Progetto: eSecurity - ICT for knowledge-based and predictive urban security
Coordinatore: eCrime, Facoltà di Giurisprudenza, Università degli Studi di Trento
Beneficiari: Fondazione Bruno Kessler, Comune di Trento
Partner Associato: Questura di Trento

Con il supporto finanziario del Programma
prevenzione e lotta contro la criminalità dell'Unione europea
Commissione europea - Direzione generale Migrazione e affari interni

04

eCRIME
WORKING
PAPERS

Le applicazioni mobili per la sicurezza urbana

Sicurezza dei cittadini, protezione della privacy e dei dati personali nella smart city

Serena Bressan
Giulia Iseppi

eCrime Working Papers

n. 04

Le applicazioni mobili per la sicurezza urbana

Sicurezza dei cittadini, protezione della privacy e dei dati personali nella smart city

Serena Bressan (Project Manager)
Giulia Iseppi (Junior Researcher)

ISSN 2284-399X
ISBN 978-88-8443-671-9

eCrime - ICT, Law & Criminology
Facoltà di Giurisprudenza
Università degli Studi di Trento
Via G. Verdi, 53
38122 - Trento
0461 282336
www.ecrime.unitn.it

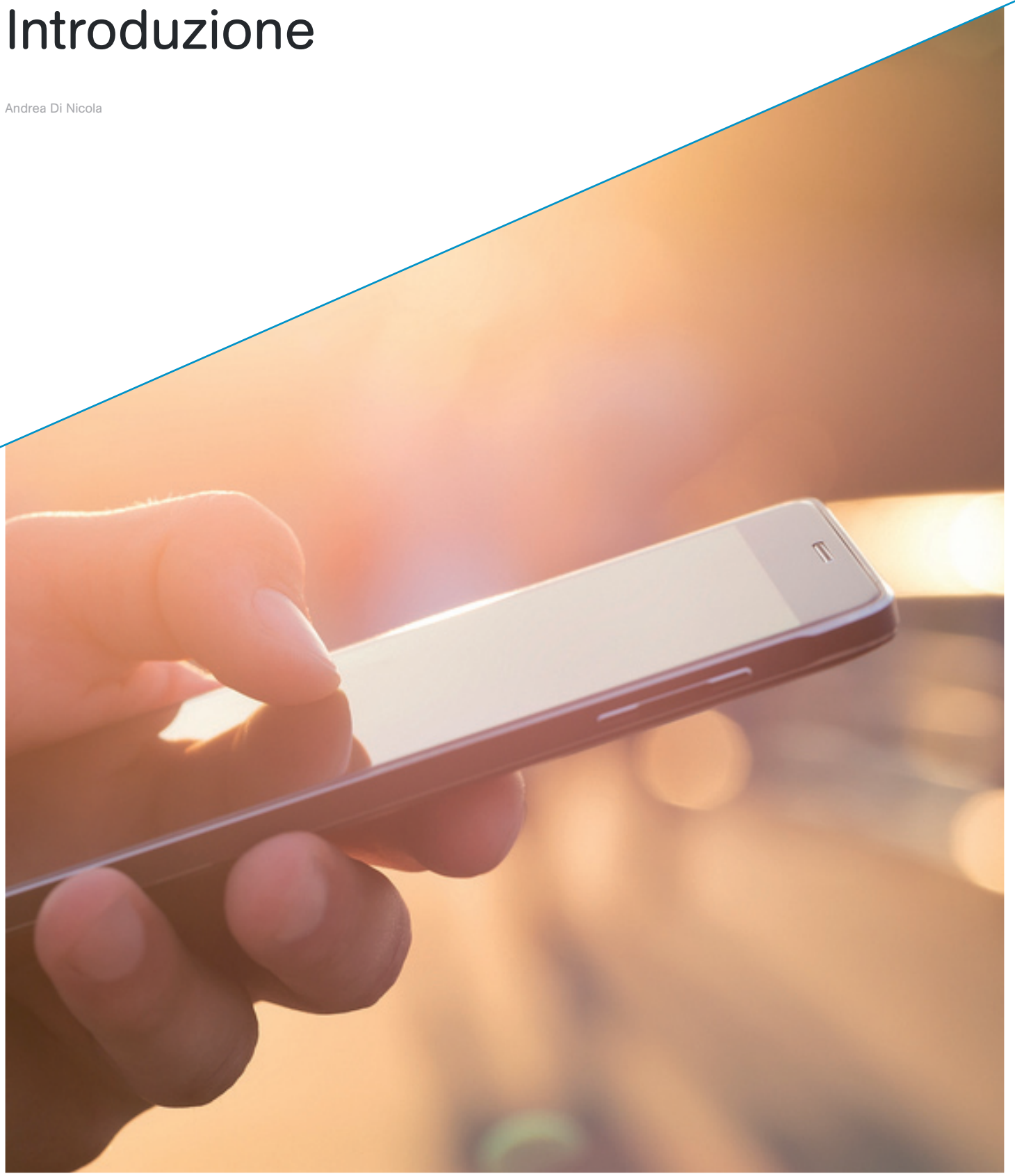
Stampa digitale: www.rotooffset.it - Trento

Trento, novembre 2015

Indice

Introduzione

Andrea Di Nicola



Questo documento s'inserisce nell'ambito dei *Workpackages* n. 7 e 8 ("Elaborazione di *report* criminologici" – "Coordinamento e divulgazione dei risultati") del progetto europeo "*eSecurity - ICT for knowledge-based and predictive urban security*" (eSecurity), co-finanziato dalla Commissione europea (Programma ISEC 2011 "Prevention of and Fight against Crime" della Direzione Generale Migration and Home Affairs - HOME/2011/ISEC/AG), primo progetto al mondo di sicurezza urbana predittiva. Il progetto, durato 36 mesi da novembre 2012 a novembre 2015, è stato coordinato dal gruppo di ricerca eCrime della Facoltà di Giurisprudenza dell'Università degli Studi di Trento, in *partnership* con Fondazione Bruno Kessler, Questura di Trento e Comune di Trento.

Obiettivo e organizzazione del lavoro

Com'è cambiata la gestione della sicurezza urbana nella *touch era*? L'utilizzo di applicazioni *mobile* da parte dei cittadini per "sentirsi più sicuri" è compatibile con i profili minimi di *privacy*? Queste sono alcune delle domande cui risponderà questo rapporto di ricerca, il cui obiettivo è di elaborare una guida essenziale delle applicazioni mobili in materia di sicurezza urbana attualmente esistenti sul mercato, con lo scopo ultimo di valutare se le stesse siano conformi ai dettami della normativa vigente a livello sovranazionale sulla *privacy* e la protezione dei dati personali, ovvero se siano *privacy-compliant*. I destinatari di questo *Working Paper*, realizzato all'interno del progetto eSecurity, sono principalmente ricercatori, agenti delle forze dell'ordine e funzionari degli enti pubblici interessati al tema in oggetto, oltre che tutti i cittadini che vogliono diventare protagonisti della gestione della propria sicurezza, con un occhio di riguardo alla tutela della propria riservatezza.

Per raggiungere quest'obiettivo, dopo aver definito il concetto di sicurezza urbana e aver analizzato in breve come le modalità di gestione della stessa siano cambiate a mano a mano che le città sono diventate sempre più *smart* (capitolo 01), si passerà alla redazione di una rassegna sulle principali applicazioni *mobile* in questo contesto e alla loro classificazione (capitolo 02). Infine, sarà svolta una valutazione di *compliance* delle applicazioni sulla sicurezza urbana selezionate, alla luce dei principi cardine della normativa sovranazionale in tema di *privacy* e tutela dei dati personali (capitolo 03).[1]

Il progetto eSecurity e la knowledge-based and predictive urban security

Il progetto "*eSecurity - ICT for knowledge-based and predictive urban security*" si basa sui principi delle teorie razionali del crimine e della criminologia ambientale, secondo i quali la criminalità a livello urbano si concentra in alcuni "luoghi" (punti, strade, zone) e la vittimizzazione passata è predittore di quella futura. Questa concentrazione spazio-temporale di criminalità è legata a una concentrazione spazio-temporale di opportunità, di cause, e queste vanno investigate per incidere sulla criminalità nelle città (Brantingham e Brantingham, 1991). Pertanto, la conoscenza dei punti "caldi" del territorio ("*hot spot*") e delle opportunità criminali esistenti permette di poter valutare al meglio quali siano i fattori criminogeni da tenere in considerazione nell'elaborazione di politiche e interventi di prevenzione e contrasto efficaci ed efficienti (Clarke, 1997; Wartell e Gallagher, 2012).

Seguendo questi presupposti teorici, eSecurity ha preso le mosse dalle esperienze pilota di *predictive policing*. Si tratta, in particolare, di progetti anglosassoni: l'esperienza dell'IBM insieme all'Università e alla Polizia di Memphis (USA), quella dell'Università della California Los Angeles e dell'Università della California Irvine con la Polizia di Los Angeles (USA) e, infine, il progetto del Jill Dando Institute of Security and Crime Science (University College of London) e della Polizia di Trafford, Greater Manchester (UK). Per *predictive policing* s'intende nel dettaglio l'attività di analisi dei dati di polizia sui crimini avvenuti in passato, della loro collocazione spazio-temporale (reati denunciati georiferiti) e delle ricorrenze riscontrate negli schemi

[1] La parte della ricerca di eSecurity a cui questo documento si riferisce è stata svolta da Giulia Iseppi (Junior Researcher ad eCrime) e Serena Bressan (Project Manager di eSecurity e ricercatrice ad eCrime), sotto la supervisione di Andrea Di Nicola (coordinatore scientifico di eSecurity e professore aggregato di criminologia presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trento).

di comportamento dei criminali, per prevedere i luoghi di futura concentrazione della criminalità sul territorio, con il fine ultimo di allocare le risorse di polizia in modo ottimale (RAND, 2013).

Il progetto eSecurity, nel disegnare nuovi approcci per la gestione della sicurezza urbana, ha effettuato dei passi avanti rispetto a queste esperienze, al fine di sperimentare il modello della sicurezza urbana predittiva. Secondo questo nuovo approccio, le informazioni su vittimizzazione, disordine urbano e altre variabili ambientali (ad esempio, illuminazione e dati sul clima) georiferiti, se letti in combinazione con i dati di polizia, possono evidenziare regole predittive in materia di sicurezza oggettiva e soggettiva, a supporto dell'azione di forze dell'ordine e amministratori locali nella città. Questa proposta per la prevenzione e il contrasto del crimine ha ricombinato, grazie all'utilizzo delle tecnologie ICT, le conoscenze che provenivano dagli studi delle teorie razionali e della criminologia ambientale e la grande quantità di dati di cui possiamo disporre al giorno d'oggi nella società dell'informazione (Di Nicola e Bressan, 2014).

Nello specifico, eSecurity ha avuto l'obiettivo di sviluppare uno strumento ICT innovativo e georiferito (prototipo) per la raccolta dati, con lo scopo di migliorare le attività di gestione della sicurezza urbana e della prevenzione della criminalità e dei fenomeni di devianza in città. Il suo fine ultimo è assistere i decisori politici e le forze di polizia. Nell'area pilota del comune di Trento, sono stati realizzati:

1. un database georiferito (*eSecDB*), concepito per immagazzinare dati su eventi criminali e informazioni su vittimizzazione, percezione della sicurezza, disordine urbano e altre variabili rilevanti (ad esempio, variabili socio-demografiche, informazioni su condizioni climatiche e illuminazione cittadina);

2. un sistema informativo geografico (*eSecGIS*), che utilizza come input i dati provenienti da *eSecDB*, con capacità avanzate di generazione automatica di *report*, di visualizzazione di mappe di rischio e di sicurezza urbana predittiva;

3. un portale web (*eSecWEB*), per rafforzare la comunicazione e la collaborazione tra cittadini, amministrazioni locali e forze dell'ordine su politiche, iniziative e consigli su possibili comportamenti preventivi.

Per offrire un nuovo modello di gestione della sicurezza urbana, per la prevenzione e predizione delle future concentrazioni di criminalità e devianza, il sistema informativo geografico *eSecGIS* (prototipo), con i relativi algoritmi predittivi in esso inseriti, non si è servito solo dei dati sui luoghi e sulle tempistiche degli eventi criminali passati georiferiti e anonimizzati, provenienti dalla banca dati SDI (Sistema di Indagine) del Ministero dell'Interno italiano, immagazzinati in *eSecDB*. Ha, infatti, utilizzato altre variabili socio-demografiche e ambientali georiferite, derivanti anche dalla s*mart city*, la città intelligente: ad esempio, il livello dell'illuminazione nei diversi quartieri, la situazione climatica o la distribuzione degli esercizi commerciali sul territorio cittadino (Di Nicola e Bressan, 2014). Considerare queste variabili è fondamentale nella gestione della sicurezza urbana, perché nelle città esistono luoghi che sono considerati generatori o attrattori di criminalità di per sé (*crime generators/attractors/enablers areas*): ad esempio, esercizi commerciali, industrie, bar, banche, parchi o parcheggi. In queste aree, tendono a concentrarsi criminalità, disordine urbano e insicurezza. Il prototipo *eSecGIS* può aiutare a comprendere che intervenire su tali luoghi è cruciale per prevenire e ridurre i reati, massimizzando l'efficienza nell'uso delle risorse pubbliche. In tal modo, infatti, possono anche essere individuate strategie preventive *ad hoc*, mirate alla modifica dei comportamenti e alla pianificazione urbana (Brantingham e Brantingham, 1995; Lab, 2010).

Inoltre, questo strumento ICT tiene anche conto della concentrazione del disordine (o degrado) urbano fisico e sociale (reale e percepito), della vittimizzazione e dell'insicurezza percepita, anche quali predittori della concentrazione della criminalità e della devianza nel tessuto urbano (Nobili, 2003; Regione Piemonte, 2012). La paura della criminalità delle persone sembra crescere quando alla percezione del rischio di vittimizzazione si accompagna il disordine urbano. In questa categoria, si distingue tra fenomeni di disordine fisico (ad esempio, graffiti sui muri, rifiuti abbandonati, edifici in cattive condizioni) e sociale (ad esempio, presenza di tossicodipendenti, prostitute, vagabondi). Il senso d'insicurezza di chi abita in uno spazio urbano tende a intensificarsi con l'aumentare di questi segnali di degrado ambientale e, nello specifico, in corrispondenza di una più accentuata violazione delle regole riguardanti l'uso degli ambienti cittadini. I concetti di disordine, vittimizzazione e insicurezza percepita sono, quindi, anche utili strumenti di diagnosi per comprendere i processi di sicurezza oggettiva e soggettiva in città (Wilson e Kelling, 1982).

Per raccogliere questi dati, nell'ambito del progetto eSecurity, sono state svolte quattro indagini di vittimizzazione a cadenza semestrale, denominate *Indagini sulla sicurezza oggettiva e soggettiva nel comune di Trento*: dopo il primo *round* d'indagine svoltosi a ottobre 2013, il relativo questionario è stato somministrato ai cittadini nuovamente ad aprile 2014, ottobre 2014 e aprile 2015. Lo scopo delle indagini è stato

di raccogliere informazioni sui reati subiti negli ultimi sei mesi e nell'ultimo anno dai cittadini del capoluogo trentino, nonché sul senso d'insicurezza e sui livelli di disordine urbano percepiti nel territorio comunale. Invece, la raccolta dei dati georiferiti sul disordine urbano fisico e sociale presente sul territorio di Trento è avvenuta quattro volte, sempre ogni sei mesi (ottobre 2013, aprile 2014, ottobre 2014, aprile 2015) su base circoscrizionale, grazie alla Questura di Trento che ha rilevato le situazioni di degrado attraverso un *device* dedicato. I rilevatori hanno utilizzato un'applicazione per la geolocalizzazione dei fenomeni di disordine sviluppata *ad hoc* (Di Nicola et al., 2014).

Il riconoscimento della necessità di comprendere e di tener conto della concentrazione dell'insicurezza e del disordine fisico e sociale in città è fondamentale per capire l'oggi e il domani della sicurezza in città e per gestirla. Il sistema informativo *eSecGIS* cerca di prevedere il "dove" e il "quando" avverranno alcune forme di criminalità e devianza sul territorio, ma anche di capire il "perché" si verifichino crimini, episodi di disordine e situazioni d'insicurezza personale e collettiva. Vuole, infatti, offrire conoscenza avanzata per garantire una strategia di prevenzione a tutto tondo, che consideri gli svariati aspetti in cui il concetto di sicurezza urbana si declina, a servizio di tutti gli attori istituzionali che possono incidere sulla sicurezza in ambito urbano, siano essi amministratori della città o forze di polizia (Selmini, 2004; Di Nicola et al., 2014a). In questo modo, attraverso il continuo dialogo tra il database *eSecDB* e il prototipo *eSecGIS*, il progetto eSecurity ha cercato di offrire strumenti per: 1) identificare e comprendere con precisione reati, atti devianti, disordine urbano e manifestazioni di insicurezza della popolazione e di capirne le cause, e 2) prevenire e prevedere le concentrazioni spazio-temporali della criminalità e della devianza a livello urbano, con il maggiore grado di precisione possibile, considerando l'apporto di tutte queste fonti di dati (Di Nicola e Bressan, 2014).

Dopo aver brevemente analizzato questo approccio innovativo per la gestione della sicurezza a livello urbano, sviluppato nell'ambito di eSecurity, è doveroso fare un passo avanti, andando ad analizzare anche un'ulteriore possibile fonte dati in tema di sicurezza urbana: le applicazioni *mobile* che permettono ai cittadini di fare segnalazioni in tema di sicurezza oggettiva e soggettiva alle forze dell'ordine e agli enti pubblici o privati preposti, mettendoli così al centro della gestione della sicurezza in città. Osservare l'esistente e rilevare gli eventuali limiti delle *app* in materia, soprattutto con riferimento ai profili di *privacy* e tutela dei dati personali, può essere infatti un utile approfondimento in vista dei futuri sviluppi del progetto eSecurity, che ha visto negli ultimi tre anni la città di Trento come laboratorio sperimentale.

01

Spiegare il crimine e il senso d'insicurezza in città: la sicurezza urbana nella smart city

La questione della sicurezza urbana è ormai da vent'anni al centro del dibattito politico e dell'opinione pubblica italiana e mondiale, nonché della riflessione a livello accademico. La sicurezza urbana non solo va a rivestire il ruolo di "fenomeno sociale", che presenta caratteristiche differenti a seconda delle diverse aree geografiche di riferimento, ma raccoglie in sé anche il significato di "entità politica", divenendo un punto focale dell'agenda governativa e del dibattito istituzionale sulle autonomie locali (Selmini, 2004). Tale concetto viene, pertanto, ad assumere progressivamente la connotazione di un'attività volta sia a garantire il contrasto agli eventi criminosi sia l'aumento della percezione pubblica della sicurezza. Concepire la sicurezza come un "problema urbano" si collega in primo luogo all'affermazione di una nuova veste per i soggetti istituzionali nella prevenzione e nella repressione dei reati, riconoscendo perciò compiti diversi anche agli amministratori locali, oltre che alle forze di polizia. In secondo luogo, tale concetto si connette inestricabilmente con l'evoluzione delle nostre città in *smart city*: uno spazio sociale dove le nuove tecnologie diventano protagoniste di un dialogo allargato tra istituzioni pubbliche e cittadinanza nella lotta alla criminalità, al disordine urbano e all'insicurezza diffusa (Zedner, 2000; Marciano, 2015).

