Grupul de lucru pentru protecția datelor „ARTICOLUL 29”

881/11/RO
WP 185

Avizul 13/2011 privind serviciile de localizare geografică pe dispozitivele mobile inteligente

Adoptat la 16 mai 2011

CUPRINS

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL,
instituit în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolul 29 și articolul 30 alineatul (1) litera (a) și alineatul (3) din directivă,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL DOCUMENT:

1. Introducere

Informațiile geografice joacă un rol important în societatea noastră. Aproape toate activitățile și deciziile oamenilor au o componentă geografică. În general, valoarea informației crește atunci când acesteia îi corespunde o locație. Toate tipurile de informații, cum ar fi date financiare, date privind sănătatea și alte date referitoare la comportamentul consumatorilor, pot fi localizate geografic. Odată cu evoluția tehnologică rapidă și utilizarea pe scară largă a dispozitivelor mobile inteligente, se dezvoltă o nouă categorie de servicii bazate pe localizare.

Obiectivul prezentului aviz este clarificarea cadrului juridic aplicabil serviciilor de localizare geografică încorporate în și/sau generate de dispozitive mobile inteligente care se pot conecta la internet și sunt echipate cu senzori sensibili de localizare, cum ar fi GPS-ul. De exemplu, astfel de servicii sunt: hărți și navigație, servicii geografice personalizate (inclusiv puncte de interes aflate în apropiere), realitate augmentată, marcarea geografică a conținutului pe internet, urmărirea locului în care se află prietenii, controlul copiilor și publicitatea bazată pe localizare.

De asemenea, prezentul aviz abordează principalele trei tipuri de infrastructură utilizată pentru furnizarea de servicii de localizare geografică, și anume GPS, stațiile de bază GSM și WiFi. Se acordă o atenție specială noii infrastructuri bazate pe localizarea punctelor de acces WiFi.

Grupul de lucru este pe deplin conștient de faptul că există numeroase alte servicii care prelucrează date de localizare care pot, de asemenea, să ridice probleme în ceea ce privește protecția datelor. Acestea variază de la sistemele de emitere electronică a biletelor, până la sistemele de taxare a autovehiculelor și de la sistemele de navigație prin satelit, până la serviciile de localizare și urmărire, de exemplu, cu ajutorul aparatelor foto, și localizarea geografică a adreselor IP. Cu toate acestea, ținând seama de evoluția tehnologică rapidă în ceea ce privește, în special, cartografierea punctelor de acces fără fir, la care se adaugă faptul că noii intrați pe piață se pregătesc să dezvolte noi servicii bazate pe localizare care utilizează o combinație de date ale stației de bază, date GPS și date WiFi, grupul de lucru a decis să clarifice în mod specific cerințele juridice aplicabile acestor servicii, în temeiul Directivei privind protecția datelor.

În primul rând, avizul descrie tehnologia, ulterior identifică și evaluează riscurile la adresa vieții private și apoi trage concluzii cu privire la aplicarea articolelor legale relevante pentru diferiții operatori care colectează și prelucrează date de localizare derivate din dispozitive mobile. Printre acești operatori se numără, de exemplu, furnizorii de infrastructură de localizare geografică, producătorii de telefoane inteligente și dezvoltatorii aplicațiilor bazate pe localizare geografică.

Prezentul aviz nu va evalua tehnologia specifică de marcare geografică legată de așa-numitul web 2.0, prin intermediul căreia utilizatorii integrează informații cu referință geografică în rețele de socializare, cum ar fi Facebook sau Twitter. De asemenea, prezentul aviz nu va intra în detalii cu privire la alte tehnologii de localizare geografică folosite pentru interconectarea dispozitivelor pe o suprafață relativ mică (centre comerciale, aeroporturi, clădiri de birouri etc.), cum ar fi Bluetooth, ZigBee, perimetraj geografic și etichete RFID bazate pe WiFi, deși multe dintre concluziile prezentului aviz cu privire la motivul legitim, informații și drepturile persoanelor vizate se aplică, de asemenea, în cazul în care aceste tehnologii sunt utilizate pentru localizarea geografică a persoanelor, prin intermediul dispozitivelor lor.

2. Context: diferite infrastructuri de localizare geografică

2.1 Datele stației de bază

Domeniul acoperit de diferiții operatori de telecomunicații este împărțit în zone care sunt cunoscute în general sub denumirea de celule. Pentru a putea folosi telefonul mobil sau a se conecta la internet utilizând comunicarea 3G, dispozitivul mobil trebuie să se conecteze la antena (denumită în continuare: „stația de bază”) care acoperă celula respectivă. Celulele acoperă zone de diferite dimensiuni, în funcție de interferența cu, de exemplu, munți și clădiri înalte.

Tot timpul cât este pornit, dispozitivul mobil este conectat la o anumită stație de bază. Operatorul de telecomunicații înregistrează în permanență aceste conexiuni. Fiecare stație de bază are un ID unic și este înregistrată cu o anumită locație. Atât operatorii de telecomunicații, cât și multe dispozitive mobile sunt în măsură să folosească semnalele provenite de la celule care se suprapun (stații de bază învecinate) pentru a estima poziția dispozitivului mobil cu precizie sporită. Această tehnică se mai numește triangulație.

Gradul de precizie poate fi sporit în continuare cu ajutorul informațiilor, cum ar fi RSSI (indicatorul intensității semnalului primit), TDOA (diferența de timp de sosire) și AOA (unghi de sosire).

Datele stației de bază pot fi folosite în moduri inovatoare, de exemplu pentru a detecta blocajele de trafic. Fiecare cale rutieră are o viteză medie pentru fiecare segment al zilei, dar atunci când transferul către următoarea stație de bază durează mai mult decât se preconizase, există, aparent, un blocaj de trafic.

Pe scurt, această metodă de poziționare indică locația în mod rapid și general, dar nu foarte precis, comparativ cu datele GPS și datele WiFi. Precizia este de aproximativ 50 de metri în zonele urbane dens populate, dar de până la câțiva kilometri în zonele rurale.

2.2 Tehnologia GPS

Dispozitivele mobile inteligente dispun de circuite integrate cu receptori GPS care determină locația lor.

Tehnologia GPS (sistem de poziționare globală) utilizează 31 de sateliți care se rotesc pe 6 orbite diferite în jurul Pământului[1]. Fiecare satelit transmite un semnal radio foarte precis.

Dispozitivul mobil poate determina locația sa atunci când senzorul GPS captează cel puțin 4 dintre aceste semnale. Diferit de datele stației de bază, semnalul este doar unidirecțional. Entitățile care gestionează sateliții nu pot ține evidența dispozitivelor care au recepționat semnalul radio.

Tehnologia GPS furnizează o poziționare precisă, între 4 și 15 metri. Dezavantajul major al sistemului GPS este acela că pornește relativ lent[2]. Un alt dezavantaj este acela că nu funcționează sau nu funcționează bine în spații închise. Prin urmare, în practică, tehnologia GPS este adesea combinată cu datele stației de bază și/sau cu punctele de acces WiFi cartografiate.

2.3 WiFi

2.3.1 Puncte de acces WiFi

O sursă relativ nouă de informații cu privire la localizarea geografică o reprezintă utilizarea punctelor de acces Wifi. Tehnologia este similară utilizării stațiilor de bază. Ambele se bazează pe un ID unic (provenit de la stația de bază sau de la punctul de acces WiFi) care poate fi detectat de un dispozitiv mobil și trimis unui serviciu care are o locație pentru fiecare ID unic.

