PAPER
2016

RISCHI CONNESSI ALLO SFRUTTAMENTO DEI SOCIAL NETWORK COME FONTE DI INFORMAZIONI NELLA SMART CITY

CARLO SCUDERI

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

RISCHI CONNESSI ALLO SFRUTTAMENTO DEI SOCIAL NETWORK COME FONTE DI INFORMAZIONI NELLA SMART CITY

Carlo Scuderi

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

2016

RISCHI CONNESSI ALLO SFRUTTAMENTO DEI SOCIAL NETWORK COME FONTE DI INFORMAZIONI NELLA SMART CITY

Introduzione – contesto della smart city

L'attuale tendenza demografica ad affollare le città, che offrono più opportunità di connessione con il mondo e costituiscono nodi di scambio economici e di creatività, ha costretto ad interrogarsi su quali siano gli strumenti più adeguati per organizzare nuovi spazi urbani capaci di ordinare una così grande mole di cittadini, per i quali le stesse città non erano state originariamente progettate, e per soddisfare le loro aspettative.
Per farlo, le amministrazioni locali hanno bisogno di comprendere i mutamenti ed avere informazioni di prima mano.

Il concetto di città intelligente si inserisce a questo punto come la risposta a due problematiche tipiche di questo contesto: A) rilevare informazioni in maniera automatica e B) farle interagire tra di loro per creare sinergie, preferibilmente con un impiego sostenibile di risorse.

Il secondo punto può ottenersi affinando algoritmi che sostituiscano l'impiego di personale, dato che sarebbe troppo oneroso destinare la quantità di lavoratori necessaria per elaborare così tanti dati. Il primo si affida ad uno sfruttamento misto di informazioni provenienti dall' Internet of Things e dal monitoraggio dei social network in modo da carpire i dati spontaneamente concessi dagli utenti.

Sulla stessa definizione di smart city si dibatte spesso, quelle fornite dalla politica tendono spesso ad aumentare quel distacco fra la realtà e l'immaginazione creando poi incomprensioni fra quali siano le differenze tra una vera smart city e una città a cui è semplicemente applicata una etichetta. Townsend intende come smart city un luogo in cui le TIC sono combinate con infrastrutture, architetture, oggetti

quotidiani e persino corpi, per risolvere problemi sociali, economici ed ambientali (Townsend 2013).

Il modello di Giffinger e Gudrun (2010) che è largamente riconosciuto come punto di riferimento per la definizione della città intelligente, identifica le sei dimensioni di cui si compone una smart city:

1. Smart mobility
2. Smart economy
3. Smart enviroment
4. Smart governance
5. Smart people (capitale umano)
6. Smart living (vivibilità)

Dal momento che la partecipazione dei cittadini è importante per costituire una città intelligente, in molti si sono impegnati nell'affrontare il problema della privacy nel contesto urbano, al fine di contenere le paure e i sospetti che possono legittimamente svilupparsi nei confronti della tecnologia, soprattutto a seguito di incidenti che riguardano fughe di informazioni sensibili, e inibirli così dal partecipare alla vita sociale nonché a contribuire al miglioramento dell'efficienza dei servizi (Van Zoonen, 2016). La maggior parte si è concentrata su questioni di sicurezza dell'infrastruttura TIC (come IoT, rete, banche dati ecc.) e applicazioni sulle smart city (Ehnaghraby e Losavio, 2014; Van Zoonen, 2016). Mentre già da tempo si evidenzia la necessità di imporre alti livelli di sicurezza sui dispositivi IoT che vengono adoperati nelle smart city, per evitare intrusioni da parte di terzi e la dissociazione tra i dati personali e quelli urbani (Bartoli et Al. 2011).

Ad ogni modo, le smart city si comportano come "organismi viventi" che evolvono nel tempo, producono e consumano costantemente grandi moli di dati. Una grande varietà di dispositivi, fissi e mobili (per esempio sensori, telecamere, RFID ecc.), il cosiddetto Internet delle Cose (Internet of Things – IoT), ed applicazioni (ad esempio i social network, le piattaforme web, le applicazioni per smartphone) funzionano come fonti di dati, che registrano ogni aspetto della vita e producono dati eterogenei su larga scala. La diffusione degli smartphone ha facilitato il rapido aumento dell'utilizzo dei social network, i cui utenti si è stimato abbiano raggiunto i 2,62 miliardi nel 2018 e potrebbero arrivare a 3,02 nel 2021 (Fig.1 da statista.com)[1].