La sicurezza urbana nella smart city

Nell'ambito della *governance* delle città, sono emersi negli ultimi anni nuovi bisogni e temi di pari passo con l'evoluzione delle tecniche preventive e repressive per la gestione della sicurezza urbana:

1. la necessità di moderni strumenti ICT capaci di rendere maggiormente efficace ed efficiente l'attività di polizia e gli interventi di prevenzione a livello cittadino, posti in essere anche dagli enti locali;

2. il bisogno di nuove tecnologie ICT mirate a identificare e misurare il crimine, il disordine urbano e la percezione dell'insicurezza con un maggiore grado di precisione, al fine di implementare la cosiddetta "*knowledge-based urban security*";

3. lo sviluppo del "*predictive policing*" e della cosiddetta "*predictive urban security*", ovvero la capacità delle forze dell'ordine e dei *policy-makers* locali di prevedere la concentrazione del crimine (e di altri fenomeni di devianza o insicurezza) a livello urbano e, conseguentemente, di allocare le risorse in modo mirato;

4. l'importanza di rendere i cittadini protagonisti della gestione della sicurezza urbana nelle loro città, attraverso lo sviluppo di applicazioni *mobile ad hoc*, che permettano non solo di ottenere nuovi flussi informativi sullo stato della criminalità, del degrado urbano e dell'insicurezza percepita, ma anche di rendere le persone "più sicure" interagendo con la pubblica amministrazione (Brantingham e Tita, 2008; Di Nicola et al., 2014).

Allo stato attuale, esempi reali di gestione *smart* della sicurezza urbana e di "*predictive policing*" sono stati implementati in maniera efficace in poche situazioni (es. USA e Regno Unito), basandosi sulla creazione di mappe georiferite strutturate in relazione ai crimini denunciati alle forze dell'ordine. A questo riguardo, un caso di rilievo è la sperimentazione a Memphis (USA) di un *software*, sviluppato da IBM, capace di predire la concentrazione del crimine e, pertanto, di dare supporto alla polizia nel tentativo di ridurre tassi di criminalità urbana (Short et al., 2008; Jones et al. 2009). In Italia, il progetto europeo *eSecurity – ICT for knowledge-based and predictive urban security* (descritto nella parte introduttiva di questo rapporto) è stato il primo test di *"sicurezza urbana predittiva"* nel laboratorio sperimentale di Trento. eSecurity è un sistema informativo georiferito (realizzato in forma di prototipo), a utilizzo semplice e operativo, per forze di polizia e amministrazioni locali, applicabile in ogni realtà locale, che ha lo scopo di migliorare, in ambito urbano, le attività di gestione della sicurezza urbana e della prevenzione della criminalità. Non è solo un semplice sistema d'integrazione e di rappresentazione avanzata di dati. È un sistema che aiuta comprendere, prevedere, valutare e anticipare reati, insicurezza dei cittadini e disordine nella città, con riferimento allo spazio e al tempo (Di Nicola et al., 2014).

Per affrontare al meglio il concetto di sicurezza urbana, così come evoluto sino agli sviluppi contemporanei e alle moderne tecniche di prevenzione di matrice ICT, occorre riprendere le teorie criminologiche sviluppatesi dalla metà del XX secolo, partendo dalla Scuola di Chicago e arrivando alle teorie delle opportunità criminali. Difatti, le strategie di adattamento delle società contemporanee ai fenomeni criminali e al governo dei rischi a livello urbano sono state interpretate sulla base del substrato teorico-pratico della criminologia ambientale e delle teorie razionali (Clarcke, 1997). Tra le interpretazioni della criminalità come fenomeno derivante da motivazioni individuali e da cause strutturali vi sono la teoria delle attività di *routine*, la teoria degli stili di vita e la teoria della scelta razionale. Secondo la teoria delle attività di *routine*, perché avvenga un reato, devono verificarsi tre condizioni nello stesso momento e nello stesso luogo: a. la disponibilità di un bersaglio adeguato (*suitable target*); b. l'assenza di un controllore idoneo a prevenire l'evento criminale (*capable guardian*); c. la presenza di un aggressore motivato (*motivated offender*) (Felson, 1992; Felson & Clarcke, 1998).

Seguendo lo stesso filone, la teoria degli stili di vita ha lo scopo di analizzare le variazioni nei tassi di vittimizzazione e i comportamenti delle vittime potenziali. Gli stili di vita, pertanto, determinano la probabilità della vittimizzazione personale (Hindelang et al., 1978). La teoria della scelta razionale, d'altro canto, elaborata dai criminologi Cornish e Clarke alla metà degli anni '80, è il fondamento teorico su cui si basa la prevenzione situazionale, che comprende misure finalizzate a ridurre le opportunità degli eventi criminosi. Tale prospettiva assume come presupposto che l'autore dell'atto criminale cerchi di trarre dal suo comportamento un beneficio. La teoria, quindi, considera gli autori di reato persone che attivamente prendono decisioni sulla base di un'analisi costi-benefici delle opportunità criminali che si presentano loro. In relazione a questa teoria, la prevenzione situazionale risulta essere tanto più efficace quanto più specifico sia il reato su cui si voglia intervenire e quanto più precisa sia la conoscenza del contesto in cui si agisce (Clarcke & Eck, 2003).

Infine, la criminologia ambientale trova il suo *background* teorico nella tradizione della Scuola di Chicago, nelle teorie dello spazio difendibile di Newmann e nello studio sulla pianificazione urbana di Jacobs e Jeffery (Melossi, 2004). Queste ipotesi vengono in seguito riprese da Brantingham e Brantingham (1991), i padri della "*Pattern Theory*", che sposta la prospettiva verso gli interventi preventivi, adottando un approccio empirico al problema della criminalità. Tale teoria si basta sullo studio dei comportamenti e dell'ambiente, al fine di individuare i modelli di comportamento degli autori di reato e le possibili tecniche di contrasto. I due studiosi partono dall'analisi dei luoghi dove si realizzano gli eventi criminosi, dei movimenti che portano gli autori e le vittime di reato a incontrarsi e di come tali soggetti percepiscano i suddetti luoghi. Ritengono che la criminalità non sia diffusa uniformemente, ma si concentri in alcune aree, definite "*hot dots*", "*hot lines*" o "*hot areas*". Inoltre, alcuni luoghi (es. pub, parchi pubblici, aree commerciali) sono considerati generatori o attrattori di criminalità di per sé ("*crime generators/attractors/enablers*") e, pertanto, intervenire su tali luoghi è cruciale nella prevenzione e nella riduzione della criminalità.

In tal modo, possono essere individuate strategie preventive *ad hoc*, mirate alla modifica dei comportamenti e alla pianificazione urbana. Nello sviluppo ideale di tale teoria, la conoscenza delle "*crime generators areas*", "*crime attractors areas*" e "*crime enablers areas*", delle opportunità criminali esistenti e della natura situazionale del crimine permette, quindi, di valutare quali siano i fattori criminogeni da tenere in considerazione nell'elaborazione di politiche preventive e di contrasto efficaci ed efficienti (Wartell e Gallagher, 2012). Partendo, perciò, dal presupposto che i reati non sono diffusi in maniera uniforme nello spazio e nel tempo, ma si concentrano in alcune aree (es. *hot dots*), la mappatura della criminalità può permettere una migliore comprensione di tali *pattern* spazio-temporali, allo scopo di implementare nuove soluzioni preventive basate sulla predizione del verificarsi degli stessi eventi criminosi. Quindi, gli interventi in luoghi specifici sono cruciali nella prevenzione e nella riduzione della criminalità (Ratcliffe, 2010).

Le attuali esperienze di applicazione del cosiddetto "*predictive policing*", quali il sopra-menzionato caso del *software* IBM, tendono a focalizzarsi solo sulla georeferenziazione dei dati ricavati dalle denunce di reato raccolte dalle autorità di polizia, con l'obiettivo di prevedere i luoghi dove presumibilmente si verificheranno i crimini (Short et al., 2008). Queste esperienze di prevenzione basate sull'utilizzo delle nuove tecnologie non tentano però di comprendere e prevedere anche la concentrazione del disordine urbano e dell'insicurezza a livello cittadini, che sono essi stessi predittori della concentrazione della criminalità (Thacher, 2004). Solo i dati di polizia sono stati utilizzati dagli studiosi anglosassoni sopra-citati, al fine di predire l'avvenimento dei reati in luoghi specifici, non tenendo in conto altri possibili fattori causali, quali gli andamenti e la distribuzione del crimine, del disordine e dell'insicurezza, nella definizione dei luoghi di maggiore concentrazione della criminalità. Altre variabili di tipo ambientale (es. il traffico, l'illuminazio-

ne pubblica, il clima) dovrebbero, perciò, essere prese in considerazione, unitamente ai dati di polizia, allo scopo di porre in essere una più efficace ed effettiva attività di prevenzione e riduzione dei reati, del disordine e dell'insicurezza percepita dai cittadini a livello locale attraverso l'utilizzo delle nuove tecnologie ICT, come accaduto in Italia con il progetto europeo eSecurity (Di Nicola e Bressan, 2014; Di Nicola et al., 2014).

Un ulteriore passo avanti nello sviluppo di tecnologie per la gestione della sicurezza urbana nelle *smart city* è rappresentato, come già accennato nell'introduzione di questo *report*, dal mettere i cittadini "al centro" attraverso lo sviluppo di applicazioni *mobile* che permettano di renderli "più sicuri", senza dimenticare i profili di *privacy* e di protezione dei dati personali. Inoltre, queste esperienze di rete tra abitanti della città e pubbliche amministrazioni potranno aprire nuove prospettive per comprendere come le tecnologie digitali possano anche cambiare le modalità e i canali attraverso cui gli enti locali, le forze di polizia e i residenti dialogano, sviluppando forme di cittadinanza attiva. Solo comprendendo quali siano le *app* di questo tipo attualmente esistenti, i loro limiti e punti di forza, sarà possibile creare strumenti realmente efficaci ed efficienti per una migliore *governance* della sicurezza nelle nostre città.

La sicurezza urbana e la touch era

Le *applicazioni mobile* possono essere strumenti che s'inseriscono all'interno delle strategie per garantire sicurezza urbana. Non esistendo una definizione condivisa di sicurezza urbana, in questo rapporto di ricerca si utilizzerà una definizione funzionale della stessa, risultato della generalizzazione delle caratteristiche dei vari programmi che si sono implementati nel tempo. Questi programmi, a loro volta, sono stati creati sulla base delle conclusioni teoriche e degli esiti dell'applicazione delle diverse teorie sulla criminalità urbana e sulla sicurezza, di cui si è data una chiave di lettura in questo capitolo. Le teorie di cui si è parlato hanno come intento comune la spiegazione e la gestione delle problematiche di sicurezza urbana, concentrandosi sugli elementi che contraddistinguono la commissione di un reato o di un atto deviante: l'autore, il contesto in cui l'evento si svolge, la vittima e la reazione della società.

Sin dal 1995, il Consiglio Economico e Sociale delle Nazioni Unite ha predisposto delle linee guida per implementare dei programmi di sicurezza urbana che si concentrassero per prima cosa su di un approccio locale al problema della criminalità in città, cui devono partecipare in maniera coordinata diverse agenzie, dimostrando come la questione della sicurezza debba essere prima di tutto gestita a livello micro. Nel tempo, tali linee guida sono diventate sempre più articolate e suggeriscono che ogni programma d'intervento in materia sia sviluppato e valutato sulla base di alcuni principi fondamentali: (1) *leadership* dei progetti da parte di tutti i livelli di governo; (2) attenzione allo sviluppo economico e sociale e garanzia di meccanismi di inclusione; (3) cooperazione tra autorità e creazione di *partnership* pubblico-privato a tutti i livelli; (4) sostenibilità dei programmi e implementazione di metodi di *accountability*; (5) conoscenza dei problemi legati a criminalità e disordine urbano, adottando un approccio multidisciplinare (ossia creazione di progetti *knowledge-based*); (6) rispetto dei diritti umani e delle regole dello stato di diritto; (7) attenzione ai legami che possono crearsi tra la criminalità a livello locale e il crimine organizzato; (8) promozione di strategie differenti a seconda dei destinatari dei programmi (Cfr. Risoluzione 1995/9 del Consiglio Economico e Sociale delle Nazioni Unite sulle Linee guida per la sicurezza urbana, 24 luglio 1995).

L'avvento delle tecnologie informatiche ha facilitato il compito degli *stakeholders* rispetto a buona parte di questi obiettivi: la cooperazione tra agenzie pubbliche e private può essere svolta più efficacemente tramite *software*. In questo modo, i meccanismi di *accountability* e di valutazione possono essere automatizzati, la gestione e la ricerca di informazioni sulle caratteristiche della popolazione possono essere reperite in banche dati pubbliche e private, il confronto con precedenti modelli di politiche contro la criminalità può essere svolto tramite ricerca in Internet e la comunicazione tra le agenzie e i cittadini può essere potenziata (Yildiz, 2007). La praticità delle nuove tecnologie per la gestione dei problemi urbani può essere dimostrata considerando la letteratura esistente sull'*eGovernment*. Sulla scia degli studi già compiuti sulla "*appificazione* della società", i suoi vantaggi e i suoi svantaggi, si procederà con l'analisi delle applicazioni mobili per la sicurezza urbana, strumenti utili a raggiungere anche taluni degli obiettivi individuati dalle Nazioni Unite, e della loro conformità ai dettami sovranazionali in tema di *privacy* e protezione dei dati personali (Cfr. Dichiarazione di Varsavia sulla "*appificazione*" della società, 24 settembre 2013).

L'importanza che lo scopo di questa ricerca riveste al giorno d'oggi, ovvero nella cosiddetta *touch era*, trova un riscontro in una recente indagine condotta da 26 Garanti per la *privacy* a livello mondiale, la "*Global Privacy Sweep 2014*", i cui risultati dimostrano come circa metà delle applicazioni analizzate (su un campione di 1211 *app*) presentino problematiche in merito al

rispetto dell'obbligo di informativa e al numero di autorizzazioni richieste per l'installazione. Circa tre quarti delle *app* in questione richiede uno o più consensi per l'installazione, soprattutto rispetto alle funzioni più "invasive" (es. accesso ai dati di localizzazione, alla fotocamera, alla rubrica, al registro chiamate). Nonostante la richiesta di consenso, però, le autorità sottolineano la necessità di una maggiore trasparenza in quest'ambito, soprattutto se raccolgono informazioni sensibili: i termini del consenso sono stati giudicati "problematici" per il 31% delle *app* valutate. Nella maggioranza dei casi (59% delle *app* parte del campione), le autorità hanno avuto difficoltà a visualizzare l'informativa prima dell'installazione e, quando essa è stata trovata, non sempre esplicitava le finalità della raccolta dei dati. Inoltre, le informazioni cui lo strumento chiedeva di accedere sono state spesso considerate eccedenti rispetto agli scopi e alle funzionalità dell'applicazione, in ragione dell'informativa fornita dagli sviluppatori. A opinione degli esperti, solo il 15% delle applicazioni valutate era dotata di un'informativa chiara (Garante per la protezione dei dati personali, 2014).

Il risultato deludente dell'indagine "*Global Privacy Sweep 2014*" ha indicato la strada delle future iniziative che devono essere prese in considerazione dai legislatori e dalle autorità di controllo in materia di tutela della *privacy* e dei dati personali nel mondo delle applicazioni. In vista dell'implementazione del nuovo Regolamento europeo per la protezione dei dati (Cfr. Proposta di Regolamento "COM(2012) 11 final" del 25 gennaio 2012), sul quale si dovrebbe raggiungere un accordo nelle sedi europee entro la fine del 2015, vi è ora necessità di comprendere quali siano i principi fondamentali da applicare alle *mobile apps* per la sicurezza urbana, svolgendo una distinzione basata: (1) sulle tipologie di dati che vengono acquisiti e trattati; (2) sulle caratteristiche dell'informativa e del consenso; (3) sul rispetto del principio della qualità dei dati. Ciò diviene sempre più importante alla luce del fatto che il nuovo pacchetto europeo di riforma della protezione dei dati (cd. "Pacchetto protezione dati") unirà sia il Regolamento generale sulla protezione dei dati sia la Direttiva sulla protezione dei dati trattati dalla polizia e dalle autorità giudiziarie penali. Esso aggiornerà e sostituirà le attuali norme in materia di tutela dei dati che si basano sulla Direttiva sulla protezione dei dati del 1995 e sulla Decisione quadro del 2008 per i settori della polizia e della giustizia penale (Commissione europea, 2015).

Sulla base dei dati raccolti attraverso l'ultimo Eurobarometro sulla *"Data Protection"* (Unione europea, 2015), ben il 55% dei rispondenti all'indagine condotta nei Paesi Membri dell'Unione europea (UE) è preoccupato della tracciabilità delle proprie attività giornaliere attraverso le applicazioni *mobile* e solo il 15% ritiene di avere il completo controllo sulle informazioni personali che condivide *online*. Se nella Repubblica Ceca la preoccupazione circa la tracciabilità delle informazioni raggiunge picchi del 73%, in Italia è il 52% dei cittadini interpellati a essere molto intimorito dal controllo dei dati che può essere esercitato tramite le *app.* Non sorprende, a riguardo, che oltre il 90% del campione valuta fondamentale che in tutt'Europa vi siano le medesime regole in tema di tutela della riservatezza e dei dati personali. L'avanzamento tecnologico, la percezione del "problema *privacy*" misurata dall'Eurobarometro e le prossime riforme europee determinano, perciò, una nuova espansione della visuale in merito al concetto di riservatezza*,* in ragione dei diversi problemi di tutela dei dati per la collettività a seconda delle tecnologie adottate. Nel solco tracciato dalle nuove interpretazioni, che vedono la *privacy* come concetto multifattoriale, si inserisce la proposta di Maren Hartmann di considerare autonomamente la *Mobile Privacy* (Hartmann, 2011).

Concentrandosi sugli effetti dei nessi che si vengono a creare tra persone, luoghi e attività, la Hartmann afferma che la combinazione di "mobilità" e *privacy* potrebbe generare rischi ulteriori e diversi da quelli che fino ad ora si sono presentati per la tutela della riservatezza. Esamina i due aspetti di *privacy* e "mobilità" inserendoli nel contesto di riferimento: per prima cosa, le diverse definizioni di *privacy* vanno messe in relazione al rapporto tra il singolo e la collettività. Il secondo elemento di cui viene sottolineata l'importanza è il profilo fisico e correlato al luogo in cui un individuo ha diritto alla *privacy*, profilo solitamente sottaciuto, poiché tendenzialmente la *privacy* in rapporto alle nuove tecnologie viene considerata solo rispetto al profilo dell'informazione. Analizzando la questione della "mobilità", la studiosa afferma che nel contesto *mobile* possono entrare in gioco diverse tipologie di *privacy*, le quali a loro volta dipendono dai movimenti e dal luogo in cui si trova l'utente, nonché dalle attività che lo stesso svolge. Utilizzando le forme di "mobilità" illustrate da John Curry nel 2002, la Hartmann dimostra come vi siano diversi tipi di *privacy* nel contesto *mobile* e come queste non siano legate solo alle persone, ma sempre di più agli oggetti esterni a esse e alle applicazioni stesse. La *Mobile Privacy* si interessa, quindi, di queste cinque tipologie di *privacy*:

1. *Corporal Privacy:* è la *privacy* che riguarda il corpo non in quanto tale, quanto piuttosto nei suoi movimenti e attributi (come le informazioni che riguardano il movimento verso un luogo, il perché del movimento verso quel luogo, chi si incontra, ecc.);

2. *Physical Privacy:* è la *privacy* degli oggetti e del loro uso;

3. *Imaginative Privacy:* si tratta della protezione del pensiero e dell'immaginazione, ossia dell'uso di strumenti per le attività ludiche;

4. *Virtual Privacy:* è la *privacy* dei dati dell'individuo, sia dal punto di vista del loro contenuto sia delle connessioni che quegli stessi dati creano (tra persone, tra cose, tra azioni, tra momenti, ecc.);

5. *Communicative Privacy:* è la protezione delle comunicazioni interpersonali a ogni livello, qualsiasi sia lo strumento utilizzato.