ID-ul unic pentru fiecare punct de acces WiFi este adresa sa MAC (controlul accesului la mediu). O adresă MAC este un identificator unic atribuit unei interfețe de rețea și înregistrat, de obicei, în componente hardware, cum ar fi

---

1 Sistemul de poziționare globală este format din sateliți lansați de Statele Unite ale Americii, în scopuri militare. Până în 2014, Comisia Europeană intenționează să lanseze Galileo, o rețea formată din 18 sateliți care vor oferi o poziționare globală prin satelit gratuită și fără caracter militar. Primii 2 sateliți urmează să fie lansați în 2011, iar alți 2 în 2012. Sursa: Comisia Europeană, „Comisia prezintă o analiză intermediară a programului Galileo și EGNOS ", 25 ianuarie 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835

2 Pentru a accelera detectarea inițială a semnalului GPS, este posibil să se încarce în prealabil așa-numitele tabele curcubeu, care conțin poziționarea preconizată a diferiților sateliți în următoarele săptămâni.

cipuri de memorie și/sau carduri de rețea în calculatoare, telefoane, laptopuri sau puncte de acces[3].

Punctele de acces WiFi pot fi folosite ca sursă de informații cu privire la localizarea geografică deoarece acestea își anunță existența în mod continuu. Majoritatea punctelor de acces la internet în bandă largă au implicit și o antenă WiFi. Parametrii impliciți ai punctelor de acces utilizate cel mai frecvent în Europa au activată această conexiune și atunci când utilizatorul și-a conectat calculatorul (calculatoarele) la punctele de acces numai prin intermediul cablurilor. Comparabil cu un radio, punctul de acces WiFi transmite în mod continuu numele propriei sale rețele și adresa sa MAC, chiar dacă nimeni nu utilizează conexiunea și chiar și în cazul în care conținuturile comunicațiilor fără fir sunt criptate prin WEP, WPA sau WPA2.

Există două modalități diferite de colectare a adreselor MAC ale punctelor de acces WiFi[4]:

1. scanare activă: se trimit cereri active[5] către toate punctele de acces WiFi din apropiere și se înregistrează răspunsurile. Aceste răspunsuri nu includ informații cu privire la dispozitivele conectate la punctul de acces WiFi.

2. scanare pasivă: înregistrarea cadrelor-baliză transmise periodic de fiecare punct de acces (de obicei, de 10 ori pe secundă). Ca o alternativă care nu are un caracter standard, unele instrumente înregistrează, într-un mod mai general, toate cadrele WiFi transmise de punctele de acces, inclusiv cele care nu emit semnale-baliză. În cazul în care acest tip de scanare este efectuat fără a se lua în considerare în mod corespunzător viața privată începând cu momentul conceperii, acest tip de scanare poate duce la colectarea de date care au făcut obiectul unui schimb între punctele de acces și dispozitivele conectate la acestea. Astfel, adresele MAC ale calculatoarelor de birou, laptopurilor și imprimantelor ar putea fi înregistrate. De asemenea, acest tip de scanare ar putea conduce la înregistrarea ilegală a conținuturilor comunicațiilor. Aceste conținuturi sunt ușor de citit în cazul în care proprietarul punctului de acces WiFi nu a activat criptarea WiFi (WEP/WPA/WPA2).

Locația unui punct de acces WiFi poate fi calculată în două moduri diferite.

1. static/o singură dată: operatorii înșiși colectează adresele MAC ale punctelor de acces WiFi, deplasându-se în zonă cu vehicule echipate cu antene. Aceștia înregistrează latitudinea și longitudinea exacte ale vehiculului în momentul receptării semnalului și sunt în măsură să calculeze locația punctelor de acces pe baza, printre altele, a puterii semnalului.

---

3 Un exemplu de adresă MAC este următorul: 00-1F-3F-D7-3C-58. Adresa MAC a unui punct de acces WiFi se numește BSSID (identificator al setului de servicii de bază).

4 Scanarea activă și pasivă au fost reglementate prin standardul IEEE 802.11 pentru a detecta punctele de acces.

5 Pentru a obține adresele MAC, colectorul trimite o „cerere de probă” tuturor punctelor de acces.

2. dinamic/în curs: utilizatorii serviciilor de localizare geografică colectează în mod automat adresele MAC captate de dispozitivele lor cu funcție WiFi atunci când utilizează, de exemplu, o hartă online pentru a-și determina propria poziție (Unde mă aflu?). În acest caz, dispozitivul mobil transmite toate informațiile disponibile furnizorului de servicii de localizare geografică, inclusiv adresele MAC, SSID-urile și intensitatea semnalului. Operatorul poate utiliza aceste observații în curs pentru a calcula și/sau a îmbunătăți locațiile punctelor de acces WiFi din baza sa de date cu puncte de acces WiFi cartografiate.

Este important de remarcat că dispozitivele mobile nu trebuie să se „conecteze" la puncte de acces WiFi pentru a colecta informații WiFi. Dispozitivele mobile detectează automat prezența punctelor de acces (în mod de scanare activă sau pasivă) și colectează automat date cu privire la acestea.

În plus, telefoanele mobile care solicită să fie localizate geografic vor trimite nu numai date WiFi, ci și, adesea, orice alte informații cu privire la locație pe care le dețin, inclusiv date GPS și date ale stației de bază. Aceasta permite furnizorului să calculeze locația „noilor" puncte de acces WiFi și/sau să îmbunătățească locațiile punctelor de acces WiFi care au fost deja incluse în baza de date. Astfel, colectarea de informații cu privire la punctele de acces WiFi este descentralizată în mod foarte eficient, fără ca, în mod necesar, consumatorii să cunoască acest fapt.

Pe scurt: localizarea geografică bazată pe puncte de acces WiFi furnizează rapid o poziție, care, pe baza măsurătorilor continue, este din ce în ce mai precisă.

3. Riscuri la adresa vieții private

Un dispozitiv mobil inteligent este foarte strâns legat de o anumită persoană. Majoritatea oamenilor au tendința să își păstreze dispozitivele mobile foarte aproape de înșiși, în buzunar, în geantă sau pe noptiera de lângă pat.

Rareori se întâmplă ca cineva să împrumute un astfel de dispozitiv altcuiva. Majoritatea persoanelor cunosc faptul că dispozitivul mobil conține o serie de informații foarte intime, variind de la e-mail, până la poze personale, de la istoricul navigației pe internet până la, de exemplu, o listă de adrese de contact.

Aceasta permite furnizorilor de servicii bazate pe localizare geografică să aibă o imagine de ansamblu detaliată asupra obiceiurilor și modelului comportamental ale proprietarului unui astfel de dispozitiv și să creeze profiluri exhaustive. Pornind de la modelul inactivității pe timp de noapte, se poate deduce locul unde doarme cineva, iar pornind de la modelul deplasărilor frecvente dimineața, se poate deduce locația unui angajator. De asemenea, modelul poate să includă date derivate din caracteristicile de deplasare ale prietenilor, bazate pe așa-numitele *grafice sociale*[6].

[6] „Grafic social" este un termen care indică vizibilitatea prietenilor în site-urile de socializare în rețea și capacitatea de a deduce trăsături comportamentale din datele referitoare la acești prieteni.

De asemenea, un model comportamental poate să includă *categorii speciale de date*, în cazul în care dezvăluie, de exemplu, vizite la spitale și locuri de cult, prezența la demonstrații politice sau prezența în alte locații specifice care dezvăluie date cu privire la, de exemplu, viața sexuală. Aceste profile pot fi utilizate pentru a lua decizii care îl afectează în mod semnificativ pe proprietar.

