GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

00461/13/IT
WP 202

Parere 02/2013 sulle applicazioni per dispositivi intelligenti

adottato il 27 febbraio 2013

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

Sintesi

Le diverse applicazioni, o app, disponibili su una serie di app store per i dispositivi intelligenti più diffusi sono centinaia di migliaia. Secondo quanto riportato, le nuove applicazioni aggiunte quotidianamente agli app store sono oltre 1 600 e un utente medio di smartphone ne scarica 37. Le applicazioni sono offerte all'utente finale gratuitamente o a un costo minimo e possono avere una base di utilizzatori che va da alcuni individui a molti milioni.

Le applicazioni sono in grado di raccogliere grandi quantità di dati dal dispositivo (ad esempio dati memorizzati dall'utente e dati da diversi sensori, tra cui la geolocalizzazione) e di elaborarli per fornire servizi nuovi e innovativi all'utente finale. Tuttavia, le stesse fonti di dati possono essere ulteriormente elaborate, di solito per generare un flusso di entrate, con modalità che possono essere ignorate o indesiderate dall'utente finale.

Gli sviluppatori di applicazioni inconsapevoli degli obblighi in materia di protezione dei dati possono generare notevoli rischi per la vita privata e la reputazione degli utilizzatori di dispositivi intelligenti. I principali rischi per la protezione dei dati degli utenti finali sono costituiti dalla mancanza di trasparenza e di consapevolezza in merito ai tipi di trattamento che un'applicazione può effettuare, associata all'assenza di un consenso significativo degli utenti finali prima di tale trattamento. Scarse misure di sicurezza, un'apparente tendenza alla massimizzazione dei dati e la flessibilità degli scopi per i quali si raccolgono dati personali contribuiscono ulteriormente alla creazione di rischi per la protezione dei dati riscontrati nell'attuale ambiente delle applicazioni.

Un forte rischio per la protezione dei dati deriva inoltre dal grado di frammentazione tra i molti attori nello scenario dello sviluppo di applicazioni, che comprendono sviluppatori e proprietari di applicazioni, app store, produttori di sistemi operativi (OS) e dispositivi e altri soggetti terzi che possono essere coinvolti nella raccolta e nel trattamento di dati personali da dispositivi intelligenti, quali fornitori di servizi analitici e pubblicità. Le conclusioni e le raccomandazioni del presente parere sono rivolte per la maggior parte agli sviluppatori di applicazioni (in quanto esercitano il maggior controllo sulle precise modalità del trattamento o della presentazione di informazioni all'interno della app), che tuttavia, per ottenere i massimi livelli di tutela della privacy e dei dati, spesso devono collaborare con altri soggetti nell'ecosistema delle applicazioni. Questo risulta particolarmente importante per quanto concerne la sicurezza, dove la catena di molteplici attori è forte quanto il suo anello più debole.

Molte tipologie di dati disponibili su un dispositivo mobile intelligente sono dati personali. Il quadro giuridico pertinente è la direttiva sulla protezione dei dati, in associazione alla protezione dei dispositivi mobili come parte della sfera privata degli utenti contenuta nella direttiva e-privacy. Queste norme valgono per qualsiasi applicazione destinata ad utenti all'interno dell'UE, a prescindere dall'ubicazione dello sviluppatore o dell'app store.

Nel presente parere, il Gruppo di lavoro chiarisce il quadro giuridico applicabile al trattamento dei dati personali nello sviluppo, nella distribuzione e nell'utilizzo di applicazioni su dispositivi intelligenti, concentrandosi in particolare sul requisito del consenso, sui principi di limitazione della finalità e di minimizzazione dei dati, sulla necessità di prendere misure di sicurezza adeguate, sull'obbligo di informazione corretta agli utenti finali, sui relativi diritti, sui periodi ragionevoli di conservazione dei dati e, nello specifico, sull'equo trattamento dei dati provenienti da minori e relativi ad essi.

Indice

1. Introduzione

Le app sono applicazioni software spesso studiate per un compito specifico e destinate a una serie particolare di dispositivi intelligenti, quali smartphone, tablet e televisori connessi a Internet. Organizzano le informazioni in modo adatto alle caratteristiche specifiche del dispositivo, interagendo spesso strettamente con l'hardware e il sistema operativo presente sul dispositivo.

Le applicazioni disponibili su una serie di app store per i dispositivi intelligenti più diffusi sono centinaia di migliaia e svolgono un'ampia gamma di funzioni, tra cui navigazione su internet, comunicazione (e-mail, telefonia e messaggistica internet), intrattenimento (giochi, film/video e musica), social networking, operazioni bancarie e servizi basati sulla localizzazione geografica. Secondo quanto riportato, le nuove applicazioni aggiunte quotidianamente agli app store sono oltre 1 600[1] e l'utente medio di smartphone ne scarica 37[2]. Le applicazioni vengono offerte all'utente finale gratuitamente o a un costo minimo e possono avere una base di utilizzatori che va da alcuni individui a molti milioni.

Il sistema operativo sottostante comprende anche software o strutture di dati che sono importanti per i servizi principali del dispositivo intelligente, quali la rubrica di uno smartphone. Il sistema operativo è progettato per mettere queste componenti a disposizione delle app attraverso interfacce di programmazione dell'applicazione (API), le quali offrono l'accesso alla moltitudine di sensori che possono essere presenti sui dispositivi intelligenti e che comprendono: giroscopio, bussola digitale e accelerometro per la velocità e la direzione del movimento; fotocamere frontali e sul retro per acquisire filmati e fotografie; un microfono per le registrazioni audio. I dispositivi intelligenti possono anche contenere sensori di prossimità[3]; inoltre, possono connettersi attraverso una moltitudine di interfacce di rete, tra cui Wi-Fi, Bluetooth, NFC o Ethernet. Infine, è possibile determinare con precisione l'ubicazione grazie ai servizi di geolocalizzazione (come descritto nel parere 13/2011 del Gruppo di lavoro "articolo 29" sui servizi di geolocalizzazione su dispositivi mobili intelligenti[4]). La tipologia, la precisione e la frequenza di questi dati da sensori varia a seconda del dispositivo e del sistema operativo.

Grazie alle API, gli sviluppatori di applicazioni sono in grado di raccogliere continuamente tali dati, di consultare e scrivere dati dei contatti, inviare e-mail, SMS o messaggi in social network, leggere/modificare/cancellare contenuti di schede SD, effettuare registrazioni audio, utilizzare la fotocamera e accedere a immagini archiviate, leggere lo stato e l'identità del telefono, modificare le impostazioni generali del sistema e impedire la disattivazione del telefono. Le API inoltre possono fornire informazioni relative al dispositivo stesso tramite uno o più identificatori univoci e

---

[1] Relazione in *ConceivablyTech* del 19 agosto 2012, disponibile all'indirizzo www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of. Citata da Kamala D. Harris, procuratore generale del dipartimento di giustizia della California, *Privacy on the go, Recommendations for the mobile ecosystem*, gennaio 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[2] Stima mondiale per il 2012 di ABI Research, http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o.

[3] Un sensore capace di individuare la presenza di un oggetto materiale senza un contatto fisico. Cfr.: http://www.w3.org/TR/2012/WD-proximity-20121206/.

[4] Cfr. parere 13/2011 del Gruppo di lavoro "articolo 29" sui servizi di geolocalizzazione su dispositivi mobili intelligenti (maggio 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_it.pdf.

informazioni su altre applicazioni installate. Queste fonti di dati possono essere ulteriormente trattate, di solito per generare un flusso di entrate, secondo modalità ignorate o non desiderate dall'utente finale.

Il presente parere si prefigge l'obiettivo di chiarire il quadro giuridico applicabile al trattamento di dati personali nella distribuzione e nell'utilizzo di applicazioni su dispositivi intelligenti e di considerare ulteriori trattamenti che potrebbero verificarsi al di fuori delle applicazioni, quali l'utilizzo dei dati raccolti per la costruzione di profili e il *targeting* degli utenti. Il parere prende in esame i principali rischi in materia di protezione dei dati, fornisce una descrizione delle diverse parti coinvolte e mette in evidenza le varie responsabilità legali per quanto concerne sviluppatori e proprietari di applicazioni, app store, produttori di sistemi operativi (OS) e dispositivi e altri soggetti terzi che possono essere coinvolti nella raccolta e nel trattamento di dati personali da dispositivi intelligenti, quali fornitori di servizi analitici e pubblicità.

Il parere si concentra in particolare sul requisito del consenso, sui principi di limitazione della finalità e di minimizzazione dei dati, sulla necessità di adottare misure di sicurezza adeguate, sull'obbligo di informazione corretta agli utenti finali, sui relativi diritti, sui periodi ragionevoli di conservazione dei dati e nello specifico sull'equo trattamento dei dati provenienti da minori e relativi ad essi.

L'ambito di applicazione copre diversi tipi di dispositivi intelligenti, pur riguardando in particolare le applicazioni disponibili per i dispositivi mobili intelligenti.

2. Rischi per la protezione dei dati

La stretta interazione con il sistema operativo consente alle applicazioni di accedere ad un numero notevolmente maggiore di dati rispetto a un *browser*, o navigatore, tradizionale[5]. Le applicazioni sono in grado di raccogliere grandi quantità di dati dal dispositivo (dati di localizzazione, dati archiviati dall'utente e dati ottenuti dai diversi sensori) e di elaborarli per fornire servizi nuovi e innovativi all'utente finale.

Un forte rischio per la protezione dei dati è rappresentato dal grado di frammentazione tra i molti attori nello scenario dello sviluppo di applicazioni. Un singolo dato può essere trasmesso dal dispositivo in tempo reale per essere elaborato in tutto il mondo o copiato tra catene di terzi. Alcune delle applicazioni più note sono sviluppate da importanti società tecnologiche, ma molte altre sono progettate da piccole imprese innovative. Un singolo programmatore con una idea e precedenti competenze di programmazione scarse o nulle può raggiungere un pubblico mondiale in un breve lasso di tempo. Gli sviluppatori di applicazioni che ignorano gli obblighi di protezione dei dati possono creare rischi significativi per la vita privata e la reputazione degli utenti di dispositivi intelligenti. Nel contempo, si assiste al rapido sviluppo di servizi di terzi, come la pubblicità, che se integrati da uno sviluppatore senza la dovuta attenzione possono divulgare notevoli quantità di dati personali.

I principali rischi per la protezione dei dati degli utenti finali sono la mancanza di trasparenza e di consapevolezza in merito ai tipi di trattamento che un'applicazione può effettuare, associata all'assenza di un consenso significativo degli utenti finali prima di tale trattamento. Scarse misure di sicurezza, un'apparente tendenza alla massimizzazione dei dati e la flessibilità degli scopi per i quali si raccolgono dati personali contribuiscono ulteriormente ai rischi per la protezione dei dati riscontrati

[5] Benché i *browser* per desktop stiano acquisendo un accesso più ampio a dati da sensori su dispositivi di utenti finali, spinti dagli sviluppatori di giochi web.

nell'attuale ambiente delle applicazioni. Molti di questi rischi sono già stati esaminati e affrontati da altri organismi di regolamentazione internazionali, quali la *US Federal Trade Commission* (FTC) (Commissione federale per il commercio USA), il *Canadian Office of the Privacy Commissioner* (Ufficio del commissario per la privacy del Canada) e l'*Attorney General of the Californian Department of Justice* (procuratore generale del dipartimento di giustizia della California)[6].

- Un rischio fondamentale per la protezione dei dati è la mancanza di trasparenza. Gli sviluppatori di applicazioni sono vincolati dalle funzionalità fornite da produttori di sistemi operativi e app store per garantire la disponibilità di un'informazione completa e tempestiva all'utente finale. Ciononostante, non tutti gli sviluppatori sfruttano queste funzionalità, poiché molte applicazioni non prevedono una politica sulla privacy o non informano adeguatamente i potenziali utenti in merito al tipo di dati personali che l'applicazione può trattare e per quali finalità. La mancanza di trasparenza non si limita alle app gratuite o di proprietà di sviluppatori inesperti, in quanto un recente studio ha riportato che solo il 61,3% delle 150 principali applicazioni prevede una politica sulla privacy[7].

- La mancanza di trasparenza è strettamente connessa alla mancanza di un consenso libero e informato. Una volta scaricata l'applicazione, il consenso spesso si riduce a una casella da spuntare per indicare che l'utente finale accetta i termini e le condizioni, senza nemmeno offrire l'alternativa di un "No grazie". Secondo uno studio di GSMA del settembre 2011, il 92% degli utenti di applicazioni vorrebbero una scelta più articolata[8].

