Gruppo di lavoro articolo 29 per la protezione dei dati

881/11/IT
WP 185

Parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti

Adottato il 16 maggio 2011

INDICE

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI
istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, della succitata direttiva,

visto il proprio regolamento interno,

HA ADOTTATO IL PRESENTE DOCUMENTO:

1. Introduzione

L'informazione geografica svolge un ruolo importante nella nostra società. Quasi tutte le attività e le decisioni umane presentano una componente geografica e, in generale, il valore dell'informazione aumenta se è collegata a un luogo. Tutti i tipi di informazioni, quali dati finanziari, dati sanitari e altri dati comportamentali dei consumatori, si possono collegare a una ubicazione geografica. Con il rapido sviluppo tecnologico e l'ampia diffusione di dispositivi mobili intelligenti, si sta sviluppando un'intera nuova categoria di servizi basati sulla localizzazione geografica.

Il presente parere ha l'obiettivo di chiarire il quadro giuridico applicabile ai servizi di geolocalizzazione disponibili su dispositivi mobili intelligenti (e/o generati dagli stessi) che possono connettersi a Internet e sono dotati di sensori sensibili alla posizione, come i sensori GPS. Esempi di tali servizi sono mappe e navigazione, servizi geografici personalizzati (compresi punti di interesse vicini), realtà aumentata, geotagging di contenuti su Internet, individuazione della posizione di amici, controllo di minori e pubblicità basata sulla localizzazione.

Il parere tratta inoltre dei tre principali tipi di infrastrutture utilizzate per fornire servizi di geolocalizzazione, segnatamente GPS, stazioni base GSM e WiFi. Una particolare attenzione è dedicata alle nuove infrastrutture basate sulla localizzazione di punti di accesso WiFi.

Il Gruppo di lavoro è consapevole dell'esistenza di molti altri servizi che elaborano dati relativi all'ubicazione che possono sollevare preoccupazioni in merito alla protezione dei dati. Questi servizi vanno dalle biglietterie elettroniche ai sistemi di pedaggio elettronico, dai servizi di navigazione satellitare al tracciamento della posizione con l'aiuto, ad esempio, di telecamere, nonché la geolocalizzazione di indirizzi IP. Tuttavia, in considerazione dei rapidi sviluppi tecnologici concernenti in particolare la mappatura dei punti di accesso wireless, unitamente al fatto che nuovi operatori di mercato si stanno preparando a sviluppare nuovi servizi di geolocalizzazione basati su una combinazione di dati da stazioni base, GPS e WiFi, il Gruppo di lavoro ha deciso di chiarire specificamente i requisiti legali relativi a questi servizi ai sensi della direttiva sulla protezione dei dati.

Il parere descrive innanzitutto la tecnologia, successivamente individua e valuta i rischi per la privacy e infine esprime delle conclusioni in merito all'applicazione degli

articoli di legge pertinenti ai vari responsabili che raccolgono e trattano dati sulla posizione geografica derivati da dispositivi mobili, che comprendono ad esempio fornitori di infrastrutture di geolocalizzazione, produttori di smartphone e sviluppatori di applicazioni basate sulla geolocalizzazione.

Il presente parere non intende valutare la specifica tecnologia di *geotagging* collegata al cosiddetto "web 2.0", nel quale gli utenti integrano informazioni georeferenziate su social network come Facebook o Twitter. Inoltre, il parere non intende entrare nel dettaglio di altre tecnologie di geolocalizzazione utilizzate per interconnettere dispositivi in un'area relativamente limitata (centri commerciali, aeroporti, complessi di uffici, ecc.) quali Bluetooth, ZigBee, *geofencing* e tag RFID basati su WiFi, benché molte delle conclusioni del parere riguardo a legittimazione, informazioni e diritti degli interessati si applichino anche a queste tecnologie quando sono utilizzate per localizzare le persone attraverso i loro dispositivi.

2. Contesto: diverse infrastrutture di geolocalizzazione

2.1 Dati da stazioni base

Il territorio coperto dai diversi operatori di telecomunicazioni è suddiviso in aree generalmente note come celle. Per essere in grado di utilizzare un telefono cellulare o di connettersi a Internet servendosi di una comunicazione 3G, il dispositivo mobile deve connettersi all'antenna (in appresso: stazione base) che copre la cella. Le celle coprono aree di dimensioni diverse, a seconda dell'interferenza, ad esempio con montagne o edifici alti.

Per tutto il tempo in cui è acceso, il dispositivo mobile è collegato a una stazione base specifica. L'operatore di telecomunicazioni registra costantemente questi collegamenti. Ogni stazione base ha un proprio ID univoco ed è registrata con una posizione specifica. L'operatore di telecomunicazioni e molti dispositivi mobili sono in grado di utilizzare segnali provenienti da celle sovrapposte (stazioni base limitrofe) per stimare la posizione del dispositivo mobile con maggiore precisione. Questa tecnica è denominata anche triangolazione.

Il grado di precisione può essere ulteriormente aumentato con l'aiuto di informazioni quali RSSI (*Received Signal Strength Indicator*), TDOA (*Time Difference of Arrival*) e AOA (*Angle Of Arrival*).

I dati da stazione base si possono utilizzare in modi innovativi, ad esempio per individuare ingorghi di traffico. Ogni strada presenta una velocità media in ciascun segmento della giornata, ma quando i passaggi alla successiva stazione base richiedono più tempo del previsto potrebbe esserci un ingorgo.

Nel complesso, questo metodo di posizionamento fornisce un'indicazione rapida e approssimativa della posizione, non molto accurata rispetto ai dati GPS e WiFi. Il grado di precisione è all'incirca di 50 metri in zone urbane densamente popolate, ma raggiunge anche diversi chilometri nelle zone rurali.

2.2 Tecnologia GPS

I dispositivi mobili intelligenti sono dotati di chipset incorporati con ricevitori GPS che ne determinano la posizione.

La tecnologia GPS (*Global Positioning System*) si basa su 31 satelliti, ciascuno ruotante in una delle 6 diverse orbite attorno alla terra.[1] Ogni satellite trasmette un segnale radio molto preciso.

Il dispositivo mobile può stabilire la propria posizione quando il sensore GPS rileva almeno 4 di questi segnali. A differenza dei dati da stazione base, il segnale va soltanto in una direzione. Le entità che gestiscono i satelliti non possono tenere traccia dei dispositivi che hanno ricevuto il segnale radio.

La tecnologia GPS consente un posizionamento preciso, tra 4 e 15 metri, ma presenta lo svantaggio principale di una partenza relativamente lenta.[2] Oltre a ciò, spesso il funzionamento in ambienti chiusi è intermittente o del tutto assente. In pratica, la tecnologia GPS spesso è combinata con i dati da stazione base e/o punti di accesso WiFi.

2.3 WiFi

2.3.1 Punti di accesso WiFi

Una fonte relativamente nuova di informazioni di geolocalizzazione sono i punti di accesso WiFi. La tecnologia è simile a quella delle stazioni base. Entrambe si basano su un ID univoco (dalla stazione base o dal punto di accesso WiFi) che può essere rilevato da un dispositivo mobile e inviato a un servizio che ha una posizione per ciascun ID univoco.