Tehnologia dispozitivelor mobile inteligente permite monitorizarea constantă a datelor de localizare. Telefoanele inteligente pot colecta în permanență semnale provenite de la stații de bază și puncte de acces WiFi. Din punct de vedere tehnic, monitorizarea poate fi efectuată în secret, fără informarea proprietarului. De asemenea, monitorizarea poate fi efectuată în semisecret, în cazul în care persoanele „uită" sau nu sunt informate în mod corespunzător că serviciile de localizare sunt activate sau în cazul în care parametrii de accesibilitate a datelor de localizare sunt modificați din modul „privat" în cel „public ".

Chiar și atunci când persoanele își pun în mod intenționat la dispoziție pe internet datele lor de localizare geografică, prin intermediul serviciilor aferente locului în care se află și de marcare geografică, accesul global nelimitat generează noi riscuri, variind de la furtul de date, până la tâlhărie și chiar agresiuni fizice și urmărire în scopul hărțuirii.

Ca și în cazul altor tehnologii noi, un risc major al utilizării datelor de localizare este denaturarea funcției, și anume faptul că pe baza disponibilității unui nou tip de date, sunt dezvoltate scopuri noi, care nu au fost anticipate în momentul colectării inițiale a datelor.

4. Cadrul juridic

Temeiul juridic relevant este Directiva privind protecția datelor (95/46/CE). Aceasta se aplică în toate cazurile în care datele cu caracter personal sunt prelucrate, ca urmare a prelucrării datelor de localizare. Directiva asupra confidențialității și comunicațiilor electronice (2002/58/CE, astfel cum a fost rectificată prin Directiva 2009/136/CE) se aplică numai în ceea ce privește prelucrarea datelor stației de bază de către serviciile și rețelele de comunicații electronice publice (operatori de telecomunicații).

4.1 Datele stației de bază prelucrate de către operatorii de telecomunicații

Operatorii de telecomunicații prelucrează în mod continuu datele stației de bază în cadrul furnizării serviciilor de comunicații electronice publice[7]. De asemenea, aceștia pot prelucra datele stației de bază pentru a furniza servicii cu valoare adăugată. Acest caz a fost deja abordat de grupul de lucru în Avizul 5/2005 (WP115). Deși unele exemple din aviz sunt, inevitabil, depășite datorită difuzării tehnologiei internet și încorporării de senzori în dispozitive de dimensiuni tot mai mici, concluziile juridice și recomandările avizului menționat rămân valabile în ceea ce privește utilizarea datelor stației de bază.

[7] A se observa că punerea la dispoziție de hotspoturi WiFi publice de către furnizorii de telecomunicații este considerată, de asemenea, un serviciu de comunicații electronice publice și, prin urmare, ar trebui să respecte în primul rând prevederile Directivei asupra confidențialității și comunicațiilor electronice.

1. Deoarece datele de localizare derivate din staţiile de bază se referă la o persoană fizică identificată sau identificabilă, acestea fac obiectul dispoziţiilor privind protecţia datelor cu caracter personal prevăzute în Directiva 95/46/CE din 24 octombrie 1995.
2. Directiva 2002/58/CE din 12 iulie 2002 (astfel cum a fost revizuită în noiembrie 2009 în Directiva 2009/136/CE) se aplică, de asemenea, în conformitate cu definiţia prevăzută la articolul 2 litera (c) din această directivă:
   „date de localizare" înseamnă orice date prelucrate într-o reţea de comunicaţii electronice sau prin intermediul unui serviciu de comunicaţii electronice, care indică poziţia geografică a echipamentului terminal al unui utilizator al unui serviciu de comunicaţii electronice destinat publicului.

În cazul în care un operator de telecomunicaţii oferă un serviciu hibrid de localizare geografică, bazat şi pe prelucrarea altor tipuri de date de localizare, cum ar fi date GPS sau date WiFi, această activitate poate fi considerată un serviciu de comunicaţii electronice publice. Operatorul de telecomunicaţii trebuie să obţină consimţământul prealabil al clienţilor săi în cazul în care acesta furnizează datele de localizare geografică unui terţ.

4.2 Datele staţiei de bază, datele WiFi şi datele GPS prelucrate de către furnizorii de servicii ale societăţii informaţionale

4.2.1 Aplicabilitatea Directivei revizuite asupra confidenţialităţii şi comunicaţiilor electronice

În general, societăţile care furnizează servicii şi aplicaţii de localizare bazate pe o combinaţie de date ale staţiei de bază, date GPS şi date WiFi sunt *servicii ale societăţii informaţionale*. Ca atare, acestea sunt excluse în mod explicit din domeniul de aplicare al Directivei asupra confidenţialităţii şi comunicaţiilor electronice, în temeiul definiţiei stricte a serviciului de comunicaţii electronice [articolul 2 litera (c) din directiva-cadru revizuită (nemodificat)][8].

Directiva asupra confidenţialităţii şi comunicaţiilor electronice nu se aplică prelucrării datelor de localizare de către serviciile societăţii informaţionale, chiar şi în cazul în care această prelucrare este efectuată prin intermediul unei reţele de comunicaţii electronice publice. Un utilizator poate alege să transmită date GPS prin internet, de exemplu atunci când accesează servicii de navigare pe internet. În acest caz, semnalul GPS este transmis la nivelul de aplicaţie al comunicaţiei

[8] Directiva 2002/21/CE din 7 martie 2002, articolul 2 litera (c):*„serviciu de comunicaţii electronice" înseamnă serviciul furnizat de obicei contra cost şi care constă în totalitate sau în principal în transmiterea de semnale prin reţele de comunicaţii electronice, inclusiv serviciile de telecomunicaţii şi serviciile de transmisie prin reţele utilizate pentru radiodifuziune, dar nu şi servicii care constau din furnizarea de conţinuturi prin intermediul reţelelor şi serviciilor de comunicaţii electronice; nu include serviciile societăţii informaţionale astfel cum sunt acestea definite la articolul 1 din Directiva 98/34/CE care nu constau în întregime sau în principal în transmiterea de semnale prin reţele de comunicaţii electronice.*

internet, independent de rețeaua GSM. Furnizorul de servicii de telecomunicații acționează ca un simplu transmițător. Acesta nu poate avea acces la datele GPS și/sau datele WiFi și/sau datele stației de bază comunicate către și provenite de la un dispozitiv mobil inteligent între un utilizator/abonat și un serviciu al societății informaționale fără mijloace foarte invazive, cum ar fi *verificarea în profunzime a pachetului*.

4.2.2 Aplicabilitatea Directivei privind protecția datelor

În cazul în care Directiva asupra confidențialității și comunicațiilor electronice nu se aplică, în conformitate cu articolul 1 alineatul (2), se aplică Directiva 95/46/CE: *„Prevederile prezentei directive precizează și completează Directiva 95/46/CE în scopurile menționate la alineatul (1).”*

În temeiul Directivei privind protecția datelor cu caracter personal, date cu caracter personal înseamnă *orice informație referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale* – articolul 2 litera (a) din directivă.

Considerentul 26 din directivă acordă o atenție specială termenului „identificabil” atunci când prevede că *„întrucât principiile protecției trebuie să se aplice oricărei informații privind o persoană identificată sau identificabilă; întrucât, pentru a determina dacă o persoană este identificabilă este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată.”*

Considerentul 27 din directivă subliniază domeniul larg de aplicare al protecției: *„întrucât sfera protecției în cauză nu trebuie să depindă în fapt de tehnicile utilizate, în caz contrar creându-se un risc serios de eludare a dispozițiilor”*.