- Misure di sicurezza carenti possono consentire il trattamento non autorizzato di dati personali (sensibili), ad esempio se uno sviluppatore subisce una violazione di dati personali o se la stessa applicazione lascia trapelare dati personali.

- Un altro rischio per la protezione dei dati riguarda l'inosservanza (dovuta a ignoranza o intenzionale) del principio di limitazione della finalità, secondo cui i dati personali possono essere raccolti e trattati esclusivamente per finalità specifiche e legittime. I dati personali raccolti dalle applicazioni si possono ampiamente distribuire a numerosi terzi per scopi indefiniti o flessibili quali "ricerche di mercato". La stessa allarmante inosservanza si evidenzia per il principio di minimizzazione dei dati. Da recenti ricerche è emerso che molte

---

6 Cfr., tra l'altro, il rapporto informativo FTC *Mobile Privacy Disclosures, Building Trust Through Transparency*, febbraio 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf, il rapporto informativo FTC *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, febbraio 2012, http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf e la relazione di follow-up, *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, dicembre 2012, http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf, Ufficio del commissario per la privacy del Canada, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*, ottobre 2012, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf, Kamala D. Harris, procuratore generale del dipartimento di giustizia della California, *Privacy on the go, Recommendations for the mobile ecosystem*, gennaio 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

7 Studio FPF *Mobile Apps*, giugno 2012, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf.

8 "L'*89% [degli utenti] considera importante sapere quando un'informazione personale è condivisa da un'applicazione ed essere in grado di attivare o disattivare la funzione*". Fonte: *User perspectives on mobile privacy*, settembre 2011, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf.

applicazioni raccolgono quantità abbondanti di dati dagli smartphone, senza che vi sia alcun rapporto significativo con le loro apparenti funzionalità[9].

3 Principi in materia di protezione dei dati

3.1 Diritto applicabile

Il quadro giuridico pertinente dell'UE è la direttiva sulla protezione dei dati (95/46/CE) che si applica in tutti i casi in cui l'utilizzo di applicazioni su dispositivi intelligenti implica il trattamento di dati personali. Per determinare il diritto applicabile, è essenziale innanzi tutto individuare il ruolo delle diverse parti interessate coinvolte: l'identificazione dei responsabili del trattamento effettuato attraverso dispositivi mobili è particolarmente importante in relazione al diritto applicabile. Lo stabilimento del responsabile del trattamento è un elemento decisivo per determinare l'applicazione della normativa UE in materia di protezione dei dati, benché non sia l'unico criterio. A norma dell'articolo 4, paragrafo 1, lettera a), della direttiva sulla protezione dei dati, il diritto nazionale di uno Stato membro è applicabile al trattamento di dati personali effettuato "nel contesto delle attività di uno stabilimento" del responsabile del trattamento nel territorio di tale Stato membro. Ai sensi dell'articolo 4, paragrafo 1, lettera c), della direttiva sulla protezione dei dati, il diritto nazionale di uno Stato membro è applicabile anche nei casi in cui il responsabile del trattamento *non è stabilito* nel territorio della Comunità e ricorre a strumenti situati nel territorio di detto Stato membro. Poiché il dispositivo è fondamentale nel trattamento di dati personali relativi all'utente, questo criterio di norma è soddisfatto[10]. Tuttavia, è pertinente solo nei casi in cui il responsabile del trattamento non sia stabilito nell'UE.

Di conseguenza, ogniqualvolta una parte coinvolta nello sviluppo, nella distribuzione e nel funzionamento di applicazioni sia ritenuta responsabile del trattamento, tale parte è competente, singolarmente o congiuntamente ad altri, per garantire l'osservanza di tutti i requisiti previsti dalla direttiva sulla protezione dei dati. L'identificazione del ruolo delle parti interessate nelle applicazioni per dispositivi mobili sarà ulteriormente analizzata in seguito, nella sezione 3.3.

In aggiunta alla direttiva sulla protezione dei dati, la direttiva e-privacy (2002/58/CE, modificata dalla direttiva 2009/136/CE) stabilisce una norma specifica per tutte le parti a livello mondiale che desiderino archiviare informazioni o accedere a informazioni archiviate nei dispositivi di utenti nello Spazio economico europeo (SEE).

L'articolo 5, paragrafo 3, della direttiva e-privacy prevede che "*l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento (...)*".

Molte disposizioni della direttiva e-privacy si applicano solo a fornitori di servizi di comunicazione elettronica accessibili al pubblico e a fornitori di reti pubbliche di comunicazione nella Comunità,

---

[9] Wall Street Journal, *Your Apps Are Watching You*, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[10] Nella misura in cui l'applicazione genera traffico di dati personali verso responsabili del trattamento. Questo criterio potrebbe non essere soddisfatto se il trattamento dei dati avviene solo localmente nel dispositivo stesso.

mentre l'articolo 5, paragrafo 3, si applica a tutte le entità che inseriscono o leggono informazioni su dispositivi intelligenti, a prescindere dalla natura dell'entità (che si tratti di un'entità pubblica o privata, di un singolo programmatore o di una grande società, ovvero di un responsabile del trattamento, di un incaricato del trattamento o di una parte terza).

Il requisito del consenso di cui all'articolo 5, paragrafo 3, si applica a qualsiasi informazione, a prescindere dalla natura dei dati archiviati o ai quali si accede. L'ambito di applicazione non è limitato ai dati personali e per informazione si intende qualsiasi tipo di dato archiviato sul dispositivo.

Il requisito del consenso di cui all'articolo 5, paragrafo 3, della direttiva e-privacy si applica ai servizi offerti "*nella Comunità"*, ossia a tutti gli individui residenti nello Spazio economico europeo, a prescindere dall'ubicazione del fornitore dei servizi. Per gli sviluppatori di applicazioni è importante sapere che entrambe le direttive sono norme imperative, in quanto i diritti dell'individuo non sono trasferibili né sono soggetti a rinuncia contrattuale. Questo significa che l'applicabilità delle norme europee in materia di privacy non può essere esclusa in virtù di una dichiarazione unilaterale o di un accordo contrattuale[11].

3.2 Dati personali trattati mediante applicazioni

Molte tipologie di dati archiviati in un dispositivo intelligente o generati dallo stesso sono dati personali. Secondo il considerando 24 della direttiva e-privacy:

> *"Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali"*.

Si tratta di dati personali ogniqualvolta si riferiscono a un individuo, direttamente (ad esempio per nome) o indirettamente identificabile dal responsabile del trattamento o da un terzo. Si possono riferire al proprietario del dispositivo o a qualsiasi altro individuo, come nel caso dei recapiti di amici in una rubrica[12]. I dati si possono raccogliere e trattare sul dispositivo o, una volta trasferiti, anche altrove, presso infrastrutture di sviluppatori o di terzi, tramite la connessione ad un'interfaccia di programmazione dell'applicazione (API) esterna, in tempo reale senza che l'utente finale ne sia a conoscenza.

Esempi di dati personali che possono influire in misura significativa sulla vita privata degli utenti finali e altri individui sono i seguenti:

- Ubicazione
- Contatti
- Codici identificativi univoci del dispositivo e del cliente (come IMEI[13], IMSI[14], UDID[15] e numero di cellulare)

---

[11] Ad esempio, dichiarazioni sull'esclusiva applicazione del diritto di una giurisdizione al di fuori del SEE.

[12] I dati possono essere i) generati automaticamente dal dispositivo, sulla base di funzioni predeterminate dal produttore del sistema operativo e/o dispositivo o dal relativo fornitore di telefonia mobile (ad esempio dati di geolocalizzazione, impostazioni di rete, indirizzo IP); ii) generati dall'utente mediante app (liste di contatti, appunti, foto); iii) generati dalle app (ad es. cronologia di navigazione).

[13] Codice IMEI (International Mobile Equipment **Identity)**.

[14] Codice IMSI (International Mobile Subscriber **Identity)**.

[15] Codice identificativo univoco del dispositivo (Unique Device Identifier).

- Identità dell'interessato
- Identità del telefono (ossia nome del telefono[16])
- Carta di credito e dati di pagamento
- Registro delle chiamate, SMS o messaggistica istantanea
- Cronologia di navigazione
- E-mail
- Credenziali di autenticazione per i servizi della società dell'informazione (in particolare servizi con caratteristiche sociali)
- Fotografie e filmati
- Biometrica (ad es. riconoscimento facciale e modelli di impronte digitali).

3.3 Parti coinvolte nel trattamento dei dati

Le diverse parti coinvolte nello sviluppo, nella distribuzione e nella gestione di applicazioni sono numerose e con responsabilità differenti in fatto di protezione dei dati.

Le quattro parti principali che si possono identificare sono le seguenti: i) sviluppatori di applicazioni (compresi proprietari di applicazioni)[17], ii) produttori di sistemi operativi e dispositivi ("produttori di OS e dispositivi")[18]; iii), app store (distributori di applicazioni) e infine iv) altre parti coinvolte del trattamento di dati personali. In alcuni casi le responsabilità in materia di protezione dei dati sono condivise, in particolare quando la stessa entità è coinvolta in più stadi, ad esempio quando il produttore del sistema operativo controlla anche l'app store.

Anche gli utenti finali sono tenuti ad assumersi adeguate responsabilità nella misura in cui creano e memorizzano dati personali sul proprio dispositivo mobile. Se il trattamento serve per scopi puramente personali o domestici la direttiva sulla protezione dei dati non si applica (articolo 3, paragrafo 2) e l'utente s'intende esente dagli obblighi formali in materia di protezione dei dati. Tuttavia, se l'utente decide di condividere dati tramite un'applicazione, ad esempio divulgando informazioni a un numero indefinito di persone[19] mediante un'applicazione per social network, il trattamento delle informazioni non rientra nelle condizioni dell'esenzione domestica[20].

3.3.1 Sviluppatori di applicazioni

Gli sviluppatori di applicazioni creano app e/o le mettono a disposizione di utenti finali. La categoria comprende organizzazioni del settore privato e pubblico che commissionano lo sviluppo di applicazioni e le società e persone fisiche che creano e lanciano applicazioni. Progettando e/o creando il software che girerà sugli smartphone, decidono in che misura l'applicazione potrà accedere a diverse categorie di dati personali e procedere al loro trattamento, nel dispositivo e/o attraverso risorse informatiche remote (unità informatiche di sviluppatori di app o di terzi).

---

16 Gli utenti tendono a chiamare il telefono con il proprio nome: "iPhone di Mario Rossi".

17 Pur utilizzando l'espressione comune "sviluppatore di applicazioni", il Gruppo di lavoro sottolinea che il termine non si riferisce solo a programmatori o sviluppatori tecnici di applicazioni, ma comprende anche i proprietari, ossia società e organizzazioni che commissionano lo sviluppo di applicazioni e ne determinano le finalità.

18 In alcuni casi, il produttore del sistema operativo coincide con il produttore del dispositivo, mentre in altri il produttore del dispositivo è un'azienda diversa dal fornitore del sistema operativo.

19 Cfr. Corte di giustizia dell'Unione europea, causa C-101/01, procedimento penale a carico di BodilLindqvist, sentenza del 6 novembre 2003, e causa C-73/07, Tietosuojavaltuutettu contro SatakunnanMarkkinapörssiOy e SatamediaOy, sentenza del 16 dicembre 2008.

20 Cfr. parere 5/2009 del Gruppo di lavoro "articolo 29" sui social network on-line (giugno 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_it.pdf.

Nella misura in cui determina le finalità e i mezzi del trattamento di dati personali su dispositivi intelligenti, lo sviluppatore di applicazioni è il responsabile del trattamento come definito nell'articolo 2, lettera d), della direttiva sulla protezione dei dati. In tal caso, è tenuto a rispettare le disposizioni dell'intera direttiva. Le principali disposizioni sono illustrate ai paragrafi da 3.4 a 3.10 del presente parere.

Anche quando all'utente si applica l'esenzione domestica, lo sviluppatore di applicazioni s'intende comunque responsabile del trattamento dei dati qualora vi proceda per finalità proprie. Ad esempio, nel caso in cui l'applicazione richieda l'accesso all'intera rubrica di indirizzi per fornire il servizio (messaggistica istantanea, chiamate telefoniche, video chiamate).

Le responsabilità dello sviluppatore di applicazioni sono notevolmente limitate se i dati personali non vengono trattati e/o resi disponibili al di fuori del dispositivo, o se lo sviluppatore ha adottato adeguate misure tecniche e organizzative per garantire che i dati siano resi anonimi in modo irreversibile e aggregati sul dispositivo stesso prima di lasciarlo.

