Rivista Trimestrale di SCIENZA dell'AMMINISTRAZIONE
Studi di teoria e ricerca sociale
3/2020

Smart Safe city
Criticità e prospettive sociali

Melissa Sessa
Sapienza Università di Roma

Riassunto

La diffusione e la condivisione dei dati che regolano la vita della smart city ha espresso la necessità di dare importanza alla sicurezza declinata in tutti i suoi addentellati specifici, aprendo la strada a nuovi scenari che coinvolgono sia gli attori sociali che le istituzioni che governano la città. Come per tutti i fenomeni sociali, la sicurezza può sposare molteplici definizioni a seconda dell'ottica da cui viene osservata: in questo articolo si tratterà di analizzarla nelle implicazioni sociali della sua componente "cyber".

Parole chiave: sicurezza, smart city, TIC

Abstract. *Smart Safe city. Criticalities and Social Perspectives*

The dissemination and sharing of data regulating the life of the smart city has revealed the need to consider the importance of security in all its specific aspects, paving the way for the development of new scenarios involving both the social actors and the institutions governing the city. Similarly to all other social phenomena, security can be defined in many ways depending on the perspective adopted for its observation: the aim of this article is to analyze it through the lenses of the social implications of its "cyber" dimension.

Keywords: security, smart city, ICT

DOI: DOI: 10.32049/RTSA.2020.3.05

1. Introduzione

Nel presente saggio si cercherà di dimostrare come la sicurezza, declinata in tutte le sue specificità (security, safety, certainty, privacy) sia elemento essenziale e nativo della smart city, provando a fornire una chiave di lettura che integri le precedenti prospettive che legano la sicurezza al tecnologico. E che provi a ricostruire non solo le declinazioni della sicurezza, ma in particolar modo il rapporto tra la sicurezza e la smartness. Indagare tale snodo risulta necessario essendo il campo della sicurezza sottovalutato e marginale in gran parte degli studi sulla città intelligente (Lacinák e Ristvej, 2017, p. 522).

Si vedrà come la sicurezza sia strettamente legata alla fiducia istituzionale che i cittadini ripongono nelle strutture della smart city e quanto sia proprio questo aspetto a permettere alle strutture di avere presa sull'attore sociale. Tanto più la sicurezza accresce la fiducia nelle logiche smart, tanto più tali logiche saranno incentivate e coltivate dai cittadini.

Si procederà dunque per gradi:

- Si tenterà di districarsi nelle innumerevoli accezioni che il concetto/fenomeno della sicurezza porta con sé. In virtù proprio di questa abbondanza lessicale, l'accezione di sicurezza ad essere presa in considerazione, e che farà da macro contenitore anche per le altre accezioni, sarà quella *cyber*. Sebbene all'interno della città tutte le accezioni della sicurezza abbiano grande importanza (Bauman, 2005), trovandosi davanti una città che basa la sua esistenza sulla smartness, che come si vedrà dipende in larga parte dal fattore tecnologico, si è voluta porre particolare attenzione all'accezione della sicurezza più vicina al mondo digitale.
- si cercherà, poi, di capire cosa sia e cosa voglia operativamente dire "smartness" dal momento in cui la sicurezza verrà analizzata non all'interno di una città ordinaria, ma all'interno di una smart city, che dunque presenta condizioni diverse rispetto ad una normale città.
- L' accento verrà poi posto sul ruolo ricoperto dalla fiducia all'interno della smart city. Sebbene anche le accezioni della fiducia siano innumerevoli (Gambetta, 1989; Garfinkel, 1963; Giddens, 1994), ci si terrà ad un livello di riflessione tale per cui la smart people sarà solo un attore sociale tra tanti e non il protagonista di questo saggio, e si prenderà dunque in considerazione la fiducia, solamente nella sua accezione "sistemica/istituzionale". Motivo per il quale saranno analizzate le relazioni e i processi sociali tramite i quali la fiducia (istituzionale e sistemica) spinga l'individuo a credere nelle logiche smart, a replicarle e a farle diventare routine.
- Da ultimo verranno presentati i problemi che la grande quantità di dati nelle mani delle smart city crea. Se l'obiettivo della cyber sicurezza è, oltre quello di proteggere i cittadini dagli attacchi informatici e dalla perdita di dati, e di conseguenza anche quello di coltivare, come già detto, la fiducia sistemica, si vedrà come tale obiettivo sarà messo a dura prova dall'essenza stessa della smart city. Come si può garantire la privacy personale nella smart city, che per definizione trova la sua ragion d'essere proprio nella condivisione di informazioni e dati? Una volta che i dati vengono raccolti, cosa succede? Dove vengono raccolti, e chi è responsabile per la loro violazione? Ancora, la privacy degli utenti viene violata quando i sistemi delle città

intelligenti consentono a terzi di gestire quei dati?

Negli ultimi anni, dall'era digitale in poi, il fenomeno Smart City (Hollands, 2008; Giffinger *et al.*, 2007) è diventato una pietra miliare in numerosi ambiti di ricerca, anche in ambito sociologico. La città ha infatti acquisito una sempre maggiore centralità nel processo di sviluppo economico, ambientale e non da ultimo sociale, diventando l'obiettivo principale di politiche e strategie economiche nazionali e internazionali (Harvey, 2008). È divenuta il palcoscenico ideale per la sperimentazione delle tecnologie come soluzione ai problemi presenti nella società. Soluzioni che, per garantire il loro funzionamento e l'accessibilità alle stesse, sfruttano i dati che gli attori sociali della smart city concedono loro. Quali conseguenze allora si avrebbero se questi dati venissero diffusi? Quali prospettive si presenterebbero al soggetto se le informazioni fossero violate? Entra così in gioco, nel panorama della città smart, il ruolo della sicurezza cyber. Si cercherà dunque di rispondere a queste domande che risultano essere il perno su cui si muoverà l'intero saggio.