În avizul său 4/2007 privind conceptul de date cu caracter personal, grupul de lucru a furnizat orientări exhaustive privind definirea datelor cu caracter personal.

Dispozitive mobile inteligente

Dispozitivele mobile inteligente sunt strâns legate de persoanele fizice. De obicei, identificarea poate avea un caracter direct sau indirect.

În primul rând, operatorul de telecomunicații care furnizează telefonie mobilă și acces mobil la internet are, de obicei, un registru cu numele, adresa și detaliile bancare ale fiecărui client, în combinație cu mai multe numere unice ale dispozitivului, cum ar fi IMEI și IMSI.

În al doilea rând, achiziționarea de programe informatice suplimentare pentru dispozitiv (*aplicații* sau *apps*), necesită, de obicei, un număr de carte de credit și, prin aceasta, îmbogățește combinația numărului (numerelor) unic(e) și a datelor de localizare cu datele de identificare directă.

Identificarea indirectă poate fi obținută prin combinarea numărului (numerelor) unic(e) al (ale) dispozitivului, în combinație cu una sau mai multe locații calculate.

Fiecare dispozitiv mobil inteligent are cel puțin un identificator unic, adresa MAC. Dispozitivul poate avea alte numere de identificare unice, adăugate de către dezvoltatorul sistemului de operare. Acești identificatori pot fi transmiși și prelucrați ulterior în contextul unor servicii de localizare geografică. Este o realitate faptul că locația unui anumit dispozitiv poate fi calculată într-un mod foarte precis, în special atunci când se combină diferite infrastructuri de localizare geografică. O astfel de localizare poate indica o casă sau un angajator. Este posibil să se identifice proprietarul dispozitivului, în special prin observații repetate.

Atunci când se iau în considerare mijloacele disponibile de identificare, trebuie să se țină seama de evoluția conform căreia persoanele au tendința să divulge tot mai multe date de localizare personală pe internet, de exemplu prin postarea locației casei lor sau a locului lor de muncă în combinație cu alte date de identificare. De asemenea, o astfel de divulgare se poate efectua fără ca cei vizați să ia cunoștință de aceasta, în cazul în care au fost marcați geografic de alte persoane. Această dezvoltare facilitează stabilirea unei legături între o locație sau un model comportamental și o anumită persoană.

În plus, conform Avizului 4/2007 privind conceptul de date cu caracter personal, ar trebui să se observe, de asemenea, că un identificator unic, în contextul descris anterior, permite urmărirea utilizatorului unui dispozitiv specific și, astfel, îi permite utilizatorului să fie „evidențiat", chiar și în cazul în care numele real al acestuia nu este cunoscut.

Puncte de acces WiFi
Această identificare indirectă se aplică și punctelor de acces WiFi[9]. Adresa MAC a unui punct de acces WiFi, în combinație cu locația sa calculată, este strâns legată de locația proprietarului punctului de acces.

Un operator echipat în mod rezonabil poate calcula o locație din ce în ce mai precisă a unui punct de acces WiFi, pe baza intensității semnalului și a actualizărilor în curs ale locației prin intermediul utilizatorilor serviciilor sale de localizare geografică.

Cu ajutorul acestor resurse, în multe cazuri, se poate identifica un grup mic de apartamente sau de case în care locuiește proprietarul punctului de acces. Ușurința cu care este posibil să se identifice acest proprietar al adresei MAC va depinde de mediu:

- în zonele puțin populate, în cazul în care adresa MAC indică o singură casă, proprietarul reședinței poate fi identificat direct cu instrumente cum ar fi, de exemplu, registre cadastrale, anuare telefonice, registre electorale sau chiar un simplu motor de căutare[10];

[9] Punctele de acces WiFi pot fi chiar direct identificabile, în cazul în care furnizorul de acces la internet are un registru cu adresele MAC ale routerelor WiFi pe care le furnizează clienților săi identificați.

[10] Disponibilitatea acestor registre sau anuare variază în funcție de stat membru.

- în zonele mai dens populate, cu ajutorul unor resurse cum ar fi ,de exemplu, intensitatea semnalului și/sau SSID (pe care orice persoană care are un dispozitiv WiFi le pot detecta), este posibil să se determine locația exactă a punctului de acces și astfel, în numeroase cazuri, să se stabilească identitatea persoanei (persoanelor) care locuiește (locuiesc) în locul exact (casă sau apartament) în care se află punctul de acces;
- în zonele foarte dens populate, chiar și cu ajutorul informațiilor privind intensitatea semnalului, adresa MAC va indica mai multe apartamente ca locație potențială a punctului de acces. În aceste circumstanțe, nu este posibil să se identifice cu exactitate, fără un efort nerezonabil, persoana care locuiește în apartamentul în care se află punctul de acces.

Faptul că, în unele cazuri, proprietarul unui dispozitiv nu poate fi identificat fără un efort nerezonabil, nu împiedică ajungerea la concluzia generală potrivit căreia combinația adresei MAC a unui punct de acces WiFi cu locația sa calculată ar trebui să fie asimilată datelor cu caracter personal.

În aceste condiții și având în vedere faptul că este puțin probabil ca operatorul de date să poată face o distincție între cazurile în care proprietarul unui punct de acces WiFi este identificabil și cele în care acesta nu este identificabil, operatorul de date ar trebui să trateze toate datele cu privire la routerele WiFi ca date cu caracter personal.

Este important de reamintit că nu este necesar ca scopul prelucrării acestor date de localizare geografică să fie identificarea utilizatorilor. În foarte mare măsură, identificarea proprietarilor punctelor de acces WiFi necesită sau nu un efort nerezonabil în funcție de posibilitățile tehnice în materie ale operatorului sau ale oricărei alte persoane.

5. Obligații în temeiul legislației privind protecția datelor

5.1 Operatorul de date

În contextul serviciilor online de localizare geografică furnizate de serviciile societății informaționale, se pot distinge trei funcții diferite, cu responsabilități diferite în ceea ce privește prelucrarea datelor cu caracter personal. Acestea sunt: operator al infrastructurii de localizare geografică, furnizor al unei anumite aplicații sau al unui anumit serviciu de localizare geografică și dezvoltator al sistemului de operare al unui dispozitiv mobil inteligent. În practică, societățile îndeplinesc adesea mai multe roluri în același timp, de exemplu atunci când combină un sistem de operare cu o bază de date cu puncte de acces WiFi cartografiate și o platformă de publicitate.

5.1.1 Operatorii infrastructurii de localizare geografică

Ca și operatorii de telecomunicații atunci când prelucrează locația unui anumit dispozitiv cu ajutorul stațiilor lor de bază, proprietarii bazelor de date cu puncte de

acces WiFi cartografiate prelucrează date cu caracter personal atunci când calculează locația unui anumit dispozitiv mobil inteligent. Deoarece ambii stabilesc scopurile și mijloacele prelucrării respective, aceștia sunt operatori, astfel cum sunt definiți la articolul 2 litera (d) din Directiva privind protecția datelor.

Este important să se sublinieze că dispozitivul specific este esențial în calcularea locației sale, transmițând către proprietarul bazei de date propriile sale date de localizare (adesea o combinație de date GPS, date WiFi și date ale stației de bază) și ID-urile unice ale punctelor de acces WiFi din apropiere[11]. De asemenea, un astfel de dispozitiv îndeplinește criteriile prevăzute la articolul 4 alineatul (1) litera (c) din Directiva privind protecția datelor, *echipament situat pe teritoriul unui stat membru*.