[1] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

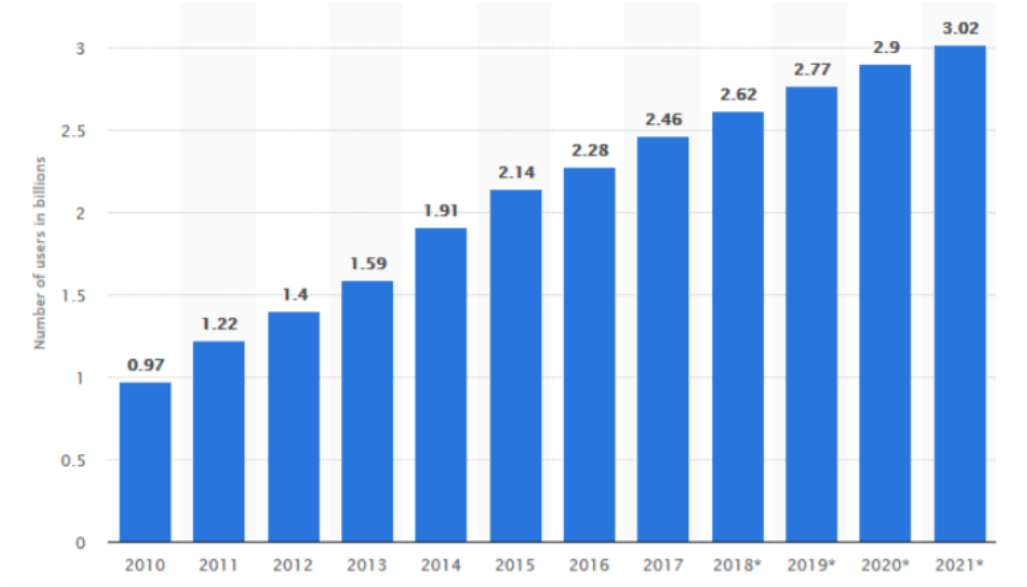

Fig.1 Utenti dei social network tra il 2010 e il 2021

Di contro, l'eccessivo zelo per registrare e controllare ogni attività all'interno delle città ha sollevato molte preoccupazioni riguardo alla sicurezza e alla privacy dei cittadini (Ehnaghraby e Losavio, 2014). I critici obiettano che l'implementazione delle smart city avrà un effetto negativo sulla libertà dei cittadini e sulla riservatezza della vita privata, in quanto baratta informazioni sensibili e personali con i vantaggi offerti da servizi intelligenti (Ahmed e Bouhorma, 2014).

Al di là dei rischi che minacciano infrastrutture e applicazioni, le maggiori preoccupazioni per la privacy e per la sicurezza derivano dai rischi sottesi all'utilizzo dei social network, i quali sono mezzi economici (praticamente gratis) per reperire dati ed estrarre un modello di smart city, ma sono vulnerabili a vari tipi di minacce ed attacchi (Fire et Al. 2014) che ne minano la credibilità ed affidabilità. Tuttavia, diversamente dall'IoT e dalle applicazioni, le questioni di sicurezza e privacy derivanti dal loro utilizzo non sono stati adeguatamente trattate, ragion per cui questo paper intende prendere l'argomento e schematizzarlo.

1.a Social network come fonti di informazioni sull'ambiente urbano

La proliferazione di social network, che sono utilizzati per lo più come mezzo di comunicazione tra individui, offre nuove opportunità per monitorare e analizzare informazioni sull'attività umana e le città in cui

vivono. Sennonché, gli usi impropri dei social network a volte possono costituire un pericolo per la privacy e la sicurezza rispettivamente delle persone e delle città.

I social network (ad esempio Facebook, Twitter, Instagram, Foursquare ecc.) funzionano come sensori umani, paragonabili all'Internet delle Cose, offre quantità di dati eterogenei, riduce i costi, l'interoperabilità e la dipendenza (Dorane e Al. 2014).

Esaminando l'impatto dei social network sulla partecipazione politica (e-partecipation) sulla rete e sull'interazione con gli enti pubblici (e-government), emerge che i social network possano contribuire in maniera significativa al miglioramento dei servizi, alla partecipazione alla vita civile, alla diffusione della cultura digitale e all'assunzione di consapevolezza riguardo il corretto utilizzo dei sistemi interconnessi. Utilizzando i dati geo-localizzati di Twitter, sono state riconosciute e visualizzate varie caratteristiche geografiche, sociali, culturali e politiche che hanno portato all'estrazione degli schemi percettivi dei cittadini in una grande città, mentre Kumar e Ahmed lo hanno sfruttato per rilevare il traffico (Kumar e Ahmed 2016). In Brasile, Fogo Cruzado[2], un'applicazione per smartphone, riceve informazioni tramite Whatsapp, Twitter, Inbox e Facebook, comunicando in tempo reale la posizione delle sparatorie, così da permettere agli utenti di cambiare strada in tempo per evitare pericoli, ingorghi o restare bloccato in operazioni di polizia. I social network, per via delle proprie caratteristiche, sono già largamente utilizzati per implementare le smart city, sia da soli che in azione combinata con l'IoT, e il loro impiego è destinato a crescere nel tempo.