In ogni caso, se lo sviluppatore accede a informazioni archiviate sul dispositivo si applica anche la direttiva e-privacy e lo sviluppatore è tenuto a rispettare il requisito del consenso sancito dall'articolo 5, paragrafo 3, della direttiva stessa.

Nella misura in cui lo sviluppatore di applicazioni ha commissionato a un terzo, in tutto in parte, l'effettivo trattamento dei dati e tale terzo assume il ruolo di incaricato del trattamento, lo sviluppatore deve adempiere a tutti gli obblighi relativi all'utilizzo di un incaricato del trattamento dei dati, che comprende anche il ricorso ad un fornitore di servizi di *cloud computing* (ad es. per l'archiviazione esterna di dati)[21].

Nella misura in cui lo sviluppatore di applicazioni consente l'accesso di terzi ai dati dell'utente (ad esempio una rete pubblicitaria che accede ai dati di geolocalizzazione del dispositivo per fornire pubblicità comportamentali) deve adottare meccanismi adeguati per rispettare i requisiti applicabili ai sensi del quadro giuridico dell'UE. Se il terzo accede a dati archiviati nel dispositivo si applica l'obbligo di ottenere il consenso informato di cui all'articolo 5, paragrafo 3, della direttiva e-privacy. Inoltre, se il terzo procede al trattamento di dati personali per finalità proprie, può considerarsi anche un responsabile del trattamento dei dati congiuntamente allo sviluppatore e deve pertanto garantire il rispetto del principio di limitazione della finalità e gli obblighi in fatto di sicurezza[22] per la parte del trattamento per la quale determina finalità e mezzi. Poiché tra sviluppatori di applicazioni e terzi possono esistere tipologie diverse di accordi commerciali e tecnici, la rispettiva responsabilità di ciascuna parte dovrà essere stabilita caso per caso, tenendo conto delle circostanze specifiche del trattamento in questione.

Uno sviluppatore di applicazioni può utilizzare librerie di terzi con un software che fornisce funzionalità comuni, come ad esempio una libreria per una piattaforma di *social gaming*. Lo sviluppatore deve garantire che gli utenti siano a conoscenza di eventuali trattamenti dei dati effettuati da tali librerie e, in tal caso, che il trattamento sia conforme al quadro giuridico dell'UE, anche

---

[21] Cfr. parere 05/2012 del Gruppo di lavoro "articolo 29" sul *cloud computing* (luglio 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_it.pdf.

[22] Cfr. parere 2/2010 del Gruppo di lavoro "articolo 29" sulla pubblicità comportamentale online (giugno 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_it.pdf e il parere 1/2010 del Gruppo di lavoro "articolo 29" sui concetti di "responsabile del trattamento" e "incaricato del trattamento" (febbraio 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_it.pdf.

richiedendo il consenso dell'utente, dove pertinente. In questo senso, gli sviluppatori devono impedire l'uso di funzionalità nascoste all'utente.

3.3.2 Produttori di sistemi operativi (OS) e dispositivi

Anche i produttori di OS e dispositivi dovrebbero essere considerati responsabili del trattamento (e, laddove pertinente, responsabili congiunti) di eventuali dati personali trattati per finalità proprie, quali il regolare funzionamento del dispositivo, la sicurezza ecc., compresi i dati generati dall'utente (ad esempio informazioni sull'utente durante la registrazione), i dati generati automaticamente dal dispositivo (ad esempio se il dispositivo possiede una funzionalità "phone home" (telefona a casa) per la sua posizione) o i dati personali trattati da produttori di OS o dispositivi in seguito all'installazione o all'utilizzo di applicazioni. Quando i produttori di OS o dispositivi offrono funzionalità aggiuntive, quali una funzione di back-up o localizzazione remota, diventano responsabili del trattamento dei dati personali trattati per tale scopo.

Le applicazioni che richiedono l'accesso a dati di geolocalizzazione devono utilizzare i servizi di localizzazione del sistema operativo. Quando un'applicazione utilizza la geolocalizzazione, il sistema operativo può raccogliere dati personali per fornire le informazioni di geolocalizzazione all'applicazione e può anche considerare di utilizzare i dati per migliorare i propri servizi di localizzazione. Per quest'ultimo scopo, il sistema operativo è il responsabile del trattamento dei dati.

I produttori di OS e dispositivi sono anche responsabili dell'interfaccia di programmazione dell'applicazione (API) che consente il trattamento di dati personali tramite applicazioni sul dispositivo intelligente. Lo sviluppatore di applicazioni sarà in grado di accedere alle caratteristiche e alle funzioni messe a disposizione dai produttori di OS e dispositivi attraverso l'API. Poiché determinano i mezzi (e la portata) dell'accesso ai dati personali, i produttori di OS e dispositivi devono garantire che la granularità del controllo dello sviluppatore di applicazioni sia sufficiente affinché l'accesso venga concesso esclusivamente ai dati necessari per il funzionamento dell'applicazione. Inoltre, dovrebbero garantire che l'accesso si possa revocare in modo semplice ed efficace.

Il concetto di "*privacy by design"*, o privacy nella progettazione, è un principio importante a cui si fa riferimento indirettamente già nella direttiva sulla protezione dei dati[23] e che, insieme alla "*privacy by default"*, o privacy di default, emerge più chiaramente nella direttiva e-privacy[24] e richiede ai produttori di un dispositivo o di un'applicazione di tenere conto della protezione dei dati fin dall'inizio della progettazione. La *privacy by design* è richiesta espressamente per la progettazione di apparecchiature di telecomunicazione, come previsto dalla direttiva riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione[25]. Di conseguenza, i produttori di OS e dispositivi, insieme agli app store, svolgono un ruolo di notevole responsabilità nel fornire garanzie per la protezione dei dati personali e della vita privata degli utenti di applicazioni, anche assicurando la disponibilità di meccanismi adeguati per informare ed educare l'utente finale in merito a quello che le applicazioni possono fare e a quali dati sono in grado di accedere, nonché offrendo agli utenti le opportune impostazioni per modificare i parametri del trattamento[26].

---

[23] Cfr. considerando 46 e articolo 17.

[24] Cfr. articolo 14, paragrafo 3.

[25] Direttiva 1999/5/CE, del 9 marzo 1999, riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità, Gazzetta ufficiale delle Comunità europee, L 91 del 7.4.1999, pag. 10. L'articolo 3, paragrafo 3, lettera c), prevede che la Commissione europea può stabilire che i dispositivi degli utenti finali "siano costruiti in modo da contenere elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata dell'utente e dell'abbonato".

[26] Il Gruppo di lavoro apprezza le raccomandazioni della FTC a questo proposito nel rapporto informativo *Mobile Privacy Disclosures* di cui alla nota 6, ad esempio a pagina 15: "(…) *le piattaforme sono in una*

3.3.3 App store

I dispositivi intelligenti più diffusi hanno tutti un proprio app store e capita di frequente che un particolare sistema operativo sia profondamente integrato con un particolare app store. Spesso gli app store gestiscono i pagamenti per le applicazioni e possono anche supportare acquisti in-app che richiedono la registrazione dell'utente con nome, indirizzo e dati finanziari. Questi dati (direttamente) identificabili si possono combinare con i dati relativi all'acquisto e al comportamento d'uso e con dati ricavati o generati dal dispositivo (come il codice identificativo univoco). Per quanto concerne questi dati personali gli app store si possono considerare responsabili del trattamento dei dati, anche quando trasmettono le informazioni agli sviluppatori di applicazioni. Quando l'app store gestisce la cronologia dei download o degli utilizzi di applicazioni da parte dell'utente o strumenti analoghi per ripristinare applicazioni scaricate in precedenza si può considerare anche responsabile del trattamento dei dati personali trattati a tale scopo.

Un app store registra le credenziali di login e la cronologia di app acquistate in precedenza. Inoltre, chiede all'utente di fornire un numero di carta di credito che sarà memorizzato con l'account dell'utente. L'app store è il responsabile del trattamento dei dati per queste operazioni.

Viceversa, i siti web che consentono il download di una app da installare sul dispositivo senza autenticazione non si considerano responsabili del trattamento di dati personali.

Gli app store svolgono un ruolo importante per mettere gli sviluppatori di applicazioni nelle condizioni di fornire informazioni adeguate sull'applicazione, compresi i tipi di dati che essa è in grado di elaborare e per quali finalità, magari tenendone conto nella propria politica di ammissione (basata su controlli ex ante o ex post). In collaborazione con il produttore del sistema operativo, l'app store può definire un quadro per consentire agli sviluppatori di fornire avvisi informativi coerenti e significativi (quali simboli che rappresentano determinati generi di accesso a dati da sensori) mettendoli in evidenza nel catalogo dell'app store.

3.3.4 Terzi

I terzi coinvolti nel trattamento dei dati attraverso l'utilizzo di applicazioni sono numerosi.

Ad esempio, molte applicazioni gratuite sono finanziate da pubblicità che, tra l'altro, possono essere contestuali o personalizzate e rese possibili da strumenti di tracciamento quali marcatori (*cookie*) o altri identificativi del dispositivo. La pubblicità può essere costituita da un banner all'interno dell'app, da annunci esterni all'app che compaiono modificando le impostazioni di navigazione o tramite icone sul desktop del dispositivo mobile o mediante l'organizzazione personalizzata del contenuto dell'app (ad esempio risultati di ricerca sponsorizzati).

Di solito le pubblicità per le applicazioni sono fornite da reti pubblicitarie e analoghi intermediari che possono essere collegati o coincidere con il produttore del sistema operativo o l'app store. Come indicato nel parere 2/2010 del Gruppo di lavoro "articolo 29"[27], la pubblicità online spesso contempla

---

posizione unica per fornire informative coerenti attraverso le app e sono incoraggiate a farlo. In linea con le osservazioni del workshop, potrebbero anche considerare di pubblicare le informative più volte in diversi momenti (...)".

[27] Parere 2/2010 del Gruppo di lavoro "articolo 29" sulla pubblicità comportamentale online (giugno 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_it.pdf.

il trattamento di dati personali quali definiti all'articolo 2 della direttiva sulla protezione dei dati e interpretati dal Gruppo di lavoro stesso[28].

Altri esempi di terzi sono i fornitori di servizi analitici e di comunicazione. I primi aiutano gli sviluppatori di applicazioni a ottenere indicazioni sull'uso, sulla popolarità e sulla fruibilità delle loro applicazioni. I fornitori di servizi di comunicazione[29] possono svolgere un ruolo importante anche nel determinare le impostazioni predefinite e gli aggiornamenti di sicurezza di molti dispositivi e trattare dati sull'uso delle app. La loro personalizzazione ("*branding*") potrebbe avere delle conseguenze sulle possibili misure tecniche e funzionali a disposizione dell'utente per proteggere i propri dati personali.

Rispetto agli sviluppatori di applicazioni, i terzi possono svolgere due diversi ruoli. Il primo consiste nell'eseguire operazioni per il proprietario dell'app, ad esempio fornire dati analitici all'interno dell'app. In tal caso, quando agiscono esclusivamente per conto dello sviluppatore e non trattano dati per finalità proprie e/o non condividono dati tra sviluppatori, si può ritenere che agiscano in qualità di incaricati del trattamento dei dati.

Il secondo ruolo consiste nella raccolta di informazioni attraverso le applicazioni per offrire servizi aggiuntivi: fornire dati analitici su scala più ampia (popolarità dell'app, raccomandazione personalizzata) o evitare di mostrare la stessa pubblicità al medesimo utente. Quando i terzi trattano dati personali per finalità proprie agiscono in qualità di responsabili del trattamento dei dati e sono pertanto tenuti a rispettare tutte le disposizioni applicabili della direttiva sulla protezione dei dati[30]. Nel caso della pubblicità comportamentale, il responsabile del trattamento deve ottenere il valido consenso informato dell'utente per la raccolta e il trattamento di dati personali, ad esempio per l'analisi e la combinazione di dati personali e la creazione e/o applicazione di profili. Come già spiegato nel parere 2/2012 del Gruppo di lavoro "articolo 29" sulla pubblicità comportamentale online, il modo migliore per ottenere tale consenso implica l'uso di un meccanismo di opt-in preliminare.

Una società fornisce metriche per proprietari di applicazioni e pubblicitari attraverso l'uso di tracker incorporati nelle applicazioni dallo sviluppatore. I tracker della società possono quindi essere installati su molti dispositivi e app. Uno dei servizi consiste nell'informare gli sviluppatori su quali altre applicazioni utilizza l'utente tramite la raccolta di un identificativo univoco. La società definisce i mezzi (*per es. la tracciatura*) e le finalità dei propri strumenti prima di offrirli a sviluppatori, pubblicitari e altri terzi e agisce pertanto da responsabile del trattamento dei dati.