Deoarece adresa MAC a unui punct de acces WiFi, în combinație cu locația sa calculată, ar trebui să fie asimilată datelor cu caracter personal, colectarea acestor date înseamnă, de asemenea, prelucrare a datelor cu caracter personal. Indiferent de modul în care aceste date sunt colectate (o singură dată sau în mod continuu), proprietarul unei astfel de baze de date ar trebui să respecte obligațiile care decurg din Directiva privind protecția datelor.

5.1.2 Furnizorii de aplicații și servicii de localizare geografică

Dispozitivele mobile inteligente permit instalarea de software de la terți, așa-numitele *aplicații*. Astfel de aplicații pot prelucra datele de localizare (și alte date) provenite de la un dispozitiv mobil inteligent, independent de dezvoltatorul sistemului de operare și/sau de operatorii infrastructurii de localizare geografică.

Exemple de astfel de servicii sunt: un serviciu de previziuni meteorologice cu privire la șansele de ploaie în următoarele câteva ore într-o regiune foarte precisă, un serviciu care oferă informații referitoare la magazine din apropiere, un serviciu de identificare a unui telefon pierdut sau un serviciu care indică locația prietenilor.

Furnizorul unei aplicații care poate prelucra date de localizare geografică este operatorul responsabil de prelucrarea datelor cu caracter personal care rezultă din instalarea și utilizarea aplicației.

Bineînțeles, nu este necesar să se instaleze întotdeauna programe informatice separate pe un dispozitiv mobil inteligent. Multe servicii de localizare geografică pot fi accesate și prin intermediul unui browser. Un exemplu de astfel de serviciu este utilizarea unei hărți online pentru orientarea unei persoane care se deplasează într-un oraș.

5.1.3 Dezvoltatorul sistemului de operare

[11] Dispozitivul mobil poate transmite operatorului diferitele date de localizare geografică pe care le primește pentru calcularea locației sale sau își calculează singur locația. În ambele cazuri, dispozitivul este un echipament esențial pentru prelucrare.

Dezvoltatorul sistemului de operare al dispozitivului mobil inteligent poate fi un operator responsabil de prelucrarea datelor de localizare geografică atunci când acesta interacționează direct cu utilizatorul și colectează date cu caracter personal (cum ar fi cerința de înregistrare a utilizatorului inițial și/sau colectarea informațiilor cu privire la locație în scopul îmbunătățirii serviciilor). Ca operator, dezvoltatorul trebuie să aplice principiile luării în considerare a vieții private începând cu momentul conceperii pentru prevenirea monitorizării secrete, fie de către dispozitivul în sine, fie de către diferite aplicații și servicii.

Dezvoltatorul este, de asemenea, operatorul datelor pe care le prelucrează, dacă dispozitivul are o funcție „telefon acasă" pentru domiciliul proprietarului său. Deoarece în acest caz dezvoltatorul decide cu privire la mijloacele și scopurile unui astfel de flux de date, acesta este operatorul responsabil de prelucrarea datelor respective. Un exemplu obișnuit de o astfel de funcție „telefon acasă" este furnizarea automată a actualizării fusului orar pe baza locației.

În al treilea rând, dezvoltatorul este un operator în cazul în care acesta oferă o platformă de publicitate și/sau un mediu de comercializare online a aplicațiilor și poate prelucra datele cu caracter personal care rezultă din (instalarea și utilizarea) aplicațiilor de localizare geografică, independent de furnizorii de aplicații.

5.2 Responsabilitățile altor părți

Există multe alte părți online care permit prelucrarea (ulterioară) a datelor de localizare, cum ar fi browsere, site-uri de socializare în rețea sau mijloace de comunicare care permit, de exemplu, „marcarea geografică". Atunci când în platforma acestora sunt integrate funcții de localizare geografică, acestea au responsabilitatea importantă de a decide cu privire la parametrii impliciți ai aplicației (activare sau dezactivare implicită). Cu toate că sunt doar operatori în măsura în care prelucrează ele însele în mod activ date cu caracter personal, acestea au un rol-cheie în legitimarea prelucrării datelor de către operatori, cum ar fi furnizorii de aplicații specifice, de exemplu în ceea ce privește vizibilitatea și calitatea informațiilor referitoare la prelucrarea datelor de localizare geografică.

5.3 Motivul legitim

5.3.1 Dispozitive mobile inteligente

În cazul în care operatorii de telecomunicații doresc să folosească datele stației de bază pentru a furniza unui client un serviciu cu valoare adăugată, în conformitate cu Directiva revizuită asupra confidențialității și comunicațiilor electronice, aceștia trebuie să obțină consimțământul prealabil al acestuia. De asemenea, aceștia trebuie să se asigure că clientul este informat cu privire la termenii unei astfel de prelucrări.

Luând în considerare caracterul sensibil al prelucrării (modelelor) datelor de localizare, *consimțământul prealabil în cunoștință de cauză* este, de asemenea, principalul motiv pentru legitimarea prelucrării datelor în ceea ce privește

prelucrarea locațiilor unui dispozitiv mobil inteligent în contextul serviciilor societății informaționale.

În conformitate cu articolul 2 litera (h) din Directiva privind protecția datelor, consimțământul trebuie să fie o manifestare de voință, liberă, specifică și informată a dorinței persoanei vizate.

În funcție de tipul de tehnologie utilizat, dispozitivul utilizatorului joacă un rol relativ activ în prelucrarea datelor privind poziția geografică. Dispozitivul este în măsură să transmită date de localizare provenite din surse diferite către orice terț. Această capacitate tehnică nu ar trebui să fie confundată cu legalitatea unei astfel de prelucrări a datelor. Dacă parametrii impliciți ai unui sistem de operare ar permite transmiterea datelor de localizare, lipsa de intervenție din partea utilizatorilor săi nu ar trebui să fie confundată cu consimțământul acordat în mod liber.

În măsura în care prelucrează ei înșiși în mod activ date de localizare geografică (de exemplu, atunci când au acces la informații cu privire la localizare provenite de la dispozitiv sau obținute prin intermediul acestuia), dezvoltatorii sistemelor de operare și alte servicii ale societății informaționale trebuie, de asemenea, să obțină consimțământul prealabil în cunoștință de cauză al utilizatorilor acestora. Trebuie să fie clar că un astfel de consimțământ nu poate fi obținut în mod liber nici prin acceptarea obligatorie a termenilor și a condițiilor cu caracter general, nici prin posibilitățile de renunțare. Serviciile de localizare ar trebui să fie implicit dezactivate, utilizatorii putând consimți să activeze în mod separat fiecare din aplicațiile specifice.

