edo aurka agertzen direnik.

- Pertsonen arteko lotura, zehazteko ea pertsona bi edo gehiago leku berean egon al diren, elkarrengana hurbildu al diren, puntu berean gelditu al diren eta abar.
- Pertsonen fluxuaren analisia, instalazio pribatueta (adibidez, lantokietan edo saltokietan), gune fisikoaren diseinua edo langile-zuzkidura hobetzeko.
- Leku publikoetan jendetzak kudeatzea: jende ugari izaten den eremuetan, adibidez aireportuetan, garraio publikoan, estadioetan, bide publikoetan eta abar, gehieneko edukierak kontrolatzeko, pertsonen edo ibilgailuen trafikoa modu efizientean kudeatzeko, ibilbideak optimizatzeko edo informazioa denbora errealean emateko eta, hala, segurtasuna eta erosotasuna hobetzeko. Erabilera horiek «smart cities» izenekoan proiektuetan maiz aurkitzen ditugu.
- Marketina eta zuzendutako publizitatea, erabiltzaileak kokaleku espezifiko batera sartu edo hurbiltzen direnean edo portaeraren edo mugimendu-ereduen arabera euren gailuetara sustapenak edo iragarkiak bidaltzeko.
- Erabiltzaile-profilak sortzea mugimendu-ereduen eta portaeraren arabera.

Laburbilduta, ezinbestekoa da konturatzea erabilera horietako askotan datu pertsonalak biltzen direla eta datu pertsonal horien tratamendua egiten dela eta, beraz, DBEOren eta DPBEDBLOn ezarritako printzipioen, pertsona fisikoen eskubideen eta tratamenduaren arduradunentzako eginbeharren mende egon behar dutela.

4. DATU PERTSONALEN TRATAMENDUAREN OINARRI LEGITIMATZAILEAK

Datu pertsonalen tratamendu oro DBEOren 5. artikuluan ezarritako printzipioetara egokitu behar zaio eta DBEOren 5. artikuluan zerrendatutako zilegitasun-baldintzetako bat bete behar du. Bada, hori Wi-Fi trackingari aplikatzea dago tratamenduaren arduradunak tratamendu hori posible egiten duen teknologia bat hautatzen duenean.

Tratamenduak fidela eta gardena izan behar du. Pertsona bati argi utzi behar zaie Wi-Fi tracking bidez zein datu tratatzen ari diren eta nola tratatzen ari diren. Informazio hori eskuratzen erraza eta ulerterraza izango da, nahiz eta Wi-Fi trackingak tratamenduaren arduradunari zailtasun tekniko edo praktiko bat edo beste ekarri ahal dion printzipio horiek betetzeko.

Wi-Fi tracking bidezko tratamenduaren xedeak esplizituak izan behar dira, hau da, argi eta garbi adierazi behar dira, legítimoak izan behar dira eta interesdunei komunikatu behar zaizkie, beranduenik datuok biltzen diren unean. Horrez gain, helburu zehatz baterako Wi-Fi tracking bidez biltzen diren datuak ezingo dira geroago beste helburu baterako erabili, helburu hori bateraezina bada. Horretarako, funtsezkoa da ziurtatzea geroagoko tratamendua ez dela desbideratzen tratamendurako lehengo ezarritako helburuetatik, kontuan hartuta interesdunei helburu horien berri eman behar zaiela. Adibidez, merkataritzako lokal baten barruan pertsonen joan-etorrien datu-tratamendua egiten bada produktu jakin batzuen kokaleku fisikoa hobetzeko, arduradunaren interes legítimo batean oinarrituta, seguruenik zaila

izango da tratamenduaren bateragarritasuna justifikatzea, baldin eta tratamendu hori egiteak esan nahi badu pertsona horiek produktu horien merkataritza-eskaintzei buruzko jakinarazpenak jasoko dituztela.

Era berean, funtsezkoa da tratatutako datu pertsonalak egokiak eta beharrezkoak izatea eta ezinbestekoaren neurrira mugatuak izatea, haien tratamenduaren helburuen arabera. Gogora ekarri behar da tratamenduaren helburua ez dela Wi-Fi trackinga egitea; hortaz, azken helburua lortu ahal bada hain intrusi-boa ez den teknika baten bitartez, ez litzateke beteko datuak minimizatzeko printzipioa. Wi-Fi trackinga ez den teknika bat posible ez bada, tratatutako datuak minimizatzeko printzipioa betetzeko, tratatutako datuak euren kategorietan, maiztasunean, ale-egituran eta abarrean ezinbestekoaren neurrira mugatuta egon beharko dira; halaber, datu horien kontserbazio-epea ahalik eta laburrena izango da eta benetan ezabatu edo anonimizatu beharko dira, ahal denean prozesu automatizatuak erabiliz.

Zehaztasunaren printzipioa ere bete beharko da, bereziki teknika probabilistikoak erabiltzen ari badira ekintza batzuk norbanako batekin lotzeko; alde horretatik, zehaztugabeak diren

datuak zuzendu edo ezabatuko dira bidezkoa denean, eta datu pertsonalen segurtasuna eta konfidentzialtasuna bermatuko da; hori, geroago xehetasun handiagoz aztertuko dugu.

Tratamenduaren arduradunaren erantzukizuna da arestian azaldutako printzipioak betetzea eta betetzen dela frogatzeko moduan egotea; gainera, arduradunak ziurtatu behar du tratamenduak DBEOren 6.1 artikuluan ezarritako zilegitasun-baldintzetako bat betetzen dituela. Dena dela, edozein zilegitasun-baldintza aplikatzea erabaki edo aztertu aurretik, gogora ekarri behar da tratamenduaren xedea beste bide batzuen bidez lortu ezin denean baino ez direla tratatu behar datu pertsonalak.

Tratamendu bakoitzari aplikatu beharreko oinarri legitimatzailea bete dadin, tratamenduaren arduradunak kasu bakoitza xehetasunez aztertu behar du, erantzukizun proaktiboaren printzipioaren arabera (DBEOren 5.2 artikulua); bada, kasua aztertzean tratamenduaren izaera, esparrua, testuingurua eta xedeak kontuan hartu beharko dira. Hala ere, arduradunei orientabide orokor batzuk eman ahal zaizkie gida bat emateko, Wi-Fi tracking teknologien bidez egindako tratamendu bat legitimatuko lukeen baldintzetako bat betetzen den ala ez identifikatzeko.

A. ADOSTASUNA (DBEOREN 6.1.A ARTIKULUA)

Arestian aztertu denaren arabera, Wi-Fi tracking teknika gehienek gailua Wi-Fi sarera konektatuta egon gabe eta gailuaren jabeak ezer jakin gabe operatzen dute. Hau da, ez dago komunikazio-biderik interesdunaren eta tratamendu-arduradunaren artean. Horregatik, ezinezkoa litzateke interesdunari adostasuna eskatzea eta, beraz, hasieran behintzat hori oinarri legitimatzaile gisa baztertu beharko litzateke.

Hala ere, egoera zehatz bat planteatzea dago: egoera horretan, erabiltzaileak Wi-Fi sarerako konexioa borondatez egingo luke eta, konektatu ondoren, informazioa emango litzaioke eta bere

datuak Wi-Fi tracking bidez tratatzeko adostasuna eskatuko litzaioke. Ez da ahaztu behar kasu horietan adostasun hori askea, zalantzarik gabea, zehatza eta arrazoitua izan beharko litzatekeela.

Adibide praktikoa:

bat beste egoera honetan agertuko litzateke: aplikazio baten bitartez erabiltzaileei eskatzea beren geolokalizazioaren jarraipena egiteko baimena eman dezatela, eskaintza komertzialen truke.¹¹

Kasu horietan, sistema batzuk ezarri beharko lirateke gardentasunaren printzipioa betetzen dela bermatzeko. Hala, informazioa laburra, eskuratzen erraza eta ulerterraza izan dadila eta hizkera argi eta erraza era argia erabil dadila, eta, hala badagokio, ikusgai egon dadila ahalbidetuko da; hala aztertzen da [9. apartatuan](#).

Kasu jakin batzuetan, esate baterako lan-esparruan, hezkuntzan edo sektore publikoan, aztertu beharko da ea botere-desoreka argia gertatu ahal den tratamenduaren arduradunaren eta interesdunaren arteko harremanean; horregatik, adostasunaren askatasuna ebaluatzean kontu handiz ibiltzea beharrezkoa izango da.

B. KONTRATU BAT GAUZATZEA (DBEOREN 6.1.B ARTIKULUA)

Kontratu bat gauzatzea edo kontratuaren aurreko neurriak aplikatzea datuen tratamendurako legitimazioa izan ahalko litzateke baldin eta lotuta balego Wi-Fi trackingaren testuinguruan zerbitzu espezifiko bat ematearekin.

Kasu horretan funtsezkoa izango da frogatu ahal izatea tratamendua beharrezkoa dela kontratu-eginbeharrak betetzeko, eta hori ez da ohikoa izango, salbu eta erabiltzaileak berak eskatutako geolokalizazio-zerbitzuen kasu jakin batzuetan.

C. LEGE-EGINBEHAR BAT BETETZEA (DBEOREN 6.1.C ARTIKULUA)

Oinarri hori aplikatu ahalko da baldin eta lege-eginbehar bat badago, zeinaren arabera arduradunak helburu bat bete behar baitu Wi-Fi tracking teknikak derrigor erabiliz. Horrez gain, DPBEBLOren arabera, eginbehar hori Europar Batasuneko zuzenbidearen arau batean edo

lege mailako batean ezarrita egon beharko litzateke. Oinarri juridiko edo legegintzako neurri horrek argia eta zehatza izan behar du, eta haren aplikazioa haren hartzaileek aurreikusteko modukoa, EBJAren jurisprudentziarekin bat etorritz.

D. BIZI-INTERESAK BABESTEA (DBEOREN 6.1.D ARTIKULUA)

Zilegitasun-baldintza hori aplikatu ahal da baldin eta tratamendua beharrezkoa bada pertsona baten bizia edo osotasun fisikoa babesteko. Hasieran, Wi-Fi trackingaren testuinguruan, arrazoi horiengatik nekez justifikatuko litzateke datu pertsonalen tratamendua.

Hala ere, ezin da guztiz baztertu teknologia hori aplikatzea bizi-interesak benetan arriskuan dauden egoeretan, adibidez larrialdietan, sorospen-lanetan edo desagertutako pertsonen bilaketa eta erreskatean eta, dena dela, kasu zehatza modu zorrotzean aztertu beharko litzateke, aplikatzea justifikatzeko¹².

¹¹ 01/2017 irizpena, pribatutasunari eta komunikazio elektronikoei buruzko erregelamenduaren proposamenari buruzkoa (2002/58/EE). 17. kontuan hartuzkoa (29LT,WP247).

¹² 39/2019 txostena, AEPDren Bulego Juridikoarena.

E. INTERES PUBLIKOA EDO BOTERE PUBLIKOAK EGIKARITZEA (DBEOREN 6.1.E ARTIKULUA)

Oinarri legitimatzaile hori ezarriz gero halako ezaugarriak dauzkan datu-tratamendu baterako, kontu handiz aztertu beharko dira datuen babeserako araudian ezartzen diren betekizunak. Hala, tratamenduaren arduradunak identifikatu beharko du lege-mailako zein arauk ematen dion eskumen zehatz bat, eta nola frogatu ahal duen Wi-Fi tracking bidezko tratamendu hori beharrezkoa eta neurrizkoa dela interes publikoaren izenean edo botere publikoen izenean burutu beharreko eginkizun bat betetzeko. Oinarri juridiko edo legegintzako neurri horrek argia eta zehatza izan behar du, eta haren aplikazioa haren hartzaileek aurreikusteko modukoa, EBJAren jurisprudentziarekin bat etorritik.

Ohartarazi behar da lege-manu orokorregiak ez direla erabili behar legitimazio-oinarri gisa. Horri buruz berariazko legeriarik ez dagoenez, gomendagarria litzateke legegintzako neurriak garatzea, arestian esan dugunaren arabera halako tratamenduak aurreikusteko eta arautzeko.

Kontuan izan behar da Administrazioaren jardura batik bat gune publikoetan egingo dela eta pertsonak aukera legitimoa dutela mugimendu-askatasunaz gozatzeko, monitorizatuta egon gabe. Tratamenduaren arduradunak bermeak kontu handiz ezartzen ez baditu, egoera horietan baliteke pertsonen pribatutasunean bete-betean eskua sartzea.¹³

F. INTERES LEGITIMOAK (DBEOREN 6.1.F ARTIKULUA)

Sektore pribatuan, interes legitimoa baliozko zilegitasun-baldintzatzat jo daiteke baldin eta beharrezkoa bada interes horiek betetzeko eta interesdunen eskubide eta askatasunak nagusitzen ez badira, kontuan hartuta interesdun horien arrazoizko iguripenak..

Nolanahi ere, kontu handiz ebaluatu behar da ea tratamendua egitea dagoen, haztapen-froga egin, interesdun batek arrazoiz aurreikus badezake ere horretarako tratamendua gerta daitekeela, datu pertsonalak bildu diren garaian eta testuinguruan¹⁴.

Arduradunak frogatu behar du «haztapen» froga egin dela. 95/46/EE -WP 217 Zuzentarauaren 29. artikulua bidez sortutako lantaldearen apirilaren 9ko 6/2014 Irizpenean, tratamenduaren arduradunaren interes legitimoaren kontzeptuari buruzkoan, zenbait gidalerro eta orientabide txertatzen dira interes legitimoa dagoen aztertzeko eta, gainera, halako tratamenduek ukitzen dituzten pertsonen eskubideak errespetatzeko eta bermatzeko beharrezkoak diren babes-elementuak ere ezartzen dira.

¹³ Ikus Datuak Babesteko Herbehereetako Agintaritzaren erabakia, gailu mugikorren datu pertsonalak tratatzeari buruzkoa, Enschede hirian gailu mugikor batzuetan Wi-Fi piztu baitzen lege-oinarri egokirik gabe.