1.b Influenza dei social network sui comportamenti sociali

Giacché i social network influenzano i comportamenti sociali di quelli che li usano e a volte per conseguenza condizionano anche quelli di non li usa mi concentrerò sulle ultime due dimensioni, *smart people* e *smart living*, poiché si ricollegano alla prospettiva sociale della smart city (Batty et Al. 2012).

[2] https://fogocruzado.org.br/

Inoltre, tra le dimensioni che caratterizzano le smart city (Giffinger e Gundrun 2010) sono di particolare interesse, nell'ottica delle relative ripercussioni sulla privacy e sulla sicurezza, le dimensioni smart people e smart living.

Il **fattore umano** è riconosciuto da molti studiosi come il pilastro principale della smart city, visto che, comprensibilmente, le TIC e le altre infrastrutture della smart city sarebbero soggette a costanti inadeguatezze senza il continuo intervento della componente umana ad aggiornare e ad aggiustare il tiro (Batty et Al. 2012; Giffinger e Gudrun 2010). Le caratteristiche della dimensione smart people si riassumono in A) fattori umani (creatività, istruzione, social learning) e B) fattori sociali (apertura mentale, partecipazione alla vita pubblica, senso di comunità) (Nam e Pardo, 2011; Batty et Al. 2012). La gente condivide opinioni, stati d'animo e contenuti sui social network, registrano dati attraverso l'Internet delle Cose (dispositivi indossabili, applicazioni su smartphone che misurano i parametri vitali, sensori, centraline, ecc.) e in alcuni casi partecipano a delle rilevazioni statistiche tramite sondaggi e piattaforme all'uopo preposte. Queste sono fonti di informazioni che aiutano le amministrazioni a comprendere meglio la realtà e ad aumentare l'efficienza dei servizi erogati. I dati sono risorse, strumenti nelle mani dei *decision maker*.

Quando, relativamente ai social network, i singoli uniscono uno o più fattori sopracitati e forniscono coscientemente e responsabilmente i propri dati personali, tenendo conto di tutti i rischi per la privacy, possono contribuire significativamente a preservare e a migliorare la sicurezza della città nella sua interezza. Privacy significa innanzitutto responsabilità personale, può essere assicurata solo da un uso appropriato delle impostazioni. Nel complesso può portare alla protezione sicura quando i singoli non saranno più vulnerabili agli attacchi. In pratica la sicurezza generale dipende dalla somma delle attenzioni individuali.

Così la sensazione di sicurezza e la fiducia nei social network accrescerà la partecipazione degli utenti, i quali in collaborazione con i propri concittadini e con gli enti locali creeranno nuovi servizi intelligenti e rafforzeranno la coesione sociale (Van Zoonen 2016).

Al contrario, la mancanza di competenze, di istruzione e consapevolezza riguardo l'uso sicuro dei social, porta inevitabilmente all'involontaria

perdita di controllo che li rende vulnerabili ai suddetti rischi di privacy e sicurezza (Fire et Al. 2014).

Sicché i malfattori hanno l'opportunità di aggredire e raggiungere il loro obiettivo, riducendo il livello di sicurezza percepito sui social network, il che provoca di conseguenza, preoccupazione e paura nella generalità degli utenti. Questo genere di remore scoraggiano l'utilizzo di social network e così a catena diminuisce la partecipazione alla vita sociale, rendendo difficile registrare informazioni con una certa accuratezza, poiché i risultati vengono falsati dalla paura. Alla fine va a detrimento dell'impianto della smart city e della *smartness* individuale (Van Zoonen 2016).

Possiamo affermare che c'è un carattere incrementale della città intelligente, in quanto funziona meglio quanto più persone, dispositivi e dati vi sono connessi. Al contrario, un calo di fiducia favorisce una fuoriuscita dalla partecipazione e sabota le stesse basi del concetto.

La **vivibilità** è una delle dimensioni di cui si è parlato di più poiché è indissolubilmente legata alla dimensione della partecipazione civica, che determina il livello dei servizi erogati e misura il benessere nei contesti urbani.