Consimțământul angajaților

Consimțământul ca motiv legitim pentru prelucrare este problematic în contextul angajării. În avizul său cu privire la prelucrarea datelor cu caracter personal în contextul angajării, grupul de lucru scria: „*în cazul în care consimțământul unui lucrător este necesar și eventualul refuz al acordării acestuia generează un prejudiciu relevant, real sau potențial, consimțământul nu este valabil și nu îndeplinește prevederile de la articolul 7 sau articolul 8 deoarece nu este acordat în mod liber. Dacă nu este posibil ca lucrătorul să refuze, acesta nu este un consimțământ. (...) Un caz dificil este acela în care acordarea consimțământului reprezintă o condiție de angajare. Teoretic, lucrătorul este în măsură să refuze acordarea consimțământului, dar consecința acestui fapt poate fi pierderea unui loc de muncă. În astfel de circumstanțe, consimțământul nu este acordat în mod liber și, prin urmare, nu este valabil.*”[12] În loc să solicite consimțământul, angajatorii trebuie să investigheze dacă este necesar în mod demonstrabil să supravegheze locațiile exacte ale angajaților într-un scop legitim și să cântărească această necesitate în raport cu drepturile și libertățile fundamentale ale angajaților. În cazurile în care necesitatea poate fi justificată în mod corespunzător, temeiul juridic al unei astfel de prelucrări s-ar putea baza pe interesul legitim al operatorului [articolul 7 litera (f) din Directiva privind protecția datelor]. Angajatorul trebuie să caute întotdeauna mijloace cât mai puțin intruzive, să evite monitorizarea continuă și, de exemplu, să aleagă un sistem care transmite o alertă

[12] WP48, Avizul 8/2001 privind prelucrarea datelor cu caracter personal în contextul angajării.

atunci când un angajat trece o frontieră virtuală prestabilită. Un angajat trebuie să poată dezactiva orice dispozitiv de monitorizare în afara orelor de serviciu și trebuie să i se arate cum să facă acest lucru. Dispozitivele de urmărire a vehiculelor nu sunt instrumente de urmărire a personalului. Funcția acestora este să urmărească sau să monitorizeze locația vehiculelor în care sunt instalate. Angajatorii nu ar trebui să le considere drept dispozitive de urmărire sau de monitorizare a comportamentului șoferilor sau a locului în care se află aceștia ori alți membri ai personalului, de exemplu, prin transmiterea de alerte în legătură cu viteza vehiculului.

Consimțământul copiilor

În unele cazuri, consimțământul copiilor trebuie să fie acordat de părinții lor sau de alți reprezentanți legali ai lor. Aceasta înseamnă, de exemplu, că furnizorul unei aplicații de localizare geografică trebuie să îi informeze pe părinți cu privire la colectarea și utilizarea datelor de localizare geografică provenite de la copii și să obțină consimțământul acestora înainte de colectarea și utilizarea ulterioară a informațiilor referitoare la copiii lor. Unele aplicații de localizare geografică sunt concepute în mod specific pentru supravegherea copiilor de către părinți, de exemplu, dezvăluind în permanență locațiile dispozitivului pe un site internet sau emițând o alertă în cazul în care dispozitivul părăsește teritoriul stabilit în prealabil. Utilizarea unor astfel de aplicații este problematică. În avizul său 2/2009[13] privind protecția datelor cu caracter personal ale copiilor, Grupul de lucru „articolul 29" scria: *„Niciodată, din motive de securitate, copiii nu trebuie să fie supuși unui nivel prea ridicat de supraveghere, care să le reducă autonomia. În acest context, trebuie să se ajungă la un echilibru între protecția intimității și a vieții private a copiilor și siguranța lor."*

Cadrul juridic prevede că părinții copiilor sunt responsabili de garantarea dreptului la viață privată al copiilor. Cel puțin, în cazul în care părinții consideră că utilizarea unei astfel de aplicații este justificată în circumstanțe specifice, copiii trebuie să fie informați și, de îndată ce acest lucru este posibil în mod rezonabil, să aibă permisiunea de a participa la decizia de a utiliza o astfel de aplicație.

Consimțământul trebuie să fie specific, pentru fiecare dintre diferitele scopuri în care sunt prelucrate datele. Operatorul trebuie să indice foarte clar dacă serviciul său se limitează la furnizarea unui răspuns la întrebarea intenționată „Unde mă aflu acum?" sau dacă scopul său este de a crea răspunsuri la întrebările „Unde te afli, unde ai fost și unde vei fi săptămâna viitoare?" Cu alte cuvinte, operatorul trebuie să acorde consimțământului o atenție specifică în cazul scopurilor la care persoanele vizate nu se așteaptă, cum ar fi, de exemplu, elaborarea de profile și/sau publicitatea comportamentală.

Dacă scopul prelucrării se modifică în mod substanțial, operatorul trebuie să solicite un consimțământ reînnoit specific. De exemplu, în cazul în care o societate a declarat inițial că nu va divulga date cu caracter personal unor terți, dar acum dorește să le divulge, aceasta trebuie să solicite consimțământul prealabil

[13] WP160, Avizul 2/2009 privind protecția datelor cu caracter personal ale copiilor (orientări generale și cazul special al școlilor).

activ al fiecărui client. Lipsa unui răspuns (sau orice alt tip de scenariu de renunțare) nu este suficientă.

Este important să se facă distincție între consimțământul în favoarea unui serviciu unic și consimțământul în favoarea unui abonament. De exemplu, în vederea utilizării unui anumit serviciu de localizare geografică, poate fi necesar să se activeze serviciile de localizare geografică ale dispozitivului sau ale browserului. În cazul în care capacitatea de localizare geografică este activată, fiecare site internet poate citi detaliile locației utilizatorului dispozitivului mobil inteligent respectiv. Pentru a preveni riscurile de monitorizare secretă, Grupul de lucru „articolul 29" consideră că este esențial ca dispozitivul să avertizeze în mod continuu că localizarea geografică este activată, de exemplu printr-un icon vizibil în mod permanent.

Grupul de lucru recomandă ca furnizorii de aplicații sau servicii de localizare geografică să reînnoiască consimțământul individual (chiar și în cazul în care nu există nicio modificare în ceea ce privește natura prelucrării), într-un termen corespunzător. De exemplu, nu ar fi adecvat să prelucreze în continuare date de localizare în cazul în care o persoană nu au utilizat în mod activ acest serviciu în ultimele 12 luni. Chiar și în cazul în care cineva a utilizat serviciul, ar trebui să i se reamintească cel puțin o dată pe an (sau mai des, în cazul în care natura prelucrării o justifică) natura prelucrării datelor sale cu caracter personal și ar trebui să i se prezinte un mijloc accesibil de renunțare la serviciul respectiv.

În cele din urmă, dar nu în ultimul rând, persoanele vizate trebuie să aibă posibilitatea de a-și retrage consimțământul foarte ușor, fără consecințe negative pentru utilizarea dispozitivului lor. Independent de directivele europene privind protecția datelor, Consorțiul World Wide Web (W3C) a elaborat un proiect de standard pentru localizarea geografică API care subliniază necesitatea unui consimțământ prealabil, expres și în cunoștință de cauză[14]. W3C explică în mod specific necesitatea de a respecta retragerea consimțământului, sfătuindu-i pe cei care pun în aplicare standardul să ia în considerare următoarele: *„conținutul găzduit de un anumit URL se modifică astfel încât permisiunea de localizare acordată anterior nu se mai aplică în ceea ce îl privește pe utilizator. Sau utilizatorii ar putea pur și simplu să se răzgândească."*

Exemplu de bune practici pentru furnizorii de aplicații de localizare geografică

O aplicație care dorește să utilizeze date de localizare geografică informează în mod clar utilizatorul cu privire la scopurile în care dorește să le folosească și solicită consimțământul neechivoc pentru fiecare dintre eventualele scopuri diferite. Utilizatorul alege în mod activ nivelul de detaliere al localizării geografice (de exemplu, la nivel de țară, de oraș, de cod poștal sau cât mai precis posibil). Odată ce serviciul de localizare este activat, un icon este vizibil în mod permanent pe fiecare ecran, indicând că serviciile de localizare sunt activate. Utilizatorul își poate retrage consimțământul în orice moment, fără a fi nevoit să părăsească aplicația. De asemenea, utilizatorul poate să șteargă cu ușurință și în mod permanent orice date de localizare stocate pe dispozitiv.