L'ID univoco per ciascun punto di accesso WiFi è il suo indirizzo MAC (*Medium Access Control*), un identificatore univoco attribuito a un'interfaccia di rete e solitamente registrato in un hardware, come chip di memoria e/o schede di rete in computer, telefoni, laptop o punti di accesso.[3]

I punti di accesso WiFi possono essere utilizzati come fonte di informazioni di geolocalizzazione perché segnalano costantemente la propria esistenza. La maggior parte dei punti di accesso a Internet a banda larga dispone anche di un'antenna WiFi. Secondo l'impostazione predefinita dei punti di accesso più comunemente utilizzati in

---

1 Il sistema di posizionamento globale (GPS) è costituito da satelliti lanciati dagli Stati Uniti d'America per scopi militari. Entro il 2014, la Commissione europea intende lanciare Galileo, una rete di 18 satelliti che offre un sistema di posizionamento satellitare globale gratuito civile. Il lancio dei primi due satelliti è previsto nel 2011, seguiti da altri 2 nel 2012. Fonte: Commissione europea, ""La Commissione presenta il riesame intermedio di Galileo e EGNOS"" 25 gennaio 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835

2 Al fine di accelerare la rilevazione iniziale del segnale GPS, è possibile precaricare le cosiddette *rainbow tables*, con la posizione prevista dei diversi satelliti nelle settimane successive.

3 Un esempio di indirizzo MAC: 00-1F-3F-D7-3C-58. L'indirizzo MAC di un punto di accesso WiFi è denominato BSSID (*Basic Service Set Identifier*).

Europa, la connessione è "on" (attiva), anche quando l'utente ha collegato il proprio computer solo via cavo al punto di accesso. Come una radio, il punto di accesso WiFi trasmette continuamente il proprio nome di rete e l'indirizzo MAC, anche se nessuno utilizza la connessione e persino quando i contenuti della comunicazione wireless sono criptati con WEP, WPA o WPA2.

Gli indirizzi MAC dei punti di accesso WiFi si possono raccogliere in due diversi modi.[4]

1. Scansione attiva: invio di richieste attive[5] a tutti i punti di accesso WiFi vicini e registrazione delle risposte, che non comprendono informazioni sui dispositivi connessi al punto di accesso WiFi.

2. Scansione passiva: registrazione dei frame di segnalamento periodici trasmessi da ogni punto di accesso (di solito 10 volte al secondo). Come alternativa non standard, alcuni strumenti registrano tutti i frame WiFi trasmessi da punti di accesso, compresi quelli che non trasmettono frame di segnalamento. Se viene eseguita senza una corretta applicazione della privacy nelle specifiche di progettazione (*privacy by design*) questo tipo di scansione può consentire la raccolta di dati scambiati tra punti di accesso e tra i dispositivi ad essi connessi. In questo modo, si potrebbero registrare gli indirizzi MAC di computer da tavolo, portatili e stampanti. Con questo tipo di scansione si potrebbe anche effettuare la registrazione illegale dei contenuti delle comunicazioni, che sono facilmente leggibili se il proprietario del punto di accesso WiFi non ha attivato la criptazione WiFi (WEP/WPA/WPA2).

La posizione di un punto di accesso WiFi si può calcolare in due diversi modi.

1. Staticamente/una volta: i responsabili del trattamento raccolgono gli indirizzi MAC dei punti di accesso WiFi spostandosi con autoveicoli dotati di antenna. Essi registrano l'esatta latitudine e longitudine del veicolo nel momento in cui viene percepito il segnale e sono in grado di calcolare la posizione dei punti di accesso sulla base, tra l'altro, dell'intensità del segnale.

2. Dinamicamente/in continuo: gli utilizzatori di servizi di geolocalizzazione raccolgono automaticamente gli indirizzi MAC percepiti dai loro dispositivi WiFi, ad esempio quando usano una mappa online per stabilire la propria posizione ("Dove mi trovo?"). Il dispositivo mobile poi invia tutte le informazioni disponibili al fornitore di servizi di geolocalizzazione, compresi indirizzi MAC, SSID e intensità di segnale. Il responsabile del trattamento può utilizzare queste osservazioni continue per calcolare e/o migliorare la localizzazione dei punti di accesso WiFi nella propria banca dati con la mappatura dei punti di accesso WiFi.

È importante notare che i dispositivi mobili non devono necessariamente "connettersi" a punti di accesso WiFi per raccogliere informazioni WiFi, ma rilevano

---

4 Le scansioni attive e passive sono state standardizzate in IEEE 802.11 per rilevare punti di accesso.

5 Per raccogliere gli indirizzi MAC, il collector invia un frame sonda di richiesta a tutti i punti di accesso.

automaticamente la presenza dei punti di accesso (in modalità di scansione attiva o passiva) e raccolgono automaticamente i relativi dati.

Inoltre, i telefoni cellulari che richiedono di essere geolocalizzati non si limitano a inviare dati WiFi, ma spesso trasmettono anche altre informazioni di cui dispongono, ivi compresi dati GPS e da stazione base. Questo consente al provider di calcolare la posizione di "nuovi" punti di accesso WiFi e/o migliorare la localizzazione di punti di accesso WiFi già compresi nella banca dati. In questo modo, la raccolta di informazioni sui punti di accesso WiFi risulta decentrata in modo molto efficiente, senza che i clienti ne siano necessariamente consapevoli.

In sintesi: la geolocalizzazione basata su punti di accesso WiFi offre un posizionamento rapido e sempre più preciso, sulla base di costanti misurazioni.

3. Rischi per la privacy

Un dispositivo mobile intelligente è intimamente connesso a un individuo specifico. La maggior parte delle persone tende a tenere i propri dispositivi mobili molto vicini, dalle tasche o dalla borsa al comodino, vicino al letto.

Succede raramente che una persona presti questi oggetti ad un'altra. Per la maggior parte, le persone sono consapevoli del fatto che i loro dispositivi mobili contengono una certa quantità di informazioni molto personali, che vanno da messaggi e-mail a fotografie private, dalla storia di navigazione del browser a, ad esempio, una lista di contatti.

Questo consente ai fornitori di servizi basati sulla geolocalizzazione di ottenere una panoramica approfondita di abitudini e modelli di comportamento del proprietario del dispositivo e di costruire profili dettagliati. Da un modello di inattività notturna è possibile dedurre il luogo preposto al sonno, e dal modello di un percorso regolare la mattina è possibile dedurre l'ubicazione del datore di lavoro. Il modello può includere anche dati ricavati dai modelli di spostamento di amici, sulla base del cosiddetto *grafico sociale*.[6]

Un modello comportamentale può anche comprendere *speciali categorie di dati*, ad esempio se rivela visite in ospedali o luoghi di culto, la partecipazione a manifestazioni politiche o la presenza in altri luoghi specifici, magari che rivelino dati sulla vita sessuale dell'utente. Questi profili si possono utilizzare per prendere decisioni che influiscono in misura significativa sul proprietario.