Questa dimensione copre servizi che soddisfano quasi tutti i bisogni umani, come i trasporti, la sanità, l'istruzione, la pubblica sicurezza, la cultura, la manutenzione, l'economia, l'intrattenimento, ecc. (Batty 2012; Giffinger e Gudrun, 2010). Sanità, assistenza sociale e sicurezza sono gli ambiti dove si registrano i principali interventi nel dominio inerente i servizi offerti al cittadino. Nei primi due casi si tratta prevalentemente di soluzioni destinate al monitoraggio in remoto di pazienti o anziani, mentre nell'ultimo di software in grado di prevenire con buona accortezza eventi rischiosi. Nel campo dell'istruzione l'introduzione di banda larga, Lavagne Interattive Multimediali (LIM), e-book e più in generale di nuovi paradigmi per la didattica può segnare l'avvio di un processo strategico di innovazione digitale. Infine, il crescente utilizzo di applicativi basati su Realtà Aumentata e Near Field Communication può cambiare radicalmente la fruizione della città nelle aree cultura e turismo. L'efficacia della vivibilità richiede la comprensione dei bisogni e lo sviluppo di servizi intelligenti, così come il loro monitoraggio e miglioramento (Batty 2012; Giffinger e Gudrum, 2010). Tra i vari ambiti, Istruzione e Sanità sono quelli maggiormente *public value driven*. Questo

fa sì che gli investimenti debbano essere necessariamente supportati dal settore pubblico.

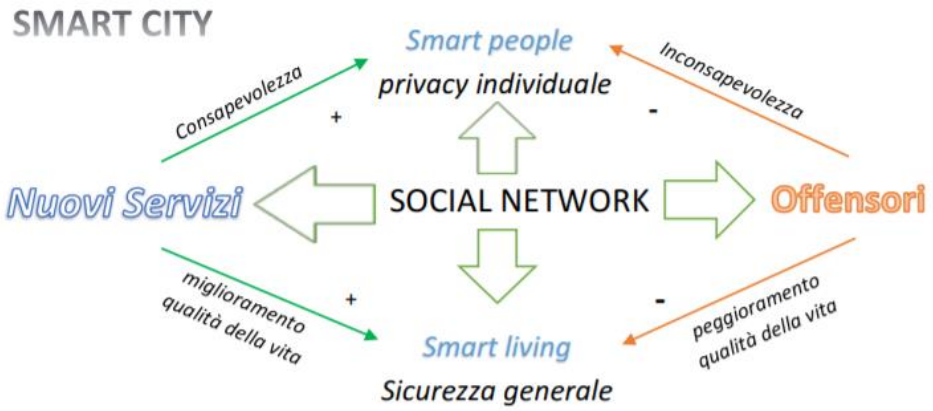

Fig.2 Influenza dei social network sulla smart city

Nell'ambito della pubblica sicurezza, le piattaforme orizzontali ai vari dipartimenti possono già permettere azioni preventive e interventi tempestivi. Il settore è ad oggi caratterizzato da un buon sistema infrastrutturale diffuso nelle città (le telecamere pubbliche e private), che da solo non è però sufficiente, poiché il costo per avere un numero adeguato di operatori per il monitoraggio risulta insostenibile.

Questa attività non a valore aggiunto può invece essere sostituita da tecnologie di riconoscimento in grado di segnalare situazioni di pericolo grazie all'utilizzo di *analytics*, sempre nella tutela degli aspetti legati alla privacy. In queste soluzioni, quindi, la principale criticità non riguarda la tecnologia, che presenta già un buon livello di maturità, ma il modello di governance da instaurare tra i differenti attori nell'ambito della sicurezza cittadina, poiché le piattaforme sono in grado di elaborare procedure di intervento standardizzate a seconda del tipo di allarme, in modo da creare precisi centri di responsabilità[3].

Poiché i dati, generati da tutte le fonti di informazioni disponibili, sono diffuse rapidamente, sorgono nuovi problemi di privacy e sicurezza, che hanno duplice impatto sulla dimensione smart living: da un lato, i rischi legati agli attacchi alle infrastrutture della smart city (banche dati, IoT, applicazioni, ecc.) e i social network sono abbastanza devastanti per la sicurezza pubblica e la privacy privata (Ehnaghraby e Losavio 2014); da

[3] Servizio Ricerca e Studi di Cassa depositi e prestiti 2013 "*Smart City – Progetti di sviluppo e strumenti di finanziamento*" http://osservatoriosmartcity.it/smart-city-progetti-di-sviluppo-strumenti-di-finanziamento-lindaginedi-cassa-depositi-prestiti/

un altro lato, i soggetti influenzati e intimoriti dalla perdita di garanzie circa la protezione dei loro dati online, non vogliono più partecipare alla costruzione, al sostentamento e allo sviluppo dei servizi intelligenti, che sono alla base della smart city (Van Zoonen 2016).