¹⁴ DBEOren 47. kontuan hartuzkoa: «Bereziki, interesdunaren interesak eta oinarritzko eskubideak tratamenduaren arduradunaren interesen gainetik egon litezke interesdunak datuen geroagoko tratamendua egiterik arrazoiz espero ez duen egoeretan egiten bada datu pertsonalen tratamendua».

Lehenengo hurbilketa batean, haztatu beharko dira interesdunaren interes eta eskubideak, baita arduradunak egin nahi dituen tratamenduak ere, eta pribatutasuna nola ukitzen den baloratu. Ez da ahaztu behar interes legitimoari dagokionez DBEOren 47. kontuan hartuzkoak honako hau adierazten duela: *«interesdunaren interesak eta oinarritzko eskubideak tratamenduaren arduradunaren interesen gainetik egon litezke interesdunak datuen geroagoko tratamendua egiterik arrazoiz espero ez duen egoeretan egiten bada datu pertsonalen tratamendua»*. Eta, Wi-Fi trackingaren kasuan, hasieran azaldu denez, askotan terminalaren titularrak ez daki datuak atzitzen ari direnik. Laburbilduta, kasu horietan, frogatu ahal izan beharko litzateke arduradunaren interes legitimoa nagusi dela.

Egindako haztapenaren emaitza gisa ukituen interesak eta oinarritzko eskubideak nagusi ez diren kasuetan, eta kasu horietan soilik, interes legitimo batekin justifikatutako datu pertsonalen tratamendua egin ahalko litzateke; gainera, tratatutako datu pertsonalak babesteko, tratamenduan beharrezko babesak, bermeak eta neurri teknikoak eta antolakuntzakoak txertatu beharko lirateke, baita informazioaren segurtasunari buruzkoak ere.

Hau da, oinarri honetan babestutako tratamendua zilegi izango da baldin eta berme egokiak badaude, eta berme horiek behar bezalako intentsitatea badute. Berme horiek, zalantzarik gabe, proposatutako tratamenduaren araberakoak izango dira, hau da, inbasiboa zenbateraino den kontuan hartuta eta, neurri handi batean datu pertsonalen disoziazio itzulezina nola eta noiz egiten den kontuan hartuta.

Orokorrean, datuen anonimizazioa Wi-Fi aktibatuta duen gailuaren bitartez trafikoko datuak sortu zireneko edo jaso zireneko unetik hurbil eginez gero, tratamendua hain intrusiboa ez dela ulertuko da.

Kasurik kasu aztertzea beharrezkoa da; dena dela, eta betiere DBEOren betekizunak erabat errespetatuta, aldeko haztapena egitea errazagoa izango litzateke hainbat neurri hartuz gero, besteak beste bildutako datuak goiz anonimizatzea, informazio agregatua soilik establezimendu baten barrualdeko bisitarien kopuruari eta gehiago edo gutxiago bisitatutako zonei buruz (bero-mapak) jasotzea, datuak kanpoaldean, denon igarobiderako zonetan edo bide publikoan hartzen ez direla bermatzea eta pertsonen jarraipena posible ez dela bermatzea, ezertan ere galarazi gabe datu-babesaren gaineko eraginaren ebaluazioak izan dezakeen emaitza.

Beste egoera batzuetan, aldiz, datu pertsonal gehiago bildu behar badira espazioan (estaldura-eremu handiagoak), denboran (denbora-epe luzeagoak) edo esparruan (mugikortasunari buruzko datuak, bisiten errepikapenari buruzko datuak eta abar), aldeko haztapena nekezagoa izango da, kontuan hartuta Wi-Fi trackingean tratamenduaren aurka egiteko mekanismo efektibo eta praktikoak (opt-out mekanismoak) ezartzea zaila den ala ez.

5. PERTSONA FISIKOEN ESKUBIDE ETA ASKATASUNETARAKO ARRISKUAK

DBEOren 24.1. artikuluan ezartzen denez, datu pertsonalen tratamenduak pertsona fisikoek eskubide eta askatasunetarako dakarren arriskua kudeatu behar da, tratamenduaren nolakotasuna, eremua, testuingurua eta helburuak kontuan hartuta. Beraz, datu pertsonalen tratamendu bat abian jartzea erabakitzen duen erakunde orok arrisku horiek kudeatu behar ditu.

Apartatu honetan azaltzen dira Wi-Fi tracking teknologia erabiliz inplementatzen diren datu pertsonalen tratamenduen ondorioz sor daitezkeen arrisku nagusiak. Ez da arriskuen zerrenda exhaustibo bat, baizik eta kontuan hartu beharreko arrisku nagusien panoramika bat eta, nolanahi ere, tratamenduaren arduradunek, tratamendu bakoitzaren berezitasunetan oinarrituta, zehaztu beharko dute zein arrisku aplikatu behar diren, hala badagokio, eta gida honetan identifikatuta ez dagoen beste arriskuren bat dagoen ala ez zehaztu.

Diferenteak dira pertsona fisikoek eskubide eta askatasunetarako arriskuaren kudeaketa, alde batetik, eta DBEOren eta aplikatzekoa den datuen babeserako araudian ezarritako printzipioak betetzeari buruzko arriskuaren kudeaketa, bestetik. Araudia betetzeari buruzko arriskuen kudeaketa, bestelako helburu batzuk dauzkaten beste arrisku-kudeaketa batzuk bezala (legeen, finantzen, negozioen, iruzurren, proiektuen eta abarren arlokoak), beharrezkoa izan daiteke erakundearen helburu jakin batzuk betetzeko, baina ez die erantzunik ematen DBEOren arabera pertsona fisikoek eskubide eta askatasunetarako arriskuak kudeatzeko eginbeharrei. Hasi nahi den tratamenduak DBEOren printzipioak betetzen ez baditu, adibidez, lege-oinarri egokirik ez izateagatik edo beharrianaren eta proportzionaltasunaren printzipioa ez betetzeagatik, tratamendua ez-zilegia izango litzateke, eta debekatuta egongo litzateke.

Wi-Fi trackinga datu pertsonalen tratamendu baten barruan erabiliko da, eta teknologia hori inplementatzen duen erakundeak DBEOren ezarritako betekizun eta eginbeharrak bete beharko ditu; gainera, besteak beste, tratamenduak oro har ukituko dituen pertsonentzako arriskuak kudeatu beharko ditu.

Adibidea:

Ekitaldi masibo bateko sarbideetan pertsonen segurtasuna babesteko asmoz, baliteke sarbideren batean jende gehiegi pilatzen ari ote den jakin nahi izatea. Jende-pilaketa hori neurtzeko, Wi-Fi tracking teknologia erabiltzea pentsatu ahal da, gutxi gorabeherako zenbaketa bat egiteko eta, horren bidez, tratamenduaren eragiketetako bat –jende-pilaketaren neurketa– inplementatu ahal da. Soilik jende-pilaketa neurtuz ez da lortuko pertsonen segurtasuna babestea; izan ere, tratamenduan beste eragiketa batzuk xedatu behar dira, adibidez une jakin batean jende-pilaketa gutxitzeko erabakia hartzea, jende-pilaketa hori modu efektiboan gutxitzeko gaitasuna izatea eta hori modu efiziente eta ordenatuan gertatzeko ekintzak egitea. Tratamenduaren azken xedeari zentzua ematen dioten eragiketa horiek behar bezala inplementatuta ez badaude, tratamenduarekin bete nahi duen helburuak ez du beteko lege-oinarri bat. Halaber, helburu horiek lortzeko bitartekoak badaude aurretiaz (bideo-zaintza, pertsonen kontagailuak eta abar), tratamendua ez da beharrezkoa izango; aldi berean, baliteke desegokia izatea, neurri horrek arrisku gehigarri bat dakarrelako; izan ere, sistema horrek izan dezakeen helburua lortzeko hain kaltegarriak ez diren beste bitarteko batzuk daude.

Arriskuak kudeatzeko, datu pertsonalen tratamendua multzo gisa kontuan hartu behar da. Wi-Fi tracking teknologia ekar ditzakeen arriskuak modu isolatuan aztertzea ez litzateke zentzuzkoa izango, eta DBEOren arabera ez litzateke nahikoa izango, teknologia hori askotariko konplexutasuna duten tratamenduetan erabili ahal den bitarteko bat delako, beste teknologia batzuen erabilerarekin (hodeia, blockchain, AA, IOT eta abar) konbinatuta.

Adibidez:

ez dakar arrisku berbera Wi-Fi trackinga erabiliz ETE baten denda fisiko individual baten segurtasuna bermatzeko edukiera kontrolatzeko helburua (eta helburu hori soilik) duen tratamendu batek edo, helburu berbera izanik,

kate batek estatu osoan dauzkan denda fisiko guztietan egin nahi den tratamendu batek, edo establezimendu baten barruan bisitatzen diren establezimendu edo atalen arabera pertsonen zuzendutako online publizitatea egitea helburu duen tratamendu batek.

Teknologia hori bera probintzian edo autonomia-erkidegoan erabiltzea turisten ohiko fluxuak zehazteko edo bisita turistikoaren errepikapen-tasak ateratzeko erabilita, arduraduna agintaritzak edo organismo publiko bat dela, arrisku handiagoa egongo da denda fisiko bakar batean edukierak kalkulatzeko erabilita baino. Funtsean teknologia berbera erabili arren, tratamenduak diferenteak dira, eta diferenteak ere arriskuak.

A. PERTSONEN INTIMITATEAREN GAINEKO ERAGINA

Wi-Fi tracking teknologia erabiltzeak esan nahi du inguruabar jakin batuetan posible izango dela pertsonak singularizatzea¹⁵, pertsona horiek kokaleku zehatz batean lokalizatzea eta pertsonen buruzko datuak inferitzea¹⁶ kokalekuaren testuinguruaren arabera.

Adibidea:

Teknika hori lan-eremuan inplementatu ahal da, adibidez eraikin batean. Informazioa lortu ahal da jardueraren zati bati buruz, zeini eta gauregun lan-arloko araudiaren babespean dagoen zati bati buruz: langileak denontzako eremuetan zenbat denbora ematen duten kontrolatzea, norekin aritzen diren hizketan eta zenbat denbora ematen duten horretan, komunetara joatea, langileak lanekoak ez diren orduetan lokalizatzea (liburutegiak, aisialdi-zonak), eta abar.

¹⁵ Singularizazioak esan nahi du datu-multzo batean pertsona bat individualizatu ahal dela erregistro jakin batzuk nabarmenduz. Singularizazioa gertatzean, baliteke pertsona identifikatzeko beharrianik ere ez egotea.

¹⁶ Inferentzia gertatzen da ezaugarri pertsonal baten balioa probabilitate handiarekin deduzitu ahal denean bestelako atributu batzuen balioetatik abiatuta; hain zuzen ere, bestelako atributu horiek izan daitezke kokaleku jakin batzuetan lokalizatzea edo kokaleku horien testuinguruak, eta beste hainbat.

B. BIZILEKUAN EDO GUNE PUBLIKOETAN ESKUA SARTZEA

Wi-Fi tracking teknologiak zail bihurtzen du muga fisiko argiak eta zehatzak ezartzea, jakiteko gailuaren seinalea non jasotzen den eta non ezin den jaso.

Bideokamera batean maskara jakin batzuk ezarri ahal dira, lenteak orientatu, baina halako mugak inplementatzea garestiagoa da irratifrekuentzian oinarritutako sistema batean.

Adibidea:

Baliteke eraikin batean instalatutako Wi-Fi tracking sistema batek horma baten atzean dauden etxeetako edo bizileku pribatuetako gailuen seinalea jasotzea, edo beste entitate batzuetako langileen gailuenak, edo entitate berean egonik tratamenduko datuen subjektu izan beharko ez liratekeen langileen gailuenak edo, areago, bide publikoan dabiltzan pertsonen gailuenak. Modu horretan bidegabe sartzeari ez litzateke arrisku bat izango, baizik eta tratamenduaren legitimazio-printzipioaren urraketa.

C. TRATAMENDUAREN ESKALA ETA ZIRKULATZEKO ASKATASUNAREN MUGAKETA

Sistema teknologiko batzuen eragina aztertzean soilik entitate baten esparrua kontuan hartzeak ikuspegi mugatua ematen du pertsonen pribatasunean bidegabe sartzeari izan daitekeenari buruz.

Gaur egun, teknologiak eskala handian inplementatzen dira, eta masiboki inplementatzen direnean teknologia horien eragina aztertzea beharrezkoa da, multzoan hartuta ondorioa herritarren eskubide eta askatasunak mugatzea izan ahal baita.

Adibidea:

Segurtasun-enpresa batek, ohiko zerbitzuez gain, saltoki txikietarako Wi-Fi trackingeko zerbitzu bat eskaintzen du; bada, hiri bateko merkataritza-lokalen % 30ek merkataritza-lokaletik hurbil dauden oinezkoen identifikatzaileak erregistratzeko modua ematen duen zerbitzu hori inplementatzen du. Hala, edozein herritarrek une jakin batean egiten dituen ibilaldi guztiak erregistratuta eta kontrolatuta egon ahalko lirateke.

D. EZ-EGITEZKO JARRAIPENA: ERLIJIO-ASKATASUNEAN EDO DATU-KATEGORIA BEREZIEKIN TRATAMENDUAN BIDEGABE SARTZEA

Pertsona batek bisitatzen dituen lekuak erregistratuz, bizi-ohiturak eta gustuak edo interesak ondorioztatu ahal dira, pertsona horiek zein tokitan lokalizatu ahal diren eta puntu horiekin lotutako gaietatik abiatuta.

Hala ere, kontuan hartu behar da pertsona batek bisitatzen ez dituen guneek ere informazio asko ematen dutela, edo are gehiago ere, horiei esker datu-kategoria berezietan oinarritutako profila sortzea baitago.

Gainera, horretatik guztitik aparte, tratamenduak agerian jartzen duen informazioa zehatza izan daiteke, edo ez, eta tratamenduaren arduradunak kategoria berezietako baten barruan dagoen informazioa lortzeko egin beharrezkoa egin dezake¹⁷.