[14] Informații cu privire la standardul API de localizare geografică propus de W3C: http://www.w3.org/TR/geolocation-API

5.3.2 Puncte de acces WiFi

Pe baza Directivei privind protecția datelor, societățile pot avea un interes legitim în colectarea și prelucrarea cu caracter necesar ale adreselor MAC și ale locațiilor calculate ale punctelor de acces WiFi în scopul specific de a oferi servicii de localizare geografică.

Motivul legitim de la articolul 7 litera (f) din Directiva privind protecția datelor prevede un echilibru între interesele legitime ale operatorului și drepturile fundamentale ale persoanelor vizate. Luând în considerare natura semistatică a punctelor de acces WiFi, în principiu, cartografierea acestora constituie o amenințare mai mică la adresa vieții private a proprietarilor lor decât urmărirea în timp real a locațiilor dispozitivelor inteligente mobile.

Echilibrul dintre drepturile operatorilor și drepturile persoanelor vizate este dinamic. Pentru ca interesele legitime ale operatorilor să prevaleze cu succes în timp asupra intereselor persoanelor vizate, aceștia trebuie să dezvolte și să pună în aplicare garanții, cum ar fi dreptul de a renunța cu ușurință și în mod permanent la înscrierea în baza de date, fără a fi nevoie să se furnizeze date cu caracter personal suplimentare operatorului unei astfel de baze de date. Aceștia pot, de exemplu, să utilizeze programe informatice pentru a detecta în mod automat că o persoană este conectată la un punct de acces specific[15].

În plus, în scopul de a oferi servicii de localizare geografică, colectarea și prelucrarea SSID-urilor nu este necesară. Prin urmare, colectarea și prelucrarea SSID-urilor este excesivă atunci când se utilizează pentru a oferi servicii de localizare geografică pe baza cartografierii locației punctelor de acces WiFi.

5.4 Informații

Diferiții operatori trebuie să se asigure că proprietarii dispozitivului mobil inteligent sunt informați în mod corespunzător cu privire la principalele elemente ale prelucrării, în conformitate cu articolul 10 din Directiva privind protecția datelor, cum ar fi identitatea lor ca operatori, scopurile prelucrării datelor, tipul de date, durata prelucrării, drepturile persoanelor vizate de a accesa, a rectifica sau a anula datele lor și dreptul de a-și retrage consimțământul.

---

[15] O eventuală utilizare este următoarea:
1. O persoană vizată accesează o pagină de internet specifică, pe care poate introduce adresa MAC a punctului său de acces WiFi.
2. Dacă adresa MAC figurează în baza de date cu punctele de acces WiFi cartografiate, operatorul poate afișa o pagină de verificare care conține un text prin care se solicită tabelul ARP al instrumentului de conectare la internet. Teoretic, adresa MAC a rețelei WLAN poate fi afișată prin comanda „ARP -a". Cu ajutorul codului conținut de browser, cum ar fi Java, acest tabel ARP poate fi generat în fundal.
3. Dacă adresa MAC apare în tabelul ARP, se stabilește că utilizatorul conectat la WLAN este, de asemenea, cel care are acces la adresa MAC a rețelei WLAN locale. Astfel, operatorul verifică cererea de ștergere în mod automat și cu ușurință.

Valabilitatea consimțământului este strâns legată de calitatea informațiilor cu privire la serviciu. Informațiile trebuie să fie clare, complete, inteligibile pentru un public larg, fără cunoștințe tehnice și accesibile în mod permanent și cu ușurință.

Informațiile trebuie să vizeze un public larg. Operatorii nu pot prezuma că clienții lor sunt persoane cu abilități tehnice, doar pentru că aceştia dețin un dispozitiv mobil inteligent. Informațiile trebuie să fie adaptate în funcție de vârstă, în cazul în care operatorul știe că atrage un public tânăr.

În cazul în care furnizorii de aplicații de localizare geografică intenționează să calculeze locațiile unui dispozitiv mai mult de o singură dată, aceştia trebuie să își informeze clienții atât timp cât prelucrează date de localizare. De asemenea, aceştia trebuie să permită clienților lor să își dea în continuare consimțământul sau să și-l retragă. Pentru a atinge aceste obiective, furnizorii aplicațiilor ar trebui să colaboreze strâns cu dezvoltatorul sistemului de operare. Din punct de vedere tehnic, dezvoltatorul este cel mai în măsură să creeze o avertizare vizibilă în mod permanent care să indice că datele de localizare sunt prelucrate. De asemenea, dezvoltatorul este cel mai în măsură să controleze că nu sunt oferite aplicații care monitorizează în secret locul în care se află dispozitivele mobile inteligente.

În cazul în care dezvoltatorul sistemului de operare a creat o funcție telefonică „acasă" sau alte mijloace de obținere a accesului la date stocate în dispozitiv, sau are acces la datele de localizare în alte moduri, de exemplu prin intermediul unor terți care desfășoară o activitate în domeniul publicității, acesta trebuie să informeze anticipat persoana vizată cu privire la scopurile (specifice și legitime) în care el intenționează să prelucreze aceste date și la durata prelucrării.

Obligația de a informa persoanele vizate se aplică, de asemenea, operatorilor bazelor de date cu puncte de acces WiFi localizate geografic. Aceştia trebuie să informeze publicul larg în mod corespunzător cu privire la identitatea lor, scopurile prelucrării și alte informații relevante. Simpla menționare a eventualei colectări a datelor cu privire la punctele de acces WiFi într-o declarație de confidențialitate specifică ce vizează utilizatorii unei aplicații de localizare geografică nu este suficientă. Există suficiente mijloace, online și offline, de a informa publicul larg.

5.5 Drepturile persoanelor vizate

Persoanele vizate au dreptul să obțină, din partea diferiților operatori, acces la datele de localizare colectate, provenite de la dispozitivele lor mobile inteligente, precum și la informații privind scopurile prelucrării și destinatarii sau categoriile de destinatari cărora le sunt divulgate datele. Informațiile trebuie să fie furnizate într-un format care să permită citirea acestora de către orice persoană, și anume, sub formă de locații geografice, în loc de numere abstracte ca, de exemplu, cele ale stațiilor de bază.

De asemenea, persoanele vizate beneficiază de drept de acces la eventualele profiluri bazate pe aceste date de localizare. În cazul în care informațiile de localizare sunt stocate, utilizatorii ar trebui să fie autorizați să actualizeze, să rectifice sau să șteargă aceste informații.

Grupul de lucru recomandă ca operatorii să caute modalități sigure pentru a oferi acces online direct la datele de localizare și eventualele profiluri. Este foarte important ca acest acces să fie furnizat fără a se cere date cu caracter personal suplimentare în vederea verificării identității persoanelor vizate.

5.6. Perioadele de păstrare a datelor

Furnizorii serviciilor și aplicațiilor de localizare geografică ar trebui să stabilească o perioadă de păstrare a datelor de localizare care să nu o depășească pe cea necesară scopurilor în care datele au fost colectate sau în care acestea sunt prelucrate ulterior. Aceștia trebuie să se asigure că datele de localizare geografică, sau profilele derivate din astfel de date, sunt șterse după o perioadă justificată.

