ASSIRM
RICERCHE DI MERCATO, SOCIALI, DI OPINIONE

Corso Magenta, 85 - 20123 Milano
Tel. 02 58315750 - Fax 02 58315727
C.F. 10499960150
www.assirm.it

NORME
MOBILE RESEARCH

Dicembre 2015

Indice

1. Introduzione

Il documento in essere rappresenta il codice etico e le norme Assirm per la conduzione di ricerche di mercato, sociali e di opinione attraverso i dispositivi mobili (da qui in poi descritte come "Ricerche di mercato attraverso dispositivi mobili") di due tipologie:

- dispositivi **tradizionali** (telefoni cellulari non dotati di sistema operativo che possono avere o meno la possibilità di connettersi ad Internet) da qui in poi descritti solo come **"cellulari"**;

- dispositivi **di nuova generazione** (Smartphone e Tablet dotati di specifici sistemi operativi mobile che consentono l'installazione di App o altri tipi di software oltre alla possibilità di connettersi ad Internet) da qui in poi descritti solo come **"dispositivi mobile"**.

I sistemi operativi mobile ("mobile OS") attualmente più diffusi sono: iOS, Android, Windows Phone; Blackberry. Meno diffusi ma in sviluppo: Firefox OS, Sailfish OS, Tizen, Ubuntu Touch OS.

Questo documento ha l'obiettivo di affrontare nella sua completezza il tema in essere: un complesso di strumenti e metodi di ricerca in continuo divenire, inevitabilmente legati alla continua evoluzione tecnologica che caratterizza il mercato dei dispostivi mobili. Le ricerche di mercato attraverso dispositivi mobili rappresentano un canale privilegiato per la rilevazione di dati ed informazioni vista:

- la forte diffusione dei dispositivi mobili in Italia;
- la natura più personale/individuale di questi dispositivi rispetto ai dispositivi fissi;
- la natura portatile di questi dispositivi che consente di raggiungere i rispondenti con meno vincoli spazio-temporali rispetto ai canali di ricerca tradizionali.

Gli strumenti di ricerca attraverso dispositivi mobili continuano ad espandersi, sia per numero che per complessità. Questi strumenti possono potenzialmente raccogliere anche una grande quantità di dati personali e/o sensibili e, seppur esplicitato, non è sempre chiaro ai rispondenti quali dati vengono raccolti, con quale frequenza e come saranno usati. Anche i Termini di Utilizzo, seppur esplicitati, spesso vengono ignorati dai rispondenti che soprattutto su questi dispositivi tendono per comodità a non leggere testi e documenti più lunghi di una "schermata". In questo contesto è quindi buona norma studiare le soluzioni più adeguate e porre la massima attenzione affinché i rispondenti siano sempre pienamente consapevoli e informati quando si stanno raccogliendo e condividendo dati e informazioni personali potenzialmente sensibili attraverso i loro dispositivi mobili. A tal proposito aree di speciale interesse alle quali dedicare particolare attenzione sono: la notifica, il consenso, la sicurezza e la responsabilità del trattamento dei dati.
Lo scopo finale di Assirm è quello di promuovere in questo contesto degli scambi con i soggetti contattati per le ricerche basati su rispetto e chiarezza, oltre che quello di assistere i ricercatori nell'affrontare le questioni legali, etiche e pratiche della conduzione delle ricerche attraverso i dispositivi mobili tradizionali e di nuova generazione.

Questo documento **affronta le questioni legali, etiche e pratiche della conduzione delle**:

- **Survey via SMS** -> messaggi di testo (SMS) per contattare i rispondenti sui loro dispositivi mobili e che richiedono una risposta dei rispondenti attraverso il medesimo canale (non contengono dei link ipertestuali per compilare survey online).

- **ricerche Mobile** (tramite strumenti multimediali; App o altri tipi di software) -> raccolta attiva o passiva di dati, notifiche push, mobile survey, geo-localizzazione, forme di etnografia mobile (con possibilità di inserimento di foto, video o registrazioni audio).

  A titolo di esempio: App o altri tipi di software per il monitoraggio passivo dei comportamenti di utilizzo dei dispositivi mobile; App di ricerca attraverso le quali inviare survey mobile (via App e/o notifica push); App di ricerca attraverso le quali svolgere etnografie con raccolta di materiale multimediale (foto, video o audio).