Adibidea:

Merkataritza-zentro batean Wi-Fi tracking teknologia duen tratamendu batek pertsona bat singularizatzeko modua ematen du. Pertsona horren jarraipena egin ahalko litzateke, kirol-dendetara, herri jakin bateko janari tradizionaleko jatetxeetara sartze da, geldialdiak egiten ditu erlijio jakin bateko gurtzarako ohiko orduetan, beste erlijio batzuekin lotutako establezimenduetara ez da sartzen eta alkoholaren erakusleihoetan ez da sekula gelditzen; hala, pertsona horren adinaren, sexuaren eta, gutxi gorabehera, jatorriaren profila egin ahalko litzateke.

teke, funts handiago edo txikiagoarekin. Era berean, inguruan erlijio-zentro jakin bat duen merkataritza-zentro batek beren sinesmenen arabera erlijio-gurtza egitera joan ohi diren pertsonen informazioa jaso ahalko luke, baita adingabeena edo gizarte-bazterkeria edo bestelako arrisku-egoeran jasan ditzaketen pertsonena ere.

Funtsean, tratamendu horiek datu-kategoria bereziekin zerikusia duten lekuetan egiten direnean, adibidez ospitale batean, espezialitate mediko bateko klinikan, edo alderdi politiko baten egoitzan, baliteke arduraduna datu-kategoria berezien tratamendu egiten aritzea; horren ondorioz, pertsonen eskubide eta askatasunetarako arriskua handitzen da.

Adibidea:

Pertsona indibidual bati klinika onkologiko batera egindako bisitak esleitu ahal zaizkio, ospitale horretan Wi-Fi tracking teknologia erabiltzen baita; bide horretatik baliteke pertsona horren gaixotasuna ondorioztatzea eta, etorkizunean, pertsona horrek eragozpenak izatea osasun-aseguru bat kontratatzeke.

¹⁷ EBJAren iritziz, (EBJAren C-252/21 Epaia, Meta vs. Lehiaren Defentsarako Alemaniako Bulegoa) kategoria berezietako datuen tratamendua da datu-kategoria berezi batekin edo gehiagorekin zerikusia duten orrialdetara edo app-etara egindako bisitak biltzea, bereziki babestutako daturik berez bildu ez arren. Erabaki hori estrapolatzen badugu Wi-Fi Trackinga erabiliz egiten diren tratamenduetara, tratamendu horiek datu-kategoria bereziekin lotutako barruti edo establezimenduetan eginez gero baliteke arduradunak kategoria berezietako datuak tratatzea.

E. ASKATASUN PERTSONALA ETA AUTOZENTSURA

Pertsona batek jakiten badu jarraipena egingo zaiola zona publikoetan, eraikin batean edo merkataritza-zentro batean, baliteke bere burua zentsuratzea elkarre politiko edo erlijio-elkarre, kultura-zentro edo aisialdi-jarduerak jakin batzuei buruz duen interesa babes-teko. Horrek bere askatasun pertsonala eta mugitzeko askatasuna baldintzatu ahal du, eta autozentsurako egoerak sor daitezke.

Hori gertatu ahal da interesdunari bere datu pertsonalen tratamenduari buruzko informazioa behar bezala ematen zaionean ere bai, bere terminal mugikorretik atzitutako datuei aplikatuko zaien tratamenduari buruz berak dauzkan iguripenak direla eta.

Adibidea:

Pertsona batek jakin-mina dauka merkataritza-zentro batean eskaintzen den produktu, zerbitzu edo aisialdi-jarduera bati buruz, baina horrek agian bere ingurugiro sozialeko agindu etikoren baten aurka egiten du, agian hedabideetan ager daiteke edo beste inguruabar batean gaizki interpretatuko da; orduan, inguruan ibiltze hutsa erregistratu ahal dela jakinez gero, baliteke bere portaera aldatzea.

F. BERRIDENTIFIKAZIOAREN ERAGINA

Datu kolektiboak edo estatistika agregatuak lortzea helburu denean ere, eta nahiz eta pertsonak singularizatu nahi ez izan, datuen jatorria identifikatzaile bakarrei buruzko tratamendueragiketak izango dira. Hain zuzen ere, identifikatzaile horiek izan daitezke gailuen MAC helbideak, gailu horien aztarna digital edo fingerprint bat edo beste batzuk eta, horiei, datu pertsonalen tratamendurik aplikatzekotan, seudonimizazioa edo anonimizazioa aplikatuko zaie¹⁸.

Seudonimizazioa datu pertsonalen tratamendu bat da zeinean, datu pertsonalen multzo batetik abiatuta, informazio seudonimoko multzo berri bat eta pertsonak berridentifikatzeko informazioa sortzen baitira. Edonola ere, DBEO datu-multzo seudonimizatu bati aplikatu ahal zaio.

Adibidea:

Datu-multzo bateko MAC helbideen multzoaren ordezkari MAC helbidearen hash bat jartzea, seudonimizazio-tratamenduko eragiketa bat izan liteke.

Anonimizazioa datu pertsonalen tratamendu bat da zeinean, datu pertsonalen multzo batetik abiatuta, informazio anonimoko multzo berri bat sortzen baita. Beraz, datuak biltzen direnetik anonimizatzen diren arte, fase batean datu pertsonalen tratamendu bat egoten da beti.

Bestalde, datuen anonimizazioko tratamendu orotan, probabilitate bat dago interesdunen berridentifikazioa gertatzeko¹⁹.

¹⁸ Seudonimizazioa eta anonimizazioa tratamendu-eragiketa diferenteak dira eta ez dira elkarren artean nahastu behar. Ikus [Anonimización y seudonimización](#).

¹⁹ [Anonimización \(III\); el riesgo de la reidentificación](#).

Hau da, ustez anonimoa den datu-multzo batek anonimo izateari uzten dio²⁰ interesdunak identifikatuta geratu direlako edo identifikatu ahal direlako. Hori gertatzen denean, pertsonen eskubide eta askatasunetarako arriskua agertzen da, hainbat ondorio gerta daitezkeelako, besteak beste singularizazioa, lotura edo inferentzia.

Anonimizazio-estrategiak aplikatu arren, ebaluatu behar da zein probabilitate dagoen berridentifikazioa eta datu pertsonalen arrakalak gertatzeko, baita interesdunen eskubide eta askatasunek jasan dezaketen eragina ere.

Horretarako, kontuan hartu behar dira kasurik txarrenaren baldintzak, adibidez erakundearen barruko edo kanpoko pertsonen berridentifikazio-saiakerak egitea, eskura dituztelako datu lagungarriak, baita legez kanpoko bitartekoen bidez, agindu judizialen bidez edo informazio-agentzien bidez eskuragarri daudenak ere.

Gainera, kontuan hartu behar da baliabide egokiak eskura daudela eta gogoan izan behar da tratamenduaren unean erabilgarri dagoen teknologia, baita uneko aurrerapen teknologikoak ere.

Adibidea:

Aplikazio batzuetan, Wi-Fi trackingeko informazioa berrerabiltzea ezinezkoa dela bermatu nahi da; horretarako, hash metodo espezifiko bat erabiltzen da, «gatzak» edo jabe bakoitzaren gakoak. Segurtasuna handitzeko metodo bat da, baina kontuan izan behar da «iluntasunean zeharko segurtasuneko» teknika bat egikaritzen ari dela, segurtasuneko

printzipio guztien arabera ez dela izan behar bermeen oinarria, berez ahula baita. Nolanahi ere, har daitezkeen neurri ugarien artean bat izan daiteke, erabat efikaza izateko bermerik egon ez arren.

Probabilitate hori dago, biltzen diren datuen motarengatik, ziurrenik anonimizaziorako mekanismo sendorik ez egoteagatik, tratamenduaren barruan anonimizazioa aplikatzen den une edo fasearengatik, anonimizazioa benetan egotea edo ez egotea gertatu ahal izateagatik edo berridentifikazioa egin ahal izateko teknologia egoteagatik.

Adibidea:

Ustez anonimizatuta dagoen datu-base batean 8 milioitik gora Probe Request trametan bildutako datuak daude. Halako trametan bildutako eremuetako baten bitartez (WPS), posible izan zen eremu hori transmititzen zuten terminalen identifikazio-datuen % 90 baino gehiago berridentifikatzea.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, pp. 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 Wi-Fi Network Discovery Mechanisms*. ACM AsiaCCS, May 2016, Xi'an, China. [ff10.1145/2897845.2897883](https://doi.org/10.1145/2897845.2897883)ff. [ffhal-01282900](https://doi.org/10.1145/2897845.2897883)

G. LOKALIZAZIO-DATUEI LOTUTAKO ARRISKUAK

Azpimarratu behar da oso zaila dela datu-multzoak anonimizatzea multzo horietan pertsona beraren askotariko lokalizazio-datuak edo ibilbideen datuak sartzen direnean,²² berri-identifikatzeko oso errazak direlako.

Adibidea:

New Yorken 173 milioi taxiren ibilbideak argitaratu ziren, eta taxi bakoitzaren lizentzia-zenbakia hash baten bidez anonimizatu zen (ustez). Datuen barruan lizentzia-zenbakia, ibilbidearen hasiera, amaiera, iraupena, denbora, kostua eta eskupekoa biltzen zituen hash bat zegoen. Oso denbora laburrean, taxien lizentzia-zenbakia berri-identifikatu zen eta, Googlen egindako bilaketan bidez, garrantzi publikoa zuten pertsonen irudiak lortu ziren, berri-identifikatutako taxiak hartzen ari zirela.²³

Datuak Babesteko Europako Lantaldeak (EPDB) eta, lehenago, 29. artikuluko Lantaldeak hainbat aldiz ohartarazi dute lokalizazio-datuak kontu bereziaz hartu beharrekoak direla²⁴.

Pertsona baten joan-etorriek informazio argigarria eman dezakete, haren lantokia, bizilekua eta interes-guneak, besteak beste gurtza-lekuak edo haren sexu-orientazioarekin zerikusia duten jarduerak eta, hala, pertsona horren portaeren profil xehatua sor liteke.

Oso jakina da erraza dela lokalizazio-datuak identifikatzea eta, sarritan, puntu espazial gutxi batzuk behar izaten dira pertsona bat biztanlegune baten barruan zehaztasun handiz singularizatzeko, ohiko mugikortasun-ereduak kontuan hartuta. Horrek zera esan nahi du: identifikatzaile bakarrak –adibidez, MAC helbidea– ezabatu arren, gailua singularizatu dagoenez, lokalizazio-datuei esker pertsona bat identifikatu ahal da. Zentzuzkoa denez, lokalizazioaren denbora- eta espazio-esparrua zenbat eta handiagoa izan, hainbat eta errazagoa izango da identifikazioa.

Denboran zehar pertsona baten lokalizazioa biltzen duen datu-eredu bat ezin da osorik anonimizatu, erregistratutako koordenatu geografikoen zehaztasuna murriztu edo ibilbidearen xehetasun espezifikoak ezabatu arren. Gainera, hori osorik agregatuta ez dauden lokalizazio-datuei ere aplikatzen zaie.

Hau da, datuen anonimizazio hutsaz ez da bermatzen pribatutasunaren babesa; izan ere, mugikortasun-ereduak behar bezain bakarrak ez badira, kanpoko informazioa erabili ahalko da datuak berriro norbanako espezifiko batekin lotzeko. Hala, inguruabar espezifiko batzuk gerta daitezke, adibidez ordu jakin batzuetan jende gutxi izaten den eremuak egotea.

Eremu horietan erraza izango litzateke pertsona bat eta bere portaerak identifikatzea edo, areago, adierazle baten atzipena eta bideozaintza-sistema baten irudiak konbinatzea; hala, pertsona hori automatikoki identifikatu ahalko litzateke.

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 Ikus 29LTren 13/2011 eta 01/2017 irizpenak, eta EDPBren 04/2020 gidalerroak.

H. BITARTEKOEN “ACCOUNTABILITY” DELAKOA EZ EGOTEA

Normalean, tratamenduetan mota horretako teknologiak erabiltzen dituzten arduradunek tratamenduaren eragileak hartzen dituzte bitarteko gisa edo, bestela, Wi-Fi trackingeko zerbitzuak –baita beste teknologia batzuekin konbinatuta ere– ematen dituzten hornitzaileak.

Halako proiektuetan, sarritan ikusten da tratamenduaren arduradunak ez dituela behar bezala kontrolatzen tratamendua inplementatzeko erabiltzen ari diren bitartekoak. Arduradun askok, aholkularitza-enpresa independente bat erabili beharrean, soil-soilik komertziala den informazioan oinarritutako erabakiak hartuko dituzte, eta ez dute jakingo zein ondorio dauden eskubide eta askatasunetarako, ezta alboko zein tratamendu egon daitekeen eta tratamenduaren kontrola galdu ahal den.

Tratamendu-arduradunen ingurune teknologikoan, datuak normalean erlazio oso konplexuen artean agoten dira, datuen lagapen ugari egiten dira, eta hodeiko azpiegiturak tartean egon ohi dira, datuak analitika aurreratuen mendean egoten dira eta, egoera askotan, tartean egoten dira ikasketa automatikoko teknikak eta tratamendu-eragileen kontura egindako tratamenduak.

Halako zerbitzuak ziurrenik orokor bilakatu dira, eta eskala-ekonomiak lehiakorrak dira; hori dela eta, etorkizunean, ziurrenik, tratamendu-eragile berak, edo gutxi batzuek, arduradun guztiei edo askori emango dizkiete zerbitzuak. Beraz, eragile horiek jatorri diferente askotako datuak tratatuko dituzte, arduradun baten baino gehiagoren datuak. Hori dela eta, dagoeneko datu pertsonalen arrakalek biderkatze-eragina daukate hainbat entitatei zerbitzua ematen dioten eragileetan, eta gogoan izan behar da eragile horiek datuak euren helburu propioetarako erabili ahal dituz-

tela,²⁵ esate baterako euren zerbitzua hobetzeko, online publizitate pertsonalizatua emateko edo datuak hirugarrenen esku utziz datu horietatik errentagarritasuna eskuratzeko. Hala, pertsonen eskubide eta askatasunetarako arriskua sortzen da, eta hori tratamenduaren arduradunak kudeatu behar du.