În cazul în care se poate demonstra necesitatea ca dezvoltatorul sistemului de operare și/sau operatorul unei infrastructuri de localizare geografică să colecteze date anonime privind istoricul localizării în vederea actualizării sau a consolidării serviciului său, trebuie să se acorde o atenție deosebită pentru a se evita ca aceste date să poată fi (în mod indirect) identificate. În special, chiar dacă dispozitivul mobil este identificat printr-un dispozitiv unic de identificare (UDID) atribuit aleatoriu, un astfel de număr unic ar trebui să fie stocat doar pentru o perioadă maximă de 24 de ore în scopuri operaționale. La încheierea perioadei respective, acest UDID ar trebui anonimizat în continuare, ținând, în același timp, seama de faptul că anonimizarea reală este din ce în ce mai greu de realizat și că datele de localizare combinate ar putea să conducă în continuare la identificare. Un astfel de UDID nu ar trebui să poată fi asociat niciunor UDID-uri anterioare sau viitoare atribuite dispozitivului, nici vreunui identificator fix al utilizatorului sau al telefonului (cum ar fi o adresă MAC, un număr IMEI sau IMSI sau orice alte numere de cont).

Referitor la datele cu privire la punctele de acces WiFi, odată ce adresa MAC a unui punct de acces WiFi este asociată cu o nouă locație, pe baza observațiilor continue ale proprietarilor dispozitivelor mobile inteligente, locația anterioară trebuie să fie imediat ștearsă, pentru a preveni orice utilizare ulterioară a datelor în scopuri necorespunzătoare, cum ar fi comercializarea orientată către persoane care și-au schimbat locația.

6. Concluzii

Cu ajutorul tehnologiilor de localizare geografică, cum ar fi datele stației de bază, datele GPS și punctele de acces WiFi cartografiate, dispozitivele mobile inteligente pot fi urmărite de toate tipurile de operatori, în scopuri care variază de la publicitatea comportamentală, la monitorizarea copiilor.

Deoarece telefoanele inteligente și tabletele electronice sunt strâns legate de proprietarii lor, modelele de deplasare ale dispozitivelor oferă o perspectivă foarte intimă asupra vieții private a proprietarilor. Unul dintre cele mai mari riscuri este acela ca proprietarii să nu știe că transmit locația lor și cui o transmit. Un alt risc asociat este acela că, în cazul anumitor aplicații, consimțământul de a utiliza

datele lor de localizare nu este valabil, deoarece informațiile cu privire la principalele elemente ale prelucrării sunt de neînțeles, caduce sau inadecvate în alt mod.

Există diferite obligații aferente diverselor părți interesate, de la dezvoltatorii sistemelor de operare și furnizorii de aplicații, până la părți cum ar fi site-urile de socializare în rețea care au integrate în platformele lor funcții de localizare pentru dispozitive mobile.

6.1 Cadrul juridic

- Cadrul juridic al UE pentru utilizarea datelor de localizare geografică provenite de la dispozitive mobile inteligente este, în primul rând, Directiva privind protecția datelor. Datele de localizare provenite de la dispozitivele mobile inteligente sunt date cu caracter personal. Combinația adresei MAC unice și a locației calculate a unui punct de acces WiFi ar trebui să fie asimilată datelor cu caracter personal.
- În plus, Directiva 2002/58/CE revizuită asupra confidențialității și comunicațiilor electronice se aplică numai în ceea ce privește prelucrarea datelor stației de bază de către operatorii de telecomunicații.

6.2 Operatorii

- Se pot distinge trei tipuri de operatori. Acestea sunt: operatorii infrastructurii de localizare geografică (în special operatorii punctelor de acces WiFi cartografiate); furnizorii aplicațiilor și ai serviciilor de localizare geografică și dezvoltatorii sistemului de operare al dispozitivelor mobile inteligente.

6.3 Motivul legitim

- Deoarece datele de localizare provenite de la dispozitive mobile inteligente dezvăluie detalii intime cu privire la viața personală a proprietarului lor, principalul motiv legitim aplicabil este consimțământul prealabil în cunoștință de cauză.
- Consimțământul nu poate fi obținut prin intermediul unor termeni și condiții cu caracter general.
- Consimțământul trebuie să fie specific, pentru diferitele scopuri în care sunt prelucrate datele, inclusiv, de exemplu pentru elaborarea de profile și/sau publicitate comportamentală. Dacă scopul prelucrării se modifică în mod substanțial, operatorul trebuie să solicite un consimțământ reînnoit specific.
- Implicit, serviciile de localizare trebuie să fie dezactivate. Un eventual mecanism de renunțare nu constituie un mecanism adecvat pentru obținerea consimțământului în cunoștință de cauză al utilizatorului.
- Consimțământul este problematic în ceea ce privește angajații și copiii. Referitor la salariați, angajatorii pot adopta această tehnologie numai atunci când este necesar în mod demonstrabil, într-un scop legitim și când aceleași obiective nu pot fi atinse cu mijloace mai puțin intruzive. Referitor la copiii, părinții trebuie să aprecieze dacă utilizarea unei astfel

de aplicații este justificată în circumstanțe specifice. Cel puțin, aceştia trebuie să își informeze copiii şi, de îndată ce acest lucru este posibil în mod rezonabil, să le permită să participe la decizia de a utiliza o astfel de aplicație.

- Grupul de lucru recomandă să se limiteze perioada de valabilitate a consimțământului şi să se reamintească utilizatorilor existența acestuia cel puțin o dată pe an. Grupul de lucru recomandă, de asemenea, un nivel suficient de detaliere al consimțământului cu privire la precizia datelor de localizare.
- Persoanele vizate trebuie să aibă posibilitatea de a-şi retrage consimțământul foarte uşor, fără consecințe negative pentru utilizarea dispozitivului lor.
- În ceea ce privește cartografierea punctelor de acces WiFi, societățile pot avea un interes legitim în colectarea şi prelucrarea cu caracter necesar a adreselor MAC şi a locațiilor calculate ale punctelor de acces WiFi în scopul specific de a oferi servicii de localizare geografică. Echilibrul intereselor între drepturile operatorului şi drepturile persoanelor vizate necesită ca operatorul să ofere dreptul de a renunța cu uşurință şi în mod permanent la înscrierea în baza de date, fără a se solicita date cu caracter personal suplimentare.

6.4 Informații

- Informațiile trebuie să fie clare, complete, inteligibile pentru un public larg, fără cunoştințe tehnice şi accesibile în mod permanent şi cu uşurință. Valabilitatea consimțământului este strâns legată de calitatea informațiilor cu privire la serviciu.
- Browserele terților şi site-urile de socializare în rețea au un rol-cheie în ceea ce privește vizibilitatea şi calitatea informațiilor referitoare la prelucrarea datelor de localizare geografică.

6.5 Drepturile persoanelor vizate

- Diferiții operatori ai informațiilor de localizare geografică provenite de la dispozitive mobile ar trebuie să permită clienților să aibă acces la datele lor de localizare într-un format în care să poată fi citite de către orice persoană şi să autorizeze rectificarea şi ştergerea fără colectarea excesivă de date cu caracter personal.
- De asemenea, persoanele vizate au dreptul de a accesa, a rectifica şi a şterge eventualele profiluri bazate pe aceste date de localizare.
- Grupul de lucru recomandă crearea unui acces online (securizat).

6.6. Perioadele de păstrare a datelor

- Furnizorii de aplicații sau servicii de localizare geografică ar trebui să pună în aplicare politici de păstrare care să asigure că datele de localizare geografică, sau profilele derivate din astfel de date, sunt şterse după o perioadă justificată.
- În cazul în care dezvoltatorul sistemului de operare şi/sau operatorul infrastructurii de localizare geografică prelucrează un număr unic, cum ar

fi o adresă MAC sau un UDID în ceea ce privește datele de localizare, numărul unic de identificare poate fi stocat doar pentru o perioadă maximă de 24 de ore, în scopuri operaționale.

Adoptat la Bruxelles,
la 16 mai 2011

Pentru grupul de lucru
Președintele
Jacob KOHNSTAMM