La tecnologia dei dispositivi mobili intelligenti consente il monitoraggio costante dei dati di localizzazione. Gli smartphone possono raccogliere permanentemente segnali da stazioni base e punti di accesso WiFi. Tecnicamente, il monitoraggio può avvenire segretamente, senza che il proprietario ne sia informato. Il monitoraggio può anche essere effettuato semi-segretamente, quando le persone "dimenticano" o non sono adeguatamente informate sul fatto che i servizi di localizzazione sono attivi o quando

[6] Il "grafico sociale" è un termine che indica la visibilità degli amici in siti di social networking e la capacità di dedurre tratti comportamentali dai dati su questi amici.

le impostazioni di accessibilità dei dati di localizzazione vengono modificate da "privato" a "pubblico".

Anche quando le persone rendono intenzionalmente disponibili su Internet i propri dati di geolocalizzazione, attraverso servizi di posizionamento e *geotagging*, l'accesso globale illimitato pone nuovi rischi, che vanno dal furto di dati all'effrazione, o addirittura a episodi di aggressione fisica o stalking.

Come per altre nuove tecnologie, un rischio rilevante insito nell'uso di dati di localizzazione è la *function creep*, o estensione indebita delle funzionalità, ossia il fatto che sulla base della disponibilità di un nuovo tipo di dati si possano sviluppare nuove finalità che non erano previste al momento della raccolta dei dati.

4. Quadro giuridico

Il quadro giuridico pertinente è costituito dalla direttiva sulla protezione dei dati (95/46/CE) che si applica ogniqualvolta vengano trattati dati personali in conseguenza dell'elaborazione di dati relativi all'ubicazione. La direttiva e-privacy (2002/58/CE, modificata dalla direttiva 2009/136/CE) si applica esclusivamente al trattamento di dati da stazioni base da parte di servizi e reti di comunicazione elettronica accessibili al pubblico (operatori delle telecomunicazioni).

4.1 Dati da stazioni base trattati da operatori delle telecomunicazioni

Gli operatori delle telecomunicazioni elaborano continuamente dati da stazioni base nel quadro dell'offerta di servizi pubblici di comunicazione elettronica.[7] Inoltre, possono trattare dati da stazioni base per fornire servizi a valore aggiunto. Questo caso è già stato affrontato dal Gruppo di lavoro nel parere 5/2005 (WP115). Benché alcuni degli esempi contenuti nel parere risultino inevitabilmente superati con la diffusione della tecnologia Internet e di sensori inseriti in dispositivi sempre più piccoli, le conclusioni giuridiche e le raccomandazioni del documento restano valide per quanto concerne l'uso di dati da stazioni base.

1. Poiché i dati relativi all'ubicazione ricavati da stazioni base si riferiscono a una persona fisica identificata o identificabile, sono soggetti alle disposizioni sulla protezione dei dati personali di cui alla direttiva 95/46/CE del 24 ottobre 1995.
2. Si applica anche la direttiva 2002/58/CE del 12 luglio 2002 (modificata nel novembre 2009 dalla direttiva 2009/136/CE), secondo la definizione di cui all'articolo 2, lettera c), della stessa:
   "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

Se un operatore delle telecomunicazioni offre un servizio di geolocalizzazione ibrido, ossia che si basi anche sul trattamento di altri tipi di dati di localizzazione, quali dati

[7] Si noti che anche l'offerta di hotspot WiFi pubblici da parte di operatori delle telecomunicazioni si qualifica come un servizio pubblico di comunicazione elettronica e dovrebbe pertanto rispettare le disposizioni della direttiva e-privacy.

GPS o WiFi, tale attività si qualifica come servizio pubblico di comunicazione elettronica. L'operatore deve ottenere il consenso preventivo dei suoi clienti se fornisce a terzi questi dati di geolocalizzazione.

4.2 Dati da stazioni base, WiFi e GPS trattati da fornitori di servizi della società dell'informazione

4.2.1 Applicabilità della direttiva e-privacy modificata

Tipicamente, le società che forniscono servizi di localizzazione e applicazioni basate su una combinazione di dati da stazioni base, GPS e WiFi costituiscono *servizi della società dell'informazione.* In quanto tali, sono espressamente escluse dalla direttiva e-privacy e dalla rigorosa definizione di "servizio di comunicazione elettronica" (articolo 2, lettera c), della direttiva quadro modificata (inalterata).[8]

La direttiva e-Privacy non si applica al trattamento di dati relativi all'ubicazione da parte di servizi della società dell'informazione, anche quando tale trattamento avviene mediante una rete pubblica di comunicazione elettronica. Un utente può scegliere di trasmettere dati GPS su Internet, ad esempio quando accede a servizi di navigazione su Internet. In tal caso, il segnale GPS è trasmesso nel livello applicativo della comunicazione via Internet, a prescindere dalla rete GSM. Il fornitore di servizi di telecomunicazione funge semplicemente da tramite e non può ottenere l'accesso a dati GPS e/o WiFi e/o da stazione base comunicati da e verso un dispositivo mobile intelligente tra un utente/abbonato e un servizio della società dell'informazione senza ricorrere a mezzi molto invadenti, quali la *deep packet inspection* (DPI).

4.2.2 Applicabilità della direttiva sulla protezione dei dati

Dove non si applica la direttiva e-privacy modificata, ai sensi dell'articolo 1, paragrafo 2, si applica la direttiva 95/46/CE: *"Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE."*

Secondo la direttiva sulla protezione dei dati, per dati personali s'intende "*qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"* (articolo 2, lettera a), della direttiva).

[8] Direttiva 2002/21/CE, del 7 marzo 2002, articolo 2, lettera c): «servizio di comunicazione elettronica», i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva 98/34/CE non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica;

Il considerando 26 della direttiva presta un'attenzione particolare al termine "identificabile" laddove afferma che *"per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona.*"

Il considerando 27 della direttiva definisce l'ampia portata della tutela: "*la portata della tutela non deve infatti dipendere dalle tecniche impiegate poiché, in caso contrario, sussisterebbero gravi rischi di elusione delle disposizioni;*".

Nel parere 4/2007 sul concetto di dati personali, il Gruppo di lavoro fornisce ampie indicazioni sulla definizione di dati personali.

Dispositivi mobili intelligenti
I dispositivi mobili intelligenti sono inestricabilmente collegati a persone fisiche e di norma sussiste un'identificabilità diretta e indiretta.
In primo luogo, l'operatore delle telecomunicazioni che fornisce l'accesso Internet GSM e mobile di solito tiene un registro con il nominativo, l'indirizzo e i dettagli bancari di ciascun cliente, in combinazione con una serie di codici univoci del dispositivo, quali IMEI e IMSI.

In secondo luogo, nell'acquisto di software extra per il dispositivo (*applicazioni* o "*apps*"*)* di solito è richiesto un numero di carta di credito che pertanto arricchisce la combinazione di codici univoci e dati di localizzazione con dati direttamente identificativi.