Nella misura in cui accedono a informazioni o le archiviano sul dispositivo intelligente, i terzi sono tenuti a rispettare il requisito del consenso di cui all'articolo 5, paragrafo 3, della direttiva e-privacy.

In quest'ambito, è importante notare che, in genere, gli utenti dispongono di possibilità limitate di installare su dispositivi intelligenti software in grado di controllare il trattamento di dati personali, comuni nell'ambiente web desktop. In alternativa all'utilizzo di cookie HTTP, i terzi spesso accedono a codici identificativi univoci per selezionare (gruppi di) utenti e offrire servizi mirati, compresa la pubblicità. Poiché gli utenti non possono modificare né cancellare molti di questi identificativi (quali i codici IMEI, IMSI, MSISDN[31] e gli identificativi univoci specifici aggiunti dal sistema operativo)

---

[28] Cfr. anche l'interpretazione del concetto di dati personali nel parere 4/2007 del Gruppo di lavoro "articolo 29" sul concetto di dati personali (giugno 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_it.pdf.

[29] I fornitori di servizi di comunicazione sono soggetti anche ad obblighi specifici del settore in materia di protezione dei dati non rientranti nell'ambito di applicazione del presente parere.

[30] Parere 2/2010 del Gruppo di lavoro "articolo 29" sulla pubblicità comportamentale online, pagg. 10-11.

[31] *Mobile Station Integrated Services Digital Network* (rete digitale integrata dell'abbonato mobile).

questi terzi possono potenzialmente trattare quantità significative di dati personali sfuggendo al controllo dell'utente finale.

3.4 Fondamento giuridico

Per procedere al trattamento di dati personali occorre una base giuridica, come indicato all'articolo 7 della direttiva sulla protezione dei dati, che distingue sei fondamenti giuridici per il trattamento dei dati: il consenso inequivocabile dell'interessato; la necessità per l'esecuzione di un contratto concluso con l'interessato; la salvaguardia dell'interesse vitale dell'interessato; la necessità per l'adempimento di un obbligo legale; (per le autorità pubbliche) l'esecuzione di un compito di interesse pubblico e il perseguimento di legittimi interessi (commerciali).

Per quanto concerne l'archiviazione di informazioni o l'accesso a informazioni già archiviate nel dispositivo intelligente, l'articolo 5, paragrafo 3, della direttiva e-privacy (ossia il requisito del consenso per l'archiviazione o il recupero di informazioni da un dispositivo) crea una limitazione/restrizione più dettagliata dei fondamenti giuridici di cui tenere conto.

3.4.1 Consenso preventivo all'installazione e al trattamento di dati personali

Nel caso delle applicazioni, il principale fondamento giuridico applicabile è il consenso. Con l'installazione di un'applicazione, nel dispositivo dell'utente finale vengono inserite delle informazioni. Molte applicazioni accedono anche a dati memorizzati nel dispositivo, a contatti nella rubrica, fotografie, filmati e altri documenti personali. In tutti questi casi, l'articolo 5, paragrafo 3, della direttiva e-privacy richiede il consenso dell'utente, dopo che è stato informato in modo chiaro e completo, prima dell'archiviazione o del recupero di informazioni dal dispositivo.

È importante notare la distinzione tra il consenso richiesto per inserire o consultare informazioni nel dispositivo e il consenso necessario per legittimare il trattamento di diversi tipi di dati personali. Benché i due requisiti siano applicabili simultaneamente, ciascuno in virtù di una diversa base giuridica, sono entrambi soggetti alla condizione che si tratti di una "manifestazione di volontà *libera, specifica e informata*" (ai sensi della definizione all'articolo 2, lettera h), della direttiva sulla protezione dei dati). Di conseguenza, i due tipi di consenso si possono fondere nella pratica, durante l'installazione o prima che l'applicazione cominci a raccogliere dati personali dal dispositivo, purché l'utente sia reso consapevole in modo inequivocabile di quello a cui acconsente.

Molti app store offrono agli sviluppatori l'opportunità di informare gli utenti finali in merito alle funzioni di base di un'applicazione prima della sua installazione e richiedono un'azione positiva dell'utente prima che l'applicazione venga scaricata e installata (ossia cliccare su un tasto "installa"). In talune circostanze, un'azione di questo tipo può soddisfare il requisito del consenso di cui all'articolo 5, paragrafo 3, ma è improbabile che fornisca informazioni sufficienti per la validità del consenso ai fini del trattamento di dati personali. L'argomento è già stato discusso dal Gruppo di lavoro "articolo 29" nel suo parere sulla definizione di consenso[32].

Nel contesto dei dispositivi intelligenti, "libera" significa che l'utente deve poter scegliere se accettare o rifiutare il trattamento dei suoi dati personali. Quindi, se un'applicazione richiede il trattamento di dati personali, l'utente deve essere libero di accettare o rifiutare, senza trovarsi di fronte a uno schermo

[32] Parere 15/2011 del Gruppo di lavoro "articolo 29" sulla definizione di consenso (luglio 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_it.pdf.

contenente un'unica opzione "Sì, accetto", per completare l'installazione; deve essere disponibile anche un'opzione "Cancella" o che comunque blocchi l'installazione.

"Informata" significa che l'interessato deve disporre delle informazioni necessarie per formulare un giudizio accurato[33]. Onde evitare ambiguità, le informazioni devono essere disponibili prima di qualunque trattamento di dati personali, ivi compreso il trattamento che potrebbe avere luogo durante l'installazione, ad esempio per scopi di *debugging* o *tracking*. Il contenuto e la forma di tali informazioni sono trattati nel paragrafo 3.7 del presente parere.

"Specifica" significa che la manifestazione di volontà deve riferirsi al trattamento di un particolare dato o di una categoria limitata di dati. Per questo motivo, il semplice clic su un tasto "installa" non si può considerare un valido consenso per il trattamento di dati personali, in virtù del fatto che il consenso non può essere un'autorizzazione formulata genericamente. In alcuni casi, gli utenti sono in grado di fornire un consenso granulare, laddove il consenso è richiesto per ciascun tipo di dati ai quali l'applicazione intende accedere[34]. Un simile approccio soddisfa due importanti requisiti giuridici: in primo luogo quello di informare adeguatamente l'utente in merito a elementi importanti del servizio e in secondo luogo quello di chiedere il consenso specifico per ognuno di essi[35]. L'approccio alternativo per cui lo sviluppatore chiede ai propri utenti di accettare una lunga serie di termini e condizioni e/o politiche sulla privacy non costituisce un consenso specifico[36].

La specificità si riferisce anche alla prassi di tracciare il comportamento dell'utente da parte di pubblicitari e altri terzi. Le impostazioni di default previste da sistemi operativi e applicazioni devono essere tali da evitare qualunque tracciamento (*tracking*), per consentire agli utenti di esprimere un consenso specifico a questo tipo di trattamento dei dati. Le impostazioni predefinite non possono essere eluse da terzi, come spesso accade attualmente con i meccanismi di "Do Not Track" inseriti nei *browser*.

Esempi di consenso specifico

Un'applicazione fornisce informazioni sui ristoranti nelle vicinanze. Per l'installazione, lo sviluppatore deve ottenere il consenso. Per accedere ai dati di geolocalizzazione, lo sviluppatore deve chiede il consenso separatamente, ad esempio durante l'installazione o prima di accedere alla geolocalizzazione. Per consenso specifico s'intende il consenso limitato allo scopo specifico di informare l'utente in merito a ristoranti nelle vicinanze. Quindi è possibile accedere a dati di geolocalizzazione dal dispositivo solo quando l'utente utilizza l'applicazione a tale scopo. Il consenso dell'utente al trattamento di dati di geolocalizzazione non permette all'applicazione di raccogliere costantemente dati sull'ubicazione dal dispositivo. Questo ulteriore trattamento richiederebbe informazioni aggiuntive e un consenso separato.

---

[33] Idem, pag. 19.

[34] Consenso granulare significa che le persone possono controllare con esattezza (in modo specifico) quali funzioni di trattamento di dati offerte dall'applicazione intendono attivare.

[35] La necessità di tale consenso granulare è anche espressamente sostenuta dalla FTC nel suo rapporto più recente (cfr. nota 6), pagg. 15-16: "(…) *le piattaforme dovrebbero considerare di fornire informative in tempo reale (just-in-time) e ottenere l'esplicito consenso affermativo alla raccolta di altri contenuti che molti consumatori troverebbero sensibili in molti contesti, quali fotografie, contatti, appuntamenti o la registrazione di contenuti audio e video"*.

[36] Idem, pagg. 34-35: "*Il consenso generico senza una precisa indicazione dell'intento del trattamento al quale l'interessato acconsente non soddisfa il presente requisito. Ciò significa che l'informazione sulla finalità del trattamento non deve essere compresa nelle disposizioni generali, bensì in una clausola di consenso separata"*.

Analogamente, quando una app di comunicazione accede alla rubrica dei contatti, l'utente deve essere in grado di selezionare i contatti con i quali intende comunicare, invece di essere costretto a concedere l'accesso all'intera rubrica (compresi i contatti di persone che non utilizzano il servizio e non possono aver acconsentito al trattamento dei propri dati).

Tuttavia, è importante notare che, anche se il consenso soddisfa i tre elementi descritti sopra, non rappresenta un'autorizzazione a trattamenti sleali e illeciti. Se il trattamento è eccessivo e/o sproporzionato rispetto alla finalità, anche se l'utente vi ha acconsentito, lo sviluppatore dell'applicazione non disporrà di un fondamento giuridico valido, violando probabilmente la direttiva sulla protezione dei dati.

Esempio di trattamento dei dati eccessivo e illecito

Una app per la sveglia offre una funzione facoltativa per cui l'utente può dare l'ordine verbale di spegnere la sveglia o lasciarla in funzione "snooze". In questo esempio, il consenso alla registrazione sarebbe limitato a quando la sveglia suona. L'eventuale monitoraggio o registrazione o audio quando la sveglia non suona sarebbero considerati eccessivi e illeciti.

In caso di applicazioni automaticamente incorporate nel dispositivo (prima che ne diventi proprietario l'utente finale) o altri trattamenti effettuati dal sistema operativo che si basano sul consenso come fondamento giuridico, i responsabili del trattamento dei dati devono valutare attentamente se tale consenso è effettivamente valido. In molti casi, bisognerebbe considerare un meccanismo di consenso separato, magari quando la app viene attivata per la prima volta, per offrire al responsabile del trattamento un'adeguata opportunità di informare pienamente l'utente finale. Nell'ipotesi di categorie particolari di dati, come definite all'articolo 8 della direttiva sulla protezione dei dati, il consenso deve essere esplicito.

Infine, gli utenti devono avere l'opportunità di revocare il loro consenso in modo semplice ed efficace. Questo aspetto sarà trattato nella sezione 3.8 del presente parere.

3.4.2 Fondamenti giuridici del trattamento dei dati durante l'utilizzo dell'applicazione

Come illustrato in precedenza, il consenso è il fondamento giuridico necessario per permettere allo sviluppatore di leggere e/o scrivere legalmente informazioni e, di conseguenza, procedere al trattamento di dati personali. In una fase successiva, durante l'utilizzo dell'applicazione, lo sviluppatore può invocare altri fondamenti giuridici per ulteriori tipologie di trattamento, nella misura in cui non comportino il trattamento di dati personali sensibili.

Tali fondamenti giuridici possono essere la necessità di eseguire un contratto concluso con l'interessato o di perseguire interessi (commerciali) legittimi, ai sensi dell'articolo 7, lettere b) e f), della direttiva sulla protezione dei dati.

Detti fondamenti giuridici si limitano al trattamento di dati personali non sensibili di un utente specifico e possono essere invocati solo nella misura in cui un determinato trattamento sia strettamente necessario per svolgere il servizio desiderato o, nel caso dell'articolo 7, lettera f), solo se non prevalgono l'interesse o i diritti e le libertà fondamentali dell'interessato.

Esempi di fondamento giuridico contrattuale

Un utente acconsente all'installazione di una app di mobile banking. Per adempiere a una richiesta di effettuazione di un pagamento la banca non deve chiedere il consenso separato dell'utente a divulgare il suo nome e numero di conto bancario al beneficiario del pagamento. Queste informazioni sono strettamente necessarie per eseguire il contratto con questo specifico utente e pertanto la banca trova un fondamento giuridico nell'articolo 7, lettera b), della direttiva sulla protezione dei dati. Stesso ragionamento vale per le app di comunicazione; quando forniscono informazioni essenziali quali nome di account, indirizzo e-mail o numero di telefono a un altro individuo con cui l'utente desidera comunicare, la divulgazione è ovviamente necessaria per l'esecuzione del contratto.