2.a Rischi e minacce (Privacy individuale e Sicurezza generale)

Nonostante siano utili per racimolare dati, lo sfruttamento dei social network fa sorgere qualche timore circa la tutela della privacy e della sicurezza. La gente registra e condivide sui social sempre più informazioni personali (quali date di nascita, indirizzi email, numeri di telefono, domicili, foto, video ed altro) e queste possono essere usate in tanti modi, magari senza il loro consenso, a volte mettendo gli stessi utenti in pericolo. In molti casi, oltre ai meri dati sono le opinioni e le interazioni umane degli individui ad essere analizzate, ma anche in questo caso si entra nell'inquietante e nell'illegale se avviene all'insaputa degli interessati.

Al fine di consentire una migliore comprensione, è necessario chiarire la differenza tra due concetti, come quelli di privacy e sicurezza, che spesso ritroviamo insieme ma che nel contesto delle smart city assumono due significati distinti per quanto interconnessi.

La **privacy** attiene alla protezione delle informazioni personali degli individui da intrusioni illegali o potenzialmente usabili da terzi malintenzionati, nonché ai comportamenti individuali sul web e alle preferenze di navigazione (Patsakis et Al. 2015).
Sui social network la privacy consiste in:

- Anonimato: riguarda la protezione dell'identità dell'utente, cosicché non possa essere identificato su internet.
- Riservatezza dello spazio personale: si riferisce al controllo dell'acceso al profilo dell'utente, ai particolari informazioni e ai contenuti pubblicati al suo interno.
- Riservatezza delle comunicazioni: concerne la protezione di informazioni legate alla rete di connessione (indirizzo IP, localizzazione) e alle attività di navigazione dell'utente (preferenze, messaggi, collegamenti, ecc.). (Zhang e Sun, 2010).

La sicurezza si riferisce alla protezione degli utenti dei social network dalle minacce messe in atto sia da offensori interni (come altri utenti dello stesso social network) sia da offensori esterni (soggetti che non partecipano al social network ma che commettono attacchi al sistema dello stesso), che sfruttano l'inconsapevolezza e l'ingenuità delle loro potenziali vittime (Zhang e Sun, 2010).

Molte ricerche si sono concentrate sull'identificazione e la gestione dei rischi e delle minacce che affliggono i social network.
Queste possono essere divise in quattro macro categorie e successive sottocategorie (Fire et Al. 2014):

- Classiche: minacce che c'erano già agli albori di internet, e poi si sono diffuse, come gli attacchi malware, il phishing, lo spam, il cross-site scripting ecc.
- Moderne: minacce legate ai social network che mirano alle informazioni personali degli utenti o dei loro amici/collegamenti. Furto di informazioni, clonazione di identità e riconoscimento facciale sono alcuni esempi.
- Combinate: minacce ibride tra le classiche e le moderne, per avere un effetto più efficace.
- Rivolte ai minorenni: minacce rivolte esclusivamente a bambini e adolescenti, che quindi non si caratterizzano per le modalità quanto per i soggetti a cui sono indirizzate. Tra le minacce più pericolose c'è la pedofilia online, il cyberbullismo e i comportamenti rischiosi dei minori che, comunicando con estranei su internet, pubblicano informazioni private e foto sui social network.

Ogni utente dei social network è esposto anche ai rischi dalla condivisione di contenuti multimediali, molti dei quali sono indiretti o spesso ignorati dalla maggior parte di essi. A tutti è capitato di essere finiti in una foto o un video pubblicato da qualcun altro su un social network senza averne idea, e così far sapere a tutti dov'eravamo e cosa abbiamo fatto la sera prima. I rischi più pericolosi derivano da A) i contenuti multimediali, B) mancanza di politiche adeguate in materia, C) vulnerabilità della piattaforma e D) accesso aperto.

I contenuti sensibili e personali degli utenti, come file multimediali, vengono archiviati quotidianamente su social network, che sono piattaforme software vulnerabili ai bug e ai malintenzionati. Inoltre, la mancanza di politiche per normare ogni possibile problema di privacy o

la tendenza a rendere sempre più facile la procedura di registrazione per accedere ai servizi online, consentendo però la creazione di profili multipli e falsi account, complica lo scenario e rende difficile l'individuazione dei soggetti pericolosi (Patsakis et Al. 2015).