Le dimensioni per la protezione della *privacy* nel contesto dei dispositivi *mobile* che si sono appena illustrate sono necessariamente adottabili rispetto alle applicazioni *mobile* in generale. A maggior ragione, potranno essere adottate per comprendere i problemi di *privacy* sollevati dalle applicazioni *mobile* per la sicurezza urbana. Un'applicazione *mobile* per la sicurezza urbana è un tipo di applicazione caratterizzato grazie allo scopo che intende raggiungere. È un programma informatico creato per funzionare su dispositivi *mobile* (come *smartphone* e *tablet*) che può: (1) svolgere funzioni di informazione dell'utente rispetto al disordine urbano o ai reati compiuti in una zona della città; (2) consentire l'invio di segnalazioni ai diversi *stakeholders* (es. forze dell'ordine o enti locali); (3) rassicurare l'utente creando una rete di "guardiani" da contattare in caso di emergenza .Nel capitolo successivo, si fornirà una definizione più dettagliata di cosa sia un'applicazione *mobile* e quali siano le sue componenti, in modo da poter giustificare la definizione di *mobile app* per la sicurezza urbana data e classificare le applicazioni esistenti in questo settore, sulla base di alcune caratteristiche comuni rinvenute tramite l'analisi di alcune applicazioni presenti sul *Market App Google Play*.

02

Le applicazioni mobili per la sicurezza urbana: dalla teoria alla pratica

L'evoluzione degli strumenti tecnologici negli ultimi decenni ha avuto un'accelerazione impressionante: dalla controcultura degli anni '70, si è passati alla filosofia del "computer in ogni casa", sino agli anni '90, quando l'integrazione di componenti informatiche negli oggetti di uso quotidiano è diventata un dato ormai acquisito e gli elementi tecnologici si sono miniaturizzati e sono diventati più potenti. I movimenti a cui stiamo assistendo hanno investito ogni elemento della nostra vita, grazie ad un *network* globale tramite cui chiunque può comunicare liberamente: Internet (Ziccardi, 2012; Chaouchi, 2013).

Nel mondo delle comunicazioni, si è avuto un passaggio repentino dai dispositivi *mobile* utili solo a ricevere chiamate sino agli attuali dispositivi *touch* (*smartphone* e *tablet*), capaci di offrire all'utilizzatore nuovi e diversi modi per interagire con le informazioni a disposizione su Internet. Sono considerati attualmente qualcosa di diverso dai computer e qualcosa di diverso ancora dai telefoni: uno strumento dotato di un proprio mercato che riunisce le capacità di entrambi i *devices* precedenti in una forma innovativa. La differenza sostanziale riguarda le possibilità che i dispositivi *touch* garantiscono: (1) interfaccia intuitiva, (2) funzionamento standardizzato e semplificato, (3) presenza di funzioni avanzate in un pacchetto base, (4) la possibilità per l'utente e per gli sviluppatori di personalizzare a piacimento il proprio *device*, grazie ad applicazioni di diverso tipo che funzionano sullo stesso sistema operativo interoperabile (Fling, 2009).

Un'applicazione *mobile* (o *mobile application*; più semplicemente *app*) è un programma informatico atto a svolgere una o più funzioni determinate creato per funzionare su *smartphone*, *tablet* o altri dispositivi *mobile* (soprattutto *touch)*, preinstallato sul dispositivo o disponibile gratuitamente o a pagamento presso le piattaforme (o *stores*) di distribuzione. Queste ultime si differenziano tra loro a seconda del sistema operativo (d'ora in poi "OS", *operating system*) che supporta i prodotti. Ci sono *stores* ufficiali (come *Google Play store*, *App store*, *Windows Phone Store* e *BB App world*) ufficialmente supportati dai produttori di OS e solitamente preinstallati sui dispositivi, e *store* di terze parti, come *Amazon app store*, che vanno scaricati appositamente e fanno capo ad aziende solitamente non legate ai produttori dell'OS (Garante per la protezione dei dati personali, 2014).

Dato l'alto numero di *stores* dove scaricare le applicazioni a disposizione degli utenti, i prodotti si sono via via moltiplicati e il numero delle *app* dal 2008, periodo in cui sono stati lanciati *Android Market* di *Google* (ora *Google Play*) e *App Store* di *Apple*, è salito vertiginosamente, raggiungendo vette impressionanti[2]. Riprendendo le considerazioni svolte da Deborah Lupton, si può affermare all'estremo che l'idea di cultura o società non può venir pienamente compresa senza riconoscere che computer, *software* e *device* non sono più solo alla base della costruzione dell'io, della rappresentazione della persona, della vita sociale, delle relazioni e delle istituzioni sociali, ma attualmente li costituiscono (Lupton, 2014). Se computer e *software* sono arrivati a "creare" la personalità di ognuno di noi e a sostenere la nostra vita sociale, la nostra cultura, non deve sorprendere il tentativo di cercare risposte alle domande di sicurezza e benessere in ambito cittadino in uno strumento come l'applicazione, che garantisce velocità, immediatezza ma soprattutto opera solo a richiesta (Gardner e Davies, 2014).

Si deve ammettere che l'importanza che stanno assumendo queste tecnologie nella nostra vita non è più trascurabile, a mano a mano che le nostre città stanno diventando sempre più *smart* e, con esse, la cittadinanza stessa. Se la base della comprensione è la conoscenza, vi è necessità di comprendere non solo cosa sia un'*app* per la sicurezza urbana, ma anche capire quali siano le sue proprietà. Un'applicazione per la sicurezza urbana, come già accennato in precedenza, è un programma informatico creato per funzionare su dispositivi *mobile* che può: (1) svolgere funzioni di informazione dell'utente rispetto al degrado urbano o ai reati compiuti in una zona; (2) consentire l'invio di segnalazioni ai diversi *stakeholders* (es. forze dell'ordine, enti locali, servizi di sicurezza privati); (3) rassicurare l'utente creando una rete di "guardiani" (es. amici e parenti) da contattare in caso di emergenza. Questa definizione è stata creata utilizzando la definizione base di applicazione, per caratterizzarla rispetto allo scopo specifico che gli

[2] Per avere un'idea dei prodotti disponibili nei maggiori Store ci si può riferire a queste stime http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (data ultima consultazione: 09/12/2015).

sviluppatori vogliono raggiungere (ovvero la gestione della sicurezza urbana attraverso il coinvolgimento del cittadino), grazie alle funzionalità integrate nello strumento.

Le funzionalità delle *app* si basano su caratteristiche che consentono agli sviluppatori di identificare chi invia la richiesta, dove si trova l'utente, quali attività intende svolgere tramite lo strumento, a chi desidera comunicare la propria posizione, ecc. La raccolta di questo tipo di informazioni da parte degli sviluppatori e dalle agenzie dell'emergenza e dalla pubblica amministrazione può creare un rischio per la riservatezza e la tutela dei dati personali degli utenti degli strumenti e per quella di chi è in contatto con loro. Per comprendere concretamente quale tipologia di informazioni vengono raccolte dalle applicazioni per la sicurezza urbana, si svolgerà una descrizione di un gruppo di esse, selezionato secondo i criteri che verranno esposti nel prosieguo della trattazione. Tramite questa categorizzazione, sarà possibile comprendere le peculiarità delle applicazioni per la sicurezza, utili per una successiva valutazione di conformità delle stesse con la normativa attualmente in vigore a livello sovranazionale sulla *privacy* e la protezione dei dati personali.

Selezionare le applicazioni mobili per la sicurezza urbana

Per realizzare una panoramica accurata e categorizzare le *app* in tema di sicurezza urbana, allo scopo di procedere poi a una valutazione di *compliance* delle stesse in relazione alla *privacy* e alla protezione dei dati personali (capitolo 03), si è svolta una ricerca preliminare sulla letteratura esistente in materia di categorizzazione generale di applicazioni *mobile*. Le analisi per la maggior parte si sono concentrate sulle caratteristiche delle funzionalità dell'applicazione e sulla descrizione di tali strumenti. Per la creazione di gruppi di *app* da studiare, si sono scelte le migliori applicazioni disponibili, "le più famose" o categorie eterogenee di strumenti scelti casualmente. Dato lo scopo di questa analisi conoscitiva, ossia fornire un'*overview* delle caratteristiche delle applicazioni mobili per la sicurezza urbana al fine di individuare quali profili di criticità questi strumenti abbiano rispetto alla normativa esistente che tutela protezione di dati personali e *privacy*, si è scelto svolgere l'analisi rispetto al sistema operativo *Android*, essendo attualmente l'OS installato su un numero maggiore di dispositivi a livello mondiale (Office of the Privacy Commissioner for Personal Data, 2013; Chittaro e Sioni, 2014).

In secondo luogo, si è scelto di analizzare i prodotti del più fornito *store* disponibile per l'OS (nonché *store* ufficiale dello stesso): *Google Play*. Si sono poi cercate delle parole chiave da utilizzare nel motore di ricerca dello *store*, connesse alla sicurezza urbana e al senso di sicurezza in base alla letteratura di riferimento, tradotte poi in inglese, francese, spagnolo e tedesco, per garantire una copertura della ricerca più ampia. L'elenco delle parole chiave usate per la ricerca delle *app* è il seguente: 1. Reati/Degrado; 2. Crimine/Criminale; 3. Città/Zona urbana; 4. Polizia/Forze dell'ordine; 5. Sicurezza/Insicurezza; 6. Allarme/Segnalazione. Le parole chiave sono state inserite nel motore di ricerca prima singolarmente, poi in maniera aggregata per raffinare la ricerca. Si è, da ultimo, tenuto conto della funzione "applicazioni simili" a quella scelta. Eliminando le applicazioni categorizzabili come giochi, *eBook* o dai contenuti meramente informativi, si è creato il primo gruppo di applicazioni utili per il presente studio. Sulla base delle informazioni fornite dagli sviluppatori, dallo *store* e dalle immagini illustrative, si è scremato ulteriormente il gruppo, eliminando le *app* ormai non più attive e quelle che non si collegavano all'oggetto della ricerca, ottenendo un secondo gruppo di 140 applicazioni.

Per ridurre questo numero al fine di selezionare un gruppo di *app* significative per l'analisi da svolgere in questo rapporto, si è scelto di guardare al parametro relativo al numero di installazioni dell'*app* su di un *device*. Dovendo comprendere quali rischi per la *privacy* e la riservatezza possano creare le applicazioni per la sicurezza urbana, si è scelto questo parametro proprio per la possibilità delle stesse di "carpire" dati agli utilizzatori, anche nel caso in cui dovessero successivamente disinstallare l'applicazione. Controllando il numero di installazioni di ognuna delle 140 applicazioni selezionate, si ottengono le informazioni contenute nella Tabella 1, ovvero il cosiddetto "valore di installazione":

Tabella 1 - Applicazioni per la sicurezza urbana selezionate in Google Play e numero assoluto totale di installazioni. Anno 2015

Numero assoluto di installazioni	Numero di applicazioni per la sicurezza urbana selezionate
0-10	0
10-50	2
50-100	4
100-500	25
500-1.000	14
1.000-5.000	33
5.000-10.000	12
10.000-50.000	27
50.000-100.000	11
100.000-500.000	10
500.000-1.000.000	1
1.000.000-5.000.000	1
Totale	140

Fonte: elaborazione degli autori

A questo punto, si è scelto di procedere a un'ulteriore aggregazione di tali valori in base al numero di installazioni, per semplificare la classificazione delle *app* esistenti sul mercato, creando delle "classi di valore": alle applicazioni installate da 10 fino a 1.000 volte si è assegnato il valore "Basso"; alle *app* installate dalle 1.000 alle 50.000 il valore "Medio"; alle *app* installate dalle 50.000 volte alle 5.000.000 il valore "Alto". In questo modo, si è ottenuta un'ulteriore suddivisione delle applicazioni contenuta nella Tabella 2:

Tabella 2 - Le applicazioni per la sicurezza urbana selezionate in Google Play per classi di valore. Anno 2015

Classi di valore	Numero di applicazioni per la sicurezza urbana selezionate
Basso	45
Medio	72
Alto	23
Totale	140

Fonte: elaborazione degli autori

Sono state così prese in considerazione 6 applicazioni per ogni valore di installazione, quindi 18 oggetti d'analisi, per fornire una panoramica più completa delle tipologie di applicazioni per la sicurezza urbana. In questo modo, si potranno avere maggiori elementi per svolgere la successiva valutazione di conformità di questi strumenti con la legislazione sovranazionale in tema di *privacy* e tutela della riservatezza. Le applicazioni scelte con un livello di installazione "Basso" sono: *Crime Spy UK, Berlin Police Crime Watch Kiez, みまもり防犯ブザ (Tracking Crime Buzzer), Crime Check, City of Cape Coral, Crime Watch* e *Crime Rates Stats. Crime HotSpot – UK, Crime Watch, Fightback, Safe-U, Alarm 112* e *AlertCops* hanno un valore di installazione "Medio"; mentre *Safe Neighborhood*, *Mobile Tracker*, *bSafe – Personal Safety App, Crime Maps, MobilePatrol Public Safety App* e *Cuadrante Amigo* fanno parte della categoria che comprende le *app* installate su di un maggior numero di dispositivi. Nel seguito, le applicazioni per la sicurezza urbana in tal modo selezionate sono brevemente descritte.

Crime Spy UK

L'applicazione *Crime Spy UK* fornisce statistiche relative a diversi reati avvenuti nel Regno Unito e funziona solo all'interno dei suoi confini. Richiede l'accesso completo alla rete e la visualizzazione delle connessioni di rete dei dispositivi su cui viene installata, senza ulteriori richieste di autorizzazioni speciali. L'utente,dopo aver installato il prodotto, può scegliere la zona oppure la sede dell'ufficio di polizia di interesse e può consultare l'elenco dei reati e dei comportamenti devianti (es. prostituzione) compiuti in quella zona. Per ogni comportamento venuto all'attenzione delle forze dell'ordine viene indicato il livello di allarme ("*crime level*") dell'area, il numero assoluto di crimini/atti devianti e il relativo tasso di delittuosità basandosi sui dati provenienti dal *database* ufficiale della polizia britannica. Le categorie di atti segnalabili elencate sono le seguenti: comportamento antisociale, furto (di oggetti personali, di veicoli, da veicoli, con scasso, categoria "altro"), borseggio, rapina, omicidio, taccheggio, violenza sessuale, altri atti contrari all'ordine pubblico, danneggiamento e incendio, possesso di droga, possesso di armi, "altri reati". L'applicazione non prevede la visualizzazione dei dati su una mappa, ma mostra le informazioni rispetto a ogni singolo comportamento criminale/deviante compiuto nel luogo prescelto in forma di elenco.

Berlin Police Crime Watch Kiez

L'*app Berlin Police Crime Watch Kiez* si propone di visualizzare i reati e gli atti devianti compiuti a Berlino ed estratti dalle comunicazioni ufficiali della polizia cittadina della capitale tedesca, su mappa, grafico o in formato di lista. L'utente può anche svolgere una ricer-

ca dei comportamenti illeciti sulla base di data, mese e anno, nonché svolgere una ricerca spaziale *random* o di uno specifico indirizzo/quartiere. C'è inoltre la possibilità di ricevere *alert* sulla base delle aree selezionate dall'utente e delle varie ore del giorno: lo sviluppatore può inviare agli utenti che si trovano in una specifica zona di Berlino in un dato momento della giornata delle notifiche sui reati che sono stati compiuti nei dintorni. Per la sua installazione richiede una serie di autorizzazioni: (1) l'applicazione deve essere dall'utente autorizzata ad accedere alla sua posizione precisa (GPS e basata sulla rete) e alla posizione approssimativa (basata sulla rete); (2) per quanto riguarda le raccolte di foto, elementi multimediali o file, richiede l'autorizzazione per effettuare modifiche o eliminare contenuti dell'archivio USB, per svolgere un test dell'accesso all'archivio protetto; (3) richiede, inoltre, la possibilità di visualizzare le connessioni *Wi-Fi* presenti attorno all'utente, visualizzare le connessioni di rete, avere accesso alla lettura della configurazione del servizio *Google*, un accesso di rete completo e il controllo di licenza di *Google Play*. Le condotte devianti, i reati e le ulteriori informazioni di cui l'*app* si occupa riguardano comportamenti di spaccio di stupefacenti, rapine, episodi di degrado urbano (come la presenza di graffiti, sporcizia, rifiuti, ecc.), furti (di oggetti da veicoli, di veicoli, con scasso, di oggetti personali), altri comportamenti antisociali, taccheggi, violenze sessuali, omicidi, incidenti stradali e altre comunicazioni da parte della polizia (come la richiesta di informazioni a eventuali testimoni di reati). Gli sviluppatori fanno presente di non essere *partner* della polizia di Berlino e di utilizzare i dati già resi pubblici da quest'ultima.

みまもり防犯ブザ (Tracking Crime Buzzer)

La *Tracking Crime Buzzer* è un'*app* giapponese sviluppata da privati, pensata per garantire la sicurezza personale degli utenti, creando una rete di persone di "guardiani", persone di cui l'utente si fida, a cui inviare informazioni sulla sua posizione in caso di necessità. Richiede per l'installazione, come autorizzazione speciale, l'accesso alle posizione precisa dell'utente (GPS e basata sulla rete) e della posizione approssimativa (basata sulla rete). Le altre autorizzazioni richieste sono l'accesso di rete completo, la visualizzazione di connessioni di rete e l'utilizzo di fonti di geolocalizzazione fittizie a scopo di test. Gli utenti, al primo avvio dell'applicazione, devono registrarsi al servizio e inserire gli indirizzi email di amici o parenti, non necessariamente registrati al servizio, per creare la rete di sicurezza.
Nel momento in cui viene lanciata sul dispositivo, l'*app* invia un'email contenente le coordinate dell'utente e fa emettere al telefono un suono acuto, sempre più forte a seconda del tempo di pressione sul pulsante di accensione. I destinatari dell'email ricevono un *link* con la posizione dell'utente visibile su *Google Maps*. Secondo la descrizione fornita dagli sviluppatori, è possibile impostare il numero di minuti per inviare nuovamente la propria posizione, a intervalli regolari, in modo da consentire un monitoraggio da parte dei "guardiani" del percorso dell'utente o in generale del dispositivo, nel caso in cui venga perso o rubato. Utilizzando la funzione "*Silent*", l'*app* consente di disattivare l'allarme sonoro e inviare solo l'email con la propria localizzazione.

Crime Check

Crime Check è un'applicazione sviluppata da privati che si basa sull'elaborazione automatica di mappe dei crimini in una determinata area (funziona praticamente in qualsiasi Paese a livello mondiale) e consente all'utente registrato al servizio di inviare al gestore *report* geolocalizzati su reati di cui è stato vittima o testimone. Per la sua installazione, l'*app* richiede e permette: (1) l'autorizzazione speciale per accedere alla lista dei contatti registrati sul dispositivo; (2) la posizione approssimativa (basata sulla rete) e quella precisa (GPS e basata sulla rete) dell'utente; (3) la possibilità di chiamare i numeri di telefono dei "guardiani" inseriti dall'utente, (4) di modificare o eliminare contenuti dell'archivio USB, (5) di effettuare test dell'accesso all'archivio protetto, (6) di acquisire foto e video tramite fotocamera, (7) di registrare file audio (sia per fornire *report* agli altri utenti registrati al servizio, sia per inviare messaggi vocali) e, in ultimo, (8) di leggere stato e identità telefono. Altre autorizzazioni richieste sono quelle per l'accesso di rete completo, la visualizzazione delle connessioni di rete e la lettura della configurazione del servizio *Google*.
L'utente può scegliere di inviare resoconti di eventi criminali o episodi di devianza/degrado urbano di cui è stato testimone, vittima o di cui è venuto altrimenti a conoscenza, scegliendo tra sei categorie: investimento di pedone con mancato soccorso, incendio doloso, furto, rapina,incidente con danno alle persone o "altro". Ha inoltre la possibilità di descrivere l'evento in maniera dettagliata (es. inviare informazioni rispetto al numero di persone coinvolte, all'ammontare del danno, se vi è stato o meno l'uso di armi da fuoco, il luogo e l'ora dell'evento, ecc.), anche tramite l'allegazione di *file* audio e video. È possibile, infine, inviare messaggi vocali geolocalizzati ai "guardiani", che devono anch'essi essere registrati al servizio.

City of Cape Coral

L'*app City of Cape Coral* (Florida, USA) è stata sviluppata dall'amministrazione della città. Per la sua installazione, richiede e prevede: (1) l'accesso alla posizione precisa dell'utente (GPS e basata sulla rete) e alla sua posizione approssimativa (basata sulla rete); (2) la

possibilità di effettuare una chiamata diretta al numero di telefono delle autorità e (3) la chiamata diretta di qualsiasi numero di telefono; (4) la possibilità di modificare o eliminare contenuti dell'archivio USB; (5) l'opportunità di svolgere test dell'accesso all'archivio protetto, e infine (6) di leggere lo stato e l'identità del telefono, come autorizzazioni speciali. È prevista una sola autorizzazione diversa da quelle sopra elencate, ovvero l'accesso di rete completo. Il suo scopo è incrementare il dialogo tra amministrazione locale e cittadinanza, fornendo notizie sulla città, informazioni sul mondo del lavoro, eventi e attività di interesse pubblico e permessi, mettendo a disposizione i contatti delle diverse autorità e, in ultimo, creando una rete "*social*" tra i cittadini.
Gli utenti dopo averla installata possono accedere ai profili *social media* delle autorità amministrative (*Twitter* e *Facebook*), pagare le multe, la bolletta dell'elettricità e dell'acqua e possono segnalare all'amministrazione e ai concittadini una situazione di degrado urbano connessa con la presenza di rifiuti abbandonati, di piante non curate, di lampioni non funzionanti, o altre situazioni simili (inserendo il luogo, la descrizione, il proprio nome, cognome, l'indirizzo email e/o il numero di telefono e, se lo si desidera, una foto) e ottenere informazioni rispetto alle proprie precedenti segnalazioni. Un'ulteriore funzione è quella di ottenere notizie sui reati che sono stati compiuti in città, consentendo l'accesso diretto alle pagine Internet della polizia cittadina: quest'ultima permette, a scelta dell'utente, di svolgere una ricerca per data dell'evento.

Crime Watch - Crime Rates Stats

L'applicazione *Crime Watch - Crime Rates Stats* è stata sviluppata dal *Bureau of Crime Statistics and Research* del distretto australiano di New South Wales e informa gli utenti sull'andamento dei reati nelle diverse città dell'Australia. Per l'installazione, richiede diverse autorizzazioni speciali: (1) l'individuazione dell'account attivo sul dispositivo; (2) la lettura e modifica dei contatti personali; (3) l'accesso alla posizione approssimativa (basata sulla rete) e la posizione precisa dell'utente (GPS e basata sulla rete); (4) l'accesso a comandi aggiuntivi del *provider* di localizzazione. Richiede, inoltre: (5) l'autorizzazione per la ricezione messaggi di testo (SMS); (6) la lettura e scrittura del registro chiamate; (7) la possibilità di modificare o eliminare contenuti dell'archivio USB, e (8) di effettuare un test dell'accesso all'archivio protetto. Per effettuare la registrazione di file audio, prevede (9) l'autorizzazione all'accesso al microfono del dispositivo e, in ultimo, (10) la lettura dello stato e dell'identità del telefono. Le autorizzazioni ulteriori prevedono il controllo della vibrazione, l'accesso di rete completo e la modifica delle impostazioni audio del dispositivo.

L'applicazione permette la visualizzazione di mappe che identificano con diversi colori le zone che presentano differenti tassi di criminalità e/o devianza. I reati e gli atti devianti presi in considerazione sono: sequestro di persona, reati contro l'amministrazione della giustizia, incendio, aggressione, gioco d'azzardo, estorsione, comportamenti antisociali, spaccio di droga, molestie, minacce, omicidio, illeciti correlati con l'abuso di alcool, danneggiamento, possesso di materiale pornografico, possesso di armi, prostituzione, rapina, violenza sessuale, furto, illeciti da circolazione stradale e "altri reati". L'utente inserisce la propria posizione e l'*app* mostra i reati compiuti nelle vicinanze su di una mappa interattiva. Inoltre, questo strumento consente di comparare i dati di questi reati con le percentuali di tutta l'area selezionata e le percentuali delle aree vicine. L'utente può anche scegliere una città e conoscere il suo livello di rischio, l'andamento dei reati durante l'anno e ottenere una lista degli otto reati compiuti più spesso. Per ogni reato o atto deviante, si forniscono informazioni sul luogo di commissione, la data, l'ora, la tipologia di atto, la distanza dall'utente e quale sia la "zona cuscinetto" tra l'utente e il *locus commissi delicti*. È possibile anche fornire *report* di reati e atti devianti di cui si è stati testimoni, vittime o di cui si è venuti a conoscenza, scegliendo il luogo in cui si è compiuto il fatto, il tipo di reato/atto deviante ed eventualmente fornendo commenti e note aggiuntivi.

Crime HotSpot – UK

Crime HotSpot-UK mostra le percentuali relative ai reati e atti devianti compiuti in Inghilterra e Galles sulla base della posizione dell'utente, oppure svolgendo una ricerca per codice postale o selezionando specifiche aree sulla mappa interattiva. Per l'installazione, richiede: (1) l'accesso alla posizione precisa (GPS e basata sulla rete) dell'utente, (2) l'accesso di rete completo e la (3) visualizzazione delle connessioni di rete a cui si aggancia il dispositivo. È interessante notare come non vengano fornite informazioni solo sui reati compiuti, ma per ogni zona sia possibile valutare quanti reati e atti devianti siano stati compiuti in numero assoluto, la loro percentuale rispetto a quelli compiuti nella zona stessa e il livello di "frequenza-pericolosità percepita" di ogni categoria di atto. I reati presi in considerazione sono: rapina, furto con scasso, crimini violenti (non ulteriormente specificati), possesso di armi, taccheggio, danneggiamento e incendio, spaccio di droga. Sono poi presenti categorie residuali, definite come "altri furti" e "altri reati". Gli utenti possono anche accedere a informazioni su eventi di interesse pubblico che si stanno svolgendo nella zona, agli indirizzi delle più vicine stazioni di polizia e dei *Safer Neighbourhoods Teams* (poliziotti di quartiere), oltre che ai riferimenti degli ufficiali di polizia.

Crime Watch

Crime Watch è l'applicazione vincitrice all'AT&T Hackaton di Orlando in Florida (USA) nel dicembre 2011. È disponibile solo per questa città e mostra il resoconto delle ultime quattro ore di attività della polizia locale su di una mappa interattiva. Per l'installazione, richiede un'unica autorizzazione speciale, ossia l'accesso alla posizione precisa dell'utente (GPS e basata sulla rete), mentre richiede come autorizzazione di base l'accesso di rete completo e la visualizzazione delle connessioni di rete a cui si collega il dispositivo. L'*app* mostra le attività della polizia ed i reati commessi a Orlando, anche con funzionalità *street view*. Per ogni intervento geolocalizzato delle forze dell'ordine, sono indicate informazioni sul tipo di azione portata a termine, una sua descrizione sommaria, l'indirizzo completo, la data e l'ora. L'utente può svolgere anche una ricerca sulla base delle categorie di reato e delle situazioni di degrado urbano prese in considerazione, ossia: furto, furto con scasso, presenza di veicoli abbandonati, incidenti stradali, violenze sessuali, stupri, violazione di domicilio e violazione del mandato di arresto.

Fightback

Fightback è un'*app* pensata per aumentare il livello di sensibilità nei confronti dei reati contro le donne: è uno strumento per renderle più sicure tramite una rete di "guardiani" che può venire a conoscenza della loro posizione. Per l'installazione, richiede: (1) l'autorizzazione speciale per la lettura della lista dei contatti personali; (2) l'accesso alla posizione precisa (GPS e basata sulla rete) e alla posizione approssimativa dell'utente (basata sulla rete); (3) l'autorizzazione per l'invio di SMS, la modifica e lettura dei messaggi di testo personali (SMS o MMS); (4) la lettura del registro chiamate; (5) la possibilità di modificare o eliminare contenuti dell'archivio USB e svolgere un test dell'accesso all'archivio protetto e (6) l'accesso al microfono per registrare file audio. Inoltre, prevede: (7) l'acquisizione di informazioni sulla connessione *Wi-Fi* attualmente in uso, (8) la visualizzazione delle connessioni *Wi-Fi* a cui il dispositivo si può connettere e, in ultimo, (9) richiede la lettura dello stato e dell'identità del telefono. Le altre autorizzazioni richieste riguardano (10) la possibilità di visualizzazione delle connessioni di rete, (11) l'accesso di rete completo, (12) la disattivazione della funzione *stand-by* del dispositivo, (13) la chiusura di altre *app* nel momento in cui Fightback è in esecuzione, (14) il controllo della vibrazione e (15) l'esecuzione all'avvio, in modo che l'*app* rimanga in esecuzione in *background* da quando il *device* viene avviato.
L'utente si deve registrare al servizio per poter inviare degli *alert* georeferenziati con GPS, ossia messaggi di allarme contenenti le proprie coordinate, tramite SMS o email a cinque contatti di cui deve inserire le informazioni, oppure per vedere la propria posizione su di una mappa interattiva per orientarsi rispetto alla propria posizione. È possibile collegare all'applicazione anche il proprio *account Facebook*, in modo da poter rendere noto ai contatti la propria posizione. L'*app* può funzionare anche in *background*, in maniera tale da poter essere utilizzata nel momento del bisogno e non essere lanciata tramite l'inserimento delle proprie credenziali ogni volta.

Safe-U

Safe-U è un'applicazione coreana che consente di inserire in un'unica "cartella" i contatti dei servizi di emergenza (es. vigili del fuoco, guardia costiera, polizia, ospedali) e raggiungerli tramite semplici chiamate *in-app* o via SMS. Per l'installazione, questa applicazione richiede diverse autorizzazioni speciali: (1) l'accesso alla posizione approssimativa (basata sulla rete) ed alla posizione precisa dell'utente (GPS e basata sulla rete); (2) la possibilità di inviare SMS, (3) di operare un reindirizzamento delle chiamate in uscita, (4) di chiamare direttamente un numero di telefono, (5) di modificare o eliminare contenuti dell'archivio USB e di effettuare un test dell'accesso all'archivio protetto. In ultimo, (6) legge lo stato e l'identità del telefono. Rispetto alle altre categorie di autorizzazioni, richiede: (7) l'accesso di rete completo, (8) la visualizzazione delle connessioni di rete, (9) la lettura della configurazione del servizio *Google* e (10) la possibilità di effettuare una modifica delle impostazioni audio. La chiamata *in-app* è la possibilità per l'applicazione di attivare la funzione di chiamata del dispositivo, per telefonare ad un numero di telefono registrato al suo interno, senza che questo sia inserito nell'elenco contatti. L'utente può inserire i numeri di telefono dei servizi di emergenza negli appositi spazi ed i contatti telefonici di persone fidate, a cui, selezionando l'apposita funzione, possono essere inviati SMS contenenti il *link* per individuare l'utente su *Google Maps*, oppure scegliere di fare la chiamata diretta. In quest'ultimo caso, non ci sarà bisogno di comunicare all'operatore la propria posizione.

Alarm 112

Alarm 112 consente una chiamata *in-app* verso il numero unico europeo per le emergenze (112). Quest'*app* richiede: (1) l'accesso alla posizione approssimativa (basata sulla rete) ed alla posizione precisa dell'utente (GPS e basata sulla rete) e (2) l'accesso a comandi aggiuntivi del *provider* di localizzazione per quanto riguarda le autorizzazioni speciali; mentre le altre autorizzazioni richieste prevedono: (3) l'accesso di rete completo e (4) la visualizzazione delle connessioni di rete a cui il dispositivo si può collegare. L'utente attiva l'applicazione e può selezionare direttamente la funzione di chiamata georeferenziata. Viene così messo in

contatto con il *call center* europeo interforze. L'applicazione, inoltre, include un servizio di geolocalizzazione dell'utente per consentirgli di orientarsi rispetto alla sua posizione, tramite un servizio di mappe interattivo basato su *Google Maps*.

AlertCops

AlertCops è un'*app* creata con la supervisione del Ministero dell'Interno spagnolo, attiva nelle città di Madrid, Alicante e Malaga. L'applicazione per essere installata richiede: (1) l'accesso alla posizione precisa (GPS e basata sulla rete) dell'utente; (2) la possibilità di ricezione e invio di messaggi di testo (SMS); l'autorizzazione (3) per effettuare chiamate dirette al numero di telefono della polizia spagnola, (4) per effettuare un test dell'accesso all'archivio protetto e (5) per leggere stato ed identità del telefono. Le autorizzazioni aggiuntive prevedono la (6) visualizzazione delle connessioni di rete e (7) l'accesso di rete completo.
Al primo avvio dell'applicazione, l'utente deve registrarsi al servizio con nome, cognome, numero di telefono e identificativo di un documento ed attendere un SMS di conferma contenente un codice per la sua attivazione. Dopo l'attivazione, appare la schermata principale dello strumento, che consente di inviare *alert* geolocalizzati rispetto a diverse categorie di reato e atti di devianza, ossia: furto, rapina, violenza sessuale, vandalismi, risse, aggressioni, atti di bullismo e la possibilità di segnalare la scomparsa o il ritrovamento di una persona, inserendo diverse informazioni utili per l'intervento della polizia, raggiungibile anche tramite una chiamata *in-app*. L'applicazione funziona, inoltre,come punto di raccolta delle notizie utili per un'assistenza immediata nelle situazioni di emergenza: è possibile anche inserire il proprio indirizzo, il gruppo sanguigno ed eventuali altre problematiche mediche dell'utente.

Safe Neighborhood

Safe Neighborhood è un'applicazione che mostra i luoghi di residenza (tramite il servizio *Google Maps*) degli autori di reati sessuali condannati negli Stati Uniti ed inseriti nel *National Sex Offender Registry*. L'applicazione richiede l'autorizzazione speciale per avere accesso: (1) alla posizione approssimativa (basata sulla rete) ed alla posizione precisa (GPS e basata sulla rete) dell'utente; (2) alla modifica ed eliminazione di contenuti dell'archivio USB e (3) ad effettuare un test dell'accesso all'archivio protetto, oltre che (4) a leggere lo stato e l'identità del telefono. Le autorizzazioni aggiuntive sono previste per (5) l'accesso di rete completo, (6) la visualizzazione delle connessioni di rete e (7) la lettura della configurazione del servizio *Google*.
L'applicazione consente la ricerca degli autori di reati sessuali tramite l'inserimento di una via, di un indirizzo completo, selezionando una zona o tramite la posizione attuale dell'utente ricavata tramite GPS e rete Internet. Selezionando uno dei 100 autori che per ogni ricerca vengono visualizzati, si possono ottenere le informazioni anagrafiche di ognuno di essi, il reato per il quale sono stati condannati e la foto, oltre alla distanza della loro residenza dal luogo in cui si trova l'utente.

Mobile Tracker

Mobile Tracker è un'*app* sviluppata da privati, pensata per dare all'utente una sensazione di sicurezza tramite la creazione di una rete di contatti, che può venire a conoscenza della sua posizione. Per la sua installazione richiede: (1) l'autorizzazione speciale per la lettura dei contatti personali; (2) di individuare la posizione precisa (GPS e basata sulla rete) e la posizione approssimativa dell'utente (basata sulla rete); (3) la possibilità di inviare e ricevere SMS, (4) di leggere il registro chiamate, (5) di ottenere informazioni sulla connessione *Wi-Fi*, (6) di visualizzare le connessioni *Wi-Fi* disponibili ed, in ultimo, (7) di leggere lo stato e l'identità telefono. Le autorizzazioni aggiuntive richieste riguardano: (8) la disattivazione della funzione *stand-by* del dispositivo; (9) l'accesso di rete completo; (10) la possibilità di esecuzione dell'applicazione all'avvio del dispositivo e (11) la visualizzazione delle connessioni di rete.
Dopo l'installazione, l'utente deve registrarsi al servizio con un *username* ed una *password* personali per ricevere la conferma dell'attivazione al proprio indirizzo email ed accedere così alle funzionalità dell'applicazione. In questo modo, è possibile per l'utente inviare automaticamente un messaggio SMS o email contenente un *link* georeferenziato della propria posizione in un'ora prestabilita o ad intervalli ripetuti ad una lista di contatti ("guardiani") che devono essere inseriti. L'utente o i contatti possono ricevere via SMS la posizione del dispositivo inviando al numero di telefono dell'utente un SMS con una specifica "parola chiave" (di *default* è la sigla "*zentrack*", che può essere modificata a piacimento dall'utente, che deve comunicarla in questo caso anche ai propri contatti). È, inoltre, possibile inviare un SMS o email di allarme scuotendo il *device* con una certa intensità. L'applicazione funziona anche in mancanza di copertura di una rete *Internet Wi-Fi*, 3G o 4G, utilizzando il GPS e *Google Maps*.

bSafe - Personal Safety App

bSafe è una delle *app* per la sicurezza personale che crea una rete *social* di "guardiani". Per le sue caratteristiche, richiede l'accettazione di numerose autorizzazioni speciali: è prevista la possibilità (1) di acquisti *in-app*, (2) di individuare quale *account* viene utilizzato sul dispositivo, (3) di leggere la lista dei contatti personali, (4) di accedere alla posizione approssimativa (basata sulla rete) ed alla posizione precisa dell'utente

(GPS e basata sulla rete), (5) di inviare SMS, (6) di effettuare una chiamata diretta ai numeri di telefono dei "guardiani" inseriti dall'utente nell'applicazione, (7) di leggere il registro chiamate, (8) di re-indirizzare le chiamate in uscita, (9) di modificare il registro chiamate, (10) di modificare o eliminare i contenuti dell'archivio USB, (11) di svolgere un test dell'accesso all'archivio protetto, (12) di acquisire foto e video, (13) di registrare file audio, (14) di visualizzare le connessioni *Wi-Fi* che circondano l'utente e (15) di leggere stato e identità del telefono. Le altre autorizzazioni richieste riguardano (16) la ricezione di dati da Internet, (17) l'accesso di rete completo, (18) la visualizzazione delle connessioni di rete, (19) la connessione e disconnessione dalle reti *Wi-Fi*, (20) l'aggiunta di scorciatoie per attivare l'*app* in maniera più immediata, (21) la disattivazione della funzione *stand-by* del dispositivo e (22) della funzione di blocco schermo, (23) lo spostamento sopra altre *app*, (24) la lettura della configurazione del servizio *Google*, (25) il controllo della vibrazione, (26) la possibilità di esecuzione all'avvio del dispositivo e (27) la modifica della connettività di rete.
L'*app* ha lo scopo di costruire una rete "*social*" per la sicurezza e si basa su un sistema di mappe che mostrano la posizione dell'utente e su richiesta anche il percorso degli altri contatti "amici" in tempo reale, tramite il sistema GPS. Per accedere al servizio, l'utente deve registrarsi e scegliere un contatto primario, che in caso di selezione della funzione *"Alert"* riceverà un SMS o una -mail contenente il *link* georeferenziato con la posizione dell'utente e una registrazione audio-video di qualche secondo. Inoltre, verrà automaticamente chiamato. In secondo luogo, può scegliere altri contatti (che in caso della selezione della funzione *"Alert"*riceveranno solo l'SMS) da inserire come "amici" nella propria "rete di sicurezza". Una seconda funzione dell'applicazione è l'impostazione di un *timer* che avvisi i membri della rete se entro una data ora l'utente non ha raggiunto uno specifico punto precedentemente inserito (es. il luogo di residenza). Se, alla scadenza del conto alla rovescia l'utente non ha ancora raggiunto il punto inserito, l'applicazione invia un SMS per comunicare la sua posizione (senza lanciare un allarme).
È prevista anche la funzione "*fake call*", ossia la funzione che consente di far suonare il telefono come se si stesse ricevendo una telefonata da un contatto inserito in rubrica e scelto dall'utente. In questo modo, la falsa chiamata crea l'occasione per l'utente di allontanarsi da una situazione spiacevole quando lo desidera. Una terza funzione dell'*app* consente di comunicare semplicemente la propria posizione ai membri della rete di contatti, selezionando dalla schermata principale l'icona della puntina di posizionamento. In ultimo, lo strumento consente di "farsi accompagnare a casa", ossia permette, selezionando l'apposita icona, di mostrare sui dispositivi dei membri della rete di contatti la traccia GPS *live* dell'utente, in modo che essi abbiano sempre sott'occhio la sua posizione e il suo percorso. In Italia, esiste una versione attiva di quest'applicazione con una rete sufficientemente estesa di utenti connessi.

Crime Maps

Crime Maps ha lo scopo di informare gli utenti sui livelli di criminalità e degrado nelle zone urbane in Portogallo. Per la sua installazione, vengono richieste delle autorizzazioni speciali: *l'app* richiede (1) di individuare quale *account* viene utilizzato sul dispositivo, (2) l'autorizzazione per l'accesso alla posizione approssimativa (basata sulla rete) ed (3) alla posizione precisa dell'utente (GPS e basata sulla rete), (4) di modificare o eliminare contenuti dell'archivio USB e (5) di effettuare un test dell'accesso all'archivio protetto. Le altre autorizzazioni riguardano invece: (6) la ricezione di dati da Internet, (7) l'accesso di rete completo, (8) la visualizzazione delle connessioni di rete a cui si connette il *device*, (9) la lettura della configurazione del servizio *Google* ed, in ultimo, (10) la disattivazione della funzione *stand-by* del dispositivo.
Crime Maps crea una rete sociale tra gli utenti che usufruiscono del servizio dopo essersi registrati tramite l'inserimento del proprio nome, un nome utente, l'indirizzo email, che servirà anche per l'attivazione del servizio, una *password*, oppure tramite la connessione dell'applicazione a *Facebook*. Dopo la registrazione, gli utenti hanno la possibilità di inserire *report* georeferenziati su reati (aggressioni, furti di veicoli, violenze, molestie sessuali, omicidi, ecc.), atti di devianza (vandalismi, presenza di tossicodipendenti o spacciatori, parcheggiatori abusivi, ecc.) o situazioni di degrado (presenza di sporcizia lungo le strade o rifiuti, presenza di luoghi pericolosi, ecc.), di cui siano stati testimoni o vittime o di cui siano venuti a conoscenza, scegliendo l'icona corrispondente al tipo di comportamento o situazione di cui si vuole comunicare, inserendo data e ora approssimativi dell'evento e una sua breve descrizione. È possibile anche ottenere informazioni rispetto agli eventi segnalati dagli altri utenti, commentarli e mettere un *"like"* all'evento, e la lista delle ultime notizie inserite nel sistema. In ultimo, l'applicazione mostra l'ubicazione delle stazioni di polizia.

MobilePatrol Public Safety App

MobilePatrol Public Safety App copre tutto il territorio degli Stati Uniti ed è pensata come strumento di comunicazione tra cittadini e forze dell'ordine. Il suo scopo è fornire informazioni su situazioni di emergenza e attività delle forze dell'ordine in tempo reale. Richiede numerose autorizzazioni. Quelle speciali riguardano: (1) l'individuazione dell'*account* in uso sul dispositivo; (2) l'accesso alla posizione precisa (GPS e basata

sulla rete) ed alla posizione approssimativa dell'utente (basata sulla rete); (3) l'invio di SMS; (4) la chiamata diretta ai numeri di telefono dei servizi per l'emergenza; (5) la modifica o l'eliminazione dei contenuti dell'archivio USB; (6) l'autorizzazione ad effettuare un test dell'accesso all'archivio protetto; (7) la visualizzazione delle connessioni *Wi-Fi* presenti e (8) la lettura dello stato e dell'identità del telefono. Le altre autorizzazioni richieste riguardano: (9) la ricezione di dati da Internet; (10) la lettura della configurazione del servizio *Google*; (11) l'accesso di rete completo; (12) la disattivazione della funzione *stand-by* del dispositivo; (13) la visualizzazione delle connessioni di rete a cui il dispositivo si può agganciare; (14) l'eliminazione di tutti i dati della *cache* delle altre applicazioni; (15) l'utilizzo dell'*account* sul dispositivo ed (16) il controllo della funzione di vibrazione.
Le forze dell'ordine devono registrarsi al sistema per poter attivare il servizio nel proprio distretto e renderlo disponibile ai cittadini. L'utente deve registrarsi al servizio inserendo la propria email ed una *password* personale, il sesso, l'età ed eventualmente la propria qualifica di membro di agenzie di sicurezza, oppure può accedere tramite *Facebook*. L'utente, registrato o meno, ha la possibilità di ricevere informazioni aggiornate da parte delle agenzie della sicurezza su eventi che si sono realizzati in luoghi scelti dall'utente, inviare *report* con foto e video su reati, sulla situazione del traffico o sui segnali di degrado, anche anonimamente. Le ulteriori funzioni dello strumento sono l'accesso alle informazioni pubbliche sui detenuti, alle liste di ricercati e di autori di reati sessuali ed ai mandati di arresto, oltre che accedere alla lista di persone scomparse nella propria area.

Cuadrante Amigo

Cuadrante Amigo è un'*app* sviluppata con il supporto della polizia nazionale colombiana che contiene informazioni e dati relativi a circa 3.000 tra città e paesi della Colombia. Si tratta di uno strumento che mostra l'ubicazione delle stazioni di polizia e la possibilità di svolgere chiamate *in-app* verso di esse. Per l'installazione, richiede come autorizzazioni speciali: (1) l'accesso alla posizione approssimativa (basata sulla rete) ed alla posizione precisa dell'utente (GPS e basata sulla rete); la possibilità (2) di effettuare chiamate dirette ai numeri di telefono presenti nell'applicazione, (3) di modificare o eliminare contenuti dall'archivio USB e (4) di svolgere un test dell'accesso all'archivio protetto. Le altre autorizzazioni richieste sono: (5) l'accesso di rete completo; (6) la visualizzazione delle connessioni di rete a cui si può connettere il dispositivo; (7) la lettura della configurazione del servizio *Google*; (8) la disattivazione della funzione *stand-by* del dispositivo ed (9) il controllo della vibrazione. Lo strumento offre la possibilità di svolgere chiamate *in-app* verso la stazione di polizia assegnata al quadrante più vicino all'utente: si tratta della zona cittadina dove è stato rafforzato il pattugliamento e che viene controllata maggiormente allo scopo di studiare il crimine, le sue cause e rafforzare i legami con la comunità. La posizione dell'utente e delle stazioni di polizia più vicine è presentata grazie all'ausilio di mappe interattive. Tramite GPS, è possibile calcolare il percorso che distanzia l'utente dalla stazione di polizia più vicina e raggiungerla, anche senza la connessione ad *Internet* attiva sul dispositivo.

Classificare le applicazioni mobili per la sicurezza urbana

Dopo una breve descrizione del contenuto di alcune applicazioni sviluppate in tema di sicurezza urbana a livello mondiale,in questo paragrafo si analizzerà nel dettaglio il contenuto di tali *app* cercando di comprendere se queste possano avere dei caratteri comuni. Risulta evidente come vi siano delle criticità negli strumenti analizzati: buona parte di essi acquisisce informazioni sulla posizione dell'utente, alcuni richiedono una registrazione, altri ancora per essere funzionali devono essere installati da più persone. I dati inseriti dagli utenti, compresi quelli che vengono contenuti nelle "denunce" alle autorità di polizia, sono informazioni molto sensibili[3], che nelle mani sbagliate potrebbero causare gravi danni. Gli utenti non sempre sono consapevoli del tipo di dati che vengono raccolti, aumentando il rischio di un monitoraggio digitale permanente. Guardando alle caratteristiche sopra-descritte, le applicazioni per la sicurezza urbana selezionate possono essere classificate nel modo seguente:

[3] In questa parte, si farà riferimento al concetto comunemente accettato di "informazione sensibile". In seguito, il concetto di "dato sensibile" verrà specificato ed utilizzato secondo il significato che esso ha nell'ambito dei diversi strumenti normativi sovranazionali. Alcune di queste categorie di informazioni che possono avere un impatto significativo sulla vita privata degli utenti e degli altri cittadini sono presenti nella lista fornita nell'articolo 29 del Data Protection Working Party, Opinion 02/2013 on apps on smart devices (2013).

- *Applicazioni informative*: sono le *app* che richiedono un livello di interazione dell'utente molto basso. Costui si limita ad interagire con lo strumento interrogando il sistema affinché gli fornisca indicazioni in merito ai reati/atti devianti che sono avvenuti in uno specifico luogo (es. come nel caso di *Crime Spy UK* o *Berlin Police Crime Watch Kiez*) ed il sistema fornisce elenchi o mostra un punto o in generale gli elementi richiesti su di una mappa. Sono le applicazioni che meno causano rischi per quanto riguarda la tutela di dati personali e la riservatezza, se non per quanto riguarda la (eventuale) geolocalizzazione dell'utente.
- *Applicazioni di denuncia*: si tratta di *app* che richiedono un livello di interazione dell'utente molto alto. Costui non solo troverà nello strumento informazioni sulle attività delle forze dell'ordine o su eventi che si svolgono nelle vicinanze (es. come nel caso di *Crime Watch* o *City of Cape Coral*), ma avrà anche la possibilità di segnalare alle autorità o ai membri del *social network* di cui l'utente fa parte la presenza di segni di degrado urbano o la commissione di reati o atti devianti sul territorio. Solitamente, queste applicazioni richiedono una registrazione per poter accedere al servizio, utilizzano la georeferenziazione e raccolgono diversi tipi di informazioni (es. commenti, file audio o video). Per quanto riguarda i rischi per la tutela di riservatezza e dati personali, si tratta indubbiamente di strumenti cui prestare particolare attenzione.
- *Applicazioni di "auto-aiuto"*: creano dei *social network* "privati" solo tra gli utenti che si registrano al servizio e consentono un controllo reciproco tra gli stessi, oppure inviano *alert* ai membri della lista dei "guardiani" (es. familiari o amici) su richiesta dell'utente. Richiedono un'iscrizione, registrano la posizione dell'utente, i suoi percorsi, le comunicazioni con i membri della rete di contatti (es. come *Mobile Tracker* o *Crime Check*) e i loro dati. Sono da tenere sotto stretto controllo per quanto riguarda la tutela dei dati inseriti.

È possibile suddividere le applicazioni descritte nel paragrafo precedente nelle tre diverse categorie individuate per catalogare le *app* (Tab. 3).

In secondo luogo, guardando, invece, al "percorso" svolto dalle informazioni inserite dagli utenti, o che le applicazioni richiedono di processare, possiamo suddividere le *app* per la sicurezza urbana in due grandi categorie: (1) applicazioni che inviano dati alle autorità pubbliche (intese come amministrazioni comunali, ospedali, forze dell'ordine, vigili del fuoco, ecc.) ed (2) applicazioni che inviano dati ad aziende private di sviluppatori che effettuano poi il servizio di interazione con l'utente (Tab. 4). Il simbolo "x" rappresenta un segno affermativo.

Come è possibile comprendere dalla Tabella 4, rispetto all'insieme di applicazioni che si sono prese in considerazione, la maggior parte di esse invia i dati degli utenti a sviluppatori privati (12 applicazioni su 18), mentre per la restante parte i dati vengono messi a disposizione della pubblica amministrazione (in questo caso, comprensiva dei servizi di emergenza). Solo *Crime Spy UK* non acquisisce informazioni dall'utente. Le applicazioni informative (a parte *Crime Spy UK*), che in base alla prima classificazione effettuata (Tab. 3) dovrebbero essere quelle meno problematiche per quanto riguarda la tutela dei dati personali degli utenti e della loro riservatezza, forniscono agli sviluppatori privati una serie di informazioni (soprattutto la geolocalizzazione dell'utente), che sono necessarie al funzionamento del servizio e contemporaneamente sono invasive della *privacy* dell'utente stesso (es. attraverso l'autorizzazione ad effettuare modifiche o eliminare contenuti dell'archivio USB comporta l'accesso alla memoria del dispositivo).

Tabella 3 – La classificazione delle applicazioni per la sicurezza urbana secondo la tipologia

Applicazioni informative	**Applicazioni di denuncia**	**Applicazioni di "auto-aiuto"**
Crime Spy UK	Crime Check	みまもり防犯ブザ (Tracking Crime Buzzer)
Berlin Police Crime Watch Kiez	City of Cape Coral	Fightback
Crime Watch, Crime Rates Stats	Alarm 112	Safe-U
Crime HotSpot – UK	AlertCops	Mobile Tracker
Crime Watch	Crime Maps	bSafe - Personal Safety App
Safe Neighborhood	MobilePatrol Public Safety App	
	Cuadrante Amigo	

Fonte: elaborazione degli autori

Tabella 4 - La classificazione delle applicazioni per la sicurezza urbana secondo i destinatari (pubblici o privati) dei dati inseriti dagli utenti

Nome dell'applicazione	Invio di dati ad autorità pubbliche	Invio di dati a soggetti privati
Crime Spy UK	-	
Berlin Police Crime Watch Kiez		X
Crime Watch, Crime Rates Stats		X
Crime HotSpot – UK		X
Safe Neighborhood		X
Crime Check		X
City of Cape Coral	X	
Alarm 112	X	
AlertCops	X	
Crime Maps		X
MobilePatrol Public Safety App	X	
Cuadrante Amigo		X
みまもり防犯ブザ (Tracking Crime Buzzer)	X	
Fightback		X
Safe-U	X	
Mobile Tracker		X
bSafe - Personal Safety App		X
Crime Watch		X

Fonte: elaborazione degli autori

Rimangono molto rischiose, per quanto riguarda il tema della tutela dei dati personali e della riservatezza, le applicazioni pensate come strumenti di "auto-aiuto" e di denuncia, che consentono all'utente di inserire informazioni sensibili non strettamente necessarie alla fruizione del servizio: ad esempio, *AlertCops* consente di inserire dati utili per ottenere un'assistenza medica mirata in caso di emergenza; ma le informazioni personali idonee a rivelare lo stato di salute godono, almeno nella disciplina europea, di una tutela rafforzata in quanto parte della categoria dei dati sensibili. La loro raccolta tramite un'*app* che ha uno scopo diverso dal trattamento di dati in ambito medico potrebbe comportare dei rischi ingenti, soprattutto per quanto riguarda le attività di *storage* dei dati, di adozione di misure di sicurezza e di cessione degli stessi dati a terzi.

In ragione di questi ed altri rischi che la raccolta di informazioni personali da parte delle applicazioni per la sicurezza urbana può creare, nel capitolo successivo sarà svolta una valutazione della *compliance* delle applicazioni esistenti in materia di sicurezza urbana classificate in relazione alla normativa sovranazionale vigente sulla tutela dei dati personali e della riservatezza. L'obiettivo è di individuare degli "indicatori normativi" che possano permettere una valutazione di tali *app* e di indirizzare le *policy* delle pubbliche amministrazioni e dei servizi dell'emergenza (es. forze di polizia), per evitare non solo la violazione della legislazione stessa, ma anche di fornire un facilitatore per la commissione di reati (quali il furto d'identità), atti discriminatori o attività di profilazione illecita dei cittadini. In terzo luogo, siffatta valutazione risulta utile per individuare le migliori strategie per gli sviluppatori, affinché questi nel trattamento dei dati degli utenti e nella concessione del servizio non infrangano la normativa di riferimento e possano sviluppare strumenti sicuri per gli utenti, in modo da poter considerare le misure di sicurezza dei dati e del processo di sviluppo come "fattore aggiunto", che valorizzi i loro prodotti.

03

Le applicazioni mobili per la sicurezza urbana e la protezione della privacy e dei dati personali

L'obiettivo di questo capitolo è di valutare se e come le applicazioni *mobile* per la sicurezza urbana, esistenti sul mercato, siano conformi ai dettami della normativa attualmente in vigore a livello sovranazionale sulla *privacy* e la protezione dei dati personali, ovvero se siano *privacy-compliant*. Nella prima parte di questo rapporto di ricerca, è stato possibile svolgere un'esplorazione nel "mondo" delle applicazioni in tema di sicurezza urbana, individuando un gruppo di *app* in base al numero di installazioni effettuate dagli utenti, successivamente classificate in base alle loro funzioni principali: (a) informare l'utente rispetto al degrado urbano o ai reati compiuti in una zona (applicazioni informative); (b) consentire l'invio di segnalazioni ai diversi *stakeholders* (ad esempio, la polizia) (applicazioni di denuncia); (c) rassicurare gli utenti, creando una rete di "guardiani" (es. parenti e amici) da contattare in caso di emergenza (applicazioni di "auto-aiuto"). La valutazione circa la *compliance* di queste *app mobile* rispetto alla legislazione internazionale ed europea vigente sarà effettuata seguendo questi *step*:

1. saranno in primo luogo identificati degli "indicatori normativi", scelti sulla base delle disposizioni rilevanti in vigore sulla *privacy* e la protezione dei dati personali a livello internazionale ed europeo, tramite i quali poi sarà possibile svolgere la valutazione delle *app* per la sicurezza urbana selezionate;

2. verrà svolta la fase di valutazione, in base agli "indicatori normativi" individuati, e saranno presentate delle conclusioni specifiche per ogni gruppo di applicazioni in materia di sicurezza urbana: (a) applicazioni informative; (b) applicazioni di denuncia; (c) applicazioni di "auto-aiuto";

3. saranno illustrati i risultati della valutazione effettuata anche alla luce: (a) della Proposta di Regolamento Europeo ("COM(2012) 11 final"), presentata dalla Commissione Europea nel 2012, sulla quale si dovrebbe raggiungere un accordo nelle sedi europee entro la fine del 2015; (b) della dottrina in materia di profilazione e di raccolta di *big data* da parte di enti pubblici e privati.

Valutare la compliance delle applicazioni mobili per la sicurezza urbana

Al fine di effettuare una valutazione della *compliance* delle applicazioni in materia di sicurezza urbana, descritte nel capitolo precedente, si terrà in conto delle Convenzioni internazionali in vigore direttamente vincolanti per gli Stati firmatari in tema di *privacy* e protezione dei dati personali, dal momento che le *app* analizzate possono essere utilizzate a livello globale. Gli indicatori per la valutazione di conformità delle applicazioni selezionate al quadro giuridico di riferimento sono, pertanto, identificati principalmente in base ai tre strumenti internazionali direttamente vincolanti, attualmente vigenti per il maggior numero di Paesi su scala mondiale, ossia: il *Patto per i diritti civili e politici* (1966), la *Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali - CEDU* (1950) e la *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale*, *n. 108* (1981), nel seguito anche *Convenzione di Strasburgo*.

Per la selezione degli indicatori, si è tenuto conto anche della normativa europea, attualmente applicata in materia negli Stati Membri, ossia: la *Direttiva 95/46/CE sul trattamento dei dati personali e della libera circolazione dei dati*, la *Direttiva 2002/58/CE sul trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche* (Direttiva *ePrivacy*) e la *Carta dei diritti fondamentali dell'Unione europea* (2000). In questa prima parte della valutazione, invece, non viene preso in considerazione il Regolamento sulla protezione dei dati personali e la Direttiva dell'Unione europea sulla protezione dei dati personali nelle attività di polizia (cd. "Pacchetto protezione dati"), i cui testi definitivi stanno per essere approvati dalle istituzioni europee (Cfr. Proposta di Regolamento "COM(2012) 11 final" del 25 gennaio 2012; Commissione europea, 2015).

Con riferimento ai concetti cardine desumibili da questo quadro normativo sovranazionale, il trattamento dei dati deve essere svolto nel rispetto dei principi di qualità, liceità, finalità e correttezza, ovvero i dati: (1)

devono essere ottenuti ed elaborati lealmente e legalmente; (2) devono essere registrati per fini determinati e legittimi; (3) non devono essere utilizzati in modo diverso rispetto ai fini determinati; (4) devono essere adeguati, pertinenti e non eccessivi in rapporto a quei fini; (5) devono essere esatti e, se necessario, aggiornati; (6) devono essere conservati in modo tale da poter identificare le persone interessate per il periodo strettamente necessario al trattamento (Consiglio d'Europa, 2011; 2014). Il principio di liceità del trattamento si desume dalla *CEDU*, articolo 5, lettere a) e b) e dalla *Direttiva sulla protezione dei dati personali*, articolo 6, comma 1, lettere a) e b). Il principio di finalità del trattamento, invece, è inquadrato nell'articolo 5, lettera b) della *Convenzione n.108* e nell'articolo 6, lettera b) della Direttiva summenzionata. Il principio di correttezza è esplicitato all'articolo 5, lettera a) della *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale* e all'articolo 6, comma 1, lettera a). In ultimo, l'articolo 5, lettere c), d) ed e) della Convenzione e l'articolo 6, lettere c), d), ed e) della Direttiva concretano il principio di qualità dei dati.

Il trattamento dei dati sensibili può essere svolto solo se vi sia: (1) il consenso espresso (e specifico, quindi disgiunto dal consenso generale per il trattamento) dell'interessato; (2) una legge che preveda una deroga al divieto di trattamento dei dati sensibili, per assolvere obblighi e diritti del responsabile del trattamento in materia di diritto del lavoro; (3) una legge che preveda una deroga al divieto di trattamento a scopo sanitario, ossia per salvaguardare un interesse vitale della persona interessata o di un terzo. La disciplina sulla liceità del trattamento dei dati sensibili è contenuta nell'articolo 6 della *Convenzione di Strasburgo* e nell'articolo 8 della *Direttiva sulla protezione dei dati personali*. Si prevedono, in capo all'interessato, una serie di diritti che egli può esercitare nei confronti del titolare dei dati, il primo dei quali è (1) il diritto ad ottenere l'informativa preventiva di trattamento, nella quale deve essere presente l'indicazione: (a) del titolare dei dati (o del responsabile di trattamento); (b) sulla natura del trattamento; (c) dello scopo per il quale i dati sono raccolti; (d) dei destinatari o categorie di destinatari dei dati; (e) in merito all'obbligatorietà o meno della risposta alle domande e le conseguenze delle sue scelte; (f) dei diritti di cui l'interessato è titolare. L'interessato, inoltre, può esercitare: (2) il diritto di accesso ai dati, funzionale all'esercizio del (3) diritto di chiedere la rettifica dei dati, se inesatti, e del (4) diritto di chiedere la cancellazione dei dati che lo riguardano. I diritti dell'interessato vengono concretizzati nuovamente dall'articolo 8 della *Convenzione n.108 del Consiglio d'Europa* e dagli articoli 12 e 14 della *Direttiva sulla tutela dei dati* (Consiglio d'Europa, 2011; 2014).

Il principio fondante il trattamento automatizzato dei dati, individuato sulla base dell'innovazione realizzata dall'Unione europea a riguardo, è il consenso informato: i dati dell'individuo possono essere acquisiti e trattati solo ove egli abbia ricevuto un'informativa dettagliata, sia conscio dei suoi diritti ed espressamente acconsenta al trattamento dei dati. Il trattamento può essere svolto senza il consenso dell'interessato quando esso: (1) sia necessario per l'adempimento di un contratto a suo favore o per l'esecuzione di obbligazioni precontrattuali; (2) nell'interesse del responsabile del trattamento o di terzi; (3) per superiori interessi pubblici; (4) per obbligo di legge e nel caso in cui (5) vi sia necessità di salvaguardare i diritti dell'interessato. La definizione ed i requisiti per un valido consenso sono individuati dalla *Direttiva sulla protezione dei dati*, alla lettera h) dell'articolo 2 (Consiglio d'Europa, 2011; 2014). Sulla base di questa premessa, è possibile definire degli "indicatori normativi" utili alla valutazione delle *app* in materia di sicurezza urbana selezionate, desumibili dal quadro giuridico internazionale ed europeo attualmente in vigore sopra-descritto:

Indicatore (1) - Principio di qualità dei dati

Il trattamento dei dati deve rispondere al principio di qualità, che ricomprende nello specifico:

- Principio di pertinenza dei dati: i dati possono essere trattati solo nel caso in cui essi siano adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;

- Principio di esattezza dei dati: i dati possono essere trattati solo ove esatti. In caso di inesattezza, devono essere aggiornati;

- Principio della necessità: i dati devono essere conservati in modo da consentire l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati e/o sono successivamente trattati.

Indicatore (2) - Principio di finalità del trattamento

La finalità del trattamento deve essere specificata e resa manifesta dal titolare del trattamento prima che il trattamento abbia inizio.

Indicatore (3) - Principio di correttezza del trattamento

I dati devono essere trattati garantendo la liceità e la correttezza del trattamento, tanto durante la raccolta quanto durante l'elaborazione vera e propria. Il trattamento è lecito quando è conforme alla legge, mentre è corretto quando la raccolta avviene senza ricorso ad artifizi e raggiri.

Indicatore (4) - Principio di trasparenza

Il titolare del trattamento ha l'obbligo di mantenere informati gli interessati sulle modalità di utilizzo dei loro dati.

Indicatore (5) - Divieto di trattamento dei dati sensibili.

I dati sensibili possono essere sottoposti a trattamento solo se ciò sia previsto in una legge allo scopo di assolvere obblighi e diritti del responsabile del trattamento in materia di diritto del lavoro o a scopi sanitari, ossia per salvaguardare un interesse vitale della persona interessata o di un terzo.

Indicatore (6) - Diritti dell'interessato

Tra i diritti dell'interessato, vi è il diritto ad essere informato sulla natura del trattamento, sul titolare del trattamento e lo scopo per il quale i dati sono acquisiti, sui destinatari o le categorie di destinatari dei dati, sulla obbligatorietà o meno della risposta alle domande che vengono poste, sulle conseguenze della mancata risposta e sui propri diritti.

Indicatore (7) - Consenso

Il consenso dell'interessato deve essere esplicito, specifico ed informato. Esso è previsto per il trattamento di tutte le categorie di dati. Non è necessario per l'adempimento di un contratto a favore dell'interessato, per l'esecuzione di obbligazioni precontrattuali, nell'interesse del responsabile del trattamento o di terzi, per superiori interessi pubblici, per obbligo di legge e nel caso in cui vi sia necessità di salvaguardare i diritti dell'interessato.

Con riferimento al principio del consenso, si approfondirà la specificità del consenso fornito dall'interessato nel contesto delle applicazioni *mobile*, così come illustrato dal il *Gruppo di lavoro ex Articolo 29*, organo di cooperazione fra le autorità garanti della protezione dei dati nell'Unione europea: (1) esso è libero nel momento in cui è concesso all'utente di accettare o rifiutare il trattamento dei dati personali prima dell'installazione dell'*app*; (2) è informato nella misura in cui l'utente può scegliere di installare o meno l'*app* sulla base di informazioni sufficienti sul trattamento e sul tipo di dati su cui vengono svolte operazioni; (3) è specifico quando l'espressione di volontà è riferita al trattamento di una tipologia di dato o di insiemi limitati ed omogenei degli stessi (Article 29 Data Protection Working Party, 2013).

La valutazione di *privacy-compliance* delle *mobile apps* in materia di sicurezza urbana selezionate nel capitolo precedente si svolgerà utilizzando questi indicatori. Per semplificare l'analisi, la stessa verrà svolta prendendo in considerazione, di volta in volta, le *app* per la sicurezza urbana scelte e distinte nelle tre categorie: (a) le applicazioni informative, (b) le applicazioni di denuncia e (3) le applicazioni di "auto-aiuto".

Valutazione delle applicazioni informative

Le applicazioni per la sicurezza urbana informative sono applicazioni che forniscono all'utente indicazioni in merito ai reati o episodi di devianza che sono avvenuti in un luogo, mostrando i risultati della sua ricerca in forma di elenco o attraverso un punto su di una mappa. Queste *app* potrebbero apparire come le meno rischiose per i dati dell'utente. All'interno di questa categoria rientrano cinque applicazioni per la sicurezza urbana, tra quelle selezionate in questo lavoro: *Crime Spy UK*, *Berlin Police Crime Watch Kiez*, *Crime HotSpot – UK*, *Crime Watch* e *Safe Neighborhood*. Nella Tabella 5, la valutazione di *compliance* sui temi della *privacy* e la protezione dei dati personali di queste *app* è effettuata in relazione alla conformità o meno dell'applicazione rispetto agli indicatori normativi selezionati precedentemente. La conformità è identificata tramite il simbolo "x".

Indicatore (1) - Principio di qualità dei dati

Il principio di qualità dei dati prevede che essi siano raccolti solo ove pertinenti rispetto allo scopo dell'applicazione. Tutte le applicazioni informative per la sicurezza urbana rispettano il principio di qualità dei dati. Dubbi, a riguardo, potrebbero sorgere su *Safe Neighborhood*. Gli elementi che fanno sorgere perplessità, anche rispetto alle valutazioni svolte dal *Global Privacy Enforcement Network* (GPEN) nel 2014, sono (1) l'accesso all'archivio protetto e (2) la possibilità di svolgere operazioni su di esso. Tuttavia, la richiesta di queste autorizzazioni è spesso connessa con la necessità da parte dell'*app* di scaricare dati nella memoria del telefono utili per il suo funzionamento (e, di conseguenza, di modificarli ed eliminarli in caso di disinstallazione). Per questi motivi, la valutazione di conformità di questa *app* rispetto all'indicatore in oggetto rimane positiva. Anche un'altra applicazione ha fatto sorgere dubbi rispetto a queste due autorizzazioni, *Berlin Police Crime Watch Kiez*; in questo caso, l'accesso all'archivio protetto e la possibilità di svolgere operazioni è fondamentale per scaricare nella *cache* del dispositivo le mappe su cui si basa l'applicazione, in modo che non vi sia nuovamente necessità di connettersi a Internet per far funzionare l'*app*.

Indicatore (2) - Principio di finalità del trattamento

Il principio è rispettato nel momento in cui il titolare del trattamento rende manifesto all'utente lo scopo proprio della raccolta delle informazioni e il trattamento dei dati personali. Questo indicatore è strettamente legato al primo (principio di qualità dei dati), in ragione della definizione di quest'ultimo: il principio viene rispettato nel momento in cui i dati trattati sono pertinenti rispetto alle finalità di trattamento. Se dalla descrizione delle funzionalità dell'*app* fornite dallo sviluppatore è possibile evincere uno scopo sufficientemente preciso, sarà possibile affermare o meno il rispetto del principio di pertinenza. Gli sviluppatori delle *app* valutate secondo questo indicatore tendono ad illustrare la finalità del trattamento dei dati degli utenti in modo sufficientemente preciso: il fine delle applicazioni *mobile* informative è comunicare agli utenti la quantità/qualità degli atti devianti o dei reati che sono stati compiuti in una specifica zona.

Tabella 5 - Valutazione di privacy-compliance delle applicazioni informative

	Applicazioni informative				
Indicatori	**Safe Neighbor-hood**	**Crime Watch**	**Crime HotSpot – UK**	**Berlin Police Crime Watch Kiez**	**Crime Spy UK**
Principio di qualità dei dati	X	X	X	X	X
Principio di finalità del trattamento	X	X	X	X	X
Principio di correttezza del trattamento					X
Divieto di trattamento dei dati sensibili	X	X	X	X	X
Diritti dell'interessato					
Consenso					

Fonte: elaborazione degli autori

Indicatore (3) - Principio di correttezza del trattamento

Il principio di correttezza del trattamento prevede che il titolare del trattamento svolga la sua attività in modo corretto nei confronti degli interessati, mantenendoli informati sull'utilizzo dei loro dati. Tranne *Crime Spy UK*, tutte altre applicazioni (quattro *app* su cinque) non rispondono al principio di correttezza. Ciò significa che, dalla descrizione fornita, non si riesce ad individuare in modo chiaro quale utilizzo viene fatto dagli sviluppatori dei dati degli utenti. Le descrizioni delle *app* danno generalmente giustificazione di alcuni permessi (es. lettura dell'ID del dispositivo, accesso alla posizione dell'utente), ma non contengono indicazioni sulla *privacy-policy*. In seguito all'installazione, l'utente può trovare solo una giustificazione dei permessi richiesti. Ancor più grave è che nemmeno presso i siti degli sviluppatori la *privacy-policy* sia presente, oppure che ne sia illustrata una non riferita specificamente all'*app* in questione.

Indicatore (4) - Divieto di trattamento di dati sensibili

Il divieto si applica in generale a tutti i trattamenti automatizzati, a meno che: (a) non intervenga il consenso specifico dell'utente, (b) il trattamento sia previsto in una legge allo scopo di assolvere obblighi e diritti del responsabile del trattamento in materia di diritto del lavoro o a scopi sanitari. Le applicazioni informative per la sicurezza urbana non raccolgono nessuna tipologia di dato sensibile, ovvero informazioni riguardo l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute e la vita sessuale dell'individuo. Raccogliere informazioni di questo tipo, in aggiunta, sarebbe contrario alla finalità dichiarata del trattamento dei dati raccolti con l'*app*.

Indicatore (5) - Diritti dell'interessato

L'utente ha diritto ad ottenere l'informativa sulla natura del trattamento, sul titolare del trattamento, sugli eventuali altri destinatari dei dati, sullo scopo dello stesso e sulle modalità di esercizio dei diritti di cui è titolare. L'informativa deve essere fornita all'utente prima dell'inizio del trattamento o, al più tardi, nel momento in cui i suoi dati vengono ceduti a terzi.
Le applicazioni informative in merito alla sicurezza urbana, nel complesso, non rispettano i diritti dell'interessato poiché non forniscono un'informativa completa per quanto riguarda l'indicazione del titolare di trattamento, la natura dello stesso e l'identità degli eventuali destinatari dei dati. Il parere del Gruppo ex Articolo 29 della Direttiva 95/46 UE sottolinea anche che gli utenti dovrebbero essere informati sulle modalità di esercizio dei loro diritti, almeno sul ritiro del consenso al trattamento e la cancellazione dei dati che li riguardano. Da questo punto di vista, le applicazioni valutate non rispettano i diritti degli interessati, poiché non indicano in nessun modo come questi possano essere esercitati. Le applicazioni che sollevano le maggiori perplessità sono *Crime HotSpot – UK* e *Safe Neighborhood*. Della prima viene fornita descrizione della natura del trattamento dei dati, ma non si riesce ad individuare con sufficiente chiarezza l'identità del titolare del trattamento. Per *Safe Neighbourhood* risulta impossibile individuare il titolare del trattamento e non risulta chiaro l'utilizzo delle informazioni inviate dall'utente perché l'applicazione non è fornita di una *privacy policy*. Inoltre, le giustificazioni date dallo sviluppatore ai permessi richiesti per l'installazione non sono complete (essa è presentata per intero solo successivamente all'installazione, quando l'utente seleziona l'icona "informazioni"). Per tutti questi motivi, la valutazione generale circa la conformità delle applicazioni per la sicurezza urbana di tipo informativo in relazione a questo indicatore è negativa (Cfr. Article 29 Data Protection Working Party, 2013).

Indicatore (6) - Consenso

Il trattamento dei dati personali può essere svolto nel momento in cui vi sia il consenso esplicito, specifico ed informato degli utenti. In linea di principio, tutte le applicazioni che si valutano in questa sede richiedono il consenso dell'interessato per essere installate. Il consenso, sulla piattaforma *Google Play,* viene richiesto per ogni installazione, dando la possibilità all'utente, tramite una finestra *pop-up*, di ottenere informazioni sui tipi di permessi richiesti dall'*app* che sta installando. Seguendo le indicazioni fornite nel parere del 2013 del Gruppo Articolo 29, *Google Play* prevede la possibilità di annullare l'operazione di installazione, nel caso in cui l'utente non gradisca la quantità o il tipo di permessi di accesso richiesti. Gli utenti dovrebbero fornire un consenso granulare ai permessi delle *app*, ovvero poter scegliere di autorizzare il trattamento dei loro dati personali per un fine (es. l'individuazione della loro posizione), ma non per un altro (es. sapere che il programma sta accedendo alla memoria protetta del telefono). Per tutelarsi da queste intrusioni, gli utenti hanno inoltre l'opportunità di utilizzare le potenzialità del *device* (es. alcuni dispositivi consentono di gestire le autorizzazioni delle diverse applicazioni), oppure di installare appositi antivirus o programmi che consentano di bloccare l'accesso delle *app* a taluni sensori (FTC staff report, 2013). Dinnanzi alla distanza tra le prassi degli sviluppatori con riguardo all'informazione degli utenti e dell'impossibilità per talune applicazioni di individuare una *privacy-policy* e di comprendere con quali modalità esercitare i propri diritti, la valutazione di conformità in base questo indicatore è negativa.

Valutazione delle applicazioni di denuncia

Le applicazioni di denuncia nell'ambito sicurezza urbana sono *app* che forniscono all'utente informazioni sull'attività delle forze dell'ordine e su eventi di rilievo che accadono in città. In particolare, consentono di segnalare alle autorità o ai membri del *social network* di cui l'utente fa parte la presenza di segni di degrado in città o la commissione di reati o atti devianti nella zona in cui lo stesso si trova. Nel capitolo precedente si è affermato, ad una prima sommaria analisi, che le applicazioni di denuncia possono essere considerate abbastanza rischiose per la *privacy* degli utenti. All'interno di questa categoria, rientrano sette applicazioni tra quelle selezionate: *Crime Check*, *City of Cape Coral*, *Alarm 112*, *AlertCops*, *Crime Maps*, *MobilePatrol Public Safety App*, *Cuadrante Amigo*, *Crime Watch* e *Crime Rates Stats*. Nella Tabella 6, la valutazione di *compliance* sui temi della *privacy* e la protezione dei dati personali di queste *app* è realizzata in base alla conformità o meno dell'applicazione rispetto agli indicatori normativi selezionati in precedenza. La conformità è identificata attraverso il simbolo "x".

Indicatore (1) - Principio di qualità dei dati

Il principio di qualità dei dati prevede che essi siano raccolti solo ove pertinenti rispetto allo scopo dell'applicazione. Le applicazioni di denuncia, a questo riguardo, possono essere divise in due gruppi: (1) le *app* che raccolgono una quantità di dati proporzionata allo scopo che intendono raggiungere e (2) le applicazioni che raccolgono una quantità eccessiva di informazioni rispetto ad esso. In questo secondo gruppo si fanno rientrare *Crime Check*, *MobilePatrol Public Safety App*, *City of Cape Coral* e *AlertCops*. Il profilo di rischio di *MobilePatrol Public Safety App*, *City of Cape Coral* e *AlertCops* è legato alla richiesta di autorizzazione ad accedere allo stato del telefono. Se la lettura dell'ID del telefono può essere giustificata con la necessità di connessione alla rete e con il rispetto delle licenze *Google*, ci si chiede la necessità per le applicazioni, e quindi degli sviluppatori, di ricevere informazioni sullo stato del telefono. Questa autorizzazione è particolarmente invasiva, poiché consente all'applicazione di "sapere" se l'utente stia facendo una chiamata e di conoscere il numero relativo a una chiamata. Un ulteriore dubbio può sorgere, inoltre, su di un permesso richiesto da *Cuadrante Amigo*, ossia il controllo della vibrazione. Rispetto allo scopo dell'applicazione, ossia fornire informazioni sulla stazione di polizia più vicina all'interno del quadrante in cui si trova l'utente e svolgere chiamate dirette al numero di telefono della stazione di polizia o verso il cellulare di un'agente addetto a quel quadrante, non ha molto senso impedire l'attivazione della vibrazione sul dispositivo. La valutazione di *compliance* di quest'ultima *app* rispetto all'indicatore è stata negativa.

Tabella 6 - Valutazione di privacy-compliance delle applicazioni di denuncia

	Applicazioni di denuncia							
Indicatori	**Crime Check**	**City of Cape Coral**	**Alarm 112**	**AlertCops**	**Crime Maps**	**MobilePatrol Public Safety App**	**Cuadrante Amigo**	**Crime Watch, Crime Rates Stats**
Principio di qualità dei dati	X		X		X			X
Principio di finalità del trattamento	X	X	X	X	X	X	X	X
Principio di correttezza del trattamento				X		X	X	
Divieto di trattamento dei dati sensibili	X	X	X	X	X	X	X	X
Diritti dell'interessato				X		X	X	
Consenso							X	

Fonte: elaborazione degli autori

Indicatore (2) - Principio di finalità del trattamento

Il principio è rispettato nel momento in cui il titolare del trattamento rende manifesto all'utente uno scopo definito per la raccolta e il trattamento dei dati personali. Le applicazioni per la sicurezza urbana valutate rispondono al principio di finalità del trattamento: a differenza delle descrizioni fornite dalle *app* informative, quelle delle applicazioni di denuncia sono molto più dettagliate.

Indicatore (3) - Principio di correttezza del trattamento

Il principio di correttezza del trattamento prevede che il titolare del trattamento svolga la sua attività in modo corretto nei confronti degli interessati, mantenendoli informati sull'utilizzo dei loro dati. Solo tre applicazioni su otto sono fornite di *privacy-policy*. Si aggiunga che la *privacy-policy* di *Cuadrante Amigo* non è disponibile fino a dopo l'installazione dell'*app*. In merito a questo punto, neppure *Crime Check*, *Crime Watch* e *Crime Rates Stats* forniscono informazioni. Se si cerca di raggiungere il sito dello sviluppatore cliccando l'apposito *link*, questo non è contiene una pagina apposita. Lo stesso dicasi per *City of Cape Coral*, per la quale si rinvia al *link* di una pagina Internet dedicata ma lasciata in bianco. Se invece si cerca di raggiungere il sito dello sviluppatore di *Alarm 112*, ci si rende conto che il *link* non funziona. Nel caso poi di *Crime Maps*, si scopre che il *link* fornito rimanda alla pagina di un *social network* (*Facebook),* a cui si deve accedere con ulteriori credenziali, che non prevede una *privacy-policy*.

Indicatore (4) - Divieto di trattamento di dati sensibili

Il divieto si applica in generale a tutti i trattamenti automatizzati, a meno che: (1) non intervenga il consenso specifico dell'utente, (2) il trattamento sia previsto in una legge allo scopo di assolvere obblighi e diritti del responsabile del trattamento in materia di diritto del lavoro o a scopi sanitari, ossia per salvaguardare un interesse vitale della persona interessata o di un terzo. Nell'ambito delle applicazioni di denuncia, infatti, ve n'è una, ossia *AlertCops*, che consente all'utente di inserire notizie utili per ottenere un'assistenza immediata nelle situazioni di emergenza (es. indirizzo, gruppo sanguigno, eventuali altre problematiche mediche). Il divieto di trattamento dei dati sensibili cade nel momento in cui vi sia il consenso esplicito dell'utente al trattamento e nel caso in cui il trattamento dei dati sia necessario alla prevenzione ed alla diagnostica medica. Ci si potrebbe chiedere, però, se la modalità in cui viene acquisito il consenso dell'utente (ossia la decisione dell'utente di inserire i propri dati sensibili nell'apposito spazio dell'applicazione) possa essere considerata un vero e proprio consenso specifico. Si potrebbe discutere anche la rispondenza del trattamento di questi dati al principio di necessità. L'utente inserisce, più o meno consapevolmente, queste informazioni nell'*app* ed esse non dovrebbero essere trattate automaticamente, pena la violazione del divieto, se non nel momento in cui vi sia una reale necessità.

Indicatore (5) - Diritti dell'interessato

L'utente ha diritto ad ottenere l'informativa sulla natura del trattamento dei suoi dati, sul titolare del trattamento, sugli eventuali altri destinatari dei dati, sullo scopo dello stesso e sui suoi diritti. L'informativa deve essere fornita all'utente prima dell'inizio del trattamento o, al più tardi, nel momento in cui i suoi dati vengono ceduti a terzi. Le conclusioni che si possono trarre dall'analisi delle applicazioni in oggetto con riferimento a questo indicatore sono negative: a parte *AlertCops* e *MobilePatrol Public Safety App*, le altre applicazioni sono carenti di *privacy-policy*, fondamentale per comprendere appieno la natura del trattamento, o non viene individuato in modo chiaro chi sia lo sviluppatore ed il titolare del trattamento. *Crime Check*, *City of Cape Coral* e *Crime Watch*, *Crime Rates Stats* consentono di ottenere informazioni sul titolare del trattamento, ma non hanno una *privacy-policy* chiara. Le prime due sono state valutate negativamente anche in ragione della non rispondenza della valutazione al terzo indicatore (principio di correttezza del trattamento) e al primo (principio di qualità dei dati). In conclusione, queste applicazioni acquisiscono informazioni eccedenti rispetto alle loro funzionalità e non vi è un'informazione effettiva sulle *privacy-policy*. *Alarm 112* non ha ricevuto una valutazione positiva poiché non è possibile ottenere informazioni sulla *privacy-policy* né sul titolare. Per *Crime Maps*, non è possibile reperire informazioni sul titolare del trattamento/sviluppatore (poiché si rimanda ad una pagina *Facebook*) e neppure una *privacy-policy*. Quanto a *Cuadrante Amigo*, si richiamano i commenti fatti sulle difficoltà a trovare la *privacy-policy* illustrate a commento del terzo indicatore (principio di correttezza del trattamento). La sua esistenza, superate le difficoltà di reperimento del dato, ha comportato comunque una valutazione positiva.

Indicatore (6) - Consenso

Il trattamento dei dati personali può essere svolto nel momento in cui vi sia il consenso esplicito, specifico ed informato degli utenti. In ragione delle caratteristiche del consenso, si può dubitare che esso, per quanto richiesto per il trattamento dei dati degli utenti anche dalle applicazioni di denuncia, possa dirsi specifico ed informato (tranne che per *Cuadrante Amigo*), date le indubbie carenze delle applicazioni analizzate nel: (1) rispettare il principio di qualità dei dati, richiedendo l'accesso ad informazioni pertinenti rispetto ai loro scopi; (2) prevedere una *privacy-policy ad hoc*.

Valutazione delle applicazioni di “auto-aiuto”

Le applicazioni per la sicurezza urbana definite di “auto-aiuto” sono strumenti che creano dei *social network* “privati” tra gli utenti registrati al servizio, consentendo un controllo reciproco sulla posizione attuale. Tramite queste applicazioni, è possibile anche inviare *alert* ai membri della lista dei “guardiani” (es. familiari o amici dell’utente) in situazioni di insicurezza o di pericolo. Questi strumenti sono il più delle volte collegati ad un servizio *online* che consente la registrazione, quindi acquisiscono i dati di registrazione di ogni utente, la sua posizione, le sue comunicazioni con gli altri membri del *social network* ed i suoi percorsi. In particolar modo, le applicazioni dotate del maggior numero di funzioni (come *bSafe – Personal Safety App*) possono creare un *vulnus* alla *privacy* degli utenti. All’interno di questa categoria, rientrano cinque applicazioni per la sicurezza urbana, tra quelle selezionate: みまもり防犯ブザ *(Tracking Crime Buzzer)*, *Fightback*, *Safe-U*, *Mobile Tracker* e bSafe - *Personal Safety App*. Nella Tabella 7, la valutazione di *compliance* sui temi della *privacy* e la protezione dei dati personali di queste applicazioni è realizzata in base alla conformità o meno dell’*app* in relazione agli indicatori normativi precedentemente descritti. La conformità è identificata attraverso il simbolo “x”.

Indicatore (1) - Principio di qualità dei dati

Il principio di qualità dei dati prevede che essi siano raccolti solo ove pertinenti rispetto allo scopo dell’applicazione. *Fightback* e *Mobile Tracker* creano problemi da questo punto di vista, poiché viene richiesto l’accesso allo stato del telefono e al registro chiamate dell’utente. Considerando le finalità di trattamento descritte per le due applicazioni, riassumibile nella possibilità di creare un *social network* “privato” per gli utenti, non vi è giustificazione per la richiesta di accesso alle informazioni contenute nel registro chiamate: quest’ultimo contiene notizie sui numeri di telefono di persone non necessariamente registrate al servizio, la risposta o meno alla chiamata e l’ora in cui essa è stata effettuata. Lo stesso dicasi per quanto riguarda la lettura dello stato del telefono: non vi è necessità per gli sviluppatori di sapere quando l’utente sta ricevendo una telefonata e da chi. A queste perplessità si aggiunge, nella valutazione di rispondenza di *Fightback* ai principi rappresentati dal presente indicatore, l‘impossibilità di reperire il permesso che prevede la possibilità dell’*app* di connettersi ad *account* già presenti sul telefono: questa informazione non figura come autorizzazione specifica.

Indicatore (2) - Principio di finalità del trattamento

Il principio è rispettato nel momento in cui il titolare del trattamento rende manifesto all’utente uno scopo definito per la raccolta e il trattamento dei dati personali. Le applicazioni di “auto-aiuto” per la sicurezza urbana

Tabella 7 - Valutazione di privacy-compliance delle applicazioni di auto-aiuto

	Applicazioni di auto-aiuto				
Indicatori	**みまもり防犯ブザ (Tracking Crime Buzzer)**	**Fightback**	**Safe-U**	**Mobile Tracker**	**bSafe - Personal Safety App**
Principio di qualità dei dati			X		X
Principio di finalità del trattamento	X	X	X	X	X
Principio di correttezza del trattamento	X	X		X	X
Divieto di trattamento dei dati sensibili	X	X	X	X	X
Diritti dell’interessato		X			X
Consenso					X

Fonte: elaborazione degli autori

descrivono in modo abbastanza preciso le finalità del trattamento dei dati che vengono acquisiti presso l'utente sia nella descrizione dell'*app*, sia all'interno delle *privacy-policy* appositamente redatte, probabilmente in ragione della peculiarità del loro scopo, della numerosità di funzioni e della rischiosità dell'uso dei molti dati personali raccoglibili.

Indicatore (3) - Principio di correttezza del trattamento

Il principio di correttezza del trattamento prevede che il titolare del trattamento svolga la sua attività in modo corretto nei confronti degli interessati, mantenendoli informati sull'utilizzo dei loro dati. Anche in questo caso, la valutazione delle applicazioni di "auto-aiuto" è positiva: è presente l'indicazione d'uso dei dati degli utenti. Questa informazione è reperibile nella descrizione delle funzionalità dell'*app* (per quanto riguarda *Tracking Crime Buzzer*) oppure nelle diverse *privacy-policy*, facilmente raggiungibili dall'utente tramite appositi *link* dall'interno delle stesse o tramite la pagina di presentazione del prodotto. Qualche perplessità solleva *Mobile Tracker*, applicazione per la quale è stata redatta una *privacy-policy* molto generica e non modellata sulle funzionalità dell'*app* e sulle potenzialità dannose dell'utilizzo non conforme dei dati degli utenti. L'unica applicazione di questa categoria che non è fornita per nulla di *privacy-policy* è *Safe-U*, per la quale la valutazione di conformità è stata negativa.

Indicatore (4) - Divieto di trattamento di dati sensibili

Il divieto si applica in generale a tutti i trattamenti automatizzati, a meno che non intervenga il consenso specifico dell'utente, il trattamento sia previsto in una legge allo scopo di assolvere obblighi e diritti del responsabile del trattamento in materia di diritto del lavoro o a scopi sanitari, ossia per salvaguardare un interesse vitale della persona interessata o di un terzo. La valutazione di *privacy-compliance* con riferimento alle applicazioni *mobile* per la sicurezza urbana di "auto-aiuto", rispetto a questo indicatore, è molto positiva: nessuna informazione di tipo sensibile viene raccolta e si può dire che dalle *privacy-policy* di questi strumenti sia possibile estrarre delle *best practices*. In particolare, nella *privacy-policy* di *Fightback* sono contenuti dei consigli per mantenere la propria sicurezza in rete e nell'utilizzo dell'applicazione. Nella *privacy-policy* di *bSafe – Personal Safety App*, inoltre, è espressamente sottolineato che gli sviluppatori non trattano dati di minori, a meno che non vi sia l'espressa autorizzazione al trattamento da parte dei genitori, tutori o di chi ne fa le veci.

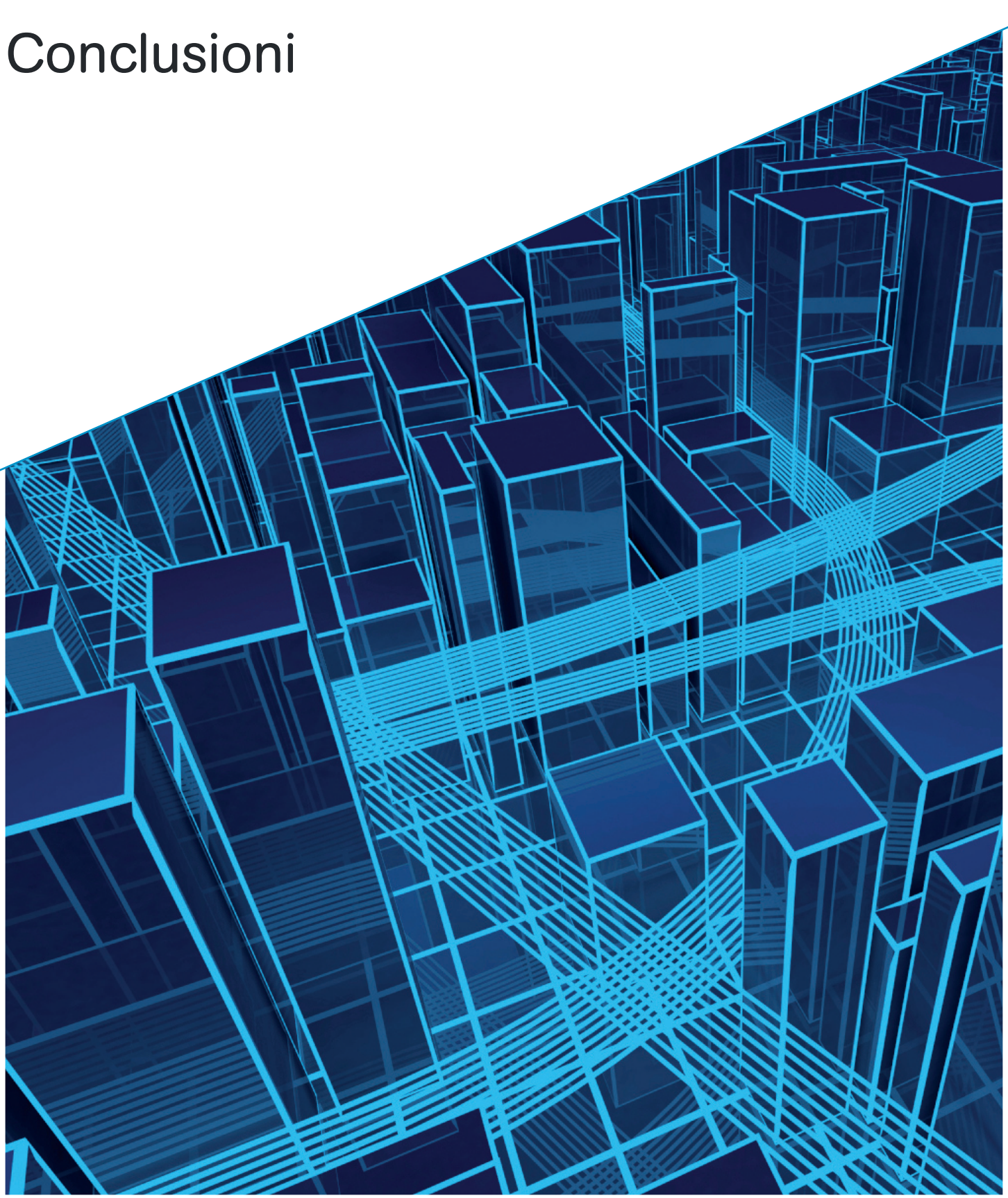
Indicatore (5) - Diritti dell'interessato

L'utente ha diritto ad ottenere l'informativa sulla natura del trattamento dei suoi dati, sul titolare del trattamento, sugli eventuali altri destinatari dei dati, sullo scopo dello stesso e sui diritti di cui è titolare. L'informativa deve essere fornita all'utente prima dell'inizio del trattamento o, al più tardi, nel momento in cui i suoi dati vengono ceduti a terzi. La valutazione di conformità ai dettami in materia di *privacy* mostra come *Safe-U*, *Mobile Tracker* e *Tracking Crime Buzzer* non possano ottenere una valutazione positiva. *Safe-U*, in ragione della mancanza di *privacy-policy* e dell'impossibilità di comprendere chi sia lo sviluppatore, di cui viene fornito solo l'indirizzo email, non può ricevere valutazione positiva. Se si cerca di comprendere chi sia lo sviluppatore, e quindi titolare del trattamento dei dati degli utenti, di *Tracking Crime Buzzer* si viene reindirizzati ad un *blog* che non presenta, però, informazioni precise su chi lo stesso sia. In ragione della non completezza delle informazioni fornite dalla *privacy-policy* di *Mobile Tracker* e dell'impossibilità di individuare uno sviluppatore (è presente anche in questo caso solo un indirizzo email), questa applicazione ha ricevuto una valutazione negativa.

Indicatore (6) - Consenso

Il trattamento dei dati personali può essere svolto nel momento in cui vi sia il consenso esplicito, specifico ed informato degli utenti. In ragione della presenza di *privacy-policy* ben definite o di descrizioni delle funzionalità delle applicazioni da cui è possibile evincere l'uso che può essere fatto dei dati degli utenti, il consenso acquisito dai titolari del trattamento può dirsi esplicito e "parzialmente informato". Rimangono dubbi nei confronti delle applicazioni che violano il principio di qualità dei dati, a cui si riferiscono *privacy-policy* imprecise e per le quali non sia possibile individuare dei titolari del trattamento (es. *Tracking Crime Buzzer, Fightback, Safe-U* e *Mobile Tracker*).

Conclusioni



L'obiettivo di questo rapporto di ricerca, inserito nell'ambito del progetto europeo *eSecurity – ICT for knowledge-based and predictive urban* security, è stato di valutare se e come le applicazioni mobili per la sicurezza urbana, esistenti sul mercato, siano conformi ai dettami della normativa attualmente in vigore a livello sovranazionale sulla *privacy* e la protezione dei dati personali, ovvero se siano *privacy-compliant*. La valutazione è stata svolta utilizzando degli "indicatori normativi", identificati sulla base della legislazione applicabile, grazie ai quali è stato possibile notare come queste *app*, nonostante gli appelli delle autorità garanti della *privacy* a livello globale, in generale non rispondano ai paradigmi legali dettati dalla disciplina sovranazionale in materia.

Questa conclusione è particolarmente "pericolosa" in termini di protezione della riservatezza e dei dati personali, soprattutto se messa a confronto con gli scopi che si prefiggono queste applicazioni: (1) informare gli utenti rispetto al degrado urbano o ai reati/atti devianti compiuti in una zona; (2) consentire l'invio di segnalazioni ai diversi *stakeholders* (ad esempio, alle forze di polizia); (3) rassicurare l'utente creando una rete di "guardiani" da contattare in caso di emergenza (ad esempio, parenti e amici). In una frase: creare sicurezza, per l'utente e la sua famiglia. Volendo effettuare una valutazione generale in base ai risultati ottenuti nel precedente paragrafo, si può affermare che i rischi più gravi per la *privacy* e la tutela dei dati personali degli utenti di queste applicazioni sono rappresentati dalla violazione, da parte degli sviluppatori: (1) del principio di qualità dei dati, (2) del principio di trasparenza, e quindi (3) dei diritti dell'interessato. Inoltre, da ciò può evincersi (4) la non genuinità, in ragione delle violazioni precedenti, del consenso richiesto.