L'identificabilità indiretta si può ottenere mediante la combinazione del codice univoco del dispositivo con una o più posizioni calcolate.

Ogni dispositivo mobile intelligente ha almeno un identificatore univoco, l'indirizzo MAC, ma può avere anche altri numeri di identificazione univoci, aggiunti dallo sviluppatore del sistema operativo. Questi identificatori possono essere trasmessi e ulteriormente trattati nel contesto dei servizi di geolocalizzazione. È un fatto che la posizione di un particolare dispositivo si può calcolare in modo molto preciso, soprattutto quando si combinano le diverse infrastrutture di geolocalizzazione. Tale posizione può indicare una casa o un datore di lavoro. Soprattutto con osservazioni ripetute, è possibile individuare il proprietario del dispositivo.

Nel considerare i mezzi disponibili per l'identificazione, occorre tenere presente la tendenza delle persone a divulgare su Internet un numero sempre maggiore di dati personali di localizzazione, ad esempio pubblicando l'ubicazione della propria casa o del proprio luogo di lavoro, in combinazione con altri dati identificativi. La divulgazione di queste informazioni può avvenire anche senza che gli interessati lo sappiano, se vengono "geotaggati" da altre persone. Questi sviluppi rendono più agevole il collegamento di un luogo o di un modello comportamentale con un individuo specifico.

Inoltre, secondo il parere 4/2007 sul concetto di dati personali, andrebbe anche rilevato che un identificatore univoco, nel contesto descritto sopra, consente di

tracciare l'utente di un dispositivo specifico e pertanto rende possibile individuarlo anche se il suo nome reale non è noto.

Punti di accesso WiFi
Questa identificabilità indiretta si applica anche ai punti di accesso WiFi.[9] L'indirizzo MAC di un punto di accesso WiFi, in combinazione con la sua posizione calcolata, è inestricabilmente collegato all'ubicazione del proprietario del punto di accesso.

Un responsabile del trattamento dotato di attrezzature adeguate può calcolare con precisione sempre maggiore la posizione di un punto di accesso WiFi sulla base dell'intensità del segnale e dei costanti aggiornamenti della posizione attraverso gli utenti del suo servizio di geolocalizzazione.

Con l'aiuto di queste risorse, in molti casi è possibile identificare un piccolo gruppo di appartamenti o case dove vive il proprietario del punto di accesso. La facilità con cui è possibile individuare il proprietario dall'indirizzo MAC dipende dall'ambiente:

- In aree scarsamente popolate, dove l'indirizzo MAC indica una casa singola, il proprietario della residenza può essere individuato direttamente con strumenti come registri catastali, elenchi telefonici, registrazioni elettorali o persino una semplice interrogazione su un motore di ricerca.[10]
- In zone più densamente popolate, con l'aiuto di risorse come l'intensità del segnale e/o SSID (che chiunque disponga di un dispositivo WiFi può rilevare), è possibile stabilire la precisa posizione del punto di accesso e quindi, in molti casi, accertare l'identità delle persone che vivono nel luogo preciso (casa o appartamento) dove è ubicato il punto di accesso.
- In zone ad alta densità di popolazione, anche con l'aiuto di informazioni sull'intensità del segnale l'indirizzo MAC indicherà numerosi appartamenti come potenziale ubicazione del punto di accesso. In queste circostanze non è possibile, senza uno sforzo irragionevole, individuare con precisione la persona che vive nell'appartamento dove si trova il punto di accesso.

Il fatto che in alcuni casi il proprietario del dispositivo non possa essere identificato senza uno sforzo irragionevole non impedisce di concludere in generale che la combinazione dell'indirizzo MAC di un punto di accesso WiFi con la sua posizione calcolata dovrebbe essere assimilata a dati personali.

In simili circostanze, e tenendo conto del fatto che è improbabile che il responsabile del trattamento sia in grado di distinguere tra i casi nei quali il proprietario del punto di accesso WiFi è identificabile e quelli nei quali non lo è, il responsabile del trattamento dovrebbe trattare tutti i dati su router WiFi come dati personali.

È importante ricordare che non è necessario che lo scopo del trattamento di questi dati di geolocalizzazione sia quello di identificare gli utenti. Il fatto che l'identificazione dei proprietari dei punti di accesso WiFi richieda uno sforzo irragionevole dipende in

---

9 I punti di accesso WiFi possono anche essere direttamente identificabili, se il fornitore dell'accesso a Internet tiene un registro degli indirizzi MAC dei router WiFi che fornisce ai propri clienti identificati.

10 La disponibilità di tali registri o elenchi varia a seconda dello Stato membro.

larga misura dalle possibilità tecniche del responsabile del trattamento o di qualsivoglia altra persona ai fini dell'identificazione.

5. Obblighi derivanti dalle leggi sulla protezione dei dati

5.1 Responsabile del trattamento

Nel contesto dei servizi di geolocalizzazione online forniti da servizi della società dell'informazione si possono distinguere tre diverse funzionalità, con diverse responsabilità per il trattamento di dati personali. Si tratta delle seguenti: responsabile di un'infrastruttura di geolocalizzazione; fornitore di specifici servizi o applicazioni di geolocalizzazione e sviluppatore del sistema operativo di un dispositivo mobile intelligente. In pratica, le aziende spesso svolgono molti ruoli contemporaneamente, ad esempio quando combinano un sistema operativo con una banca dati di punti di accesso WiFi mappati e una piattaforma pubblicitaria.

5.1.1 Responsabili di un'infrastruttura di geolocalizzazione

Allo stesso modo degli operatori delle telecomunicazioni che elaborano la posizione di un dispositivo specifico con l'aiuto delle stazioni base, anche i proprietari di banche dati con punti di accesso WiFi mappati trattano dati personali quando calcolano la posizione di uno specifico dispositivo mobile intelligente. Poiché entrambi determinano le finalità e le modalità del trattamento, sono da considerarsi responsabili del trattamento ai sensi della definizione di cui all'articolo 2, lettera d), della direttiva sulla protezione dei dati.

È importante sottolineare che il dispositivo specifico è determinante nel calcolo della posizione, poiché trasmette i propri dati di localizzazione (spesso una combinazione di GPS, WiFi e stazione base) e gli ID univoci dai vicini punti di accesso WiFi al proprietario della banca dati.[11] Il dispositivo inoltre soddisfa il criterio dell'articolo 4, paragrafo 1, lettera c), della direttiva sulla protezione dei dati, di *strumento situato nel territorio di uno Stato membro*.

Poiché l'indirizzo MAC di un punto di accesso WiFi, in combinazione con la sua posizione calcolata, dovrebbe essere assimilato a dei dati personali, anche la raccolta di tali dati si configura come trattamento di dati personali. Quindi, a prescindere dalla modalità con cui tali dati vengono raccolti (una tantum o continuativa) il proprietario della banca dati dovrebbe rispettare gli obblighi della direttiva sulla protezione dei dati.