Combinate				Rivolte ai minori
Classiche		Moderne		
Spam	*Malware*	*Socware*	*Click-jacking*	*Comportamenti incauti*
Frodi	*Cross-site scripting XXS*	*Information leakage*	*Clonazione di identità*	*Cyberbullismo*
Phishing		*Interference attacks*	*Riconoscimento facciale*	*Online predators*

Fig.3 elenco delle minacce

Le minacce più peculiari e pericolose di cui sopra sono minacce rivolte ai bambini. Queste minacce, che possono essere estese agli adulti, sono solitamente causate da fattori psicologici e si verificano sia nella vita reale che nella vita online. I predatori online e gli attacchi di cyberbullismo sono in pieno boom al giorno d'oggi. Adulti o minori per soddisfare le loro fantasie e per cancellare la loro frustrazione e rabbia, spesso, molestare o intimidire sessualmente le loro potenziali vittime (Fire et Al. 2014).

I genitori non possono proteggere completamente i loro figli dall'utilizzo scorretto o incauto che potrebbero fare dei social network, in quanto le loro cui capacità di interpretazione e di autoprotezione su internet sono minime, eppure in molti casi sono gli stessi adulti a condividere informazioni personali e sensibili come foto e video in cui ritraggono ai loro figli sui social, esponendoli a rischi per la loro privacy oltre che per la loro sicurezza.

2.b Modello di relazione

Intuibilmente, c'è una forte interazione e correlazione tra percezione della privacy individuale e la percezione pubblica della sicurezza in città, queste si ripercuotono significativamente sulle dimensioni smart people e smart living, nel senso che la protezione della privacy individuale può portare alla percezione generale di sicurezza in ambienti urbani e viceversa. Il livello di influenza dei fattori umani e

sociali sui cittadini determina i loro comportamenti e le loro attitudini verso la fornitura di dati, e le questioni legate alla riservatezza hanno effetti positivi o negativi sulla sicurezza della città. Nello specifico, quando i social network vengono fruiti coscientemente, prendendosi la briga di stare attenti alla propria privacy si contribuisce al raggiungimento della sicurezza collettiva ad un livello più alto e, per estensione, al miglioramento della qualità della vita.

D'altro canto, nel circolo chiuso della smart city le attitudini individuali e la percezione della privacy sono influenzati dalla prevalenza delle percezioni pubbliche e dal livello di sicurezza e qualità della vita che si respira in città. Spesso si perde fiducia nel web per via della paura che i propri dati vengano usati in maniera impropria e pericolosa, sfiducia e sospetto creano un ostacolo ai dati in entrata e non consente l'approvvigionamento di nuove informazioni.

Una buona politica di informazione e sensibilizzazione degli utenti, nonché lo sviluppo e la diffusione di strumenti utili a proteggere la privacy delle persone, può portare a comportamenti intelligenti e responsabilizzare le persone nella partecipazione attiva nella realizzazione della smart living. Poiché il contributo dei social network è fondamentale per la smart city, occorre prestare particolare attenzione alla soluzione delle problematiche relative alla privacy e alla sicurezza che colpiscono la partecipazione sociale e quindi la vivibilità. A tale scopo, distinguiamo due passaggi principali: il primo riguarda la comprensione delle differenze tra le minacce alla privacy e alla sicurezza per identificare le vulnerabilità che affliggono gli utenti e il secondo passaggio riguarda l'adozione delle contromisure necessarie (ad es. legislazione, strumenti, ecc.) per prevenirle e gestirle.

La privacy delle persone sui social network è minacciata da rischi associati alla loro identità, al contenuto del profilo e alle informazioni sulla rete di comunicazione (Zhang et Al. 2010). Successivamente, si sono aggiunti anche i rischi che minacciano la privacy dei minori, che sono un caso speciale. Sono state analizzate le minacce alla sicurezza (Fire et Al. 2014) causate da terzi che degradano la qualità della vita, e sono state definite le loro relazioni con le minacce alla privacy citate in precedenza.