Esistono molti metodi di ricerca tradizionali (es. CATI, CAWI, CAMI) che possono essere, per scelta del ricercatore, del cliente o del rispondente stesso, attivati attraverso i dispositivi mobili ma in questi casi non parleremo di "Ricerche di mercato attraverso dispositivi mobili". Per **ricerche attraverso i dispositivi mobili ed in particolare le ricerche Mobile si intendono quei metodi di ricerca che possono essere attivati solo ed esclusivamente attraverso l'utilizzo dei dispositivi mobili.** Parliamo quindi della possibilità di raccogliere informazioni attivamente (es. tramite survey su app nativo o mediante device agnostic) oppure tramite tracciamento passivo grazie ad app native.

Data la natura variegata dei dati potenzialmente rilevabili attraverso questi metodi di ricerca è fondamentale che i ricercatori non permettano che i dati raccolti in un progetto di ricerca di mercato siano usati per scopi diversi da quello della ricerca di mercato stessa.

Nell'intero documento si utilizza il verbo "devono" per descrivere un principio che i ricercatori sono obbligati a seguire se vogliono attenersi alle Norme di Qualità Assirm. Il verbo "dovrebbero" è invece utilizzato per descrivere l'adempimento ad un principio etico. Questo utilizzo distinto dei due verbi riconosce ai ricercatori la possibilità di scegliere di adempiere a dei principi etici in modi diversi in base al progetto di ricerca.

Queste norme dovrebbero essere lette insieme alle Norme di Qualità Assirm sulla Ricerca di Mercato.

2.Principi fondamentali

Tutti i principi fondamentali delle Ricerche di Mercato contenuti nelle Norme di Qualità Assirm si applicano anche alle diverse tecniche di ricerca attraverso i dispositivi mobili. Questo paragrafo descrive la maniera in cui questi principi dovrebbero essere resi operativi in tale specifico contesto.

2.1Essere conformi con la legge

La tecnologia e le comunicazioni tramite dispositivi mobili sono cresciute molto rapidamente nel mondo e in Italia e il quadro legale in materia è ancora in fase di evoluzione. Solo pochi paesi hanno affrontato la questione dei parametri legali delle comunicazioni e delle interazioni indesiderate con dei potenziali rispondenti che utilizzano dispositivi mobili. Il quadro normativo è complicato a causa dai molteplici mezzi di comunicazione che questi dispositivi forniscono (es. servizi voce, sms, chat&messaging, mailing, social networking).
Inoltre esistono leggi nazionali che riguardano in maniera specifica gli utenti di dispositivi mobili, ad esempio quella sulla restrizione all'uso dei dispositivi mobili alla guida. Queste norme potrebbero danneggiare indirettamente o comunque potenzialmente essere stabilite in maniera tale da costituire dei vincoli legali per il ricercatore che contatta un potenziale partecipante ad una ricerca attraverso un cellulare o un dispositivo Mobile. Visti questi aspetti, è fondamentale che i ricercatori siano a conoscenza e che rispettino: le leggi e le normative locali, regionali e nazionali, nondimeno gli specifici usi e costumi di ogni realtà contestuale che potrebbero anche esigere degli standard etici più severi rispetto a quelli descritti in queste norme.

Le leggi anti *spam* proibiscono gli approcci indesiderati o i messaggi a potenziali partecipanti attraverso testi o mezzi elettronici come le email. Anche quando queste leggi non esistono i fornitori di servizi internet o gli operatori di servizi di telefonia mobile potrebbero avere le loro politiche per proteggere i consumatori dai contatti indesiderati. In tutti i casi i ricercatori devono tenere bene a mente quali siano tutte le implicazioni per la privacy generati dall'intrusione e dagli approcci indesiderati tramite contatto attraverso i dispositivi mobili a potenziali partecipanti, a meno che i soggetti non si aspettino di essere contattati per delle ricerche in questo modo a causa di relazioni preesistenti con la società o l'organizzazione. I ricercatori dovrebbero anche ridurre al minimo i disagi che i contatti (SMS e altri tipi di messaggi elettronici come la messaggistica istantanea, le notifiche push o le email) sui dispositivi mobili potrebbero causare ai destinatari, affermando chiaramente lo scopo del contatto in prima battuta nella comunicazione e provando sempre a ridurre il più possibile le dimensioni e la durata del messaggio. Oltre allo scopo del contatto, in prima battuta, è buona norma ricordare sempre ai rispondenti di leggere i messaggi a loro inviati e/o rispondere alle survey quando si trovano in situazioni sicure ed adeguate all'utilizzo di dispositivi mobili.

2.2 Consenso e notifica

Le Norme di Qualità Assirm affermano che la cooperazione dei partecipanti alla ricerca deve essere basata su informazioni adeguate circa lo scopo e la natura della ricerca (*4.3.2. Informativa al rispondente*) e che bisogna ottenere il consenso di questi a partecipare. Con specifico riferimento alle ricerche Mobile i ricercatori devono anche informare i partecipanti se si tratta di raccogliere informazioni attivamente (es. tramite survey) oppure se vengono raccolti dati mediante tracciamento passivo come ad esempio:

> *download e utilizzo di App; fruizioni di contenuti multimediali (musica, video, etc.); indirizzi Url di tuti siti visitati geo-localizzazione puntuale del partecipante.*

Come per altre forme di raccolta dei dati a scopo di ricerca, i ricercatori devono informare i partecipanti alla ricerca tramite dispositivi mobili delle normative sulla privacy vigenti, spiegandogli come tutti i dati personali raccolti verranno utilizzati, trattati e protetti.

Quando la normativa sulla privacy deve essere visualizzata su un dispositivo mobile, i limiti di spazio dello schermo di molti dispositivi ne rendono difficile la visualizzazione chiara e per intero, quindi i ricercatori devono massimizzare la facilità di accesso alle informazioni rilevanti. Ci possono essere diverse strategie ma una possibile soluzione è l'utilizzo di un documento ipertestuale a due strati: con una sezione iniziale sulla protezione della privacy ed il trattamento dei dati personali; ed un secondo livello riguardante le Condizioni di Partecipazione alla ricerca.

2.3 Protezione dei dati personali

La legislazione sulla privacy (ai sensi del d.lg n. 196/2003) si applica solo ai dati personali identificativi e non ai dati tramite i quali è impossibile identificare un soggetto. A titolo di esempio: il nome, l'indirizzo, l'indirizzo email, l'account di un social network e il numero di telefono fan sì che i dati siano identificativi.
I ricercatori devono tenere in considerazione anche i possibili casi in cui si combinano informazioni non identificative, che se affiancate l'una all'altra consentono di derivare dati identificativi (come ad esempio la posizione geografica esatta affiancata al codice di avviamento postale o altri dati).
I ricercatori devono assicurarsi che i dati o altro materiale (come fotografie, registrazioni, documenti cartacei, etc.) raccolto per la ricerca di mercato contenente informazioni personali identificative, sia tenuto al sicuro e sia usato solo a scopo di ricerca.
I dati personali identificativi possono essere trasferiti al fruitore della ricerca solo se i partecipanti:

- hanno esplicitamente espresso la loro volontà o hanno dato il loro specifico consenso informato
- e nel caso in cui ci sia un accordo che stabilisca che nessuna attività commerciale sarà loro diretta come conseguenza dell'aver fornito informazioni personali.

Si consiglia ai ricercatori di far firmare ai clienti della ricerca degli accordi scritti per assicurarsi che questi requisiti vengano rispettati.
I dati personali identificativi raccolti a scopo di ricerca non possono in alcun modo essere usati per scopi diversi. I dati anonimizzati (es. tramite "codice ID" identificativo di ciascun partecipante ma impersonale) non più identificativi del partecipante possono invece essere trasmessi ai clienti ed elaborati per altri scopi.

I ricercatori dovrebbero anche riconoscere il fatto che alcuni dati identificativi potrebbero essere ritenuti "sensibili" e quindi dovrebbero essere gestiti con molta cura.

Esistono due caratteristiche delle ricerche Mobile che rendono la protezione dei dati personali ancora più complessa:

- un coinvolgimento maggiore dei clienti nel processo di ricerca
- dei tempi molto più brevi.

E' fondamentale che i ricercatori prevedano in anticipo alcuni potenziali rischi, come ad esempio che i clienti inavvertitamente vedano o sentano cose che potrebbero essere definite dati personali e si impegnino quindi a progettare la ricerca in modo da minimizzare questi rischi. Allo stesso modo la condivisione o la trasmissione temporanea di materiale di ricerca attraverso delle App, quali i portali online o più in generale i server (fisici o in *cloud*) dovrebbe essere programmata con lo stesso livello di protezione della trasmissione finale dei dati.

La legislazione sulla privacy (ai sensi del d.lg n. 196/2003) specifica quali sono i diritti di accesso di un soggetto ai dati che vengono immagazzinati sotto forma di dati personali identificativi e gli permette di visualizzare tutte le registrazioni fatte a suo nome e di richiedere delle modifiche se ci sono degli errori. Nel caso di dati anonimizzati il diritto di accedervi non può più essere esercitato dal partecipante perché questi non sono più ad esso riconducibili in nessuna forma.

Prima che i dati personali vengano trasferiti dal paese della raccolta a un paese terzo, il ricercatore deve essere sicuro che il trasferimento dei dati sia legale e di aver preso tutte le cautele necessarie per assicurarsi un livello adeguato di protezione e tutela dei soggetti interessati. Ciò vale anche nei casi in cui si usano dei server "remoti" in un paese diverso per raccogliere i dati dei rispondenti o quando questi vengono elaborati all'interno di un *cloud* internazionale.
Il ricercatore deve spiegare questo processo anche all'interno della normativa sulla privacy e deve fornire degli strumenti adeguati di salvaguardia, al fine di tutelare i dati personali del rispondente al quale viene chiesto il permesso di trasferirli.
Visto che la questione dei dati personali è sempre molto delicata da affrontare, i ricercatori dovrebbero sempre usare degli approcci molto cauti in merito alla pubblicazione e al trasferimento dei dati, cercando costantemente di mantenere intatta la fiducia del consumatore e rispettando le leggi vigenti.

2.4 Assicurarsi di non arrecare danno

Un altro principio chiave stabilito e condiviso dalle Norme di qualità Assirm (*4.3.4. Assicurarsi di non arrecare danno*) è che i rispondenti non debbono mai ed in alcun modo subire conseguenze negative come risultato diretto della loro partecipazione ad una ricerca. I ricercatori dovrebbero anche tenere conto del fatto che quando si immagazzinano i dati personali dei rispondenti a livello locale (sul dispositivo mobile di un partecipante alla ricerca) c'è la possibilità che questi dati siano disponibili anche per altri nel caso in cui il dispositivo venga rubato o usato da un'altra persona. I dati raccolti su delle App che vengono installate sul dispositivo ne sono un esempio, come anche le fotografie che potrebbero essere scattate per uno studio etnografico o i messaggi di testo che potrebbero essere usati per inviare o scambiare dati.
E' fondamentale che i partecipanti siano consapevoli di questi rischi e che i ricercatori applichino tutte le misure disponibili per proteggere i dati personali, quali ad esempio: il criptaggio dei dati, la protezione mediante *password* oppure fornendo ai rispondenti delle istruzioni su come eliminare le informazioni personali alla fine della ricerca.
A differenza di molti altri metodi di ricerca, i partecipanti di ricerche tramite dispositivi mobili potrebbero avere dei costi legati alla partecipazione alla ricerca. I costi specifici legati alla ricerca possono variare in base alle specifiche caratteristiche (anche in base ai *provider* dei servizi) e possono includere dei costi per:

- il *download/upload* dei dati;
- l'accesso alla rete internet;
- i messaggi di testo;
- il superamento della quantità di traffico dati disponibile con una determinata tariffa;
- le spese per il roaming;
- i costi standard della telefonia.

Se possibile i ricercatori dovrebbero progettare la ricerca in modo da non dover addebitare alcun costo ai partecipanti. Se ciò non risulta possibile, i ricercatori dovrebbero prevedere dei compensi da versare ai partecipanti in modo tale da coprire almeno le spese da loro sostenute per partecipare alla ricerca.

Quando i partecipanti si iscrivono ad un panel o ad una ricerca di mercato attraverso dispositivi mobili, la questione dei costi e dei compensi dovrebbe essere affrontata al momento della registrazione e/o al momento dell'accettazione iniziale della ricerca, sia che questa venga effettuata tramite il dispositivo mobile stesso sia in caso di iscrizione da e con altri dispositivi elettronici o telefonici.
Prima dell'installazione di qualsiasi App di ricerca i ricercatori dovrebbero anche dire ai partecipanti che l'App potrebbe -come tutti i *software* di questo tipo- incidere negativamente sul consumo di batteria del dispositivo e, se possibile, precisare l'incremento percentuale su tale consumo.

Alcuni metodi di ricerca attraverso dispositivi mobili richiedono che i partecipanti vadano in un determinato posto o compiano determinate azioni. In questi casi i ricercatori devono avvertire i partecipanti e metterli in guardia dal fare cose che potrebbero metterli a rischio o fargli infrangere la legge.

Alcuni esempi in tal senso includono: degli avvisi ai partecipanti a non inviare messaggi o comunque a non utilizzare il dispositivo mentre sono alla guida; scattare foto in situazioni o luoghi in cui ciò non è permesso o ancora filmare e diffondere video con coinvolti altri soggetti senza chiederne l'autorizzazione.

Quando il progetto di ricerca comporta metodologie come survey via SMS o mobile survey (tramite App, *device agnostic* o altro *software*) potrebbe capitare ai ricercatori di contattare i potenziali rispondenti in momenti in cui questi stanno svolgendo altre attività oppure in una situazione che non corrisponde a quelle idonea per partecipare alla ricerca. Alcuni esempi in tal senso includono contatti a rispondenti: mentre sono alla guida di un veicolo; mentre maneggiano altre apparecchiature; mentre camminano in un luogo pubblico oppure quando il rispondente si trova in un altro fuso orario. Il ricercatore deve sempre innanzitutto accertarsi che il rispondente si trovi in una situazione in cui essere contattato è legale, sicuro e conveniente.

2.5 Bambini

I ricercatori devono essere particolarmente cauti quando conducono delle ricerche in cui sono coinvolti dei bambini o dei giovani (4.3.4 La raccolta dati da minori o da rispondenti vulnerabili). Bisogna porre in essere tutte le misure più appropriate per assicurarsi di ottenere il permesso esplicito e verificabile di un genitore o di un tutore legale (da qui in poi definito solo "genitore") prima di invitare un bambino a partecipare ad una ricerca o ad installare un'App o qualsiasi altro software di ricerca (anche se è noto che l'identificazione di un bambino o un giovane non è sempre possibile con certezza).

2.6 Reputazione del settore

I ricercatori non devono fare nulla di potenzialmente dannoso per la reputazione del settore della ricerca di mercato. Essi devono sempre tenere bene a mente i principi chiave delle Norme di Qualità Assirm per il lavoro che essi e le loro società svolgono e devono evitare attività e prassi che potrebbero minare la fiducia del pubblico nel settore delle ricerche di mercato.

Il ricercatore deve tenere presente che alcuni soggetti considerano il proprio dispositivo mobile come uno strumento personale e privato. Il ricercatore deve essere attento a questi aspetti della privacy e deve differenziare i protocolli di contatto di qualsiasi forma che utilizza per i contatti personali da quelli usati per le ricerche che si effettuano tramite contatto su account impersonali.

3. Considerazioni speciali per la ricerca attraverso dispositivi mobili

3.1 App di ricerca

Quando i ricercatori richiedono ai partecipanti alla ricerca di installare delle App sui loro dispositivi mobile o quando la ricerca richiede l'uso di applicazioni web si deve innanzitutto ottenere il loro consenso offrendogli un canale ed un meccanismo appropriato per farlo in prima battuta (generalmente tramite specifico "*flag*" di accettazione/consenso prima del *download* dell'App stessa). E' fondamentale inoltre che vengano forniti i riferimenti sul dove i partecipanti possano leggere in ogni momento e nel dettaglio la normativa sulla privacy.

I ricercatori devono svelare ai potenziali partecipanti: lo scopo dell'App, i dati specifici che si raccolgono o caricano e ogni possibile impatto sul funzionamento di altre App installate o sulla prestazioni del dispositivo mobile in generale. I ricercatori devono anche fare del loro meglio per assicurarsi che ogni App installata per la ricerca non:

- installi software che modificano le impostazioni del dispositivo oltre il livello che è necessario alla conduzione della ricerca e che non causino conflitti con i sistemi operativi o con altri *software* installati;
- installi *software* nascosti che siano difficili da disinstallare;
- installi *software* che producono contenuto pubblicitario, ad eccezione dei *software* che servono per testare delle pubblicità;
- installi aggiornamenti del *software* senza avvertire gli utenti e senza dare ai partecipanti l'opportunità di non farlo;
- crei il rischio di esporre i dati raccolti durante la trasmissione o la conservazione a personale non autorizzato;
- cambi la natura di qualunque tecnologia di identificazione o monitoraggio senza avvisarne l'utente;
- eviti di avvisare l'utente di cambiamenti alle prassi relative alla privacy attuati nell'aggiornamento del *software*;
- raccolga dati identificativi che possono essere usati dal fornitore dell'App per scopi diversi dalla ricerca.

I ricercatori che utilizzano tecnologie di monitoraggio per la ricerca dovrebbero anche avere visibilità sul processo di gestione e distribuzione del *software* da parte degli sviluppatori dello stesso, in modo da poter controllare attentamente i canali di distribuzione ed eventualmente cercare segnali che suggeriscano eventi indesiderabili (es. un gran numero di utenti che si cancellano nello stesso momento).

3.2 Monitoraggio passivo dei dati tramite App o altro tipo di software (Proxy / VPN / etc.)

La raccolta passiva dei dati fa parte di una categoria di metodi di ricerca nei quali si acquisiscono dati dai partecipanti senza il processo tradizionale di domande e risposte delle survey. I dati passivi raccolti da strumenti quali "*meter*" o "*agent*" di monitoraggio sono considerati dati oggettivi, mentre i dati raccolti tramite intervista tradizionale sono considerati dati soggettivi/percepiti.
Le fonti per la raccolta passiva dei dati attraverso dispositivi mobile possono includere i dati:

- di navigazione web ("*browsing*");
- di utilizzo delle App;
- di prestazione della rete mobile (dati e fonia)
- di utilizzo quali-quanti delle carte fedeltà;
- dei lettori di codici a barre dei negozi (*QR code*);
- i dati di geo localizzazione provenienti dai dispositivi mobili;
- alcuni tipi di dati raccolti dai social media (es. i "*like*" o i post che si condividono sui social network).

Tutti questi dati che la tecnologia ha oggi reso leggibili portano in primo luogo ad un bisogno crescente di differenziare la ricerca di mercato da altre attività, ed anche ad un bisogno di trasparenza nei confronti dei rispondenti riguardo le informazioni raccolte, specialmente dal punto di vista legale e della protezione dei dati. I dati di questo tipo (essendo potenzialmente o accidentalmente "sensibili") devono essere resi anonimi, sempre tenendo conto del fatto che il consenso è comunque necessario per i dati sensibili e per installare App o altri tipi di *software* simili come descritto in precedenza.

Anche se è possibile individuare passivamente il tipo di dispositivo che il partecipante sta usando, questo tipo di informazione non è considerata un dato personale poiché lo scopo della raccolta di questa informazione è solo la verifica della compatibilità del *software* con il dispositivo in essere, oltre che il miglioramento della prestazioni dell'App e l'adattamento del suo *layout* allo specifico dispositivo (es. differenze visuali tra Smartphone e Tablet).

3.3 Etnografie & Mystery Shopping: fotografie, registrazioni audio-video

I cellulari -non tutti- ed i dispositivi mobile -tutti- hanno la possibilità di creare, immagazzinare e trasmettere fotografie e registrazioni audio-video. Queste funzioni mettono a disposizione dei ricercatori tutta una serie di nuovi strumenti che si possono integrare alle metodologie di ricerca tradizionali. Due esempi importanti nei quali queste funzioni hanno migliorato i metodi di ricerca tradizionali sono l'etnografia e il mystery shopping. Esistono oggi App di ricerca che mettono insieme proprio questi due metodi tradizionali in un unico strumento (es. App che mettono a disposizione una *customer base* di utenti "mobile" in grado di reperire informazioni all'interno di punti vendita o di luoghi d'interesse e di offrire il proprio contributo attraverso contenuti digitali certificati in merito a tematiche tipiche dei "*quick poll*").

I ricercatori devono sapere che, in qualunque momento o caso, un'immagine/o un contenuto audio-video ("contenuto digitale") contenga il volto di un individuo -chiaramente visibile- ciò lo rende identificabile. In questi casi il contenuto digitale in questione deve essere trattato come un dato personale identificativo. Di conseguenza, tutte le fotografie e le registrazioni audio-video raccolte, elaborate ed immagazzinate per un progetto di ricerca devono essere considerate come potenzialmente identificative e sensibili e trattate e controllate *ex ante* con estrema cura dal ricercatore.

I contenuti digitali rilevati durante la ricerca possono essere trasmessi al cliente solo se il partecipante ha dato il suo permesso e comunque, anche in quel caso, solo a scopo di ricerca. Le informazioni che sono state rese anonime (ad esempio attraverso la "*pixelizzazione*" del viso o delle tecnologie che cambiano la voce) fino a non essere più identificative, possono essere trasmesse al cliente della ricerca ed elaborate per altri scopi.
Queste norme riconoscono l'esistenza di casi in cui altri soggetti, non partecipanti alla ricerca, vengano ritratti in una foto o ripresi in un video o registrazione audio; in questi casi potrebbe non essere pratico o addirittura impossibile chiedere loro il permesso di diffusione di quei contenuti digitali. Alcuni esempi in tal senso includono il personale di un negozio o i passanti per strada. In questi casi, anche se questi individui non sono definiti come partecipanti alla ricerca, il ricercatore ha comunque la responsabilità di mostrare lo stesso rispetto e lo stesso livello di protezione della privacy che avrebbe per i partecipanti alla ricerca.
Alcuni tipi di etnografie/Mystery Shopping potrebbero comportare: il dover scattare fotografie, registrare contenuti audio o video in contesti pubblici coinvolgendo persone che non sono state reclutate come partecipanti alla ricerca. In questi casi i ricercatori devono ottenere il permesso degli individui che sono chiaramente visibili nelle immagini e che possono essere identificati prima di condividerle. Se non si riesce ad ottenere il permesso da questi soggetti allora la loro immagine dovrebbe essere "*pixelata*" o resa anonima in altro modo.

I ricercatori devono anche avvertire i partecipanti di non scattare foto o fare registrazioni audio-video in posti in cui questo non è concesso, come ad esempio: edifici governativi, banche, scuole, aree di sicurezza all'interno degli aeroporti, spazi privati o qualunque altra area in cui ci siano dei cartelli che proibiscono l'uso di foto/telecamere. In tutti i casi i ricercatori dovrebbero essere consapevoli di quali siano tutte le leggi locali applicabili e dovrebbero quindi condurre la ricerca in modo appropriato.

Naturalmente i ricercatori dovrebbero avere una particolare attenzione quando si fotografano o riprendono dei bambini. Ciò non deve mai essere fatto senza il permesso di un genitore o di un tutore legale. Se delle immagini di bambini dovessero essere scattate inavvertitamente, le loro facce devono essere immediatamente "*pixelate*" per proteggere l'identità di questi soggetti.
Come per tutti gli altri dati personali identificativi, i ricercatori dovrebbero sempre usare degli approcci cauti nel pubblicare e trasferire questi dati. E comunque sempre consigliabile informare precedentemente e nel dettaglio il cliente della ricerca su questa questione ed in merito alla tipologia e il formato di dato che gli verrà consegnato come risultato della ricerca.

Il mystery shopping rappresenta uno di questi casi perché proprio per la sua natura i soggetti della ricerca non sono consapevoli di essere sotto osservazione. Il personale che effettua studi di mystery shopping deve avere la cura di assicurarsi che, per quanto possibile, la privacy dei soggetti

sia rispettata e che questi non subiscano danni o svantaggi come conseguenza della ricerca svolta. I loro dati personali devono essere protetti e non si potranno condividere immagini o registrazioni con i clienti, a meno che non si sia ottenuto il permesso del soggetto.

3.4.Mobile Survey tramite App/Notifiche push

L'invio di mobile survey è un metodo di ricerca nel quale il questionario di ricerca è inviato al rispondente direttamente sul suo dispositivo mobile attraverso la rete dati. L'invio può avvenire sia attraverso una specifica App che segnala al rispondente la presenza di una survey alla quale rispondere, sia attraverso una notifica push (messaggio elettronico) che via web/email o SMS (con link al questionario online). L'invio di una mobile survey può avvenire anche sulla base di determinante circostanze specifiche:

- essere basato sulla geo-localizzazione del rispondente (es. si trova nelle vicinanze di un punto d'interesse), in questi casi si può parlare di **Location based survey**;
- essere basato sull'attività del rispondente (es. utilizzo di una particolare App o al termine di una chiamata), in questi casi si può parlare di **Event based survey**.

Le mobile survey possono inoltre essere:

- **Push Survey**: nel caso in cui il rispondente riceve sul proprio dispositivo mobile l'invito a partecipare sotto diverse forme (notifica, geofencing, sms, etc.). In questo caso si presuppone che i rispondenti siano stati pre-reclutati e abbiano fornito i dati per essere contattati oppure facciano parte di un panel.

- **Pull Survey**: la richiesta di partecipare viene generata direttamente dal rispondente. In questo caso non c'è un pre-reclutamento ma la partecipazione viene indotta dal cosiddetto "*river sampling*": ovvero i rispondenti sono tutti coloro che decidono di aderire volontariamente alla ricerca (ad es. mediante la scansione di un *QR-code* o attraverso il click su un *banner* online.

Le survey mobile in alcuni casi potrebbero includere dei diari da compilare con notifica "temporizzata" (sulla base di intervalli regolabili, es.: giornaliera).
Le survey Mobile dovrebbero sempre avere una lunghezza un formato adeguato per essere compilate con facilità tramite il dispositivo mobile.
Come per le survey via SMS potrebbe capitare ai ricercatori di contattare i potenziali rispondenti in momenti in cui questi stanno svolgendo altre attività oppure in una situazione che non corrisponde a quelle idonea per partecipare alla ricerca. Il ricercatore deve sempre innanzitutto avvisare il rispondente in prima battuta di leggere e rispondere al messaggio quando si trova in una situazione sicura e conveniente.

3.5 Dati accessori

Il progresso tecnologico consente oggi molte possibilità di registrare dati personali accessori delle transazioni o attività giornaliere comportamentali dei partecipanti ad una ricerca attraverso dispositivi mobili. Un cellulare o ancor di più un dispositivo mobile creerà - inevitabilmente- svariati tipi di registrazioni "sensibili":

- chi sono gli utenti che vengono chiamati e contattati attraverso altri canali;
- ma anche alcuni dati di chi quegli utenti li ha chiamati/contatti;
- dove gli utenti sono stati e con quali aree di telefonia mobile sono stati connessi;

Tutti questi dati sono raccolti legittimamente dagli operatori mobile per scopi specifici come ad esempio la fatturazione accurata dei costi ai clienti o lo smistamento delle chiamate. Questi dati spesso sono però raccolti ad insaputa degli utenti anche da App e software installati sui loro dispositivi mobile.
Tali dati non devono essere analizzati per scopi commerciali (es. analizzare i numeri chiamati di frequente per poter offrire sconti personali, oppure analizzare le destinazioni verso le quali si vola di frequente per proporre offerte speciali per volare verso quelle destinazioni).
Il valore di ricerca di questi dati comportamentali può essere estratto quando questi vengono analizzati a livello aggregato o combinati con altri dati o altre abitudini del cliente; in quest'ultimo caso si intende quando due *file* di dati personali indipendenti vengono messi insieme (questa pratica viene spesso chiamata potenziamento del *database*). Ciò è permesso se si rispettano i seguenti criteri:

- il potenziamento è necessario allo scopo della ricerca (es. per aumentare il valore analitico dei dati);
- il partecipante alla ricerca ha espresso il suo consenso informato;
- non si intraprendono azioni (es. invio di messaggi di marketing) nei confronti del partecipante a seguito del potenziamento;
- il processo di potenziamento o di abbinamento è fatto in modo tale che l'identità personale del partecipante non sia mai svelata senza aver ottenuto il suo consenso.

3.6 Progetto di ricerca appropriato

Quando si conducono delle ricerche attraverso dispositivi mobili il ricercatore dovrebbe assicurarsi che ogni compito affidato al partecipante (ad esempio un sondaggio, un diario o delle comunicazioni informative da leggere) sia: di una lunghezza appropriata, presentato in un formato adeguato e ottimizzato per tutti i tipi di dispositivi.

Anche se la ricerca continua ad evolversi attualmente si ha ragione di pensare che un rispondente si aspetti un'interazione più breve utilizzando dispositivi mobili rispetto ad altre modalità di ricerca più tradizionali.

A causa della dimensione limitata dello schermo di alcuni dispositivi mobili è importante che ogni istruzione, domanda o formulario visualizzato sia chiaro e conciso. Data la natura della tecnologia mobile i rispondenti possono infatti essere distratti più facilmente ed è più probabile che questi perdano la concentrazione oppure che la connessione si interrompa o cada. I ricercatori dovrebbero quindi sempre strutturare *ex-ante* delle cautele per casi simili quando progettano delle ricerche di mercato attraverso dispositivi mobili.

Le ricerche di mercato attraverso dispositivi mobili sono degli strumenti molto potenti dal punto di visto conoscitivo ma i ricercatori devono sempre tenere presente che queste sono anche altrettanto delicate riguardo gli aspetti di privacy e sicurezza dei rispondenti. Inoltre i ricercatori dovrebbero sempre tenere presente che le ricerche condotte attraverso dispositivi mobili sono strettamente dipendenti dal buon funzionamento dei dispositivi stessi e che questi possono frequentemente incontrare problemi o malfunzionamenti di svariata natura, inficiando così la raccolta dei dati.