3.5 Limitazione della finalità e minimizzazione dei dati

I principi fondamentali alla base della direttiva sulla protezione dei dati sono la limitazione della finalità e la minimizzazione dei dati. La limitazione della finalità consente agli utenti di scegliere volontariamente di affidare a un terzo i propri dati personali poiché sanno in che modo vengono usati e sono in grado di basarsi sulla descrizione della finalità per capire per quali scopi saranno utilizzati. Le finalità del trattamento dei dati devono pertanto essere ben definite e comprensibili per un utente medio privo di conoscenze specialistiche di tipo giuridico o tecnico.

Nel contempo, la limitazione della finalità impone che gli sviluppatori di applicazioni abbiano un'idea precisa dei propri obiettivi prima di cominciare a raccogliere dati personali dagli utenti. I dati personali possono essere trattati solo "lealmente e lecitamente" (articolo 6, paragrafo 1, lettera a), della direttiva sulla protezione dei dati) e gli scopi devono essere definiti prima dell'inizio del trattamento.

Il principio di limitazione della finalità esclude improvvisi cambiamenti nelle condizioni fondamentali del trattamento.

Ad esempio, se una app originariamente aveva lo scopo di consentire agli utenti di scambiarsi e-mail, ma lo sviluppatore decide di modificare il modello di business e accorpa gli indirizzi e-mail degli utenti con i numeri telefonici di utenti di un'altra app. I rispettivi responsabili del trattamento dei dati a quel punto dovrebbero contattare singolarmente tutti gli utenti per richiedere il loro inequivocabile consenso preliminare per questa nuova finalità del trattamento dei loro dati personali.

La limitazione della finalità procede di pari passo con il principio della minimizzazione dei dati. Al fine di impedire trattamenti inutili e potenzialmente illeciti, gli sviluppatori di applicazioni devono valutare attentamente quali dati sono strettamente necessari per eseguire la funzionalità desiderata.

Potendo accedere a molte delle funzionalità del dispositivo, le applicazioni sono in grado di eseguire molte funzioni, come inviare un SMS invisibile, accedere a immagini e all'intera rubrica. Molti app store prevedono aggiornamenti (semi)automatici dove lo sviluppatore può integrare nuove funzioni e renderle disponibili con un intervento minimo o nullo dell'utente finale.

Il Gruppo di lavoro sottolinea a questo punto che i terzi che accedono ai dati dell'utente attraverso le applicazioni devono rispettare i principi di limitazione della finalità e minimizzazione dei dati. Non si dovrebbero utilizzare i codici identificativi dei dispositivi, univoci e spesso non modificabili, per scopi pubblicitari e/o analitici mirati, data l'impossibilità degli utenti di revocare il proprio consenso. Gli sviluppatori di applicazioni dovrebbero garantire che si impedisca l'estensione indebita delle funzionalità (*function creep*) evitando di modificare il trattamento da una versione all'altra di una stessa applicazione senza fornire all'utente finale le opportune informazioni e la possibilità di revocare il trattamento o l'intero servizio. Inoltre, agli utenti dovrebbero essere offerti i mezzi tecnici per

verificare gli enunciati in merito agli scopi dichiarati, consentendo loro di accedere a informazioni sulla quantità di traffico in uscita per applicazione, in relazione al traffico avviato dall'utente.

L'informazione e i controlli dell'utente sono fondamentali per garantire il rispetto dei principi di minimizzazione dei dati e limitazione della finalità.

L'accesso ai dati presenti nel dispositivo attraverso le API offre ai produttori di OS e dispositivi e agli app store un'opportunità per applicare regole specifiche e fornire informazioni corrette agli utenti finali. Ad esempio, i produttori di OS e dispositivi dovrebbero offrire una API con controlli precisi per distinguere ciascun tipo di dati e assicurare che gli sviluppatori possano richiedere l'accesso solo ai dati che sono strettamente necessari per la funzionalità (lecita) della loro applicazione. I tipi di dati richiesti dallo sviluppatore potranno quindi essere chiaramente evidenziati nell'app store per informare l'utente prima dell'installazione.

A questo proposito, il controllo sull'accesso ai dati archiviati nel dispositivo si basa su diversi meccanismi:

a. I produttori di OS e dispositivi e gli app store definiscono le **regole** per la presentazione di applicazioni nell'app store: gli sviluppatori devono rispettare queste regole se non vogliono rischiare di non essere presenti negli app store[37].
b. Le **API** dei sistemi operativi definiscono metodi standard per accedere ai dati memorizzati nel telefono ai quali hanno accesso le app e influiscono anche sulla raccolta di dati da parte del server.
c. **Controlli ex-ante** – controlli esistenti prima dell'installazione di una app[38].
d. **Controlli ex-post** – controlli introdotti dopo aver installato una app.

3.6 Sicurezza

Ai sensi dell'articolo 17 della direttiva sulla protezione dei dati, i responsabili e gli incaricati del trattamento dei dati devono prendere le necessarie misure organizzative e tecniche per garantire le protezione dei dati personali oggetto del trattamento. Di conseguenza, le misure devono essere prese da tutti gli attori individuati nella sezione 3.3, ciascuno secondo il proprio ruolo e responsabilità.

L'obiettivo dell'osservanza dell'obbligo di sicurezza dei trattamenti è duplice: autorizza gli utenti a controlli più rigorosi sui propri dati e rafforza la fiducia nelle entità che effettivamente gestiscono i dati degli utenti.

Per adempiere ai rispettivi obblighi di sicurezza in quanto responsabili del trattamento, gli sviluppatori di applicazioni, gli app store, i produttori di OS e dispositivi e i terzi devono tenere conto dei principi di *privacy by design* e *by default*. Questo richiede una valutazione costante dei rischi esistenti e futuri per la protezione dei dati, nonché l'attuazione e la valutazione di misure di attenuazione efficaci, tra cui la minimizzazione dei dati.

---

[37] I dispositivi *jailbroken* consentono l'installazione di app alternative a quelle degli store ufficiali; anche i dispositivi Android consentono l'installazione di app da altre fonti.

[38] Con il caso particolare delle app preinstallate.

Sviluppatori di applicazioni

Esistono molte linee guida disponibili al pubblico concernenti la sicurezza delle applicazioni per dispositivi mobili pubblicate da produttori di OS e terzi indipendenti, ad esempio dall'ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione)[39].

L'esame delle migliori prassi in fatto di sicurezza nello sviluppo di applicazioni non rientra nell'ambito del presente parere; tuttavia, il Gruppo di lavoro intende sfruttare questa opportunità per esaminare quelle che presentano un impatto potenzialmente grave sui diritti fondamentali degli utenti di applicazioni.

Prima di progettare un'applicazione è importante decidere dove saranno archiviati i dati. In alcuni casi, i dati dell'utente sono archiviati nel dispositivo, ma gli sviluppatori possono anche servirsi di un'architettura client-server. Questo significa che i dati personali vengono trasferiti o copiati nei sistemi del fornitore di servizi. L'archiviazione o il trattamento di dati nel dispositivo garantisce agli utenti finali il massimo controllo su detti dati, ad esempio con la possibilità di cancellarli in caso di revoca del consenso al trattamento. Tuttavia, l'archiviazione sicura dei dati presso un'ubicazione remota può agevolare il loro recupero a seguito della perdita o del furto di un dispositivo. Sono possibili anche soluzioni intermedie.

Gli sviluppatori di applicazioni devono individuare politiche chiare in materia di sviluppo e distribuzione del software. Anche i produttori di OS e dispositivi svolgono un ruolo nel promuovere il trattamento sicuro dei dati nelle applicazioni, che sarà esaminato in seguito. In secondo luogo, gli sviluppatori e gli app store devono studiare e realizzare un ambiente favorevole alla sicurezza, con strumenti atti a impedire la diffusione di applicazioni "maligne" e consentire l'installazione/la disinstallazione agevole di ciascuna applicazione.

Le buone prassi che si possono adottare nella fase di progettazione di un'applicazione comprendono la riduzione al minimo delle linee e della complessità del codice e l'introduzione di controlli per escludere il trasferimento o la compromissione involontari di dati. Inoltre, tutti gli input dovrebbero essere convalidati per impedire casi di riempimento del buffer o episodi di attacchi con iniezione. Altri meccanismi di sicurezza degni di nota comprendono strategie adeguate di gestione di *patch* di sicurezza e l'esecuzione di verifiche di sicurezza del sistema periodiche e indipendenti. Inoltre, i criteri per la progettazione di applicazioni dovrebbero comprendere l'attuazione del principio del privilegio minimo per default, per cui alle applicazioni è consentito accedere esclusivamente ai dati di cui hanno veramente bisogno per rendere disponibile una funzionalità all'utente. Gli sviluppatori e gli app store dovrebbero anche incoraggiare gli utenti, con apposite avvertenze, a integrare queste buone prassi di progettazione con prassi virtuose nell'uso, come aggiornare le app alle ultime versioni disponibili e ricordarsi di evitare di utilizzare la stessa password per diversi servizi.

Nella fase di progettazione dell'applicazione, gli sviluppatori devono anche prendere misure per impedire l'accesso non autorizzato a dati personali, garantendone la protezione sia quando sono in transito sia quando sono archiviati, se del caso.

Le applicazioni per dispositivi mobili dovrebbero funzionare in ubicazioni specifiche all'interno della memoria dei dispositivi (*sandbox*[40]), al fine di ridurre le conseguenze di malware/app maligne. In

---

[39] ENISA "*Smartphone Secure Development Guideline*": http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

[40] Un *sandbox* è un meccanismo di sicurezza per separare programmi in esecuzione.

stretta collaborazione con i produttori di OS e/o gli app store, gli sviluppatori devono utilizzare i meccanismi disponibili che consentono agli utenti di vedere quali dati vengono trattati e da quali applicazioni, e di attivare e disattivare selettivamente le autorizzazioni. L'uso di funzionalità nascoste non dovrebbe essere consentito.

Gli sviluppatori di applicazioni devono valutare attentamente i propri metodi di identificazione e autenticazione degli utenti. Non dovrebbero utilizzare identificativi persistenti (specifici di un dispositivo), ma piuttosto utilizzare identificativi a bassa entropia specifici di un'applicazione o identificativi temporanei per evitare il tracciamento degli utenti nel corso del tempo. Si dovrebbero considerare meccanismi di autenticazione rispettosi della privacy. Nell'autenticazione degli utenti, gli sviluppatori devono prestare un'attenzione particolare alla gestione dell'identificativo dell'utente e della password. Quest'ultima, deve essere memorizzata in modo criptato e sicuro, come un valore hash crittografico. Una tecnica utile per incoraggiare l'uso di password migliori è quella di mettere a disposizione degli utenti un test sulla robustezza delle password prescelte (controllo dell'entropia). Se del caso (accesso a dati sensibili, ma anche accesso a risorse a pagamento) si potrebbe prevedere una ri-autenticazione, anche mediante molteplici fattori e canali diversi (ad esempio codice di accesso inviato via SMS) e/o l'utilizzo di dati di autenticazione collegati all'utente finale (invece che al dispositivo). Inoltre, nel selezionare gli identificativi di sessione, si dovrebbero utilizzare stringhe non prevedibili, magari in combinazione con informazioni contestuali come data e ora, ma anche indirizzo IP o dati di geolocalizzazione.

Gli sviluppatori di applicazioni dovrebbero anche tenere conto dei requisiti indicati dalla direttiva e-privacy per quanto concerne le violazioni dei dati personali e la necessità di informare gli utenti in modo proattivo. Attualmente, tali requisiti si applicano esclusivamente ai fornitori di servizi di comunicazione elettronica disponibili al pubblico, ma si prevede che l'obbligo sarà esteso a tutti i responsabili (e gli incaricati) del trattamento dei dati in virtù del futuro regolamento sulla protezione dei dati proposto dalla Commissione (COM 2012/0011/COD). Questo rafforza ulteriormente la necessità di elaborare, e sottoporre a costante valutazione, un "piano di sicurezza" completo, che copra la raccolta, l'archiviazione e il trattamento di dati personali, al fine di impedire che si verifichino violazioni e di evitare di incorrere nelle pesanti sanzioni pecuniarie previste in simili casi. Il piano di sicurezza, tra l'altro, deve anche prevedere la gestione delle vulnerabilità e la pubblicazione tempestiva e sicura di correzioni affidabili degli errori (*bug fix*).

La responsabilità degli sviluppatori di applicazioni in merito alla sicurezza dei loro prodotti non termina con l'immissione sul mercato di una versione funzionante. Come qualsiasi altro prodotto sofware, anche le app possono presentare difetti e vulnerabilità in termini di sicurezza e gli sviluppatori devono studiare apposite correzioni, o *patch*, e fornirle ai soggetti che possono metterle a disposizione degli utenti, o provvedervi direttamente.

App store

Gli app store sono importanti intermediari tra utenti finali e sviluppatori e dovrebbero effettuare una serie di controlli approfonditi ed efficaci sulle applicazioni prima di consentire la loro immissione sul mercato, fornendo informazioni sui controlli effettivamente svolti, ivi comprese informazioni sui tipi di verifiche di conformità alle norme sulla protezione dei dati.

Benché questa misura non sia efficace al 100% per eliminare la diffusione di app maligne, le statistiche rivelano che questa prassi riduce fortemente i casi di funzionalità maligne negli app store "ufficiali"[41]. Per far fronte al gran numero di applicazioni che vengono presentate quotidianamente,

[41] *"Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets"*, Y Zhou et al., Network and Distributed System Security Symposium (NDSS) 2012.

questo processo potrebbe beneficiare della disponibilità di strumenti di analisi automatici, nonché della realizzazione di canali per lo scambio di informazioni tra esperti di sicurezza e professionisti del software, nonché di procedure e politiche efficaci per gestire i problemi segnalati.

Oltre ad essere sottoposte a verifica prima dell'ammissione negli app store, le applicazioni dovrebbero essere soggette a un meccanismo di reputazione presso il pubblico. Gli utenti non dovrebbero limitarsi a classificare le app solo per quanto sono "forti", ma anche sulla base delle loro funzionalità, con un riferimento specifico alla privacy e ai meccanismi di sicurezza. Inoltre, i meccanismi di reputazione dovrebbero essere studiati in modo da impedire recensioni false. I meccanismi di qualifica e reputazione per le app possono rivelarsi efficaci anche nella costruzione di una fiducia reciproca tra le varie entità, in particolare se i dati sono scambiati attraverso una lunga catena di terzi.
Spesso gli app store adottano un metodo per disinstallare a distanza app maligne o poco sicure. Questo meccanismo, se non è studiato correttamente, può costituire un ostacolo per la responsabilizzazione degli utenti ai fini di un controllo più rigoroso dei propri dati. Nel rispetto della privacy, lo strumento utilizzato dall'app store per la disinstallazione a distanza delle applicazioni dovrebbe basarsi sull'informazione e sul consenso dell'utente. Inoltre, da un punto di vista più pratico, gli utenti dovrebbero disporre di canali di feedback per segnalare problemi di sicurezza nelle applicazioni e riferire sull'efficacia di eventuali procedure di rimozione a distanza.

Come gli sviluppatori, anche gli app store dovrebbero essere consapevoli dei futuri obblighi di notifica di violazioni di dati personali e collaborare strettamente con gli sviluppatori per impedire il verificarsi di tali violazioni.

Produttori di OS e dispositivi
Anche i produttori di OS e dispositivi sono attori importanti nella definizione di norme minime e migliori prassi tra gli sviluppatori di applicazioni, non solo per quanto concerne la sicurezza del software sottostante e delle API, ma anche con riguardo agli strumenti, agli orientamenti e ai materiali di riferimento offerti. I produttori di OS e dispositivi dovrebbero rendere disponibili algoritmi di crittografia validi e noti e supportare chiavi di lunghezza adeguata. Essi, inoltre, dovrebbero mettere a disposizione degli sviluppatori meccanismi di autenticazione efficaci e sicuri (ad es. l'uso di certificati firmati da autorità di certificazione affidabili per verificare l'autorizzazione di una risorsa remota). In questo modo, gli sviluppatori non avrebbero la necessità di sviluppare meccanismi di autenticazione di proprietà esclusiva. Nella pratica, tali misure sono scarsamente attuate e possono rappresentare una grave vulnerabilità[42].

L'accesso ai dati personali e il loro trattamento da parte di applicazioni dovrebbero essere gestiti attraverso classi e metodi integrati di API che offrano controlli e salvaguardie adeguati. I produttori di OS e dispositivi dovrebbero garantire che i metodi e le funzioni che consentono l'accesso a dati personali includano caratteristiche volte ad effettuare richieste di consenso specifiche. Allo stesso modo, dovrebbero essere adottate misure per escludere o limitare l'accesso ai dati personali utilizzando funzioni di basso livello o altri mezzi in grado di eludere controlli e salvaguardie incorporati nelle API.

---

[42] Recentemente è stato rilevato che la mancanza di indicatori di sicurezza visivi per l'utilizzo di protocolli SSL/TLS e l'uso inadeguato di SSL/TLS si possono sfruttare per lanciare attacchi *Man-in-the-Middle* (MITM). Secondo ricerche recenti, la base cumulativa di app installate con vulnerabilità confermate nei confronti di attacchi MITM comprende diversi milioni di utenti. "*Why Eve and Mallory Love Android: An Analysis of Android SL (In)*Security", Bernd Freisleben e Matthew Smith, 19th ACM Conference on Computer and Communications Security (ACM CCS 2012).

I produttori di OS e dispositivi devono anche inserire nei dispositivi tracce di controllo (*audit trail*) chiare, affinché gli utenti possano vedere distintamente quali app hanno avuto accesso ai dati sui loro dispositivi.

Tutte le parti devono rispondere rapidamente alle vulnerabilità in termini di sicurezza, affinché gli utenti finali non risultino inutilmente esposti a difetti di sicurezza. Purtroppo alcuni produttori di OS e dispositivi (e operatori delle telecomunicazioni che distribuiscono dispositivi brandizzati) non forniscono assistenza a lungo termine a versioni successive del sistema operativo, lasciando gli utenti esposti a note vulnerabilità in termini di sicurezza. I produttori di OS e dispositivi, insieme agli sviluppatori, devono informare anticipatamente gli utenti finali in merito alla periodicità prevista per gli aggiornamenti di sicurezza. Inoltre, se la soluzione a un problema di sicurezza richiede un aggiornamento, essi dovrebbero informarne al più presto gli utenti.

Terzi
Anche i terzi, principalmente pubblicitari e fornitori di dati analitici, sono tenuti ad applicare le considerazioni e le caratteristiche di cui sopra in fatto di sicurezza quando procedono alla raccolta e al trattamento di dati personali per finalità proprie, ad esempio mediante la trasmissione sicura e l'archiviazione criptata di codici identificativi univoci di dispositivi e utenti di app e altri dati personali.

3.7 Informazione

3.7.1 Obbligo di informazione e contenuto richiesto

Ai sensi dell'articolo 10 della direttiva sulla protezione dei dati, ciascun interessato ha il diritto di conoscere l'identità del responsabile del trattamento dei suoi dati personali. Inoltre, nel contesto delle applicazioni, l'utente finale ha il diritto di sapere che tipo di dati personali sono oggetto di trattamento e per quali finalità si intende utilizzarli. Se i suoi dati personali sono raccolti da altri attori dell'ecosistema delle applicazioni (come descritto nella sezione 3.3 del presente parere), l'utente finale, a norma dell'articolo 11 della direttiva sulla protezione dei dati, ha comunque il diritto di essere informato in merito al trattamento dei dati, secondo le stesse modalità descritte. Di conseguenza, in caso di trattamento di dati personali, i responsabili del trattamento pertinenti sono tenuti a informare i potenziali utenti almeno sui seguenti aspetti:

- chi sono (identità e recapiti),
- le precise categorie di dati personali oggetto di raccolta e trattamento,
- il motivo (per quali finalità precise),
- se i dati saranno divulgati a terzi
- in che modo gli utenti possono esercitare i propri diritti, in termini di revoca del consenso e cancellazione di dati.

La disponibilità di queste informazioni sul trattamento dei dati personali è fondamentale per ottenere il consenso dell'utente, che può ritenersi valido solo se l'interessato è stato previamente informato in merito agli elementi chiave del trattamento dei dati. La comunicazione di tali informazioni solo dopo che l'applicazione ha avviato il trattamento dei dati personali (spesso già durante l'installazione) non è ritenuta sufficiente, né legalmente valida. In linea con il rapporto informativo FTC, il Gruppo di lavoro sottolinea la necessità di fornire informazioni nel momento in cui sono rilevanti per i consumatori, appena prima della raccolta dei dati da parte delle applicazioni. L'informazione in merito a quali dati sono oggetto del trattamento è particolarmente importante in considerazione dell'ampio accesso a sensori e strutture di dati presenti sul dispositivo generalmente concesso alle applicazioni e che in molti casi non è evidente a livello intuitivo. Un'informazione adeguata è inoltre di vitale importanza quando l'applicazione tratta categorie particolari di dati personali, ad esempio, concernenti condizioni di salute, convinzioni politiche, orientamento sessuale, ecc. Infine, lo sviluppatore dovrebbe differenziare chiaramente le informazioni obbligatorie e quelle facoltative e il sistema dovrebbe

consentire all'utente di rifiutare l'accesso alle informazioni facoltative utilizzando opzioni predefinite rispettose della privacy.

Per quanto concerne l'identità del responsabile del trattamento, occorre che gli utenti sappiano chi è legalmente responsabile del trattamento dei loro dati personali e in che modo è possibile contattare tale responsabile. Diversamente, non possono esercitare i loro diritti, come il diritto di accesso a dati archiviati (da remoto) che li riguardano. Data la natura frammentata del panorama delle applicazioni, è essenziale che ogni app preveda un unico punto di contatto, che assuma la responsabilità di tutti i trattamenti realizzati tramite la app. Non deve essere compito dell'utente finale individuare le relazioni tra gli sviluppatori e le altre parti che procedono al trattamento di dati personali mediante l'applicazione.

Per quanto concerne le finalità, gli utenti finali devono essere adeguatamente informati su quali dati personali vengono raccolti e per quale motivo. Inoltre, si dovrebbe comunicare agli utenti con un linguaggio semplice e chiaro se i dati potranno essere riutilizzati da terzi e in tal caso per quali scopi. Indicazioni generiche come "innovazione del prodotto" sono inadeguate per informare gli utenti. Occorre dichiarare apertamente se agli utenti sarà richiesto di acconsentire alla condivisione di dati con terzi per scopi pubblicitari e/o analitici. Gli app store hanno una responsabilità rilevante per garantire che queste informazioni siano disponibili e facilmente accessibili per ciascuna applicazione.

Agli app store viene attribuita un'importante responsabilità per garantire un'informazione corretta. Si raccomanda fortemente l'uso di simboli visivi o icone sull'utilizzo dei dati per informare gli utenti in merito alle tipologie di trattamento dei dati.

In aggiunta all'informativa minima di cui sopra, necessaria per ottenere il consenso dell'utente, il Gruppo di lavoro raccomanda fortemente, in considerazione del trattamento corretto dei dati personali, che i responsabili del trattamento forniscano agli utenti anche informazioni su quanto segue:

- considerazioni sulla proporzionalità per le tipologie di dati raccolti o visionati sul dispositivo,
- periodi di conservazione dei dati,
- misure di sicurezza applicate dal responsabile del trattamento.

Il Gruppo di lavoro raccomanda inoltre che gli sviluppatori di applicazioni includano nella propria politica sulla privacy dedicata agli utenti europei informazioni sulla conformità alla normativa sulla protezione dei dati, ivi compresi possibili trasferimenti di dati personali, ad esempio, dall'Europa agli USA e se e come, in tal caso, l'applicazione rispetta il quadro di riferimento Safe Harbor (approdo sicuro).

3.7.2 Formato dell'informazione

Le informazioni essenziali sul trattamento dei dati devono essere disponibili agli utenti prima dell'installazione dell'applicazione, tramite l'app store. In secondo luogo, le informazioni pertinenti sul trattamento dei dati devono essere accessibili anche dall'interno della app, dopo l'installazione.

In qualità di responsabili congiunti del trattamento insieme agli sviluppatori per quanto concerne l'informazione, gli app store devono garantire che ogni applicazione fornisca le informazioni essenziali sul trattamento dei dati personali, verificando i link alle pagine con informazioni sulla privacy ed eliminando le applicazioni con collegamenti interrotti o comunque con informazioni non accessibili sul trattamento dei dati.