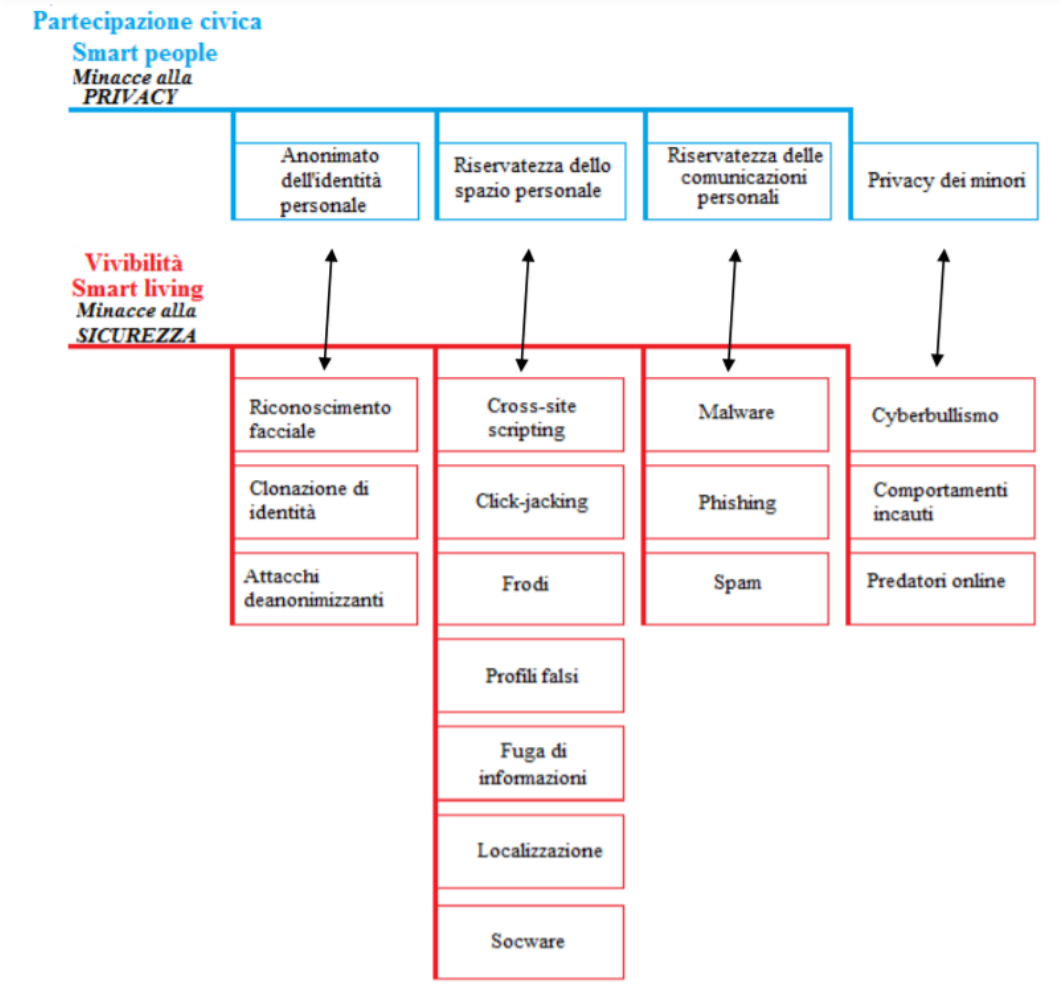

Fig.4 Modello di relazione

Il modello di relazione tra le minacce alla privacy e alla sicurezza si basa sull'analisi degli attacchi alla sicurezza, presentata da Fire che illustra in che modo questi attacchi sono correlati alle minacce alla privacy (Fire et Al. 2014). Questo studio può essere uno strumento utile per le parti interessate che utilizzano i social network come fonti di informazioni sui contesti urbani e si preoccupano della sicurezza e dell'impegno delle persone nella smart city. Ad esempio, possono sviluppare nuovi strumenti e applicazioni intelligenti e specializzate per proteggere o educare la gente sull'utilizzo corretto dei social network, contribuendo sia a smart people (ad esempio, istruzione, sensibilizzazione, coinvolgimento ecc.) che a smart living (ad es. Tutela della privacy e della sicurezza ecc.).

Conclusioni

La gestione delle minacce alla privacy e alla sicurezza dipende principalmente dal background personale degli individui (ad es. maturità, esperienze, istruzione, abilità, psicologia, consapevolezza, ecc.). Tuttavia, l'eccessiva esposizione alle TIC e ai social network, la mancanza di una normazione adeguata e il fallimento di alcuni social nel proteggere efficacemente i loro utenti, aumentano i rischi di privacy e sicurezza e gli attacchi alla smart city (Zhang e Sun 2010). Nonostante la recente normativa GDPR abbia costituito un intervento senza precedenti in materia di tutela della privacy, non si è raggiunto un livello di protezione sufficiente. Spesso agli stessi utenti non interessa cedere dati personali, lo fanno ugualmente senza accorgersene, vedendo con fastidio il dover perdere tempo per accettare condizioni di servizio a tutela della loro privacy, di fatto non modificando le loro abitudini e continuando ad esporsi inconsapevolmente a l'utilizzo che i terzi vorranno fare dei loro dati. I fornitori di servizi tarano la pubblicità sulle loro informazioni palesi, per proporgli articoli adatti alle loro esigenze e nei pressi della loro presunta collocazione geografica. Tutto questo è di dominio pubblico, perfettamente legale e largamente utilizzato dai privati a fini commerciali. La sfida è organizzare qualcosa di simile per l'erogazione di servizi pubblici, trovare un modo di elaborare le informazioni in maniera efficiente e non solamente accumularle, dal momento che mentre i privati possono venderle per il pubblico non sarebbe etico. Dopo di che si dovrebbe incentivare un piano di alfabetizzazione degli utenti per renderli consapevoli dei rischi che questi mezzi comportano e sul giusto modo di fruirne in sicurezza. Una volta sicuri dei propri comportamenti, e consci di star contribuendo a creare un ambiente più sicuro per tutti, i cittadini/utenti saranno più attivi nel produrre feedback per le amministrazioni locali e si faranno parte integrante dell'infrastruttura che rende la loro città intelligente.