[11] Il dispositivo mobile può inoltrare i diversi dati di geolocalizzazione che riceve affinché il responsabile calcoli la sua ubicazione, o per calcolarla autonomamente. In entrambi i casi il dispositivo è uno strumento essenziale per l'elaborazione.

5.1.2 Fornitori di applicazioni e servizi di geolocalizzazione

I dispositivi mobili intelligenti consentono l'installazione di software di terzi, le cosiddette *applicazioni* che possono elaborare i dati relativi all'ubicazione (e altri dati) di un dispositivo mobile intelligente, indipendentemente dallo sviluppatore del sistema operativo e/o dai responsabili dell'infrastruttura di geolocalizzazione.

Esempi di tali servizi sono: un servizio meteorologico che preveda le possibilità di pioggia nelle ore successive in una regione molto specifica, un servizio che offre informazioni su negozi nelle vicinanze, un servizio di identificazione di un telefono perso o un servizio che mostra l'ubicazione degli amici.

Il fornitore di un'applicazione in grado di elaborare dati di geolocalizzazione è il responsabile del trattamento dei dati personali derivanti dall'installazione e dall'utilizzo dell'applicazione.

Ovviamente, non è sempre necessario installare software separati su un dispositivo mobile intelligente. Infatti è possibile accedere a molti servizi di geolocalizzazione tramite un programma di navigazione (browser). Un esempio di questo tipo di servizio è l'utilizzo di una mappa online per guidare una persona per le strade di una città.

5.1.3 Sviluppatore del sistema operativo

Lo sviluppatore del sistema operativo di un dispositivo mobile intelligente può essere il responsabile del trattamento di dati di geolocalizzazione quando interagisce direttamente con l'utente e raccoglie dati personali (ad esempio richiedendo la registrazione di utente iniziale e/o raccogliendo informazioni sulla localizzazione al fine di migliorare i servizi). In quanto responsabile del trattamento, lo sviluppatore deve adottare i principi della privacy nelle specifiche di progettazione per impedire il monitoraggio segreto, da parte del dispositivo stesso o di diversi servizi e applicazioni.

Lo sviluppatore è anche il responsabile del trattamento dei dati che elabora se il dispositivo possiede una funzionalità "phone home" ("telefona a casa") per la sua posizione. Poiché in tal caso è lo sviluppatore a decidere sugli strumenti e sulle finalità del flusso di dati, è anche il responsabile del trattamento di tali dati. Un esempio comune di questa funzionalità "phone home" è la fornitura automatica di aggiornamenti sul fuso orario in base alla posizione.

In terzo luogo, lo sviluppatore è da considerarsi un responsabile del trattamento quando offre una piattaforma pubblicitaria e/o un ambiente webshop per le applicazioni ed è in grado di elaborare i dati personali derivanti dall'installazione e dall'utilizzo di applicazioni di geolocalizzazione, a prescindere dai fornitori.

5.2 Responsabilità di altre parti

Molte altre parti online consentono l'ulteriore trattamento di dati relativi all'ubicazione, quali browser, siti di social networking o mezzi di comunicazione che

permettono ad esempio il "geotagging". Quando nella loro piattaforma sono integrati strumenti di geolocalizzazione, hanno una responsabilità rilevante nel decidere in merito alle impostazioni predefinite dell'applicazione ("ON" o "OFF"). Benché siano da considerarsi responsabili del trattamento solo nella misura in cui procedono attivamente all'elaborazione dei dati personali, svolgono comunque un ruolo fondamentale nella legittimazione del trattamento dei dati da parte di soggetti quali fornitori di applicazioni specifiche, ad esempio in fatto di visibilità e qualità dell'informazione in merito al trattamento di dati di geolocalizzazione.

5.3 Motivo di legittimazione

5.3.1 Dispositivi mobili intelligenti

Se gli operatori delle telecomunicazioni intendono utilizzare i dati della stazione base per fornire un servizio a valore aggiunto a un cliente, ai sensi della direttiva e-privacy modificata devono ottenere il previo consenso del cliente stesso. Inoltre, devono assicurarsi che questi sia informato in merito ai termini del trattamento.

In considerazione della delicatezza del trattamento di (modelli di) dati relativi all'ubicazione, il *previo consenso informato* è anche il principale motivo applicabile per legittimare il trattamento dei dati quando si tratta di elaborare i dati di localizzazione di un dispositivo mobile intelligente nel contesto di servizi della società dell'informazione.

Ai sensi della direttiva sulla protezione dei dati, articolo 2, lettera h), il consenso dev'essere una manifestazione di volontà libera, specifica e informata della persona interessata.

A seconda del tipo di tecnologia utilizzata, il dispositivo dell'utente svolge un ruolo più o meno attivo nel trattamento dei dati di geoposizionamento. Il dispositivo è in grado di trasmettere a terzi da fonti diverse i dati relativi all'ubicazione. Questa capacità tecnica non dovrebbe essere confusa con la legittimità di un simile trattamento dati. Se le impostazioni predefinite di un sistema operativo consentono la trasmissione di dati di localizzazione, il mancato intervento dell'utente non dovrebbe essere inteso erroneamente come un consenso concesso liberamente.

Nella misura in cui procedono attivamente al trattamento di dati di geolocalizzazione (ad esempio quando ottengono l'accesso a informazioni di localizzazione attraverso il dispositivo), anche gli sviluppatori di sistemi operativi e altri servizi della società dell'informazione sono allo stesso modo soggetti all'obbligo di ottenere il previo consenso informato degli utenti. Occorre chiarire che tale consenso non s'intende liberamente concesso con l'accettazione obbligatoria di termini e condizioni generali, né tramite possibilità di rinuncia (opt-out). La norma dovrebbe essere che i servizi di localizzazione siano disattivati (OFF) e gli utenti possono acconsentire all'attivazione (ON) di specifiche applicazioni.

Consenso di dipendenti

Il consenso come motivo di legittimazione del trattamento è problematico in un contesto lavorativo. Nel suo parere sul trattamento di dati personali nel contesto lavorativo, il Gruppo di lavoro scrive: "*quando il consenso del lavoratore è necessario, ma un suo eventuale diniego potrebbe causare un reale o potenziale pregiudizio, il consenso non è idoneo a soddisfare gli artt. 7 e 8 e non potrebbe qualificarsi come libero. Quindi, i lavoratori devono poter negare il proprio consenso senza pregiudizio. (…) Una situazione complessa può presentarsi quando il rilascio del consenso è una condizione dell'assunzione. Il lavoratore può in teoria rifiutare il proprio consenso, ma la conseguenza potrebbe essere la perdita dell'opportunità di lavoro. In tali circostanze il consenso non si manifesta liberamente e quindi non è valido.*"[12] Invece di richiedere il consenso, i datori di lavoro devono accertarsi che sia possibile dimostrare la necessità di vigilare sull'esatta ubicazione dei dipendenti per una finalità legittima e valutare tale necessità a fronte dei diritti e delle libertà fondamentali dei dipendenti. Nei casi in cui la necessità può essere adeguatamente giustificata, il fondamento giuridico del trattamento si potrebbe basare sull'interesse legittimo del responsabile (articolo 7, lettera f) della direttiva sulla protezione dei dati). Il datore di lavoro deve sempre adottare gli strumenti meno invadenti, evitare il monitoraggio costante e ad esempio scegliere un sistema che trasmetta un allarme quando un dipendente attraversa un confine virtuale prestabilito. Il dipendente dev'essere in grado di disattivare qualsiasi dispositivo di monitoraggio al di fuori dell'orario di lavoro e gli deve essere mostrato come farlo. I dispositivi di tracciamento dei veicoli non sono dispositivi di tracciamento del personale, bensì la loro funzione consiste nel rintracciare o monitorare l'ubicazione dei veicoli sui quali sono installati. I datori di lavoro non dovrebbero considerarli come strumenti per seguire o monitorare il comportamento o gli spostamenti di autisti o di altro personale, ad esempio inviando segnali d'allarme in relazione alla velocità del veicolo.

Consenso dei minori

In alcuni casi occorre il consenso di minori, che dev'essere fornito dai genitori o altri legali rappresentanti. Questo significa ad esempio che il fornitore di un'applicazione di geolocalizzazione è tenuto ad avvisare i genitori in merito alla raccolta e all'utilizzo di dati di geolocalizzazione dai minori e ad ottenere il loro consenso prima di raccogliere e utilizzare ulteriormente le informazioni sui loro figli. Alcune applicazioni di geolocalizzazione sono studiate specificamente per il controllo da parte dei genitori, ad esempio rilevando costantemente la posizione del dispositivo su un sito web, o emettendo un segnale d'allarme se il dispositivo lascia un territorio prestabilito. L'impiego di simili applicazioni è problematico. Nel suo parere 2/2009[13] sulla protezione dei dati personali dei minori, il Gruppo di lavoro dell'articolo 29 scrive*: "I minori non devono mai essere sottoposti, per motivi di sicurezza, a una sorveglianza eccessiva che ne limiti l'autonomia. Al riguardo occorre trovare un giusto equilibrio tra la protezione dell'intimità e della vita privata dei minori e la loro sicurezza.*"

[12] WP48, parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo.

[13] WP160, parere 2/2009 sulla protezione dei dati personali dei minori (Linee guida generali e casi specifici riferiti al contesto scolastico).

Il quadro giuridico prevede che i genitori hanno la responsabilità di garantire il diritto alla privacy dei minori. Come minimo, se i genitori giudicano che l'utilizzo di una simile applicazione sia giustificato in circostanze specifiche, i minori devono esserne informati e, non appena ragionevolmente possibile, ammessi a partecipare alla decisione di utilizzarla.

Il consenso dev'essere specifico per ciascuna delle diverse finalità del trattamento dei dati. Il responsabile deve chiarire molto bene se il servizio offerto si limita a fornire una risposta alla domanda volontaria "Dove mi trovo ora?" o se ha lo scopo di fornire risposte alle domande "Dove sei? Dove sei stato?, Dove sarai la prossima settimana?". In altre parole, il responsabile del trattamento deve prestare una particolare attenzione al consenso per finalità che una persona interessata non si aspetta, quali ad esempio l'analisi del profilo (*profiling*) e/o il targeting comportamentale.

Se le finalità del trattamento cambiano in modo sostanziale, il responsabile è tenuto a richiedere un nuovo consenso specifico. Ad esempio, se all'inizio un'azienda aveva dichiarato di non voler condividere dati personali con terzi, mentre ora desidera farlo, deve ottenere il previo consenso attivo di ciascun cliente. La mancata risposta (o altri tipi di possibilità di opt-out) non è sufficiente.

È importante distinguere tra il consenso a un servizio una tantum e il consenso a un abbonamento regolare. Ad esempio, per utilizzare un particolare servizio di geolocalizzazione, può essere necessario attivare funzioni di geolocalizzazione nel dispositivo o nel programma di navigazione. Se la funzione di geolocalizzazione è attivata (ON), tutti i siti web possono leggere i dati di localizzazione dell'utente di quel dispositivo mobile intelligente. Onde prevenire i rischi del monitoraggio invisibile, il Gruppo di lavoro articolo 29 considera fondamentale che il dispositivo avverta costantemente che la funzione di geolocalizzazione è "ON"', ad esempio tramite un'icona visibile permanentemente.

Il Gruppo di lavoro raccomanda che i fornitori di applicazioni o servizi di geolocalizzazione chiedano di rinnovare i singoli consensi (anche in assenza di cambiamenti nella natura del trattamento) dopo un adeguato periodo di tempo. Per esempio, non sarebbe logico continuare a trattare dati relativi all'ubicazione se un individuo non ha utilizzato attivamente il servizio nei 12 mesi precedenti. Anche se il servizio è stato utilizzato, bisognerebbe ricordare agli interessati almeno una volta all'anno (o più spesso se la natura del servizio lo giustifica) la natura del trattamento dei loro dati personali e offrire una procedura semplice per rinunciare al servizio.

Infine, è altrettanto importante che le persone interessate siano in grado di revocare il proprio consenso in modo molto semplice, senza conseguenze negative per l'utilizzo dei loro dispositivi. Indipendentemente dalle direttive europee sulla protezione dei dati, il World Wide Web Consortium (W3C) ha formulato un progetto di standard API per la geolocalizzazione che sottolinea la necessità di un previo consenso esplicito e informato.[14] Nello specifico, il W3C spiega l'esigenza di rispettare la revoca del consenso, consigliando a chi applica lo standard di considerare che "*il contenuto ospitato in un determinato URL può cambiare in modo tale che i permessi*

[14] W3C API sulla geolocalizzazione: http://www.w3.org/TR/geolocation-API/

di localizzazione precedentemente concessi non si applicano più per quanto concerne l'utente. O comunque gli utenti potrebbero semplicemente cambiare idea."

Esempio di migliori prassi per i fornitori di applicazioni di geolocalizzazione

Un'applicazione che utilizza dati di geolocalizzazione informa chiaramente l'utente in merito alle finalità per le quali intende utilizzare i dati e chiede un consenso esplicito per ciascuna delle possibili finalità diverse. L'utente sceglie attivamente il livello di granularità della geolocalizzazione (ad esempio, a livello nazionale, di città, di codice postale o con la maggior precisione possibile). Una volta che il servizio di localizzazione è attivato, sullo schermo compare un'icona sempre visibile che segnala che i servizi sono 'ON'. L'utente può revocare il proprio consenso in qualsiasi momento, senza dover uscire dall'applicazione. Inoltre, l'utente è in grado di cancellare facilmente e definitivamente eventuali dati di localizzazione memorizzati nel dispositivo.

5.3.2 Punti di accesso WiFi

Sulla base della direttiva sulla protezione dei dati, le aziende possono avere un interesse legittimo nella raccolta e nel trattamento di indirizzi MAC e posizioni calcolate di punti di accesso WiFi per la finalità specifica di offrire servizi di geolocalizzazione.

Il motivo di legittimazione di cui all'articolo 7, lettera f), della direttiva sulla protezione dei dati richiede un equilibrio tra gli interessi legittimi del responsabile del trattamento e i diritti fondamentali dei soggetti interessati. Considerando la natura semi-statica dei punti di accesso WiFi, la loro mappatura in linea di principio costituisce una minaccia minore per la privacy dei proprietari dei punti di accesso rispetto al tracciamento in tempo reale della posizione di dispositivi mobili intelligenti.

L'equilibrio tra i diritti del responsabile del trattamento e i diritti delle persone interessate è dinamico. Per riuscire a far prevalere i propri interessi legittimi sugli interessi delle persone interessate nel corso del tempo, i responsabili del trattamento devono formulare e applicare delle garanzie, quali il diritto ad uscire facilmente e per sempre dalla banca dati, senza che sia necessario fornire ulteriori dati personali al responsabile di tale banca dati. Ad esempio, possono utilizzare un software che accerti automaticamente che una persona è connessa a uno specifico punto di accesso.[15]

[15] Un possibile utilizzo è il seguente:
1. una persona va su una specifica pagina web dove può inserire l'indirizzo MAC del proprio punto di accesso WiFi.
2. Se l'indirizzo MAC appare nella banca dati contenente i punti di accesso WiFi mappati, il responsabile del trattamento può visualizzare una pagina di verifica contenente un messaggio che richiede la tabella ARP del dispositivo Internet. In teoria, gli indirizzi WLAN MAC si possono visualizzare con il comando 'ARP –a'. Con l'aiuto di un codice contenuto nel browser, come Java, la tabella ARP può essere prodotta in background.
3. Se nella tabella ARP non compare l'indirizzo MAC, è evidente che l'utente connesso alla WLAN è lo stesso che ha accesso all'indirizzo locale WLAN MAC. Il responsabile del trattamento quindi verifica la richiesta di cancellazione in modo semplice e automatico.

Inoltre, al fine di offrire servizi di geolocalizzazione non è necessario raccogliere e trattare SSID, quindi la raccolta e il trattamento di SSID sono eccessivi per lo scopo di offrire servizi di geolocalizzazione sulla base della mappatura della posizione di punti di accesso WiFi.

5.4 Informazioni

I diversi responsabili del trattamento devono assicurarsi che i proprietari del dispositivo mobile intelligente siano adeguatamente informati in merito agli elementi chiave del trattamento conformemente all'articolo 10 della direttiva sulla protezione dei dati, quali l'identità del responsabile del trattamento, le finalità del trattamento, il tipo di dati, la durata del trattamento, i diritti delle persone interessate di accedere, rettificare o cancellare i propri dati e il diritto di revocare il consenso.

La validità del consenso è inestricabilmente collegata alla qualità dell'informazione sul servizio. Le informazioni devono essere chiare, esaurienti, comprensibili per un pubblico ampio e non tecnico e accessibili facilmente e permanentemente.

Le informazioni devono essere mirate a un pubblico ampio. I responsabili del trattamento non possono presumere che i propri clienti siano persone tecnicamente competenti solo perché possiedono un dispositivo mobile intelligente. Le informazioni devono essere adeguate alla fascia di età se il responsabile del trattamento sa di attirare un pubblico giovane.

Se i fornitori di applicazioni di geolocalizzazione intendono calcolare le posizioni di un dispositivo più di una volta, devono tenere informati i propri clienti per tutto il tempo in cui trattano dati di localizzazione. Inoltre, devono consentire ai clienti di mantenere o revocare il consenso. Per realizzare questi obiettivi, i fornitori di applicazioni dovrebbero collaborare strettamente con lo sviluppatore del sistema operativo, che tecnicamente è nella posizione migliore per creare un promemoria, visibile permanentemente, che indichi che si stanno trattando dati relativi all'ubicazione. Lo sviluppatore è nella posizione migliore anche per controllare che non vengano offerte applicazioni che consentano il monitoraggio segreto della posizione di dispositivi mobili intelligenti.

Se lo sviluppatore del sistema operativo ha creato una funzionalità "phone home" o altri mezzi per ottenere l'accesso a dati memorizzati sul dispositivo, ovvero può accedere in altri modi ai dati di localizzazione, ad esempio attraverso inserzionisti terzi, deve informare anticipatamente la persona interessata in merito alle finalità (specifiche e legittime) per le quali intende trattare questi dati e in merito alla durata del trattamento.

L'obbligo di informare le persone interessate si applica anche ai responsabili di banche dati contenenti punti di accesso WiFi geolocalizzati, che sono tenuti a informare il grande pubblico in modo adeguato in merito alla propria identità e alle finalità del trattamento, nonché a fornire altre informazioni pertinenti. La semplice citazione della possibile raccolta di dati relativi a punti di accesso WiFi in una dichiarazione specifica sulla privacy rivolta agli utilizzatori di un'applicazione di geolocalizzazione non è sufficiente. Esistono mezzi adeguati, online e offline, per informare il grande pubblico.

5.5 Diritti della persona interessata

Le persone interessate hanno il diritto di ottenere dai diversi responsabili del trattamento l'accesso ai dati di localizzazione che hanno raccolto dai loro dispositivi mobili intelligenti, nonché informazioni sulle finalità del trattamento e sui destinatari, o categorie di destinatari, a cui vengono divulgati i dati. Le informazioni devono essere fornite in formato leggibile, vale a dire in forma di località geografiche invece che di codici astratti, ad esempio di stazioni base.

Le persone interessate hanno anche il diritto di accedere a eventuali profili basati sui dati di localizzazione. Se le informazioni sulla posizione sono memorizzate, agli utenti dovrebbe essere consentito di aggiornarle, rettificarle o cancellarle.

Il Gruppo di lavoro raccomanda che i responsabili del trattamento ricerchino modi sicuri per fornire l'accesso diretto online ai dati di localizzazione e a possibili profili. È fondamentale che tale accesso venga fornito senza richiedere dati personali aggiuntivi per accertare l'identità delle persone interessate.

5.6 Periodi di conservazione dei dati

I fornitori di servizi di geolocalizzazione e applicazioni dovrebbero stabilire un periodo di conservazione dei dati di localizzazione che non sia superiore a quanto necessario per le finalità per le quali sono stati raccolti o vengono ulteriormente trattati i dati. Inoltre, devono garantire che i dati di geolocalizzazione, o i profili ricavati dagli stessi, vengano cancellati dopo un periodo di tempo giustificato.

Qualora venga dimostrata la necessità per lo sviluppatore del sistema operativo e/o il responsabile di una infrastruttura di geolocalizzazione di raccogliere dati storici di localizzazione anonimi, allo scopo di aggiornare o potenziare il servizio, occorre prestare un'estrema attenzione per evitare di rendere identificabili (indirettamente) tali dati. In particolare, anche se il dispositivo mobile è identificato da un Unique Device Identifier (UDID) attribuito a caso, tale codice univoco dovrebbe essere memorizzato solo per un massimo di 24 ore per scopi operativi. Successivamente, l'UDID dovrebbe essere ulteriormente anonimizzato, tenendo conto del fatto che l'effettiva anonimizzazione è sempre più difficile da realizzare e che i dati di localizzazione combinati potrebbero ancora consentire l'identificazione. L'UDID non dovrebbe essere collegabile a precedenti o futuri UDID attribuiti al dispositivo, né a eventuali identificatori fissi dell'utente o del telefono (quali indirizzo MAC, codici IMEI o IMSI o altri codici cliente).