Adibidea:

Wi-Fi trackingeko zerbitzuen hornitzaile batek kale, galeria edo merkataritza-zentro bateko establezimendu guztiei doan ematen die euren bezeroei Wi-Fi konektagarritasuneko zerbitzua eskaintzeko aukera. Zerbitzu horren barruan Wi-Fi tracking teknologia erabiltzen da, eta arduradun guztiek modu independentean teknologia hori baliatu ahal dute. Arduradun bakoitzak, bere establezimendura sartzeko diren bezeroen datu estatistikoak eta ustez anonimizatuak jasoko ditu, besterik ez. Hala ere, tratamenduaren eragileak establezimendu guztien datuak jasoko ditu. Eragileak datuak anonimizatu gabe mantendu ahal ditu, edo areago, datuak datu-base propioekin edo hirugarrenen datu-baseekin lotuta eduki, pertsonak singularizatuta edo identifikatuta mantentzeko eta bere negozio-eredua datu pertsonal horien salmentan oinarritzeko; hala eginez gero, baliteke datuak bere eragile-zereginetik bazter erabiltzen ari izatea eta tratamenduaren arduradun bihurtzea, horretarako legitimatuta egon gabe.

Hain zuzen ere, nahiz eta arduradunak asmorik ez izan interesdunak identifikatzeko edo tratamenduak beste helburu batzuetarako

²⁵ Kasu horretan, tratamendu propio horietarako, arduraduna eragile bihurtzen da, eta tratamendu horiek ezin ditu burutu hasierako arduradunari informaziorik eman gabe, ezta arduradunaren oniritziarik jaso edo helburu berriak hasierakoekin bateragarriak izan daitezela lortu ere.

egiteko, baliteke tratamendu-eragileren batek edo hirugarren batek bai, asmoa izatea beste tratamendu batzuk egiteko, datuak helburu propioetarako baliatzeko, datuak²⁶ beste datu-base batzuekin lotzeko eta, hala pertsonak identifikatzea lortzeko eta datuen anonimizazioa

zioa benetan efektiboa izan ez dadila lortzeko. Halako tratamenduak argi eta garbi ez-zilegiak izango dira, baina mota horretako tratamenduen inguruneak berak zail bihurtzen du bermea edo kontrola edukitzea, tratamenduak gertatzen diren ala ez jakiteko.

I. DATU PERTSONALEN ARRAKALEN EGOERAK

Ez arduradunak ez eragileek interesdunak singularizatu edo identifikatu nahi ez izateak, ezta interesdunen profilik sortu nahi ez izateak ere, ez du esan nahi hala gertatu ezin denik²⁷.

Bereziki, arrisku hori gertatzen da erakundearen barruko edo kanpoko elementuetan datu pertsonalen arrakalak gertatzen direnean. Datu pertsonalen edozein tratamendutan gerta daiteke datu pertsonalen arrakala bat, tratamenduan ezarritako neurri tekniko eta antolakuntzakoak gorabehera.

Datu pertsonalen arrakala bat arduradun batek ez ezik arduradun anitzei zerbitzua ematen dieten tratamendu-eragile batek edo azpieragile batek jasaten badu, eragina askoz handiagoa izango da agian, bai datuen bolumenarengatik, bai interesdunen bizitza pertsonalean ukitu ahal diren esparruengatik.

Orokorrean, Wi-Fi tracking erabiltzen duten datu-tratamenduetan oso garrantzitsua da gogoan hartzea konfidentzialtasun-arrakala gertatzeko probabilitatea dagoela, dela informazio-ihes bat gerta daitekeelako, bai datu-multzoari aplikatutako anonimizazioa lehengoratu daitekeelako.

Adibidea:

Segurtasun-enpresa batek, ohiko zerbitzuez gain, saltoki txikietarako Wi-Fi trackingeko zerbitzu bat eskaintzen du; bada, hiri bateko merkataritza-lokalen % 30ek merkataritza-lokaletik hurbil dauden oinezkoen identifikatzaileak erregistratzeko modua ematen duen zerbitzu hori inplementatzen du. Datuak segurtasun-enpresak anonimizatzen ditu; hala, saltoki txikiek soilik anonimizatutako datuak izango dituzte eskura. Segurtasun-enpresak zibergorabehera bat izan du eta informazio-ihesa jasan du: Wi-Fi tracking sistemaren azken 5 urteetako logak barnean dauzkaten datuak erauzi dira, datuak anonimizatuta ez daudeneko tratamendu-fase batekoak, alegia. Datu horiek modua ematen dute pertsonak singularizatzeko, kasuren batean pertsonak identifikatzeko, haien kokalekua lortzeko eta hirian azken 5 urteetan izan dituzten ibilbideen jarraipena egiteko.

Datu pertsonalen arrakalen gaur egungo egoerari erreparatuta, ageri-agerikoa da datu-multzoen gaineko mehatxuak benetakoak izango direla berandu baino lehen, eta ezezagu-

²⁶ Lotugarritasunaz ari gara datuen subjektu bakoitzari buruz edo datuen subjektu-talde bakoitzari buruz gutxienez bi erregistro lotzea posible denean (datu-base berean edo bi datu-base diferentetan).

²⁷ Ikus Datuak Babesteko Herbehereetako Agintaritzaren erabakia, gailu mugikorren datu pertsonalak tratatzeari buruzkoa, Enschede hirian gailu mugikor batzuetan Wi-Fi piztu baitzen lege-oinarri egokirik gabe. «Praktikan baliabide horiek ez dituzte erabiltzen hiriaren erdialdean pertsonak identifikatzeko, baina horrek ez du esan nahi arrazoizkoa ez denik hala egin ahal dutela uste izatea».

na den gauza bakarra arrakalak izan dezakeen dimentsioa dela. Kasu horietan, arazoa ez da soilik arduradun batetik filtratu diren datuen multzoa era batekoa edo bestekoa dela, baizik eta datuen multzo hori aurreko arrakaletako datuekin lotu ahal dela, ez soilik Wi-Fi trackinga erabiltzen duten tratamenduen barruan, baizik eta Interneteko bestelako zerbitzuen barruan ere bai.

Adibidea:

Una Wi-Fi trackingeko datu-base bat dark webera filtratu ahal da. Aintzat hartu behar da dark webean beste datu-base batzuk aurkitu ahal direla eta horien bidez norbanako batek bi ingurune diferentetan izan dituen ekintzak lotu ahal direla, edo areago, lehenago agian datu-base bat filtratu

dela eta horri esker Wi-Fi datuak beste datu pertsonalekin lotu ahal direla.

Beraz, Wi-Fi tracking teknologia duen tratamendu bat abian jarri aurretik, bereziki teknologia-hornitzaileak eta eragileak hautatzerakoan, ezinbestekoa da aurreikustea zer atera daitekeen gaizki eta datu pertsonalen arrakala batek zein ondorio izan ditzakeen pertsona fisikoen eskubide eta askatasunetarako. Hori eginda, tratamendua implementatu aurretik, pribatutasunaren babesak diseinatuko dira arrakala bat gertatzeak izan dezakeen eragina minimizatze-ko, eta arrakalaren aurka egiteko mekanismoak ezarriko dira, hala ukituen eskubide eta askatasunetarako arriskuak minimizatu ahal baitira²⁸.

J. NAZIOARTEKO TRANSFERENTZIAK ETA NAZIOARTEKO ARAU-TESTUINGURUA

Tratamendu-eragileen azpiegitura teknologikoak erabiltzen direnez, eta askotariko teknologiak konbinatuta erabiltzen direnez, askotan tratamenduaren azpieragileekin eta hodeiko azpiegitura teknologikoekin, baliteke tratamenduaren ondorioz nazioarteko datu-transferentziak egitea Europako Esparru Ekonomikotik (EEE) kanpoko herrietara.

Nazioarteko datu-transferentziak egiten diren egoeretan, arduradunak hainbat egoera baloratu beharko du, adibidez zuzenbide-estatuaren porrotak, larrialdi nazionalak edo nazioartekoak edo nazioarteko harreman eta akordioen krisiak.

Adibidea:

Demagun Wi-Fi trackinga barnean hartzen duen tratamendu batek aukera ematen duela pertsona bat alderdi politiko baten edo ideologia jakin bati lotutako sindikatu baten egoitzarekin lotzeko, eta tratamendu horretan hodeiko teknologiak erabiltzen dituzten tratamendu-eragileak baliatzen direla. Tratamendu horretan baliteke nazioarteko datu-transferentziak egitea hirugarren herrietara. Pertsona hori identifikatu ahal izateak ondorioak ekar ditzake pertsonentzat, baita lege-arloko ondorioak ere (adibidez, bisa ukatzea edo zigor-arloko karguak leporatzea).

²⁸ DBEOren 83. kontuan hartuzkoa: ...Datu-segurtasunarekiko arriskua ebaluatzean, kontuan hartu behar dira datu pertsonalen tratamendutik eratorritako arriskuak, hala nola bidalitako, kontserbatutako edo bestela tratatutako datu pertsonalak suntsitu, galdu edo aldatzea, nahi gabe zein legez kanpo, edo baimenik gabe komunikatzea edo horietarako sarbidea ematea, bereziki kalte-galera fisiko, material zein immaterialak eragin ditzaketenen kasuan.

K. ARRISKUAREN KUDEAKETARI BURUZKO ONDORIOA

Arduradunak tratamenduan interesdunentzat egon daitezkeen eskubide eta askatasunetarako arrisku guztiak kontuan hartu eta kudeatu behar ditu.

Mehatxu bakoitza aztertu behar du, mehatxu bakoitzak oinarritzko eskubideak nola ukitu ahal dituen, kasu zehatz bakoitza kontuan hartuta bere testuinguru, esparru, izaera eta xedeen arabera, eta tratamendua osorik analizatu

behar du, ez soilik tratamendu-eragiketaren bat edo beste.

Sarritan, arriskuak elkarren artean lotuta egoten dira, eta mehatxu batzuk edo arrisku-faktore batzuk gauzatzeak esan nahi du beste batzuk ere gauzatu ahal direla. Arrisku horiek minimizatzeke neurri tekniko eta antolakuntzakoak geroago jorratuko dira, apartatu espezifiko batean.

6. DATU-BABESAREN GAINEKO ERAGINAREN EBALUAZIOA NAHITAEZ EGIN BEHARRA

DBEOn datu-babesaren gaineko eraginaren ebaluazioarekin (DBGEB) lotutako eginbeharrak ezartzen ditu 35. eta 36. artikuluetan. Ez du behartzen datu pertsonalen tratamendu orotan DBGEB egitera, baina bai arrisku handia ekartzeko probabilitatea duten tratamenduetan. Tratamenduak arrisku handia ekar dezakeelako presuntzio handi samarra badago, ezinbestekoa izango da DBGEB egitea.

DBGEB tratamendua ebaluatzeko prozesu bat da, eta tratamenduaren bizitza-ziklo osoan egiten da; etengabe berrikusi behar da, gutxienez tratamendu-eragiketek dakarten arriskuan aldaketa bat gertatzen denean. Inola ere ez da hartu behar agiri-arloko formalismo huts gisa.

Orokorrean, DBGEB baten ezaugarriak honako hauek dira:

- Galdagarria da eskubide eta askatasunetarako arrisku handia egon daitekeenean.
- Arduradunaren eginbehar espezifiko bat da.
- Tratamenduaren egokitasunari, beharriaren eta proportzionaltasunari buruzko ebaluazio bat gainditu behar da, tratamenduaren xedeen arabera.
- Ebaluazioaren emaitza izan behar da neurriak eta bermeak aplikatuz hondar-arriskua neurri onargarri bateraino murriztea lortu dela.
- Tratamendu-jarduerak hasi aurretik egin behar da.
- DBOk nahitaez aholkua eman behar du, hura izendatuta egon behar denean edo arduradunak nahi izanda izendatuta dagoenean.

- DBGEBren emaitza kontuan izan behar da tratamendua datuen babesaren ikuspuntutik bideragarria den ala ez ebaluatzeko. DBGEBren emaitza loteslea da tratamenduaren arduradunarentzat eta, hondar-arriskuaren neurriaren arabera, eskumena duen datu-babeserako kontrol-agintaritzari aurretiaz kontsulta egin beharko zaio edo, areago, tratamendua egiten den ala ez erabaki beharko da.

Wi-Fi tracking teknologia duten tratamenduetarako, beste edozein tratamendutarako bezala, arriskuen ebaluazioa eta DBGEB egiteko beharizanaren ebaluazioa aztertzean tratamendua osotasun gisa hartu behar da kontuan, hau da, tratamenduaren asmoa, izaera, esparrua edo norainokoa eta testuingurua hartu behar dira kontuan.

DBEOren 35.3 artikuluaaren arabera, Wi-Fi tracking teknologia duten tratamenduetan eta, zehazki, tratamendu horretan²⁹ sarbide publikoa duen zonalde baten behaketa sistematikoa egin behar bada eskala handian, DBGEB egitea nahitaezkoa izango da. Nahiz eta tratamenduaren arduradunak eskala handiko behaketa sistematiko hori egiteko asmorik ez izan, DBGEB nahitaezkoa izango da. Tratamenduak berekin dakarren arriskua gogoan izanik, arrisku handiko tratamendua izango da eta, horrenbestez, DBEOn tratamendu horietarako ezartzen diren betekizunak aplikatuko zaizkio. Era berean, interesdunentzat beren eskubideak egikaritzea zaila izatea astungarritzat jo beharko da, Wi-Fi trackingaren barruan egiten diren eragiketa askoren izaera bera dela eta.³⁰

Tratamenduak datuen babesaren gaineko eraginaren ebaluazioa behar duten tratamenduen AEPDren zerrendako (35.4 artikulua) irizpide bat edo gehiago betetzen baditu, orduan ere beharrezkoa izango da DBGEB egitea.

Hona hemen zerrenda horretako irizpide garrantzitsu batzuk, Wi-Fi trackinga erabiltzen duten tratamenduetarako:

- Modu sistematikoan eta zorrotzean interesduna behatu, monitorizatu, gainbegiratu, geolokalizatu edo kontrolatzeko balio duten tratamenduak, honakoak barne: sareen edo aplikazioen bidez egindako edo sarbide publikoko gunetan egindako datu eta metadatu bilketak; bai eta informazioaren gizartearen zerbitzuen erabiltzaileak identifikatzeko balio duten berariazko identifikatzaileak prozesatzen dituzten tratamenduak ere, hau da, web zerbitzuak, TB interaktiboa, aplikazio mugikorak eta abar.
- DBEOren 9.1 artikuluko datu kategoria bereziak erabiltzen dituzten tratamenduak, DBEOren 10. artikuluko kondena edo arau-hauste penalei buruzko datuak edo finantza egoera eta ondare-kaudimena zehazteko balio duten datuak edo datu kategoria bereziekin lotuta dagoen pertsonen buruzko informazioa ondorioztatzen duten datuak.
- Datuak eskala handian erabiltzen dituzten tratamenduak. Tratamendu bat eskala handikoa den ala ez jakiteko, kontuan hartuko da 29. artikuluko Lan Taldearen «*Datuak babesteko ordezkari (DBO) buruzko jarraibideak*» izenburuko WP243 Gida.
- Hainbat datu basetako erregistroak lotu, konbinatu edo uztartzen dituzten tratamenduak, baldin eta helburuak beste batzuk badira edo arduradunak beste batzuk badira.
- Teknologia berriak erabiltzen dituzten edo finkatutako teknologien erabilera berritzaileak egiten dituzten tratamenduak, teknologien beste eskala bateko erabilera barne, hau da, beste helburu baterako edo beste batzuekin uztartuta erabiltzea, eta hori egitean datuak biltzeko eta erabiltzeko modu berriak sortzen badira eta arriskuan jartzen badituzte pertsonen eskubideak eta askatasunak.

²⁹ WP243 gidan «eskala handia» terminoa azaltzen da, ez soilik interesdun-kopuruaren termino absolutuetan.

³⁰ Datuak Babesteko Erregelamendu Orokorraren 91. kontuan hartuzkoa.

³¹ Guía Gestión del riesgo y evaluación de impacto en tratamientos de datos personales – Apartado XIII. Evaluación de la necesidad y proporcionalidad del tratamiento.

Irizpide horiek tratamenduaren arduradunarentzat berarentzat nahiz arduradunak erabiltzen dituen tratamendu-eragilearentzat edo eragile-entzat hartu behar dira kontuan.

Gida honetan Wi-Fi tracking teknologia erabiltzearekin batera doazen arrisku-faktore eta -elementuak azaldu dira. Bada, orokorrean, Wi-Fi tracking teknologia erabiltzen duten datu pertsonalen tratamenduetan DBGEB nahitaezkoa izateko baldintzak beteko dira. Arduradunak DBGEB egitea nahitaezkoa den ala ez argi ez daukanean ere, datuak babesteko kontrol-

agintaritzen gomendioa da ebaluazio hori egitea, gida honetan azaldu diren arrisku-faktoreak aintzat hartuta; hala eta guztiz ere, horrek ez du esan nahi lotutako arriskuak aztertu eta eguneratu behar ez direnik. Azkenik, zera ekarri behar da gogora: bidezkoa denean, arduradunak interesdunen edo haien ordezkarien iritzia eskatu beharko du egin nahi den tratamenduari buruz. Administrazio publikoen esparruan, bereziki, egokia litzateke partaidetzarako prozedura bat egitea, ukitutako herritarrek gai honi buruz zer iritzi duten azaldu ahal izan dezaten, DBEOren 6.1 artikuluko c) eta e) letren arabera egindako jarduketak direnean.

7. TRATAMENDUAREN BEHARRIZANAREN ETA PROPORTZIONALTASUNAREN EBALUAZIOA

DBGEB baten prozesuan lehenengo neurria da tratamenduaren beharrianaren eta proportzionaltasunaren ebaluazio bat egitea, lortu nahi den helburuarekin alderatuta eta hiru irizpide aintzat hartua: egokitasun-judizioa, beharrian-judizioa eta proportzionaltasun-judizioa, zentzu hertsian³¹.

Ebaluazio hori amaitutakoan, tratamendua egingo den ala ez erabaki behar da; edo, bestela, tratamendua aldatzea erabaki, arestian azaldu den judizio hirukoitzaren analisia gainditzeko duen arte. Arduradunak pribatutasunean gutxien sartzen den eta pertsonentzat arrisku gutxien dakarren aukera hartu beharko du.

Adibidea:

Arduradun batek lokal baten gehieneko edukiera kontrolatu nahi du, pertsonen segurtasuna bermatzeko. Tratamendua inplementatzean erabaki ahal du

lokalean sartzen edo bertatik irteten diren pertsonak zenbatzeko oinarritzko elementuak erabiltzea, giza baliabideak erabiltzea edo bestelakoak: beste edozein sentore, bolumetrikoak, CO2 neurtzekoak, zelula fotoelektrikoak, presio-sentoreak, analisiren bat barnean hartzen duen bideozaintza, edo Wi-Fi tracking teknologia. Kasu guztietan helburu berbera lortu nahi den arren, aukeretako batzuk –hasieran behintzat– ez dakarte datu pertsonalen tratamendurik; aldiz, baliteke beste batzuek datu pertsonalen tratamenduak ekartzea eta pertsonen pribatutasunean bidegabe sartzea neurri handiago edo txikiagoan; areago, esan genezake pertsona fisikoen eskubide eta askatasunetarako arrisku handia dakarten tratamenduak ekar ditzaketela, eta zehaztu beharko litzateke eskuragarri dauden aukeren beharrian eta proportzionaltasuna.

³¹ [Guía Gestión del riesgo y evaluación de impacto en tratamientos de datos personales – Apartado XIII. Evaluación de la necesidad y proporcionalidad del tratamiento.](#)

A. TRATAMENDUAREN EGOKITASUNAREN EBALUAZIO OBJEKTIBOA

Wi-Fi tracking eta guzti inplementatu ahal den tratamenduaren betekizunak zehazterakoan, zehaztu behar da ea teknologia hori erabiliz lortu ahal den datuaren kalitatea egokia al den tratamenduaren ekintzak egiteko, kontuan hartuta ez dela hutsezina.

motaren, aurretiaz egindako jardueraren eta beste hainbaten mende egon daiteke. Hortaz, sistema hori ez litzateke aproposa izango.

Adibidea:

Demagun tratamendu bat egin nahi dela areto jakin batean 30 lagun baino gehiago ez egotearen lege-eginbehar bat aplikatzeko. Wi-Fi trackinga erabiliz, egoera hau gerta daiteke: baliteke pertsona batzuek telefonoa aldean ez eramatea, telefonorik ez daukaten adingabeak izatea, telefonoa desaktibatuta edo bateriarik gabe eramatea zenbatsuak ez izateko, baliteke beste batzuek mugikor bi edo gehiago eramatea (pertsonala, profesionala eta abar) eta hori guztia adinaren, zerbitzu-

Adibidea:

Demagun tratamendu bat egin nahi dela erabakiak hartzeko bezeroarentzako arreta-zerbitzu batean azalera handitzeari edo langile gehiago hartzeari buruz. Horretarako, estatistika bat lortu nahi da lokal jakin baten edo itxaron-gela jakin baten okupazioari buruz. Lehenengoz, zehaztu behar da erabaki bat hartzeko modua ematen duen datuaren konfiantza-maila, adibidez %90+-%2. Horri esker zehaztu ahalko da zein metodo edo teknologia izango diren egokiak.

B. DATU PERTSONALEN TRATAMENDUA EGITEKO BEHARRIZANAREN EBALUAZIO OBJEKTIBOA

Tratamenduaren helburuaren arabera, baliteke singularizazio maila handi samarra beharrezkoa izatea tratamenduaren helburuak betetzeko, baina beste batzuetan singularizazioa ez da beharrezkoa izango lortu nahi den helbururako.

Adibidea:

Demagun Wi-Fi trackinga erabiltzen duen tratamendu bat egin nahi dela hainbat gela daukan denda fisiko batean, gela bakoitzaren edukiera zehazteko eta, hala, gehieneko edukiera ez gainditzeko. Horretarako hasieran ez litzateke beharrezkoa izango pertsonak inola ere singularizatzea. Nahikoa izango litzateke une bakoitzean bertan

guztira dauden gailuen kopurua zehaztea. Baliteke alferrikakoa ere izatea edozein identifikatzaile tratatzea, baizik eta sortzen diren Probe Request tramak zenbatzea.

Hala ere, museo batean antzeko tratamendu bat eginez gero egonaldien arteko ohiko ibilbideak lortzeko, beharrezkoa izango da norbanakoak singularizatzea gutxienez denbora-epe jakin batzuetan eta datuak anonimizatu aurretik; hala zehaztu ahalko da, adibidez, norbanako bakoitzaren egonaldien bisiten hurrenkera edo jende gehien ibiltzen den eremuen bero-mapa bat.

Nolanahi ere, jadanik egiten ari diren tratamenduetan erabiltzaileen pribatutasunean intrusio handiagoa dakarren eguneraketa teknologiko bat egitea erabakitzen bada, planteatu beharko da zein beharrizan ari den betetzen –lehenago betetzen ez zena–, arrazoizko efektibotasun-tarte batzuen barruan:

Adibidea:

Presentzia-kontrola eguneratu nahi da Wi-Fi trackinga erabiliz. Presentzia-kontrola aspalditik egiten den tratamendua da, eta arrazoizko efikazia-maila dauka. Pentsatu behar da ea intrusi-

boagoa den teknologia batera aldatzea beharrezkoa ote den; hain zuzen ere, baliteke beste teknologia horrek gainera mugak izatea efikazian, eta iruzurra gertatzeko orain arte ezezagunak diren posibilitateak egotea.

Halaber, tratamenduaren bizitza-zikloan egiaztatu beharko da beharrizan horiek oraindik ere lortzen direla eta beharrezkoak izaten jarraitzen dutela tratamenduaren helburu objektiboak lortzeko; horretarako, iraungipenak ezarri beharko dira tratamendu baten egikaritzapean, baldin eta beharrizan horiek betetzen ez baditu.

8. NEURRI TEKNIKO ETA ANTOLAKUNTZAKO NEURRI EGOKIAK

Tratamenduaren arrisku-faktoreak identifikatu eta arrisku-maila zehaztu ondoren, arrazoizko arrisku-maila hori balio onargarri batera arte murriztu behar da kontrol eta neurri tekniko eta antolakuntzako bidez, datuak babesteko politiken, diseinutik abiatutako datu-babes eta pribatutasunaren bidez eta segurtasun-neurrien bidez. Neurri horien helburua izan behar da arrisku-faktore espezifiko baten edo batzuen eragina edo faktore horiek gauzatzeko probabilitatea murriztea. Neurriak eta bermeak helburu espezifikorik gabe metatzeak arazo gehiago sor ditzake.

Hala ere, interesdunen eskubide eta askatasunetarako arriskuen kudeaketa ez da nahastu behar datuen babesari buruzko araudian ezarritako gainerako manu eta printzipioak modu zorrotzean betetzearekin. DBEOren izaerak berak askatasuna ematen dio arduradunari eta eragileari, DBEOren printzipioak eta gainerako

eginbeharrak inplementatzeko moduari dagokionez, baina horrek ez du esan nahi arduradunak edo eragileak zein manu beteko diren eta zentzuk ez diren beteko aukeratu ahal duenik. Diseinutik abiatutako datu-babeserako aplikatu beharreko neurrietako bat anonimizazioa da, baina hori ez da aukera posible bakarra; gainera, arduradunak ez dio uko egin behar beste neurri gehigarri batzuk aplikatzeari. Halako neurriak dira, besteak beste, pribatutasun diferentziala³², «compute-to-data» eta beste batzuk.

AEPDk, 2019/017 txosten juridikoan, Wi-Fi tracking teknologia erabiltzen duten tratamendu-arduradunentzako eginbeharrak azaltzen ditu.

Datuen babesari buruzko araudian ezarritako eginbeharrak direla ulertu behar da, eta horien artean neurri tekniko eta antolakuntzako batzuk daude.

³² [Anonimización y seudonimización \(II\): la privacidad diferencial](#)

Hona hemen eginbehar horietako batzuk:

- Datuen anonimizazio³³ goiztiarra bermatuko duten neurriak hartu behar dira.
- Wi-Fi trackinga egiten den esparrua baloratu behar da. Adibidez, eremu pribatua kon-tuan hartuko da merkataritza-harremanik dagoen, bezeroak ala balizko bezeroak diren eta, nolana ere, bide publikoan erabiltzea saihestuko da.
- Zein gunetan egiten den, gunek horiek mugatu eta zedarritu beharko dira; hala, saihestuko da mugimenduak oso eremu zabaletan kontrolatzea, eta pertsonen pri-batutasunean gehiegitan esku sartzea ere, adibidez, komunetan.
- Datu-kategoria bereziak agerian jar ditzake-tan gunetan –adibidez, osasunari buruzko produktuak saltzen dituzten gunetan– uki-tuen adostasunik gabe ezingo dira erabili.
- Lortzen diren geolokalizazio-datuak ezingo dira gurutzatu beste iturri batzuetatik lortutako datuekin (adibidez, kreditu-txartelarekin egindako ordainketak edo bideozaintza-sistemek atzitutako irudiak), pertsonak identifikatzeko modua ematen baitute.
- Datuak minimizatzeko irizpideari errepara-tuta, nahiz eta datu-bilketa jarraitua izan behar, posizioa biltegiratzea eta gerora posi-zio horren tratamendua egiteko eragiketarako interesgarritzat jotzen diren eremuetara mugatu behar dira eta, ahal dela, interes-dunen mugimenduen bilketa xehatua eta jarraitua saihestu behar da.
- Interesdun batengandik arduradun baten baino gehiagoren lokaletan jasotako datuak ez dira gurutzatu behar. Arduradunak lokal bat baino gehiago badauka, orduan ere iden-tifikatzaile diferenteak bildu beharko dira.
- Gailu mugikor batek kokaleku berean hain-bat aldiz bisita eginez gero gailu horri ez zaio esleitu behar bisita guztietan identifikatzaile berbera.
- Arduradunaren Wi-Firako sarbidearen bal-dintza gisa ez da jarriko interesdunak ados-tasuna ematea datuen Wi-Fi tracking bidezko tratamendua egiteari.
- Tratamenduaren lege-oinarria denean ardu-radunaren interes legitimoa edo interes publikoko helburu bat betetzea, interesdu-nei utzi behar zaie aurka egiteko eskubidea egikaritzea euren datuen bilketarako opt-out hautapena eginez³⁴.
- Bermatu behar da pertsonen erabat jakin dezatela euren datu pertsonalen tratamen-dua egiten ari dela tratamendu hori egiten den une bakoitzean eta, halaber, euren eskubideak egikaritu ahal dituztela DBEOren arabera.

Illo beretik doa Frantziako Informatika eta Askatasunerako Batzordeak (CNIL)³⁵ eta EDPBk diotena³⁶; zehazki, azken horrek honako neurri hauek azaltzen ditu:

- Anonimizazioa datu-bilketa egin eta bere-hala egin behar da; hala, berridentifikazioa teknikoki saihesten da.

³³ Ez da nahastu behar datuen seudonimizazioarekin.

³⁴ Ausazko MACs helbideak erabiltzen dituzten probe request tramak erabiltzeak opt-out aukera emateko posibilitatea eragotzi ahal du.

³⁵ CNIL: [Audience and attendance measurement devices in spaces accessible to the public: the CNIL recalls the rules](#)

³⁶ 01/2017 irizpena, pribatutasunari eta komunikazio elektronikoei buruzko erregelamenduaren proposamenari buruzkoa (2002/58/EE) (29LT,WP247).

- Helburua kontuan hartuta berehalako anonimizazioa egitea ezinezkoa bada (adibidez, ibilbide bat erregistratzen ari delako), datu pertsonalak tratatu ahalko dira anonimizatuta ez dauden epean baldin eta honako baldintza hauek betetzen badira:
- datuen bilketaren helburua zenbaketa estatistikoa izango da, besterik ez.
- jarraipena denboran eta espazioan mugatzen da, eta helburu horretarako ezinbestekoa den neurria.
- datuak berehala ezabatzen edo anonimizatzen dira.
- borondatez salbuesteko benetako aukera dago.

Tratamenduaren arduradunek, gainera, beste neurri aringarri batzuk ere hartu behar dituzte, hirugarrenen oinarritzko eskubideak ukitzen ez direla bermatzeko, adibidez, bilketa-puntu baten ondoan bizi diren pertsonen pribatutasuna babestea.

Datu pertsonalen tratamenduan arriskua kudeatzeko eta eragina ebaluatzeko gidan, VIII. apartatua (Kontrolak), arriskua murrizteko kontrolen sorta zabal bat agertzen da. Kontrol horiek aproposak izan daitezke datu pertsonalen edozein tratamendutarako. Wi-Fi tracking teknologia duen tratamendu bat inplementatzea erabakitzen duen arduradunak, aplikatu beharrezko neurri guztiak inplementatu behar ditu, egin nahi duen tratamenduaren arabera.

Jarraian, Wi-Fi tracking teknologia duten tratamenduetan arriskuak kudeatzen lagundu ahal duten neurri tekniko eta antolakuntzako batzuk azalduko dira.

A. ANONIMIZAZIOA

Anonimizazioa datu pertsonalen tratamendu bat da zeinean, datu pertsonalen multzo batetik abiatuta, informazio anonimoko multzo berri bat sortzen baita. Tratamendua den aldetik, DBEOren printzipioak bete behar ditu, besteak beste erantzukizun proaktiboarena. Horrek zera esan nahi du: arduradunak anonimizazio-tratamendua beharrezkoak diren bermeekin egikaritzeko egokiak diren neurriak hartu behar ditu eta, bereziki, pentsatu behar du pertsonentzat zein arrisku dakarren anonimizazio-prozesuan atzera egiteak.

AEPDk tresna batzuk jartzen ditu arduradunen eskura datuen anonimizazioa buruzko informazio zabalarekin, Berrikuntzari eta Teknologiari buruzko micrositean, baita 29. artikuluko Lantaldearen anonimizazio-teknikei buruzko 05/2014 irizpenean ere.

Anonimizazio-tratamendua ez da edonolako prozesua, eta probabilitate handiarekin baliteke berridentifikazioa gertatzea, hainbat faktoreren arabera; hona hemen faktore horietako batzuk:

- Datuak zein unetan anonimizatzen diren. Orokorrean, datuak zenbat eta arinago anonimizatu, hainbat eta txikiagoa izango da datu pertsonalen tratamendua eta txikiagoa ere arriskua interesdunentzat³⁷. Hala ere, tratamendu batean helburu jakin batzuk betetzeko, baliteke datuak geroagoko faseetan ere anonimizatu behar izatea. Adibidez, helburua bada pertsonen ibilbideen jarraipena egitea denbora-tarte handi samar batean, posible da datuak anonimizatu gabe biltegiratzea denbora-epe luzeetan. Datuak berandu anonimizatuz gero, arrisku batzuk handituko dira.

³⁷ DBEOren 25.2 artikulua.

- Erabilitako anonimizazio-teknika: Arriskua dago anonimizazio-prozedura ahulak erabiltzeko eta prozedura horietan atzera egiteko.
- Proposatutako anonimizazioa gorabehera, inguruabar berezi batzuk gerta daitezke, adibidez ordu jakin batzuetan eremu batzuetan jende gutxi egotea edo gailu bakar bati buruz lokalizazio-puntu bat baino gehiago eskuragarri izatea, zeinetan³⁸ erraza izango bailitzateke pertsona edo haren portaerak identifikatzea.

Horregatik guztiarengatik, arduradunak, anonimizazio-tratamendu bat egin ostean, analisien eta froga praktikoen bidez zehaztu beharko du datuak berridentifikatzea ezinezkoa dela. Arduradunak berridentifikazio-arriskuak aztertu behar ditu eta kasurik txarrenaren baldintzak gogoan hartu. Komenigarria da halakoak hirugarren batek aldian-aldian egitea. Baldintza horietan datu-multzo osoa edo datuetako batzuk berridentifikatu ahal badira, datu-multzo hori ez da anonimoa izango.

Anonimizazioa zein unetan egin behar den, anonimizazio goiztiarra da neurririk efikazena pertsonen eskubide eta askatasunak babesteko. Horretarako, anonimizazio-prozesua datuen bilketa egiten den unetik hurbil egin behar da, zenbat eta hurbilago hobeto. Sistema batek datu pertsonalak biltzen baditu eta bilketa-puntuan anonimizatzen baditu edonola prozesatu aurretik eta, areago, biltegiratu aurretik, orokorrean arrisku txikiagoa izango du pertsonen eskubide eta askatasunetarako, datuak ordu, egun edo hilabete batzuk geroago minimizatzen dituen sistema batek baino.

Funtsean, posible denean, datuak berehala anonimizatu behar dira, datuak biltzen diren puntutik ahalik eta hurbilen, ahal dela atzigailuan bertan. Lortu nahi den helburua dela eta anonimizazio-eragiketak egiteko atzeratu behar denean, anonimizazioa posible izan arte aplikatu beharko da seudonimizazio goiztiarra. Hala ere, seudonimizazioa ezin da izan anonimizazioaren ordezkia, eta datuen seudonimizazioa ez da justifikazioa datuen anonimizazioa atzeratzeko edo ez aplikatzeko.

B. MAC HELBIDEAK ETA METADATUAK MASKARATZEA

Maskaratzea, datu pertsonalen tratamenduetan datuak babesteko sarritan erabiltzen den neurri tekniko da. Datuak atzitzen diren unean atzigailuak berak adierazle bakarrak –MAC helbidea, kasu– maskaratzea, datuak biltegiratu baino lehen –ez logetan ere–, egoera batzuetan efikaza izan daiteke pertsonen singularizazioa eta identifikazioa saihesteko.

Adibidea:

MAC helbide batek fabrikatzailea identifikatzen duen 24 bit dauzka, eta 24 bit

fabrikatzaileak aske esleitzen dituenak. Lokal batean hainbat pertsona kontrolatu nahi badira, baliteke 48 bitak erabili behar ez izatea, posible da datuak atzitzen diren unean bertan maskaratzea eta MAC helbidearen zati bat bakarrik erabiltzea, adibidez azken 24 bitak. Aldi berean 1000 lagun bereizi nahi badira, 14 bitekin biak bat etortzeko posibilitateak % 6 izango dira. 100 lagun bereizi nahi badira, 11 bitekin biak bat etortzeko posibilitateak % 5 izango dira.

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).

Hala ere, identifikatzaile gisa MAC helbidea erabiltzen ez bada edo gailuek Probe Request tramak ausazko MAC helbideekin bidaltzen dituztenean, teknika hori ez da erabilgarria izango.

Erabiltzaile-gailuak identifikatzeko azterna digitala erabiltzen denean, pertsonen singularrizazioa eta identifikazioa saihesteko aplikatu beharreko neurria metadatuak atzitzen diren unean maskaratzea izango da.

C. DESLOTZEA

Gune geografiko diferentetan eta denbora-tarte diferentetan atzitutako datuak deslotu ahal izateko neurriak aplikatzean datza.

Adibidea:

Gailuaren azterna digitalen ordeztan (edo beste edozein identifikatzailearen ordeztan) gatz duen hash bat jartzen da, berezitasun batekin: kokaleku bakoitzean gatz diferente bat erabiltzen da eta denbora jakin batean behin (12/24 ordurik behin) ausaz aldatzen da. Erabilitako gatzaren historia ez da biltegiratzen, gatz berri bat sortzen den bakoitzean baztertu eta ezabatzen baitira.

D. AGREGATZEA

Orokortze eta ezabatze teknikak erabiliz subjektu batzuei buruzko informazioa taldekatzean datza³⁹. Hori erabiltzen da erregistro individualik behar ez denean eta datu agregatuak lortu nahi den helbururako nahikoak ez direnean, hala gertatzen baita Wi-Fi trackinga erabiltzen duten tratamendu batzuetan.

Adibidea:

Pertsonen Museo batean egindako ibilbide nagusiei buruzko bero-mapak lortzeko ez litzateke identifikatzaile bakarrik behar, nahikoa izango litzateke zenbaketa estatistiko bat.

E. DATUAK MINIMIZATZEA

Wi-Fi trackinga erabiltzen duten tratamenduak diseinatzean DBEOn ezarritako datuen minimizazioaren printzipioa betetzen dela bermatzeko neurriak hartzean datza (datu pertsonalak «egokiak, beharrezkoak eta ezinbestekoaren neurria mugatuak izango dira, haien tratamen-

duaren helburuen arabera»). Horren adibide praktikoa batzuk honako hauek dira:

- Sentsoreak jardunean dauden epealdia ezinbestekoaren neurria mugatzea.

³⁹ [La k-anonimidad como medida de la privacidad.](#)

- Wi-Fi trackingaren mendean dagoen eremua mugatzea eta, ahal dela zona pribaturik ez sartzea.
- Pertsonen ibilbideen monitorizazioaren mendean dagoen eremua ahal eta gehien mugatze⁴⁰.
- Ahal dela, pertsonak identifikatzeko modua ematen duten Wi-Fi trametako datuak (adibidez, SSID) ez atzitzea, ezta biltegitratzea ere.
- Ahal dela, gailu-mota jakin batzuetatik (gailu finkoak, IOT sentsoreak, gorputzeko inplantak/inplante sanitarioak eta abar) datozen datuak ez atzitzea.

F. DATUEN KONTSERBAZIO EPEA

Datu pertsonalen edozein tratamendutan bezala, oso garrantzitsua da datuen kontserbazio epea mugatzea, bai anonimizatu gabe-

koena bai anonimizatuena, berridentifikatzeko hondar-arriskua dela eta.

G. SEGURTASUN-NEURRIAK ETA HIRUGARRENEK EGIN BEHARREKO AUDITORETZA

Segurtasun-neurriak zentzu zabalenean ulertu behar dira. Administrazio publikoek abian jarritako tratamenduen kasuan, erabilitako informazio-sistemak Segurtasun Eskema Nazionalaren (SEN)⁴¹ mendean egongo dira, eskubide eta askatasunetarako arrisku-mailari dagokion kategorian, DBGEB era batekoa edo bestekoa den. Eginbehar horren barruan sartzen dira sektore pribatuko entitateen informazio-sistemak, sektore publikoko entitateei zerbitzuak ematen dizkietenean edo soluzioak ematen dizkietenean, entitate horiek euren administrazio-eskumen eta -ahalak egikaritu ahal izan ditzaten. Segurtasun-neurri egokiak ez dira soilik SENean azaltzen diren horiek; aitzitik, ahal dela, oinarritzko eskubide eta askatasunetarako arriskuari egokitutako segurtasun-maila bermatzeko neurriak ere ezarri behar dira,

tratamendu espezifiko bakoitzean, DBEOren 32. artikularen arabera.

SEN betetzeko eginbeharra ez duten tratamenduen kasuan, tratamendu espezifiko bakoitzean eskubide eta askatasunetarako arriskua kudeatzeko beharrezkoak diren neurriak hartuko dira, DBEOren 32. artikularen arabera.

Gogora ekarri behar da DBEOren 32. artikulua, 1.d) apartatuan, segurtasun-neurriak aldian-aldian egiaztatzeko, ebaluatzeko eta baloratzeko prozesua eskatzen duela.

Hirugarrenek egindako auditoretzak lagungarriak dira oinarritzko eskubideetarako arriskuaren arabera segurtasun-neurriak noraino betetzen diren frogatzeko.

⁴⁰ Soilik ibilbideak monitorizatzea beharrezkoa denean tratamenduarekin lortu nahi den helburua betetzeko.

⁴¹ DPBEBLOren lehenengo xedapen gehigarria: «Sektore publikoaren eremuko segurtasun-neurriak: 2. Lege organiko honen 77.1 artikuluan zerrendaturiko arduradunek Segurtasunaren Eskema Nazionalan dauden segurtasun-neurrietatik dagozkienak aplikatu beharko dizkiete datu pertsonalen tratamenduei, eta neurri horien baliokideen inplementazio-maila jakin bat bultzatu beharko dute beraiekin lotura duten zuzenbide pribatuko enpresa edo fundazioetan».

H. ANTOLAKUNTZAKO NEURRIAK

Arduradunak neurri tekniko eta antolakuntzako egokiak aplikatzeko bermeak dauzkaten tratamendu-eragileak hautatu behar ditu, tratamendu-mandatuaren kontratuaren arabera jokatu behar du, eragileak datuak ezingo ditu tratatu bere helburu propioetarako, baizik eta arduradunaren jarraibide dokumentatuei segituz eta, ahal dela, bermerik ez duten nazioarteko datu-transferentziak saihestuko ditu.

DBEOn tratamendu-mandatuaren kontratuetarako agertzen diren eginbeharrei jarraituz, espresuki klausula batzuk sartu behar dira.

Klausula horien bidez eragotziko da tratamendu-eragileak beste eragile batengana jo dezala aurrez arduradunaren idatzizko baimenik gabe, eta tratamendu-eragileak datu pertsonalak helburu propioetarako trata ditzala edo, kasuan kasu, mugak eta baldintzak jarriko dira, jakiteko eragileak zein tratamendu egin ditzakeen, hasierako tratamenduaren helburuarekin bateragarriak badira. Gainera, eragileak datu pertsonalen arrakalak jasanez gero, horri eman beharreko erantzuna ezarri behar da esplizituki, bai arduradunaren kontura egindako tratamendurako, bai eragilearen tratamendu propioetarako.

Arduradunak eragotzi behar du nazioarteko datuen transferentziak bermerik gabe egiten direla.

Era berean, arduradunek datuak diseinutik abiatuta eta lehenetsita babesteko neurriak ezarri behar dituzte, datu pertsonalen arrakala batek eskubide eta askatasunetan sor ditzakeen arriskuak minimizatzeko.

Segurtasun-neurriei dagokienez, gogora ekarri behar esperientziari eta Auzitegi Gorenaren doktrinari erreparatuta⁴² eginbeharra direla, baina ez xedeen aldetik, baizik eta bitartekoen aldetik.

Orokorrean, Wi-Fi trackinga erabiltzen duten datu pertsonalen tratamenduetan oso garrantzitsua da kontuan hartzea konfidentzialtasun-arrakala gertatzeko probabilitatea dagoela.

Beraz, arduradunak aurretiaz neurriak hartu beharko ditu interesdunek jasan ditzaketen arriskuak minimizatzeko eta, arrakalak gertatuz gero, arduradunak eta eragileek eman beharreko erantzuna aurreikusita eduki behar du, pertsonen eskubide eta askatasunetarako eragina minimizatzeko.

Garrantzitsua da aurretiaz identifikatzea konfidentzialtasun-arrakala bat gertatu ahal den egoera guztietan zein den tratamenduan esku hartzen duen bakoitzaren erantzukizuna, baita haietariko bakoitzean zein eginbehar izango dituen arrakala behar bezala kudeatzeko, barnean direla datuak babesteko kontrol-agintaritza eskudunari jakinarazteko eta ukituei komunikatzeko eginbeharrek, horiek egitea nahitaezkoa denean.

⁴² [C.G.P.J. - Noticias Judiciales \(poderjudicial.es\)](https://www.poderjudicial.es/cgpj/noticias)

I. ARRISKUAREN ETENGABEKO KUDEAKETA

Tratamenduaren arduradunak tratamenduaren arriskuak aztertu behar ditu berezitasun eta inguruabar guztiei erreparatuta eta, une batean edo bestean tratamenduan edo tratamenduari eragiten dioten faktoreetan aldaketarik gertatzen bada, arriskuak berriro ebaluatu eta kudeatu beharko dira.

DBEOn (24. artikulua) eta 7/2021 Lege Organikoan (27. artikulua, 680/2016 Zuzentzauearen 19. artikulua transposizioa egiten duena) ezarrita dagoenaren arabera, tratamenduaren arduradunak tratamenduan ezarritako neurriak berrikusi eta eguneratu behar ditu, datuak babesteko araudia betetzen dela bermatzeko. Arauak berak ezartzen duenez, neurriok beharrezkoa denean berrikusi eta eguneratuko dira⁴³.

9. GARDENTASUNA ETA INFORMAZIOA

Zera hartu behar da gogoan: Wi-Fi tracking teknologia erabiliz informazioa jasotzen denean pertsona fisiko baten terminalaren (telefono mugikor bat edo beste edozein gailu) eta Wi-Fi sare baten arteko komunikazioaren emaitza gisa, aztarna digital bat sortzeko eta, hala gailu hori gainerako terminaletatik bereizteko, baliteke datu pertsonalen tratamendu bat egotea eta, beraz, tratamenduaren arduradunak eta eragileak DBEOn jasotako printzipioak eta eskubideak errespetatu behar dituzte. Printzipio horien artean, DBEOn 5.1 a) artikuluan gardentasunaren printzipioa onartzen da, zilegitasunaren eta fideltasunaren printzipioez gain. Baliteke terminalen titularrak ez konturatzea tratamendu honetaz; bada, berezitasun horregatik, are beharrezkoagoa da gardentasunaren printzipioa betetzea, informazio argia eta eskuragarria emanez. DBEOn 13. artikuluan zehazten da zein informazio jakinarazi behar zaion interesdunari, berari buruzko datu pertsonalak jasotzen direnean. Pertsonaiei aldez aurretik informazioa eman beharko zaie honako alderdi hauei buruz:

➤ Tratamenduaren arduradunaren identitatea eta harremanetarako datuak, eta, halakorik ez badago, bere ordezkariarenak.

- Datuak babesteko ordezkariarekin harremanetan jartzeko datuak.
- Tratamenduaren helburuak eta oinarri juridikoa.
- Arduradunaren edo hirugarren baten interes legitimoak.
- Datu pertsonalen hartzaileak edo hartzaile-kategoriak.
- Aurreikusita dauden nazioarteko transferentziak.
- Kontserbazio-epea.
- Datuetara irispidea izateko, datuak zuzentzeko edo ezerezteko, tratamendua mugatzeko, datuei aurka egiteko eta eramangarritasuneko eskubideak.
- Adostasuna ezeztatzeko aukera.
- Kontrol-agintaritza batean erreklamazio bat aurkezteko eskubidea.

⁴³ [Cuándo hay que revisar las medidas de protección de datos.](#)

A. INFORMAZIOA HAINBAT GERUZATAN

Informazioa laburki, gardentasunez eta erraz ulertzeko eta eskuratzeko eran eta hizkera argia eta erraza erabilia emango da, batez ere hurrei zuzendutako informazioa denean.

Hala, DPBEDBLOren 11. artikuluan ezarrita dagoenez, arduradunak DBEOren 13. artikulua ezarritako informazioa emateko eginbeharra bete ahalko du interesdunari oinarritzko informazioa emanez, bai eta helbide elektroniko bat edo gainerako informazio guztira iristea –modu erraz eta berehalakoan– ahalbidetuko dion beste baliabide bat emanez ere (horri deitzen zaio «informazioa geruzatan» ematea).

Oinarritzko informazioak honako eduki hau izan behar du, gutxienez:

- Tratamenduaren arduradunaren identitatea.
- Tratamenduaren helburua.
- DBEOren 15.etik 22. artikulura artekoek ezarritako eskubideak egikaritzeko aukera.
- Informazioa ematea: jasotako datu pertsonalak profilak egiteko erabili ahal direla, ukituarengan ondorio juridikoak sor ditzaten banakako erabaki automatizatuak hartzearen aurka egiteko eskubidea duela, baldin erabaki horiek harentzat ondorio juridikoak badituzte edo antzeko moduan nabarmen eragiten badiote, DBEOren 22. artikulua xedatutakoaren arabera eskubide hori aitortzen bazaio.
- Informazioa idatziz edo bestelako bitartekoez eman ahalko da, bai eta elektronikoz ere, bidezkoa bada. Informazioa ahoz ere eman ahalko da, interesdunak hala eskatzen badu, eta baldin eta eskatzailearen identitatea egiaztatu ahal bada beste bitarteko batzuen bidez.

23. artikuluko Lantaldeak, 2017ko azaroaren 29an, DBEOren arabera gardentasunari buruzko gidalerroak eman zituen (2018ko apirilaren 11n berrikusi zituen). Gidalerro horietan, Wi-Fi trackingaren antzeko ingurune batean interesdunei informazioa transmititzeko bide batzuk jaso ziren. Gidalerro horien arabera, honako hauek egin ahal dira:

- jendeak ikusteko moduan informazioa dakarten panelak jartzea.
- seinale publikoak jartzea estaldura-eremu osoan.
- informazio-kanpaina publikoak.
- ikonoak (normalizatutako ikonoak, zeinek aurreikusitako tratamenduaren ikuspegi osoa argi ikusteko modua eta erraz ulertzeko eta irakurtzeko era eskainiko baitituzte, DBEOren 12.7 artikulua arabera).
- ahots bidezko alertak.
- idatzizko xehetasunak, ezarpenerako jarraibideen barruan.
- ezarpenetarako jarraibideetan txertatutako bideoak.
- gailu adimentsuei buruzko idatzizko informazioa, SMS bidezko mezuen edo posta elektronikoko mezuen bidez.

Administrazio publikoek teknologia horien erabiltzen badituzte, horrez gain gomendatzen da gardentasunerako neurri batzuk erabiltzea eta, horren barruan, honako hauek argitaratzea⁴⁴:

- Bide publikoan jarritako Wi-Fi tracking sentsoeren erregistroa.
- Zein helburu lortu nahi diren, tratamendua hasteko eta amaitzeko datak adierazita.

⁴⁴ Informazio gehiago eskuragarri dago hemen: Investigation Report on the Protection of Personal Data in the Development of Dutch Smart Cities

- Egin beharreko eragin-ebaluazioen laburpen egokia (kontuz erabili beharreko informaziorik gabe).
- Erabilitako anonimizazio-algoritmoen buruzko informazio esanguratsua.
- Hainbat hizkuntzatan eskuragarri dagoen informazioa, turista ugari joaten direneko gunea bada.

Nolanahi ere, DPBEBLOren 31. artikulua arabera, tratamenduaren arduradunek eta eragileek edo, hala badagokio, haien ordezkariak tratamendu-jardueren erregistroa izan beharko dute; DBEOren 30. artikulua xedatzen du erregistro hori, baina haren 5. apartatuak xedatutakoa aplikatu behar denean betebeharrorretatik salbuetsita egongo dira. DPBEBLOren 77.1 artikuluan jasotako subjektuek berentratamendu-jardueren zerrenda jarriko dute jendaurrean, baliabide elektroniko bidez irisgarri, non lege-oinarria ere jasoko baita.

10. DBEO-N ONARTUTAKO ESKUBIDEAK EGIKARITZEA

DBEOren 11. artikulua arabera, datu pertsonalen tratamenduaren helburuek ez badute eskatzen (edo jadanik ez badute eskatzen) tratamenduaren arduradunak interesduna identifikatzen, arduradun hori ez da egongo behartuta interesduna identifikatzea xede duen informazio gehigarria atxikitzea, lortzea edo tratatzea, DBEO betetzeko asmo hutsaren amoreagatik; bada, kasu horietan, arduraduna gai bada frogatzeko ez dagoela interesduna identifikatzeko moduan, horren jakitun ipiniko du arduradunak interesduna, ahal bada. Kasu horietan ez dira aplikatuko DBEOren 15.etik 20.era bitarteko artikulua salbu eta interesdunak, artikulua horien indarrez bereak dituen eskubideak egikaritzen, bera identifikatzea ahalbidetuko duen informazio gehigarria ematen badu.

Tratamenduaren arduradunak ukitua informatu beharko du DBEOren 15. artikulutik 22.era bitartean onartuta dauzkan eskubideak egikaritzeko eskura dituen baliabideen gainean.

Baliabide horietarako irispideak erraza izan beharko du ukituarentzat. Eskubideak egikaritzeko, bitarteko eskuragarriak, irisgarriak eta errazak ezarri behar ditu arduradunak, baliabide elektronikoak barne.

Bereziki, baliabide elektronikoak erabiltzen direnean, prozedura batzuk ezarri behar dira baliabide horiek erabiltzen dituzten ukituen identitatea egiaztatzeko; halaber, eskubide bat edo bestea egikaritu izanaren jakinarazpena jasotzeko eta behar bezala erantzun dela egiaztatzeko bideak ere jarri behar dira.

A. IRISPIDE-ESKUBIDEA (DBEOREN 15. ARTIKULUA)

Interesdunak eskubidea izango du tratamenduaren arduradunak egiazta diezaion berari buruzko datu pertsonalen tratamendua egiten ari den ala ez eta, hala bada, datu pertsonalak eta DBEoren 15.1 artikuluan azaltzen den informazioa izateko eskubidea ere.

DPBEDBLOren 13.3 artikulua arabera, irispide-eskubidea egikaritzea errepikakorra dela ulertuko da sei hilabeteko tartean behin baino gehiagotan baliatu bada, horretarako arrazoi legitimorik egon gabe. Hala gertatuz gero, tratamenduaren arduradunak arrazoizko kanon bat kobratu ahalko du, kontuan hartuta kostu administratiboak: bestela, eskubideari uko egin ahalko dio.

B. EZEREZTEKO ESKUBIDEA (DBEOREN 17. ARTIKULUA)

Interesdunak eskubidea izango du berari buruzko datu pertsonalak atzerapen bidegaberi gabe ezereztu ditzan tratamendu-arduradunak, baldintza hauetako bat gertatzen denean:

- Datu pertsonalak jadanik ez badira beharrezkoak, bildu zirenean edo beste modu batez tratatu zirenean zeuden helburuen argitan.
- Interesdunak bertan behera uzten badu tratamenduaren oinarria den DBEoren 6.1 artikuluko a) letraren edo 9.2 artikuluko a) letraren arabera adostasuna, eta tratamenduak ez badu beste oinarri juridikorik.
- Interesdunak tratamenduaren aurka egiten badu DBEoren 21.1 artikuluari jarraituz, eta gainera ez badago tratamendua gauzatzeko beste arrazoi legitimorik, edo interesdunak tratamenduaren aurka egiten badu DBEoren 21.2 artikuluari jarraituz.

- Datu pertsonalen tratamendua legez kontra egin bada.
- Datu pertsonalak ezereztu behar badira, tratamenduaren arduradunari aplikagarri zaion Batasuneko edo estatu kideetako zuzenbidean ezarritako lege-betebehar baten indarrez.
- Datu pertsonalak jaso badira DBEoren 8.1 artikuluan aipaturiko informazioaren gizar-teko zerbitzuen eskaintzaren ingurumarian.

Tratamenduaren arduradunak datu pertsonalak publiko egiten dituenean eta azaldu-tako inguruabarretako baten arabera datuok ezereztu behar dituenean, eskura duen teknologia eta hura erabiltzeko kostua kontuan hartuta, arrazoizko neurriak hartuko ditu, neurri teknikoak barne, datu pertsonalen tratamendua egiten ari diren arduradunak jakitun ipintzeko interesdunak egin duen eskabideaz datu pertsonal horiekiko lotura oro edo kopia edo erreplika oro ezereztu daitezzen.

DBEOren 17.3 artikuluan ezarritako kasuetan ez da bidezkoa izango datu pertsonalak ezerezte. Tratamenduaren arduradunak datuak blokeatu beharko ditu, haiek ezereztu behar dituenean (DPBEDBLOren 32. artikulua).

Blokeatutako datuak epaileen eta auzitegien, fiskaltzaren edo bestelako administrazio publiko eskudunen esku geratuko dira, batez ere, datuak babesteko agintaritzen esku, tratamenduaren ondorioz sor daitezkeen erantzukizunei erantzun ahal izateko, baina betiere erantzukizunaren preskripzio-epearen barruan.

Epe hori amaitzen denean, datuak suntsitu egin beharko dira. Blokeatutako datuak bakar-bakarrik eginkizun horiek burutzeko tratatu ahalko dira. Kontrol-agintaritzek blokeatzeko betebeharraren salbuespenak ezarri ahalko dituzte.

Datu pertsonalak ezerezten badira, horren berri emango die tratamenduaren arduradunak datu pertsonalen hartzaile guztiei, salbu eta ezinezkoa bada edo neurriz kanpoko ahalegina eskatzen badu (DBEOren 19. artikulua).

C. TRATAMENDUA MUGATZEKO ESKUBIDEA (DBEOREN 18. ARTIKULUA)

Ukituak tratamenduaren arduradunari eskatu ahal dio datuen tratamendu eten dezala, baldintza hauetako bat gertatzen denean:

- Interesdunak datu pertsonalen zehaztasunaren aurka egiten badu, arduradunak datuon zehaztasuna egiaztatzen duen bitartean.
- Interesdunak tratamenduaren aurka egiteko eskubidea egikaritu badu, eta arduradunaren arrazoi legítimoak interesdunaren gainetik dauden ala ez egiaztatzen den bitartean.
- Tratamenduaren arduradunari eskatzea datu pertsonalak kontserba ditzala, baldintza hauetako bat gertatzen denean:
 - Tratamendua legez kontrakoa bada eta interesdunak datu pertsonalak ezereztearen aurka egiten badu eta, ordainetan, haien erabilera mugatzeko eskatu.
 - Arduradunak jadanik behar ez baditu datu pertsonalak tratamenduaren helburuei begira, baina interesdunak bai, erreklamazioak formulatzeko, egikaritzeko edo aldezteko.

Ukituaren datu pertsonalen tratamendua mugatu bada, datuon tratamendua –kontserbazioa salbu– egin ahal izango da soil-soilik interesdunak bere adostasuna agertzen badu, edo erreklamazioak formulatzeko, egikaritzeko edo aldezteko, edo beste pertsona fisiko edo juridiko baten eskubideak babesteari begira, edo Batasunaren edo estatu kide jakin baten interes publiko garrantzitsuari buruzko arrazoiak direla eta.

Arduradunaren informazio-sistemetan argi eta garbi adierazi behar da datu pertsonalen tratamendua mugatuta dagoela (DPBEDBLOren 16.2 artikulua).

Tratamenduaren mugatzea lortu duen interesduna jakitun ipiniko du tratamenduaren arduradunak mugatzea amaitu baino lehen.

Tratamendua mugatzen bada, horren berri emango die tratamenduaren arduradunak datu pertsonalen hartzaile guztiei, salbu eta ezinezkoa bada edo neurriz kanpoko ahalegina eskatzen badu (DBEOren 19. artikulua).

D. DATUEN ERAMANGARRITASUN-ESKUBIDEA (DBEOREN 20. ARTIKULUA)

Tratamenduaren arduradunari emandako norberaren datu pertsonalak erabilera orokorra eta irakurketa mekanikoa duen formatu egituratu batean jasotzeko eskubidea da, eta tratamenduaren arduradunari emandako norberaren datuak beste tratamendu-arduradun bati zuzenean bidaltzeko eskubidea ere bada, baldin eta tratamenduaren oinarrian interesdu-

naren adostasuna edo interesdunak eskatuta burututako kontratu bat badago, eta baldin eta tratamendua bitarteko automatizatuen bidez egin bada. Baina, ez da eskubide hori aplikatuko tratamendua beharrezkoa denean eginkizun bat betetzeko interes publikoaren izenean edo tratamenduaren arduradunari esleitutako botere publikoen izenean.

E. AURKA EGITEKO ESKUBIDEA (DBEOREN 21. ARTIKULUA)

Bere egoera partikularra dela eta, interesdunak eskubidea izango du, edozein unetan, berari buruzko datu pertsonalen tratamenduaren aurka egiteko, tratamendu hori oinarritzen bada DBEOREN 6.1 artikuluko e) edo f) letran xedatutakoan, baita xedapen horietan oinarrituriko profilen elaborazioaren aurka ere. Aurka egiteko eskubidea egikaritzen denean, tratamenduaren arduradunak datu pertsonalak tratatzeari utziko dio, noiz eta ez duen egiaztatzen interesdunaren interes, eskubide eta askatasunen gainetik arrazoi legítimo larriak daudela tratamenduari eusteko, edo erreklamazioak formulatzeko, egikaritzeko edo aldezteko.

Aurka egiteko eskubidea esanbidez adierazi behar zaio interesdunari, eta argi aurkeztu behar da, beste edozein informaziotatik bereizita.

Interesdunei aukera eman behar zaie tratamenduaren aurka modu errazean egiteko. Datu pertsonalak Wi-Fi trackingaren bidez jaso zaizkien interesdunek jasan dezaketen eragina arintzeko edo murrizteko, arduradunak erabaki dezake «borondatezko salbuespen» orokorra ahalbidetzea, aurka egite hutsaz harago; hala eginez gero, datuen tratamendua egiteari utziko zaio inola ere justifikatu behar izan gabe.

F. BANAKAKO ERABAKI AUTOMATIZATUAK, PROFILAK EGITEA BARNE (DBEOREN 22. ARTIKULUA)

Wi-Fi tracking teknologiaren izaera bera kontuan hartuta, teknologia horretan oinarrituta profilak egitea dakarten tratamenduak egitea bideragarria izango da. Interesdunak eskubidea izango du haren datu pertsonalen tratamendu automatizatu batean soilik oinarrituta dagoen eta beraierengan ondorio juridikoak edo antzeko ondorio esanguratsuak dituen erabaki baten – arduradunak hartutako erabaki baten – objektu ez izateko, profilak egitea barne.

Hala ere, tratamendua egitea eta erabaki automatizatu bat hartzea zilegi izango da honako hau gertatuz gero:

- Beharrezkoa bada interesdunaren eta tratamenduaren arduradunaren artean kontratu bat egiteko edo betearazteko, edo interesdunak berariaz emandako adostasunean oinarritzen bada.

- Tratamenduaren arduradunari aplikagarri zaion Batasuneko edo estatu kideetako zuzenbideak baimentzen badu, zeinak interesdunaren eskubideak, askatasunak eta interes legítimoak babesteko neurri egokiak xedatzen baititu.

Kasu bietan, arduradunak behar diren neurriak hartuko ditu interesdunaren eskubideak, askatasunak eta interes legítimoak babesteko; honako hauek gutxienez: arduradunaren aldetik pertsona batek esku hartuko duela ziurtatzea, beraren ikuspuntua adierazteko eskubi-

dea eta erabakiaren kontra egiteko eskubidea. Tratamendu horietan ez dira erabiliko DBEOren 9.1 artikuluan ezarritako datu pertsonalen kategoria bereziak, salbu eta tratamendua interesdunaren adostasun bidez egiten bada edo Europar Batasuneko edo estatu kideko zuzenbideak ezarritako funtsezko interes publikoa tartean badago.

Kasu horietan, ziurtatuko da interesdunaren eskubideak, askatasunak eta interes legítimoak babesteko neurri egokiak hartu direla.

11. ADIMEN ARTIFIZIALAREN ERREGELAMENDUA

Teknologiaren gaur egungo egoera aintzat hartuta, datu pertsonalen tratamendu batzuetan baliteke Wi-Fi tracking teknologia eta adimen artifizialeko (AA) sistemak konbinatzea. Halako datu pertsonalen tratamenduak DBEOn ezartzen diren printzipioen, arduradunentzako eginbeharren eta interesdunentzako eskubideen mendeandae. Horrez gain, AAKo sistema jakin batzuen erabilera Adimen Artifizialaren Erregelamenduak (AAE) arautuko du.

Gida hau argitaratu den unean, oraindik ez da argitaratu Adimen Artifizialaren Erregelamendua (AAE). Argitaratzen denetik, 20 eguneko epean indarrean jarriko da eta, argitaratu eta handik bi urtera, xedapen gehienei dagokienez aplikatu beharko da.

Datu pertsonalen babesaren ikuspegitik, AAEn xedea ez da datuak babesteko oinarritzko eskubidearen aplikazioa ukitzea. AAek DBEO osatzen du eta ez du galaraziko DBEO aplikatzea. Hala ahalbidetuko da arduradunek eta eragileek modua dutela datuen babesaren arloan dauzkaten eginbeharrak betetzeko, euren tratamenduetan AAKo

sistemak txertatzen dituztenean (DBEOren 78. kontuan hartuzkoa), datuen babesa tratamenduaren diseinutik abiatuta inplementatzeko.

Horretarako, AAKo sistemak merkaturatzean, zerbitzuan jartzean eta erabiltzean erraztasuna eman behar da arauak aplikatzeko eta interesdunek eskubideak nahiz errekurso-bideak egikaritu ahal izateko, datuen babesari buruzko araudiak horiek nahiz oinarritzko beste eskubide batzuk bermatzen baititu.

Horren barruan sartzen dira AAKo sistemen hornitzaileek nahiz sistema horiek hedatzeko arduradunek dauzkaten eginbeharrak, edota beste esku-hartzaile edo operadore batzuenak, hala badagokio, kontuan hartuta AAKo sistemak diseinatzeak, garatzeak edo erabiltzeak datu pertsonalen tratamendua ekar dezakeela; horrez gain, datuak babesteko kontrol-agintaritzaren independenteen eginkizunak eta eskumenak ere sartzen dira. Hain zuzen ere, datuak babesteko kontrol-agintaritzaren independenteen ahaletako bat da AAEren arabera arrisku handiko AAKo sistemei buruz sortutako edo kontserbatutako

dokumentazio guztia eskatzea (sistema horiek Erregelamenduaren III. Eranskinean aipatzen dira), dokumentazio horretara irispidea izatea beharrezkoa denean kontrol-agintaritzaren eskumenak behar bezala betetzeko.

Komenigarria da argitzea, halaber, interesdunek datuak babesteko araudiaren arabera lehendik ere zeuzkaten eskubide eta berme guztiak izango dituztela, baita banakako erabaki automatizatuekin zerikusia duten eskubideak ere, profilak egitea barnean dela.

Horren haritik zera doa, adibide gisa: sarrerako informazio gisa Wi-Fi tracking teknologiaren bidez lortutako datuetatik abiatuta pertsona bati ondorio juridikoak sortzen dizkioten erabaki batzuk edo pertsona hori nabarmen ukitzen duten erabaki batzuk inplementatzen direnean adimen artifizialeko sistemen bitartez (sistema

horiek edonolakoak direla ere), eta erabaki horiek datu pertsonalen tratamenduan oinarritzen badira (eta horretan soilik), DBEOn ezarrita dagoena aplikatuko da (13., 14., 15. eta 22. artikulak eta 71. kontuan hartuzkoa).

Gainera, kasu horretarako, kasu bat gerta liteke: baldin eta erabakiaren oinarri den adimen artifizialeko sistema arrisku handikoa bada AAren arabera, Aaren araudian xedatuta dagoena aplikatuko da, DBEOn ezarrita dauden eskubideen osagarri gisa, pertsona horren ustez erabakiak ondorio txarrak sortzen baditu bere osasunean, segurtasunean edo oinarritzko eskubideetan. Zehazki, kontuan hartuko da Aaren araudiaren arabera ukituak eskubidea duela azalpen argiak eta esanguratsuak jasotzeko adimen artifizialeko sistemak erabakiak hartzeko prozeduran nahiz hartutako erabakiaren elementu nagusietan duen eraginari buruz.



**Datuak Babesteko
Euskal Agintaritza**
Autoridad Vasca de
Protección de Datos



**Consejo de Transparencia
y Protección de Datos
de Andalucía**