Il Gruppo di lavoro raccomanda che le informazioni sul trattamento dei dati personali siano disponibili e facilmente individuabili, ad esempio anche all'interno dell'app store e preferibilmente sui normali siti web dello sviluppatore responsabile dell'applicazione. È inaccettabile che gli utenti si trovino a dover ricercare in rete le informazioni sulle politiche di trattamento dei dati dell'applicazione, invece di esserne informati direttamente dallo sviluppatore o altri responsabili del trattamento dei dati.

Ogni applicazione dovrebbe prevedere, come minimo, una politica sulla privacy leggibile, comprensibile e facilmente accessibile, che comprenda tutte le informazioni summenzionate. Molte applicazioni non soddisfano neppure questo requisito minimo di trasparenza. Secondo lo studio FPF del giugno 2012, il 56% delle app a pagamento e quasi il 30% delle app gratuite non prevedono una politica sulla privacy.

Le applicazioni che non trattano i dati personali, né sono progettate per farlo, dovrebbero dichiararlo esplicitamente nella politica sulla privacy.

Naturalmente esistono alcune limitazioni alla quantità di informazioni che si possono presentare su un piccolo schermo, ma questo non giustifica il fatto di non informare adeguatamente gli utenti finali. Si possono adottare numerose strategie per garantire che gli utenti siano a conoscenza degli elementi fondamentali del servizio. Il Gruppo di lavoro rileva alcuni vantaggi nell'utilizzo di avvertenze multistrato, come indicato in dettaglio nel parere 10/2004[43], dove l'avvertenza iniziale all'utente contiene le informazioni minime richieste dal quadro giuridico dell'UE e ulteriori informazioni sono disponibili tramite collegamenti alla politica sulla privacy nella sua versione integrale. Le informazioni dovrebbero essere presentate direttamente sullo schermo, in maniera facilmente accessibile e ben visibile. Oltre a ricevere informazioni generali adatte al piccolo schermo dei dispositivi mobili, gli utenti devono essere in grado di collegarsi a spiegazioni più ampie, ad esempio contenute nella politica sulla privacy, su come l'applicazione utilizza i dati personali, chi è il responsabile del trattamento dei dati e dove è possibile esercitare i propri diritti di utente.

Tale approccio può essere associato all'utilizzo di icone, immagini, video e audio, nonché notifiche contestuali in tempo reale quando una app accede alla rubrica o a foto[44]. Queste icone devono essere significative, ossia chiare, autoesplicative e inequivocabili. Chiaramente, il produttore di OS condivide una parte rilevante di responsabilità nell'agevolare l'utilizzo di queste icone.

In effetti, gli sviluppatori di applicazioni eccellono nella programmazione e nella progettazione di interfacce complesse per piccoli schermi e il Gruppo di lavoro sollecita il settore a sfruttare questo talento creativo per fornire soluzioni più innovative ai fini di un'informazione più efficace agli utenti su dispositivi mobili. Per garantire che le informazioni siano veramente comprensibili per gli utenti privi di conoscenze tecniche o giuridiche, il Gruppo di lavoro (in linea con il rapporto informativo FTC) raccomanda vivamente di sottoporre a test tra i consumatori le strategie di informazione prescelte[45].

3.8 Diritti dell'interessato

Secondo gli articoli 12 e 14 della direttiva sulla protezione dei dati, gli sviluppatori di applicazioni e altri responsabili del trattamento nell'ecosistema delle app per dispositivi mobili devono consentire agli utenti di esercitare i propri diritti di accesso, rettifica, cancellazione e opposizione al trattamento dei dati. Se un utente esercita il diritto di accesso, il responsabile del trattamento è tenuto a informarlo in merito ai dati oggetto del trattamento e alla relativa origine. Se il responsabile del trattamento prende decisioni automatizzate sulla base dei dati compilati è tenuto anche a informare l'utente in merito alla logica applicata a tali decisioni. Questo potrebbe valere quando si valutano le prestazioni o la condotta degli utenti, ad esempio sulla base di dati finanziari o relativi alla salute, o altri dati del

---

[43] Gruppo di lavoro "articolo 29", parere 10/2004 sulla maggiore armonizzazione della fornitura di informazioni (luglio 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_it.pdf.

[44] Ad esempio, l'icona di avvertimento per il trattamento di dati di geolocalizzazione utilizzata su iPhone.

[45] Rapporto informativo FTC, nota 6, pag. 16.

profilo. Su richiesta dell'utente, il responsabile del trattamento dei dati è tenuto anche a consentire la rettifica, la cancellazione o il congelamento dei dati personali se questi sono incompleti, inesatti o trattati illecitamente.

Affinché gli utenti siano in grado di esercitare il controllo sul trattamento dei propri dati personali, le applicazioni devono informarli chiaramente e visibilmente dell'esistenza di questi meccanismi di accesso e correttivi. Il Gruppo di lavoro "articolo 29" raccomanda la progettazione e la realizzazione di strumenti semplici ma sicuri di accesso online. È preferibile che gli strumenti di accesso siano disponibili all'interno di ciascuna applicazione, o tramite un link a una funzione online, dove gli utenti possono accedere istantaneamente a tutti i dati trattati che li riguardano, con le necessarie spiegazioni. Iniziative analoghe, come le diverse *dashboard* e altri meccanismi di accesso, sono state intraprese da fornitori di servizi online.

Un accesso online agevole è particolarmente necessario nel caso di applicazioni che trattano profili utente molto ricchi, come le app di networking, sociali e di messaggistica o le app che trattano dati sensibili o finanziari. Ovviamente, l'accesso dovrebbe essere concesso solo se è stata stabilita l'identità dell'interessato, al fine di evitare perdite di dati verso terzi. Tuttavia, questo obbligo di verificare la corretta identità non dovrebbe comportare una raccolta aggiuntiva ed eccessiva di dati personali dell'interessato. In molti casi, potrebbe bastare l'autenticazione invece dell'identificazione (completa).

Inoltre, gli utenti dovrebbero sempre avere la possibilità di revocare il proprio consenso in maniera semplice e non onerosa. Un interessato può revocare il consenso al trattamento dei dati in vari modi e per una serie di motivi. È preferibile che l'opzione della revoca del consenso sia disponibile tramite i meccanismi facilmente accessibili di cui sopra. Deve essere possibile disinstallare le applicazioni eliminando nel contempo tutti i dati personali, anche dai server del responsabile del trattamento. Per consentire agli utenti di far cancellare i propri dati dallo sviluppatore dell'applicazione è importante il ruolo del produttore del sistema operativo, che trasmette un segnale allo sviluppatore quando un utente disinstalla l'applicazione. Il segnale potrebbe essere fornito attraverso la API. In linea di principio, dopo che l'utente ha disinstallato l'applicazione, lo sviluppatore non dispone più di un fondamento giuridico per continuare il trattamento dei dati personali relativi all'utente e pertanto è tenuto a cancellare tutti i dati. Uno sviluppatore che desideri conservare determinati dati, ad esempio per facilitare la reinstallazione della app, deve ottenere separatamente il relativo consenso nella procedura di disinstallazione, chiedendo all'utente di acconsentire a un ulteriore periodo di conservazione definito. L'unica eccezione a questa regola è la possibile esistenza dell'obbligo legale di conservare taluni dati per scopi specifici, ad esempio obblighi fiscali relativi a operazioni finanziarie[46].

3.9 Periodi di conservazione

Gli sviluppatori devono tener conto della conservazione dei dati raccolti con le applicazioni e dei rischi posti in termini di protezione dei dati. I tempi specifici dipendono dallo scopo dell'applicazione e dalla rilevanza dei dati per l'utente finale. Ad esempio, in un calendario, un diario o un'applicazione per la condivisione di foto, il periodo di conservazione solitamente è controllato dall'utente finale,

[46] Il Gruppo di lavoro rammenta a tutti i servizi della società dell'informazione, come le app, che l'obbligo europeo di conservazione dei dati (direttiva 2006/24/CE) non si applica nel loro caso e pertanto non può essere invocato come fondamento giuridico per continuare il trattamento dei dati di utenti di applicazioni dopo che le hanno cancellate. Il Gruppo di lavoro coglie questa opportunità per evidenziare la natura particolarmente rischiosa dei dati sul traffico, che meritano speciali precauzioni e salvaguardie di per sé – come indicato nella relazione di detto Gruppo sull'applicazione della direttiva sulla conservazione dei dati (WP172) – dove tutte le parti interessate sono state invitate ad attuare le opportune misure di sicurezza.

mentre per una app di navigazione può bastare archiviare solo gli ultimi 10 siti visitati di recente. Gli sviluppatori dovrebbero anche prendere in considerazione i dati degli utenti che non usano l'applicazione da un lungo periodo di tempo. Può darsi che abbiano perso il loro dispositivo mobile, o siano passati ad un altro dispositivo senza disinstallare attivamente tutte le app dal dispositivo precedente. Gli sviluppatori dovrebbero pertanto definire un periodo di tempo di inattività dopo il quale l'account sarà considerato scaduto e garantire che l'utente ne sia informato. Alla scadenza di tale periodo di tempo, il responsabile del trattamento dovrebbe avvertire l'utente e dargli la possibilità di recuperare i dati personali. Se l'utente non risponde all'avvertimento, i suoi dati personali e relativi all'utilizzo dell'applicazione dovrebbero essere resi anonimi o cancellati in modo irreversibile. Il periodo di promemoria dipende dalla finalità dell'applicazione e dal luogo dove sono archiviati i dati. Nel caso di dati archiviati sul dispositivo stesso, ad esempio un punteggio alto in un gioco, i dati si conservano finché resta installata l'applicazione. Nel caso di dati utilizzati solo una volta all'anno, come informazioni su una stazione sciistica, il periodo di promemoria potrebbe arrivare a 15 mesi.

3.10 Minori

I minori sono avidi utenti di applicazioni, su dispositivi propri o condivisi (ad esempio di genitori, fratelli o nel contesto scolastico) ed evidentemente esiste un mercato vasto e diversificato per le applicazioni rivolte ai minori. Nello stesso tempo però i minori hanno una comprensione e una conoscenza scarse o nulle in merito alla portata e alla delicatezza dei dati ai quali possono accedere le applicazioni, o alla portata della condivisione di dati con terzi per scopi pubblicitari.

Il Gruppo di lavoro ha affrontato ampiamente il problema del trattamento dei dati di minori nel parere 2/2009 sulla protezione dei dati personali dei minori e nel presente paragrafo tratta solo una serie di rischi e raccomandazioni specifici per le applicazioni[47].

Gli sviluppatori di applicazioni e altri responsabili del trattamento dei dati dovrebbero prestare attenzione al limite di età che definisce i minori nella legislazione nazionale, dove il consenso dei genitori al trattamento dei dati è un requisito indispensabile per il trattamento legittimo dei dati nelle applicazioni[48].

Laddove sia possibile ottenere legalmente il consenso di un minore e l'applicazione debba essere utilizzata da un bambino o un minore, il responsabile del trattamento dei dati dovrebbe tenere conto della comprensione e dell'attenzione potenzialmente limitate del minore in merito alle informazioni sul trattamento dei dati. A causa della vulnerabilità generale dei minori e considerando che i dati personali devono essere trattati lealmente e lecitamente, i responsabili del trattamento di dati di minori dovrebbero essere anche più rigorosi nel rispettare i principi di minimizzazione dei dati e limitazione della finalità. Nello specifico, i responsabili del trattamento non dovrebbero trattare dati di minori, direttamente o indirettamente, a fini di pubblicità comportamentale, poiché è al di fuori della portata della comprensione di un minore e pertanto supera i limiti del trattamento lecito.

Il Gruppo di lavoro condivide le preoccupazioni espresse dalla Federal Trade Commission nel suo rapporto informativo sulle applicazioni per dispositivi mobili destinate a minori[49].

---

[47] WP 160, parere 2/2009 sulla protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole) (11 febbraio 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_it.pdf.

[48] Negli Stati membri dell'UE il limite di età va da 12 a 18 anni.

[49] Rapporto informativo FTC Mobile *Apps for Kids: Current Privacy Disclosures are Disappointing* (febbraio 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. "*Benché si sia individuata una gamma diversificata di applicazioni per minori create da centinaia di sviluppatori diversi, si sono riscontrate*

Gli sviluppatori di applicazioni, in collaborazione con app store e produttori di OS e dispositivi, dovrebbero presentare le informazioni pertinenti in maniera semplice e con un linguaggio adatto all'età. Inoltre, i responsabili del trattamento dovrebbero evitare di raccogliere dati relativi a genitori o famigliari del minore, nonché informazioni finanziarie o relative a particolari categorie, quali i dati medici.

4 Conclusioni e raccomandazioni

Molte tipologie di dati disponibili su un dispositivo mobile intelligente sono dati personali. Il quadro giuridico pertinente è la direttiva sulla protezione dei dati, in combinazione con il requisito specifico del consenso contenuto nell'articolo 5, paragrafo 3, della direttiva e-privacy. Queste norme si applicano a qualsiasi applicazione destinata ad utenti all'interno dell'UE, a prescindere dall'ubicazione dello sviluppatore o dell'app store.

La natura frammentata dell'ecosistema delle applicazioni, l'ampia gamma di possibilità tecniche di accesso a dati archiviati in dispositivi mobili o generati dagli stessi e la scarsa consapevolezza giuridica tra gli sviluppatori creano una serie di rischi rilevanti in fatto di protezione dei dati per gli utenti delle applicazioni. Questi rischi vanno dalla mancanza di trasparenza e consapevolezza tra gli utenti a scarse misure di sicurezza e meccanismi di consenso privi di validità, nonché una tendenza alla massimizzazione dei dati e all'elasticità delle finalità del trattamento.

Esiste una sovrapposizione di responsabilità in fatto di protezione dei dati tra le diverse parti coinvolte nello sviluppo, nella distribuzione e nelle funzionalità tecniche delle applicazioni. Le conclusioni e le raccomandazioni si rivolgono per lo più agli sviluppatori (in quanto detentori del maggior controllo sulle modalità precise del trattamento o della presentazione delle informazioni all'interno delle applicazioni), che tuttavia, nell'intento di raggiungere i massimi livelli di protezione della privacy e dei dati, spesso devono collaborare con altre parti nell'ecosistema delle applicazioni, quali produttori di OS e dispositivi, app store e terzi, ad es. fornitori di dati analitici e reti pubblicitarie.

Gli sviluppatori di applicazioni devono

- essere consapevoli dei propri obblighi in qualità di responsabili del trattamento dei dati e rispettarli nel trattamento di dati degli utenti o relativi ad essi;
- essere consapevoli dei propri obblighi in qualità di responsabili del trattamento dei dati e rispettarli nell'ingaggiare incaricati del trattamento, ad esempio se affidano la raccolta e il trattamento di dati personali a sviluppatori, programmatori e fornitori di servizi di archiviazione cloud;
- chiedere il consenso prima che l'applicazione cominci a recuperare o inserire informazioni sul dispositivo, ossia prima dell'installazione. Il consenso deve essere liberamente prestato, specifico e informato;
- chiedere il consenso granulare per ciascun tipo di dati a cui avrà accesso l'applicazione, almeno per le categorie quali ubicazione, contatti, codice identificativo univoco, identità dell'interessato, identità del telefono, dati di carta di credito e pagamento, telefonia e SMS, cronologia di navigazione, e-mail, credenziali per social network e dati biometrici;
- essere consapevoli del fatto che il consenso non legittima trattamenti eccessivi o sproporzionati;

---

informazioni scarse o nulle nel mercato delle applicazioni sulle prassi per la raccolta e la condivisione dei dati previste da tali applicazioni".

- indicare finalità ben definite e comprensibili per il trattamento dei dati prima dell'installazione dell'applicazione e non modificarle senza un nuovo consenso; fornire informazioni complete se i dati saranno usati per scopi di terzi, come pubblicità o analisi;
- consentire agli utenti di revocare il consenso e disinstallare l'applicazione, cancellando i dati se del caso;
- rispettare il principio di minimizzazione dei dati e raccogliere solo i dati strettamente necessari per eseguire la funzionalità desiderata;
- adottare le necessarie misure tecniche e organizzative per garantire la protezione dei dati personali trattati, in tutte le fasi della progettazione e attuazione dell'applicazione (*privacy by design*), come definito nella sezione 3.6 del presente parere;
- fornire un unico punto di contatto per gli utenti dell'applicazione;
- prevedere una politica sulla privacy leggibile, comprensibile e facilmente accessibile, che come minimo informi gli utenti in merito a quanto segue:
  - chi sono (identità e recapiti),
  - le precise categorie di dati personali oggetto di raccolta e trattamento,
  - perché è necessario il trattamento (per quali finalità precise),
  - se i dati saranno divulgati a terzi (con una descrizione specifica, e non solo generica, dei soggetti a cui saranno divulgati i dati)
  - quali sono i diritti degli utenti, in termini di revoca del consenso e cancellazione di dati;
- consentire agli utenti di esercitare i propri diritti di accesso, rettifica, cancellazione e opposizione al trattamento dei dati, informandoli in merito all'esistenza di questi meccanismi;
- definire un periodo di conservazione ragionevole per i dati raccolti tramite l'applicazione e un periodo di inattività al termine del quale l'account sarà considerato scaduto;
- per quanto concerne le applicazioni destinate a minori: prestare attenzione al limite di età che definisce i minori nella legislazione nazionale, scegliere l'approccio più restrittivo al trattamento dei dati nel pieno rispetto dei principi di minimizzazione dei dati e limitazione della finalità, astenersi dal trattare dati di minori, direttamente o indirettamente, per scopi di pubblicità comportamentale e astenersi dal raccogliere tramite i minori dati relativi a loro parenti e/o amici.

Il Gruppo di lavoro raccomanda che gli sviluppatori di applicazioni

- studino gli orientamenti pertinenti in merito a specifici rischi per la sicurezza e relative misure;
- si attivino per informare gli utenti in merito a violazioni di dati personali secondo le disposizioni della direttiva e-privacy;
- informino gli utenti in merito a considerazioni di proporzionalità per i tipi di dati raccolti o consultati sul dispositivo, i periodi di conservazione dei dati e le misure di sicurezza applicate;
- sviluppino strumenti per consentire agli utenti di personalizzare i periodi di conservazione dei dati personali sulla base delle loro preferenze e situazioni specifiche, invece di prevedere periodi di conservazione predefiniti;
- nella politica sulla privacy includano informazioni destinate a utenti europei;
- sviluppino e attuino strumenti di accesso online semplici ma sicuri per gli utenti, senza raccogliere eccessivi dati personali aggiuntivi;
- insieme ai produttori di OS e dispositivi e agli app store sfruttino il loro talento creativo per sviluppare soluzioni innovative per informare adeguatamente gli utenti sui dispositivi mobili, ad esempio mediante un sistema di avvertenze multistrato in combinazione all'uso di icone con un chiaro significato.

Gli app store devono

- essere consapevoli dei propri obblighi in qualità di responsabili del trattamento dei dati e rispettarli nel trattare i dati degli utenti o che li riguardino;
- applicare l'obbligo di informazione dello sviluppatore, ivi compresi i tipi di dati ai quali l'applicazione è in grado di accedere e per quali scopi, e se i dati sono condivisi con terzi;
- prestare una particolare attenzione alle applicazioni destinate a minori per proteggerli nei confronti del trattamento illecito dei loro dati e in particolare applicare l'obbligo di presentare le informazioni pertinenti in modo semplice e con un linguaggio adatto all'età;
- fornire informazioni dettagliate sui controlli effettuati per l'ammissione delle applicazioni, tra cui quelli intesi a valutare aspetti relativi a privacy e protezione dei dati.

Il Gruppo di lavoro raccomanda che gli app store

- in collaborazione con i produttori di OS, sviluppino strumenti di controllo per gli utenti, quali simboli che rappresentano l'accesso a dati contenuti nel dispositivo mobile e generati dallo stesso;
- sottopongano tutte le applicazioni a meccanismi di reputazione presso il pubblico;
- prevedano un meccanismo di disinstallazione remota rispettoso della privacy;
- offrano agli utenti dei canali di feedback per segnalare problemi relativi a privacy e/o sicurezza;
- collaborino con gli sviluppatori di applicazioni per informare in modo proattivo gli utenti in merito a violazioni dei dati personali;
- avvertano gli sviluppatori di applicazioni in merito alle particolarità della legislazione europea prima di proporre l'applicazione in Europa, come ad esempio il requisito del consenso e nel caso di trasferimenti di dati personali in paesi extra-UE.

I produttori di OS e dispositivi devono

- aggiornare le loro API, regole di archiviazione e interfacce utente per offrire agli utenti un controllo sufficiente ad esercitare un valido consenso sui dati trattati dalle applicazioni;
- inserire nei sistemi operativi dei meccanismi di consenso al primo lancio dell'applicazione o la prima volta che l'applicazione cerca di accedere a una delle categorie di dati che esercitano un impatto significativo sulla privacy;
- adottare i principi della *privacy by design* per impedire il monitoraggio segreto dell'utente;
- garantire la sicurezza del trattamento;
- garantire che le (impostazioni predefinite delle) applicazioni preinstallate siano conformi alla normativa europea sulla protezione dei dati;
- offrire l'accesso granulare a dati, sensori e servizi, al fine di garantire che lo sviluppatore possa accedere solo ai dati necessari per la sua applicazione;
- fornire mezzi agevoli ed efficaci per evitare di essere tracciati da pubblicitari e altri terzi. Le impostazioni predefinite devono essere tali da evitare qualsiasi tracciamento;
- garantire la disponibilità di meccanismi adeguati per informare ed educare l'utente finale in merito a quello che possono fare le applicazioni e a quali dati sono in grado di accedere;
- garantire che l'accesso a ciascuna categoria di dati sia indicato nell'informativa all'utente prima dell'installazione dell'applicazione: le categorie presentate devono essere chiare e comprensibili;
- creare un ambiente rispettoso della sicurezza, con strumenti atti a impedire la diffusione di app maligne e consentire l'installazione/disinstallazione agevole di ciascuna funzionalità.

Il Gruppo di lavoro raccomanda che produttori di OS e dispositivi

- consentano agli utenti di disinstallare le app e trasmettano un segnale (ad esempio tramite l'API) allo sviluppatore per consentire la cancellazione dei relativi dati dell'utente;
- offrano e agevolino sistematicamente aggiornamenti di sicurezza periodici;
- garantiscano che i metodi e le funzioni che consentono l'accesso a dati personali includano funzionalità intese ad effettuare richieste di consenso granulare;
- contribuiscano attivamente allo sviluppo di icone che avvertano gli utenti in merito a diversi utilizzi dei dati da parte di applicazioni;
- sviluppino nei dispositivi tracce di controllo (*audit trail*) chiare, affinché gli utenti finali possano vedere chiaramente quali applicazioni hanno avuto accesso ai dati sui loro dispositivi e le quantità di traffico in uscita per applicazione, in relazione al traffico avviato dall'utente.

I terzi

- devono essere consapevoli dei propri obblighi in qualità di responsabili del trattamento dei dati e rispettarli nel trattare dati personali degli utenti;
- devono rispettare il requisito del consenso stabilito all'articolo 5, paragrafo 3, della direttiva e-privacy quando leggono o scrivono dati su dispositivi mobili, in collaborazione con gli sviluppatori di applicazioni e/o app store, che essenzialmente forniscono all'utente informazioni sulle finalità del trattamento dei dati;
- devono astenersi dall'eludere eventuali meccanismi studiati per evitare il tracciamento, come attualmente accade spesso con i meccanismi "*Do Not Track*" inseriti nei browser;
- i fornitori di servizi di comunicazione, quando distribuiscono dispositivi brandizzati, devono garantire il valido consenso degli utenti ad applicazioni preinstallate e assumersi le relative responsabilità nel contribuire alla determinazione di certe funzionalità del dispositivo e del sistema operativo, ad esempio, nel limitare l'accesso dell'utente a certi parametri di configurazione o nel filtrare *fix release* (di sicurezza e funzionali) fornite dai produttori di dispositivi e OS;
- i pubblicitari devono evitare specificamente di trasmettere annunci fuori dal contesto dell'applicazione, ad esempio modificando le impostazioni del browser o inserendo icone sul desktop del dispositivo mobile. Inoltre, devono astenersi dall'utilizzare codici identificativi univoci di dispositivi o abbonati a fini di tracciamento;
- devono astenersi dal trattare, direttamente o indirettamente, dati di minori per scopi di pubblicità comportamentale e devono applicare adeguate misure di sicurezza, che comprendono la trasmissione sicura e l'archiviazione criptata di codici identificativi univoci di dispositivi e utenti di app e altri dati personali.

Il Gruppo di lavoro raccomanda che i terzi

- sviluppino e realizzino strumenti di accesso online semplici ma sicuri per gli utenti, senza raccogliere eccessivi dati personali aggiuntivi;
- raccolgano e trattino solo dati coerenti con il contesto dove li fornisce l'utente.