BIBLIOGRAFIA

1. Ahmed BK. e Bouhorma MA. (2014). Age of Big Data and Smart Cities: Privacy Trade-Off. International Journal of Engineering Trends and Technology. https://www.researchgate.net/publication/267759778_Age_of_Big_Data_and_Smart_Cities_Privacy_Trade-Off/download
2. Bartoli A., Herńandez-Serrano J., Soriano M., Dohler M., Kountouris A. e Barthel D. 2011 Security and Privacy in your Smart City. In *Proceedings of Barcelona Smart Cities Congress*. https://smartcitiescouncil.com/sites/default/files/public_resources/Smart%20city%20security.pdf
3. Batty M. Axhausen KW. Giannotti F. Pozdnoukhov A. Bazzani A. Wachowicz M. Ouzounis G. e Portugali Y. 2012. Smart cities of the future. *The European Physical Journal Special Topics 214*, 1 (Nov. 2012), p. 481-518. http://www.complexcity.info/files/2013/08/BATTYEPJST-2012.pdf
4. Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, 5(4), 491-7 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4294750/
5. Fire M. Goldschmidt R. e Elovici Y. 2014 Online Social Networks: Threats and Solutions, *IEEE Communication Surveys & Tutorials 16*, 4, Fourth Quarter 2014, 2019-2036 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6809839
6. Giffinger R. & Gudrun H. 2010 Smart cities ranking: An effective instrument for the positioning of the cities. *ACE: Architecture, City and Environment*. IV, n. 12 February P. 7- 25 https://www.researchgate.net/publication/228915976_Smart_cities_ranking_An_effective_instrument_for_the_positioning_of_the_cities
7. Kumar e Ahmed (2016) Estimation of Traffic with Accuracy through Twitter Stream Analysis *International Journal of Innovative Technlogies* 04, 08 (July 2016), 1317-1324 http://ijitech.org/uploads/543216IJIT9948-234.pdf
8. Nam e Pardo 2011 Conceptualizing Smart City with Dimensions of Technology, People, and Institutions In *Proceedings of the 12th Annual International Digital Government Research Conference:*

Digital Government Innovation in Challenging Times
https://intaaivn.org/images/cc/Urbanism/background%20documents/dgo_2011_smartcity.pdf

9. Patsakis C., Zigomitros A., Papageorgiou A. e Solanas A. 2014 Privacy and Security for Multimedia Content shared on OSNs: Issues and Countermeasures *The Computer Journal*, Volume 58, Issue 4, 1 April 2015, Pages 518–535. https://academic.oup.com/comjnl/articleabstract/58/4/518/336057?redirectedFrom=fulltext
10. Townsend, A.M. 2013 *Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia*. WW Norton, New York https://books.google.it/books?hl=it&lr=&id=PSsGAQAAQBAJ&oi=fnd&pg=PA1&ots=xaus_y7mHx&sig=lG9M2dvygnlsLv_GwiaE-ysnfas&redir_esc=y#v=onepage&q&f=false
11. Van Zoonen, 2016 Privacy concerns in smart cities. *Government Information Quarterly*, Volume 33, Issue 3, July 2016, P. 472-480 https://www.sciencedirect.com/science/article/pii/S0740624X16300818
12. Zhang C. e Sun J. 2010 *Privacy and Security for Online Social Networks: Challenges and Opportunities. IEEE Network* 24, 4 (July-August 2010). http://www.fang.ece.ufl.edu/mypaper/network10chi.pdf
13. Anthopoulos L.G., *The Rise of the Smart City*, Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick? Public Administration and Information Technology 22, Springer International Publishing AG, 2017. DOI 10.1007/978-3-319-57015-0_2

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies