Datuak Babesteko
Euskal Agintaritza

Autoridad Vasca de
Protección de Datos

Esp.: CN24-007

IRIZPEN ZK.: D24-018

IRIZPENA, BILBOKO UDALEKO KANPOKO UDAL WIFI SARE BATETIK DATOZEN DATUAK ERABILTZEARI BURUZKOA

AURREKARIAK

LEHENENGO: Bilboko Udaleko datuak babesteko ordezkariak txostena egiteko eskatu dio Datuak Babesteko Euskal Agintaritzari. Honela dio eskariak:

> *«Datuak Babesteko Euskal Agintaritzari egindako kontsulta honen xedea da baieztatzea ea Bilbo hiriko Wifi sare doako, aske eta unibertsalean bildutako datuekin egiteko planteatzen ari den tratamendu berria datuak babesteko araudiaren araberakoa den (edo araudi hori aplikatzen ez zaion).*
>
> *Denboran zehar udal WIFI sarera konektatutako gailu mugikorren mugimenduari buruzko informazioa erabili nahi da, hainbat gauza identifikatzeko, hala nola hiri-mugikortasuneko joerak, kanpoko faktoreen arabera (jaiegunak, ekitaldi bereziak, ...) hainbat zonatan egon daitezkeen jende-pilaketak, kanpainen edo bestelako parametroen mendean egon daitezkeen merkataritza-zonak.*
>
> *Horretarako, kontsulta honekin batera doa Bilbo hiriko "WIFI saretik datozen datuak erabiltzeari buruzko txosten teknikoa", BILBAOTIK SAk idatzia. Txosten horretan udal WIFI saretik datozen datuekin egin nahi den tratamenduaren xedeari buruzko azterketa egiten da, eta WIFI sare horren azterlan teknikoa ere egiten da, zeinean Bilboko Udalak hartutako neurri tekniko eta antolakuntzakoak aztertzen baitira.*
>
> *DBEAren erantzunaren zain gaude, gai hauek direla eta:*
>
> *1. Datuen babesari buruz indarrean dagoen araudia aplikatzekoa den, ala osorik anonimizatutako datuak izateagatik aplikatzekoa ez den.*
>
> *2. Aplikatzekoa izanez gero, ea txostenean planteatzen den tratamendua araudiaren araberakoa den.*
>
> *3. Neurri tekniko eta antolakuntzakoei buruz egin ditzakezuen gomendio guztiak».*

BIGARRENA: Datuak Babesteko Euskal Agintaritzari dagokio egindako kontsultari erantzuteko irizpena ematea, Datuak Babesteko Euskal Agintaritzaren abenduaren 21eko 16/2023 Legearen 6. artikuluan eta Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko (EB) 2016/679 Erregelamenduaren (DBEO) 58.3 b) artikuluan ezarrita dagoenaren arabera.

GOGOETAK

I

Kontsultaren abiapuntua zera da: Bilboko Udalak jakin du lau kontrol-agintaritzek (Datuak Babesteko Espainiako Agentzia, Datuak Babesteko Kataluniako Agintaritza, Datuak Babesteko Euskal Agintaritza eta Gardentasunaren eta Datu Babesaren Kontseilua) Wi-Fi jarraipeneko teknologiei buruz tratamendu-arduradunentzako orientabide batzuk prestatu dituztela batera.

Orientabide horietan, Wi-fi jarraipeneko edo Wi-Fi trackingeko 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.

Beraz, irizpen honetan espresuki adierazten ez den guztiari dagokionez, orientabide horietara joko dugu.

Kontuan hartu beharreko lehenengo gauza da ea Bilboko udal Wifi sareak bildutako datuak datu pertsonalak diren ala ez, kontuan hartuta Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamendua, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituena eta 95/46/EE Zuzentaraua indargabetzen duena (aurrerantzean DBEO edo Datuak Babesteko Erregelamendu Orokorra).

Kontsultarekin batera doan txostenaren arabera, Wifi posizionamenduari buruz jasotako informazioak, funtsean, «gailuaren identifikatzaile anonimoa, data eta ordua, eta zein Wifi antenatara dagoen konektatuta» erregistratzen du.

DBEOren 4. 1) artikuluan honela definitzen da **datu pertsonala**:

> *«"Datu pertsonalak": pertsona fisiko identifikatu edo identifikagarri («interesdun») bati buruzko informazio guztia; pertsona fisiko identifikagarria da zuzenean edo zeharka, eta batez ere identifikatzaile baten bitartez, identifika daitekeen pertsona oro; identifikatzaile hori izen bat izan daiteke, identifikazio-zenbaki bat, kokapen-datuak, online identifikatzaile bat edo pertsona horren nortasun fisikoari, fisiologikoari, genetikoari, psikikoari, ekonomikoari, kulturalari edo sozialari buruzko elementu bat edo gehiago».*

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 zerbitzariek jasotako beste datu batzuekin konbinatzen direnean, erabil daitezke pertsona fisikoen profilak sortzeko eta beraiek identifikatzeko»*.

Halaber, 29. artikuluko Lantaldearen 2013ko otsailaren 27ko 2/2013 irizpenean, gailu adimentsuen aplikazioei buruzkoan, zera ezartzen da:

> *«Datu pertsonalak dira tratamenduaren arduradunak edo hirugarren batek zuzenean (adibidez izenaren bidez) edo zeharka identifikatu ahal duen pertsona bati dagozkionean. Datuak gailuaren jabearenak edo beste edozein pertsonarenak izan daitezke; hala gertatzen da, adibidez, helbide-liburuan jasota dauden lagunen harremanetarako datuekin. Datuak gailuan bildu eta prozesatu ahal dira, edo,*

transferitu ondoren, beste leku batean, aplikazioen garatzaileen edo hirugarrenen azpiegituren bitartez, kanpoko API baterako konexio baten bitartez, denbora errealean eta azken erabiltzaileak jakin gabe».

Eta erabiltzaileen eta beste pertsona batzuen bizitza pribatuan eragin nabarmena izan dezaketen datu pertsonalen adibide gisa 2/2013 irizpen horretan aipatzen dira kokapena edo gailuaren eta bezeroaren identifikatzaile bakarrak.

Beraz, 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.

Kontsultan azaltzen denez, udal Wifi sarean jasotzen den informazioaren artean dago gailuaren identifikatzailea (MAC helbidea).

Eta MAC helbide hori, gailua identifikatzen duen helbide hori, baliteke fabrikatzaileak esleitutakoa izatea (fabrikako MAC helbidea) edo ausazko MAC bat, Wifi sare batera konektatzen saiatzean gailuak berak sortzen duena.

Azken kasu horretan egonda ere, gailua Wifi sarera konektatuta dagoen bitartean, MAC helbidea konstantea da konexioak irauten duen denbora osoan; horri esker, konexioak iraun bitartean gailuak egindako ekintza guztiak lotu ahal dira (kokapen absolutua eta kokapen erlatiboa, beste terminal batzuen kokapenarekin alderatuta), eta baliteke lehendik dauden tekniken bitartez identifikazioa ahalbidetzea.

Gainera, Wi-Fi tracking bidez bildutako datuen lekuzko eta denborazko esparrua mantentzen denean, datu horiek berez edo beste batzuekin konbinatuta nahikoak izan daitezke pertsonak identifikatu ahal izateko.

Kontsultarekin batera doan txostenean ulertzen da gailuaren identifikatzailea, udal Wifi sareak erregistratzen duen hori (kokalekuarekin eta data-orduekin batera) ez dela datu pertsonala, gailuen % 90 ausazko MAC batekin konektatzen delako, eta gerora identifikatzaile guztiak anonimizatzen direlako atzera-bueltarik ez duen algoritmo baten bidez.

Txostenak azaltzen duenez, anonimizazio-prozesu bat dago, eta horren barruan gailuaren identifikatzailea ausazko zenbaki batekin lotzen da. Bada, hori gertatzen da datu pertsonalen multzo bat abiapuntu hartzen delako; kasu honetan, abiapuntua dira gailuen identifikatzaileak (MAC helbideak), eta anonimizazio-prozesu horren bitartez datu anonimoen multzo bat lortzen da.

Eta datuak anonimo bihurtzen direnetik ez zaizkie aplikatuko datuen babesari buruzko printzipioak, interesduna ez delako identifikagarria, edo identifikagarri izateari utziko diolako (DBEOren 26. kontuan hartuzkoa).

Era berean, DBEOk 4.2) artikuluan honela definitzen du **tratamendua**:

«datu pertsonalen gainean edo datu pertsonalen multzoen gainean egiten den edozein eragiketa eta eragiketa-multzo, prozedura automatizatuak erabilita zein erabili gabe, hala nola: datu-bilketa, erregistratzea, antolatzea, egituratzea, kontserbatzea, egokitzea edo aldatzea, ateratzea, kontsultatzea, erabiltzea, transmisioz lagatzea, hedatzea edo irispidean jartzeko beste edozein forma, datuak alderatzea edo interkonektatzea, mugatzea, ezabatzea edo suntsitzea».

Udal Wifi sareak gailuen informazioa jaso edo biltzea datu pertsonalen tratamendua da. Halaber, datu pertsonalen tratamendua da anonimizazio-prozesua bera ere, bai eta berridentifikatzeko arriskua benetan gauzatuz gero datuak kontsultan azaldutako xedeetarako erabiltzea ere.

Kontsultarekin batera doan txostenak ez du zehazten bildutako eta anonimizatutako informazioaren kontserbazio-epea. Kontuan hartu behar da gauza bat: gaur egun arrazoizko modu batean erabil daitezkeen bitartekoekin, baliteke berridentifikazioa egiteko modurik ez egotea; aurreikusitako kontserbazio-epea luzea bada, ordea, tratamenduaren arduradunak kontuan hartu behar du teknologiaren aurrerabideak berridentifikazioa egiteko aukera eman ahal duela.

II

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. Pertsonei 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, legitimoak 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.

Tratamenduaren arduradunaren erantzukizuna da DBEOn jasota dauden printzipioak betetzea eta betetzen dela frogatzeko moduan egotea; gainera, arduradunak ziurtatu behar du tratamenduak DBEOren 6.1 artikuluan ezarritako zilegitasun-baldintzaren bat betetzen duela.

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.

Kontsultan azaltzen denez, udal Wifi sarera konektatutako gailu mugikorren mugimenduari buruzko informazioa denboran zehar erabili nahi da, hainbat gauza identifikatzeko, hala nola hiri-mugikortasuneko joerak, kanpoko faktoreen arabera (jaiegunak, ekitaldi bereziak, ...) hainbat zonatan egon daitezkeen jende-pilaketak, kanpainen edo bestelako parametroen mendean izan daitezkeen merkataritza-zonak.

Kontuan hartu behar da helburua mugatzeko printzipioa bete behar dela. Hain zuzen ere, printzipio horren arabera datu pertsonalak helburu zehatz, esplizitu eta legitimoei begira bilduko dira eta, ondoren, ezin izango dira helburu horiekin bateragarriak ez diren moduan tratatu.

Helburua mugatzearen printzipioa beteko bada, tratamenduarekin lortu nahi den helburua gehiago zehaztu beharko da, kontserbazio-epeari eta kanpoko faktoreei dagokienez;

gainera, posibilitate batzuk zehaztu gabe uzten dira «beste parametro batzuk» adierazpena erabiltzean.

Zilegitasunaren printzipioa betetzeari buruz, 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.

Egin nahi den tratamenduak DBEOren 6.1 artikuluan jasota dauden oinarri juridikoetako baten babespean egon behar du eta, kontuan hartuta tratamenduaren arduraduna administrazio publiko bat dela, oinarri juridikoak honako hauek izango lirateke:

- Beharrezkoa bada tratamenduaren arduradunari aplikagarria zaion lege-eginbeharra betetzeko (DBEOren 6.1 c) artikulua). Oinarri hori aplikatu ahal izateko, Batasuneko Zuzenbideak edo lege-mailako arau batek arduraduna behartu behar du helburu bat betetzera Wi-Fi tracking teknikak derrigor erabiliz.
- Interes publikoaren izenean edo tratamenduaren arduradunari esleitutako botere publikoen izenean burututako eginkizun bat betetzea (DBEOren 6.1.e) artikulua). Tratamenduaren arduradunak identifikatu beharko du lege-mailako zein arauk edo Batasuneko zein zuzenbidek 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.
- Interesdunaren edo beste pertsona fisiko baten 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 justifikatzeko.

III

DBEOk ezartzen dituen eginbeharretako bat da arduradunak datu pertsonalen babesaren gaineko eraginaren ebaluazioa (DBGEB) egitea, 35. eta 36. artikuluetan jasota dagoenez. Ebaluazio hori beharrezkoa izango da tratamenduak arrisku handia badakar.

Wi-Fi tracking teknologia duten tratamenduetarako, beste edozein tratamendutarako bezala, arriskuen ebaluazioa eta DBGEB egiteko beharrizanaren 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 artikuluaren arabera, Wi-Fi tracking teknologia duten tratamenduetan eta, zehazki, tratamendu horretan 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.

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

DBGEB baten prozesuan lehenengo neurria da tratamenduaren beharrizanaren eta proportzionaltasunaren ebaluazio bat egitea, lortu nahi den helburuarekin alderatuta eta hiru irizpide aintzat hartuta: egokitasun-judizioa, beharrizan-judizioa eta proportzionaltasun-judizioa, zentzu hertsian. Ebaluazio hori amaitutakoan, tratamendua egingo den ala ez erabaki behar da; edo, bestela, tratamendua aldatzea erabaki, arestian azaldu den judizio hirukoitzaren analisia gainditzen duen arte. Arduradunak pribatutasunean gutxien sartzen den eta pertsonentzat arrisku gutxien dakarren aukera hartu beharko du.

Gainera, DBGEB bat egiteko prozesu horretan, eta arduraduna administrazio publiko bat izanik, 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.

IV

Egin nahi den tratamendurako egokiak diren neurri teknikoei eta antolakuntzako neurriei buruz agintaritza honek egin ditzakeen gomendioei gagozkiola, nabarmendu behar da WiFi jarraipenak edo Wifi trackingak pribatutasunerako arrisku handiak dakartzala, bidea eman dezakeelako pertsonen mugimenduen jarraipena egiteko haiek ezer egin gabe, ezer jakin gabe eta oinarri juridiko egokirik gabe. Lau kontrol-agintaritzek Wi-Fi jarraipeneko teknologiei buruz arduradunentzat egindako orientabide horien laugarren apartatuan, aplikatu beharreko neurri tekniko eta antolakuntzakoak zehazten dira.

Anonimizazioari dagokionez, komenigarria litzateke itzulgarria ez den prozesu baten bidez egitea, MAC helbidearen bertsio anonimizatuak inoiz ere biderik ez ematea jatorrizko MAC helbidea aurkitzeko. Kontsultarekin batera doan txostenak ez du zehazten zein teknologia erabili den anonimizazioa egiteko (datu-base zifratu batean, inork ere sartzerik ez den batean gordetzen den kode bakar batekin ordeztea).

Gogoeta horiek egiten ditu Datuak Babesteko Euskal Agintaritzak egin zaion kontsultari buruz. Halaber, agintaritza honek gainerako kontrol-agintaritzekin batera argitaratu dituen orientabideei lotzen gatzaizkio.

Vitoria-Gasteiz, 2024ko urriaren 10a