Per quanto concerne i dati sui punti di accesso WiFi, una volta che l'indirizzo MAC di un punto di accesso WiFi è associato con una nuova posizione, basata sull'osservazione costante di proprietari di dispositivi mobili intelligenti, la precedente posizione dev'essere immediatamente cancellata, per impedire eventuali ulteriori utilizzi dei dati per finalità inappropriate, quali attività di marketing mirato a persone che hanno cambiato la propria ubicazione.

6. Conclusioni

Con l'aiuto di tecnologie di geolocalizzazione quali dati da stazioni base, GPS e punti di accesso WiFi mappati, i dispositivi mobili intelligenti possono essere rintracciati da tutti i tipi di responsabili del trattamento dei dati, per finalità che vanno dalla pubblicità comportamentale al controllo dei minori.

Poiché smartphone e tablet computer sono inestricabilmente collegati al proprietario, i modelli di spostamento dei dispositivi offrono una percezione molto profonda della vita privata dei proprietari. Uno dei rischi maggiori è che i proprietari non siano consapevoli di trasmettere la loro posizione, né sappiano a chi la trasmettono. Un altro rischio correlato è che determinate applicazioni utilizzino dati di localizzazione senza un consenso valido, perché le informazioni sugli elementi fondamentali del trattamento sono incomprensibili, superate o comunque inadeguate.

Esistono obblighi diversi per le varie parti interessate, dagli sviluppatori dei sistemi operativi ai fornitori di applicazioni e parti quali siti di social networking che integrano nelle rispettive piattaforme funzionalità di localizzazione per dispositivi mobili.

6.1 Quadro giuridico

- Il quadro giuridico dell'UE per l'utilizzo di dati di geolocalizzazione da dispositivi mobili intelligenti comprende in primo luogo la direttiva sulla protezione dei dati. I dati relativi all'ubicazione di dispositivi mobili intelligenti sono dati personali. La combinazione dell'indirizzo MAC univoco e della posizione calcolata di un punto di accesso WiFi dovrebbe essere assimilata a dati personali.
- Inoltre, la direttiva e-privacy 2002/58/CE modificata si applica esclusivamente al trattamento di dati da stazioni base da parte di operatori delle telecomunicazioni.

6.2 Responsabili del trattamento

- Si possono distinguere tre tipi di responsabili del trattamento: responsabili delle infrastrutture di geolocalizzazione (in particolare, responsabili di punti di accesso WiFi mappati); fornitori di applicazioni e servizi di geolocalizzazione e sviluppatori del sistema operativo di dispositivi mobili intelligenti.

6.3 Motivo di legittimazione

- Poiché i dati relativi all'ubicazione di dispositivi mobili intelligenti rivelano dettagli intimi della vita privata del proprietario, la principale legittimazione applicabile è il previo consenso informato.
- Il consenso non si può ottenere attraverso i termini e le condizioni generali.
- Il consenso dev'essere specifico per le diverse finalità del trattamento dei dati, tra cui ad esempio costruzione di profili e targeting comportamentale. Se le finalità del trattamento cambiano in modo sostanziale, il responsabile deve richiedere un nuovo consenso specifico.
- Di norma, i servizi di localizzazione devono essere disattivati. Un possibile meccanismo di rinuncia non costituisce un sistema adeguato per ottenere il consenso informato dell'utente.

- Il consenso è problematico per quanto concerne dipendenti e minori. Nel caso dei dipendenti, i datori di lavoro possono adottare questa tecnologia solo quando se ne dimostri la necessità per una finalità legittima e gli stessi obiettivi non si possano raggiungere con mezzi meno invadenti. Nel caso dei minori, i genitori devono giudicare se l'uso di simili applicazioni sia giustificato in circostanze specifiche. Come minimo, devono informarne i minori e, non appena ragionevolmente possibile, ammetterli a partecipare alla decisione di utilizzare queste applicazioni.
- Il Gruppo di lavoro raccomanda di limitare la portata del consenso in termini di tempo e di inviare un promemoria agli utenti almeno una volta all'anno. Allo stesso modo, il Gruppo di lavoro raccomanda agli utenti un livello sufficiente di granularità nel consenso in merito alla precisione dei dati di localizzazione.
- Le persone interessate devono essere in grado di revocare facilmente il proprio consenso, senza conseguenze negative per l'utilizzo del proprio dispositivo.
- Per quanto concerne la mappatura di punti di accesso WiFi, le aziende possono avere un interesse legittimo nella raccolta e nel trattamento di indirizzi MAC e posizioni calcolate di punti di accesso WiFi per la finalità specifica di offrire servizi di geolocalizzazione. L'equilibrio di interessi tra i diritti del responsabile del trattamento e i diritti delle persone interessate impone che il responsabile del trattamento offra la possibilità di uscire facilmente e in via permanente dalla banca dati senza richiedere ulteriori dati personali.

6.4 Informazioni

- Le informazioni devono essere chiare, complete, comprensibili per un pubblico ampio e non tecnico, nonché facilmente e permanentemente accessibili. La validità del consenso è inscindibilmente collegata alla qualità dell'informazione sul servizio.
- Le parti terze come browser e siti di social networking svolgono un ruolo fondamentale per quanto concerne la visibilità e la qualità dell'informazione sul trattamento di dati di geolocalizzazione.

6.5 Diritti delle persone interessate

- I diversi responsabili del trattamento di informazioni di geolocalizzazione da dispositivi mobili dovrebbero consentire ai clienti di accedere ai dati di localizzazione in un formato leggibile e permettere rettifiche e cancellazioni senza raccogliere eccessivi dati personali.
- Le persone interessate hanno anche il diritto di accedere a eventuali profili basati sui dati di localizzazione e di rettificarli o cancellarli.
- Il Gruppo di lavoro raccomanda la creazione di un accesso online (sicuro).

6.6 Periodi di conservazione

- I fornitori di applicazioni o servizi di geolocalizzazione dovrebbero prevedere politiche di conservazione che garantiscano che i dati di geolocalizzazione, o i profili ricavati dagli stessi, vengano cancellati dopo un periodo di tempo giustificato.

- Se lo sviluppatore del sistema operativo e/o il responsabile della infrastruttura di geolocalizzazione elabora un codice univoco, quale un indirizzo MAC o un UDID, in relazione a dati di localizzazione, tale codice univoco di identificazione può essere conservato per un periodo massimo di 24 ore per scopi operativi.

Fatto a Bruxelles,
il 16 maggio 2011

Per il Gruppo di lavoro
Il presidente
Jacob KOHNSTAMM