Il primo problema evidenziato dalla valutazione è la difficoltà di comprendere perché le applicazioni richiedano determinate informazioni: non tutte le *app* sono corredate da note esplicative che illustrano le motivazioni dei diversi permessi richiesti, oppure esse sono indicate in modo vago. Inoltre, le informazioni raccolte tramite le applicazioni vengono spesso cedute a terze parti, all'insaputa dell'utente: soggetti che possono creare profili dettagliati ad uso commerciale. Questa mancanza di trasparenza nell'uso che viene fatto dei dati incide sulla correttezza del trattamento e spesso crea un *vulnus* ai diritti dell'interessato: costui non può tutelarsi nei confronti del soggetto a cui i dati sono stati ceduti e non può neppure esercitare un consenso davvero informato. Inoltre, gli sviluppatori delle *app* sembrano non recepire gli appelli al rispetto del principio di trasparenza e, quindi, alla correttezza del trattamento, lanciati dalle autorità garanti della *privacy* a livello globale. Non sempre vengono messe a disposizione delle *privacy-policy* o, quando esistenti, esse non sono coerenti con le funzionalità dei prodotti presentati. In mancanza di un'informativa dettagliata, contenente notizie utili sulla natura del trattamento, sul titolare del trattamento, sugli eventuali altri destinatari dei dati, sullo scopo dello stesso e sulle modalità di esercizio dei diritti di cui l'utente è titolare, lo stesso vede i suoi diritti (quasi sempre) sistematicamente violati (Shklovsky et al., 2014).

L'elemento del consenso, considerato come il *core element* della disciplina, spesso viene ad essere snaturato. Esso spesso non è informato, come detto, e, per le modalità di installazione di queste *app*, non può essere neppure specifico ed esplicito. L'utente non riceve le informazioni che dovrebbero essere necessarie per scegliere se installare o meno l'*app* in ragione dei permessi richiesti, se accettare solo alcuni di essi oppure controllare che i suoi dati siano trattati nel rispetto della disciplina vigente. Il consenso si realizza con un semplice *click* su "Installa", un'operazione automatica e spesso svolta in modo acritico, che mette in moto meccanismi che l'utente non può controllare (Article 29 Data Protection Working Party, 2013). Gli utenti sembrano preoccupati dal diffondersi delle loro informazioni tramite i nuovi *device* solo in un momento successivo alla raccolta dei dati, quando qualcuno spiega loro le potenzialità dannose del loro comportamento. Eppure, ricerche dimostrano come gli stessi utenti mettano in moto dei meccanismi *ex ante* per proteggere i propri dati personali contenuti in *mobile devices*, come fare dei *back up* degli elementi multimediali, dei contatti e di altri file contenuti sui dispositivi, installare antivirus, cancellare la *cache* del motore di ricerca, spegnere il GPS o, in generale, il sistema di localizzazione, impostare *password* per determinati dati o in generale per il dispositivo (PewResearch Center, 2012; Shklovsky et al., 2014).

Come spiegare questa "asimmetria" nel comportamento degli utenti? Molto probabilmente, come è già stato affermato da più parti, perché manca una reale alfabetizzazione elettronica. Gli utenti non conoscono i loro diritti e doveri e lo stesso accade ai fornitori di servizi. Inserire dati in rete comporta che essi, poten-

zialmente, possano essere reperibili in ogni momento: a riguardo, gli Stati Membri dell'Unione europea hanno spinto per far riconoscere il diritto all'oblio all'interno della proposta del Regolamento Europeo del 2012, in corso di approvazione, in ragione della pericolosità per l'utente di vedere i propri dati sempre disponibili a qualunque terzo (Article 29 Data Protection Working Party, 2013). Anche la Corte di Giustizia dell'Unione europea si è espressa su questo tema: con la sentenza del 13 maggio 2014, causa C-131/12 (c.d. sentenza *Google-Spain*), ha qualificato *Google* come titolare del trattamento per la sua attività di ricerca di informazioni già presenti su Internet e di successiva indicizzazione automatica, memorizzazione e messa a disposizione degli utenti, secondo un determinato ordine di preferenza. Inoltre, la Corte ha riconosciuto il diritto dell'interessato a chiedere la cancellazione di un'informazione collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca, nel caso in cui suoi diritti fondamentali prevalgano sull'interesse economico del gestore del motore di ricerca e sull'interesse del pubblico all'informazione (Article 29 Data Protection Working Party, 2013; Consiglio d'Europa, 2014).

L'adozione e l'applicazione effettiva di una normativa specifica, a livello sovranazionale e nazionale, che tenga conto di tutte queste problematiche ed imponga l'attuazione dei diritti nelle tecnologie, responsabilizzando i titolari dei trattamenti affinché adottino strategie di gestione e controllo dei dati più sicure, risulta essere doverosa. In questo senso, si è mossa la Commissione europea con la *Proposta di Regolamento del Parlamento europeo e del Consiglio*, presentata nel 2012, sulla quale le istituzioni europee dovrebbero raggiungere un accordo entro dicembre 2015. La proposta di regolamento vede tra i principi generali applicabili a qualsiasi trattamento: (1) il rafforzamento del principio di trasparenza, (2) la precisazione del principio di minimizzazione dei dati e (3) l'introduzione di una responsabilità generale del responsabile del trattamento, rafforzata rispetto a quanto previsto sinora. Il testo della proposta, contiene, all'articolo 11, l'obbligo per i responsabili del trattamento di fornire informazioni trasparenti, comprensibili e facilmente accessibili agli utenti. Questa norma è utile per garantire un corretto dialogo tra gli sviluppatori, i gestori degli *stores* e gli utenti stessi, in modo che questi ultimi possano scegliere le applicazioni per la sicurezza urbana in modo oculato e soprattutto consapevole, in funzione dei propri interessi e delle scelte di "evitamento" preferite (Cfr. Commissione europea, Proposta di Regolamento "COM(2012) 11 final" del 25 gennaio 2012).

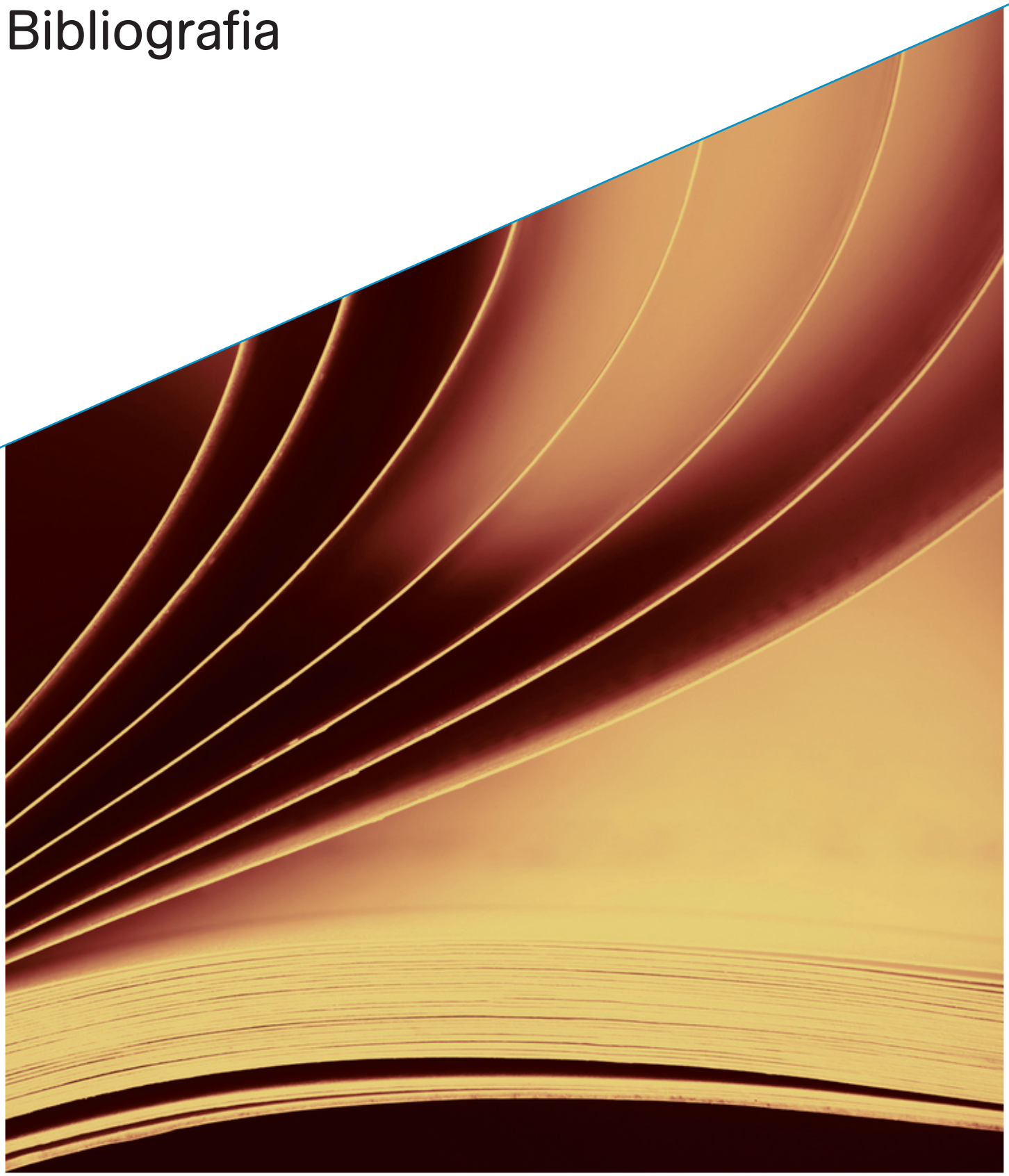
In aggiunta, la suindicata *Proposta di Regolamento* prevede che i titolari del trattamento debbano rendere noto in modo chiaro agli interessati come inviare richieste di esercizio dei propri diritti in via elettronica e telematica, predisponendo dei meccanismi di risposta che diano ragione di eventuali rifiuti entro un termine ragionevole. In questo senso, non dovrebbero essere solo gli sviluppatori (o eventuali altri titolari del trattamento) a rendere noto e soprattutto visibile nei loro prodotti questa informazione, ma anche gli *stores online* dovrebbero attrezzarsi per consentire all'utente di ottenere queste informazioni facilmente. Ad esempio, *Google Play* potrebbe richiedere agli sviluppatori di rendere disponibili dei *link* che rimandino alle loro pagine Internet e contengano informazioni sull'esercizio dei diritti, allo stesso modo in cui a volte è presente la possibilità di raggiungere le *privacy-policy* dei singoli prodotti. Di particolare interesse è il riferimento nella *Proposta di Regolamento* al diritto di opposizione e profilazione, formulato all'articolo 20: si sancisce, al secondo comma, un diritto dell'utente a non essere profilato. In questo modo, l'utente potrebbe scegliere di escludere questa pratica nei propri confronti da parte degli sviluppatori delle *app* per la sicurezza urbana, impedendo anche che essi possano operare trasferimenti dei dati ad aziende terze.

Dinnanzi alle nuove tecnologie vi è la necessità di parametrare la *privacy* al rapporto che si instaura tra persone, cose e situazioni, e, pertanto, anche la legislazione di riferimento e le campagne di sensibilizzazione devono saper garantire la sicurezza dei cittadini in risposta all'aumento di informazioni in circolazione dei singoli e sui singoli (Cfr. *big data*). Questo poiché i rischi maggiori riguardano non solo i dati stessi, ma anche i collegamenti tra i soggetti e gli oggetti connessi. Di pregio, in questo senso, è anche l'iniziativa posta in essere dalla *Mobile Marketing Association* di creare delle linee guida per strutturare la *privacy-policy* delle applicazioni *mobile*, che i titolari di trattamento possono utilizzare come modello da perfezionare con le informazioni corrispondenti ai loro prodotti (Mobile Marketing Association, 2011).

Se il diritto può servirsi delle nuove tecnologie per "perseguire obiettivi in precedenza assicurati da altre tecnologie" (Pascuzzi, 2010), le applicazioni per la sicurezza urbana possono di certo raggiungere obiettivi già assicurati dalle attività di prevenzione e repressione svolte dalle forze dell'ordine e dagli enti locali in modo innovativo ed efficace, garantendo la partecipazione attiva della cittadinanza. Ma d'altra parte, se è il diritto a modellarsi in ragione delle caratteristiche della tecnologia impiegata, le nuove norme per la tutela dei dati personali devono essere abbastanza generali da essere applicabili alle nuove modalità di trattamento automatizzato ed elettronico e, contemporaneamente, abbastanza pregnanti da non lasciare scoperte aree della vita privata dell'individuo che costui non riesca più "a nascondere", dinnanzi alla pervasività della profilazione automatica. Riuscirà il nuovo Regolamento europeo a rispondere a questa sfida?

b

Bibliografia



Article 29 Data Protection Working Party (2013), *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation,* Bruxelles, Commissione europea.

Brantingham, P.J., Brantingham, P.L. (1991) (a cura di), *Environmental Criminology* (II ed.), Prospect Heights, Waveland Press.

Brantingham, P.J., Brantingham, P.L. (1995), "Criminality of Place: Crime Generators and Crime Attractors", *European Journal on Criminal Policy and Research*, 3, 3.

Brantingham, P.J., Tita, G.E. (2008), "Offender Mobility and Crime Pattern Formation from First Principles", in Liu L., Eck J. (a cura di), *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*, Hershey, Idea Press.

Chaouchi, H. (2013), *The Internet of Things: Connecting Objects*, Hoboken, John Wiley & Sons.

Clarcke, R.V. (1997), "Introduction", in Clarcke R.V. (a cura di), *Situational Crime Prevention. Successful case studies*, New York, Harrow and Heston.

Clarke, R.V., Eck, J.E. (2003), *Become a Problem-Solving Crime Analyst: In 55 Small Steps*, Londra, Jill Dando Institute of Crime Science, University College London.

Commissione europea (2015), *Protezione dei dati nell'UE: l'accordo sulla riforma proposta dalla Commissione stimolerà il mercato unico digitale*, *Data Protection Reform*, reperibile al sito Internet: http://europa.eu/rapid/press-release_IP-15-6321_it.htm (data ultima consultazione: 15 novembre 2015).

Consiglio d'Europa - Agenzia dell'Unione europea per i diritti fondamentali (2011), *Manuale di diritto europeo della non discriminazione*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea.

Consiglio d'Europa - Agenzia dell'Unione europea per i diritti fondamentali (2014), *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea.

Di Nicola, A., Bressan, S. (2014), "Sicurezza urbana predittiva: eSecurity e le nuove prospettive per la prevenzione della criminalità nelle città", in *Sentieri Urbani*, 13, 1.

Di Nicola, A., Espa, G., Bressan, S., Dickson M.M., Nicolamarino A. (2014), *Metodi statistici per la predizione della criminalità. Rassegna della letteratura su predictive policing e moduli di data mining*, Trento: eCrime Working Papers n. 2 – Università degli Studi di Trento.

Felson, M. (1992), "Routine Activities and Crime Prevention. Armchair Concepts and Practical Actions", *Studies on Crime and Crime Prevention*, 1, 1.

Felson, M., Clarke, R.V. (1998), *Opportunity Makes the Thief*, Police Research Series, Paper 98, Londra, Home Office.

Fling, B. (2009), *Mobile Design and Development*, Sebastopol, O'Reilly Media Inc.

FTC Staff Report (2013), *Mobile Privacy Disclosure, Building Trust Through Transparence*, reperibile al sito Internet: http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (data ultima consultazione: 14 ottobre 2015).

Garante per la protezione dei dati personali (2014), *Smartphone e tablet: scenari attuali e prospettive operative*, Roma, Garante per la protezione dei dati personali.

Gardner, H., Davies, K. (2014), *Generazione App: La testa dei giovani e il nuovo mondo digitale,* Milano, Feltrinelli.

Hartmann, M. (2011), "Mobile Privacy: Contexts", in Temple S., Reinecke, L. (a cura di), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, Heidelberg, Springer.

Hindelang, M.J., Gottfredson, M.R., Garofalo, J. (1978), *Victims of Personal Crime. An Empirical Foundation for a Theory of Personal Victimization*, Cambridge, Ballinger.

Jones, P.A., Brantingham, P.J., Chayes, L.R. (2010), "Statistical Models of Criminal Behavior: The Effects of Law Enforcement Actions", *Mathematical Models and Methods in Applied Sciences*, 20, 1.

Lab, S.P. (2010), *Crime Prevention: Approaches, Practices, and Evaluations – 7th Edition*, New Providence, Matthew Bender & Company.

Lupton, D. (2014), *Digital Sociology*, Londra, Routledge.

Marciano, C. (2015), *Smart City: Lo spazio sociale della convergenza*, Roma, Edizioni Nuova Cultura.

Melossi, D. (2004), "La criminologia di impronta sociologica", in Selmini D (a cura di), *La sicurezza urbana*, Bologna, Il Mulino.

Mobile Marketing Association (2011), *Mobile Application Privacy Policy Framework*, reperibile al sito Internet: http://www.mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobile-apps, (data ultima consultazione: 3 novembre 2015).

Nobili, G. (2003), "Disordine urbano e insicurezza: una prima indagine su Bologna", in *Quaderni di Città Sicure – Regione Emilia Romagna*, n. 28, Novembre-Dicembre 2003.

Pascuzzi, G. (2010), *Il diritto dell'era digitale*, Bologna, Il Mulino.

PewResearch Center (2012), *Privacy and Data Management on Mobile Devices*, reperibile al sito Internet http://www.pewinternet.org/files/oldmedia/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf, (data ultima consultazione: 12 novembre 2015).

RAND (2013), *Predictive policing. The Role of Crime Forecasting in Law Enforcement Operations*, Washington, RAND Corporation.

Ratcliffe, J. (2010), "Crime Mapping: Spatial and Temporal Challenges", in Piquero A.R., Weisburd D. (a cura di), *Handbook of Quantitative Criminology*, New York, Springer.

Regione Piemonte (2012), *Leggere la sicurezza. I dati, il contesto, i fenomeni e le percezioni*, Regione Piemonte, Torino.

Selmini, R. (2004), "Introduzione", in Selmini R. (a cura di), *La sicurezza urbana*, Bologna, Il Mulino.

Shklovsky, I., Mainwaring, S.D., Skuladdottir, H.H., Borgthorsson H. (2014), *Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use*, reperibile al sito Internet http://scott.mainzone.com/pubs/14-leakiness-creepiness.pdf, (data ultima consultazione: 10 novembre 2015).

Short, M.B., D'Orsogna, M.R., Pasour, V.B., Tita, G.E., Brantingham, P.J., Bertozzi, A.L., Chayes, L.B. (2008), "A Statistical Model of Criminal Behavior", *Mathematical Models and Methods in Applied Sciences*, 18, 1.

Thacher, D. (2004), "Order Maintenance Reconsidered: Moving Beyond Strong Causal Reasoning", *The European Journal of Criminal Law and Criminology*, 94, 2.

Unione europea (2015), *Special Eurobarometer 431 "Data protection"*, Bruxelles, Directorate-General for Communication.

Urry, J. (2002), *Mobility and Connections*, reperibile presso il sito Internet: http://www.ville-en-mouvement.com/sites/default/files/mobility_connections_urry.pdf (data ultima consultazione: 4 novembre 2015).

Yildiz, M. (2007), "E-government research: Reviewing the literature, limitations, and ways forward", *Government Information Quarterly*, 24, 3.

Wartell, J., Gallagher, K. (2012), "Translating environmental criminology theory into crime analysis practice", *Policing. A Journal of Policy and Practice*, 6, 4.

Wilson, J.Q., Kelling, G.L. (1982), "Broken Windows", *The Atlantic Monthly,* 79, 3.

Zedner, L. (2000), "The Pursuit of Security", in Hope T., Sparks R. (a cura di), *Crime, Risks and Insecurity*, Londra, Routledge.

Ziccardi, G. (2012), *Informatica giuridica*, Vol. 1, Milano, Giuffrè.

Le opinioni espresse nel presente rapporto di ricerca sono di responsabilità esclusiva degli autori e non riflettono necessariamente la posizione ufficiale dell'Unione europea.

Stampa digitale: www.rotooffset.it - Trento

Trento, novembre 2015

ISSN 2284-399X
ISBN 978-88-8443-671-9