2. La sicurezza come bisogno primario

Tutta la modernità è storia dello scambio tra libertà e sicurezza. Secoli e secoli di elaborazioni teoriche hanno dimostrato come gran parte delle azioni sociali ruotino intorno ai diversi gradi di libertà e sicurezza che riescono a raggiungere, tanto da far affermare a Castel che il mondo sociale «è stato organizzato in funzione della continua, affannosa ricerca di protezione e sicurezza» (2011, p. 16).

È bene, dunque, fare chiarezza su cosa si intenda per sicurezza e farne una breve, ma necessaria genealogia, per circoscrivere il campo rispetto a ciò di cui effettivamente tratterà questo saggio.

Ogni cultura, asserisce Malinowsky (1976), è costituita dall'insieme di risposte che la società fornisce ai bisogni dell'attore sociale, tanto da schematizzare e dividere i bisogni fondamentali e i bisogni derivati che ogni società dovrebbe soddisfare. Difatti, ad un livello analitico, ovvero necessario alla comprensione del fenomeno, la sicurezza è un bisogno primario, «anzi, essa è, se ci si passa il bisticcio, il primo dei bisogni primari» (Battistelli e

Paci, 2008, p.5), tanto che Maslow (1954) ne fa, nelle sue teorie, una componente cruciale per la qualità della vita. La sicurezza richiama la necessità di garantirsi sia gli elementi che tutelano l'integrità fisica sia una dimensione sociale stabile e sicura, la cui solvenza è propedeutica a tutti gli altri, ovvero senza la quale gli altri bisogni non hanno modo di manifestarsi. Bauman (2006) distingue tre tipi di sicurezza che sono entrati in crisi con la post-modernità: «una sicurezza (security) che ha a che vedere con la propria condizione sociale e lavorativa e si poggia sulla stabilità e affidabilità del mondo; una sicurezza (certainty) di tipo cognitivo che ha a che fare con la prevedibilità e intelligibilità dell'ambiente che ci circonda e della nostra posizione in esso; una sicurezza (safety) di tipo fisico che riguarda le minacce alla incolumità propria o dei propri beni» (Maneri, 2013, p. 288). Si tratta di dimensioni che, per quanto importanti, esulano, tuttavia, dalle finalità conoscitive del presente saggio che intende, invece, concentrarsi sulla declinazione *cyber* della sicurezza, individuandola come macro settore sotto il quale porre tutte le altre dimensioni. Nelle pagine che seguiranno, difatti, ogni volta che si parlerà di sicurezza, ci si riferirà proprio all'accezione *cyber*, senza però specificarne l'aggettivazione che risulterebbe ridondante.

Il bisogno di sicurezza, nella smart city, ha assunto tinte ancor più diversificate di quelle appena presentate. Stabilito così come la sicurezza sia il bisogno la cui soddisfazione per l'uomo è primaria, si riesce a capire anche come la richiesta di cybersicurezza proveniente dall'essenza stessa della città, ovvero dal rapporto con le TIC (Tecnologie dell'informazione e della comunicazione), richieda soluzioni che impegnino a vari livelli. A tal proposito il concetto di sicurezza digitale è un concetto molto dinamico (Braun *et al.*, 2018, p. 499), come si è visto, e che quindi implica molte specifiche lessicali, proprio in relazione al mutare della città. Ecco quindi l'idea di una città che sia "safety", ovvero che preveda che i rischi residui correlati ad una macchina o ad un impianto non superino dei valori accettabili, e di una città che sia "security" ovvero che protegga da accessi non autorizzati dall'esterno, di qualunque natura essi siano. Alle due accezioni già utilizzate da Bauman (2006) se ne aggiunge una terza, la privacy, il "right to be let alone", il diritto alla riservatezza, il diritto ad essere lasciati soli (Warren e Brandeis, 2015). Quando si parla di privacy, due sono i principi generali (Elmaghraby e Losavio, 2014). Il primo di questi ci dice che le attività

all'interno di una qualsiasi abitazione hanno il più alto livello di protezione, il secondo, di conseguenza, è che le attività che si estendono al di fuori della casa dipendono da ragionevoli aspettative di privacy. Le sfide poste alla smart city ruotano, secondo questi principi, proprio intorno alle ragionevoli aspettative di privacy, che concernono chi la città la abita e la vive quotidianamente.

Se, dunque, le logiche smart sono servite ad abbattere i consumi per far fronte alle esigenze di sostenibilità e se nonostante il digital divide hanno aumentato la platea di attori sociali in grado di fare la differenza, grazie proprio all'interiorizzazione che ha fatto di queste logiche routine, allo stesso livello, la diffusione e la condivisione dei dati, che sono condizione necessaria, ma non sufficiente per la definizione stessa di una città come smart city, hanno sollevato l'esigenza di dare importanza alla sicurezza digitale di modo tale che questa entrasse nelle prassi delle logiche smart.

Se l'obiettivo della smart city era di eliminare le differenze e creare una comunità che grazie alla fiducia nelle logiche smart ne condividesse anche i valori, a causa di una eccessiva condivisione, che è richiesta dalla smart city proprio per la sua sopravvivenza, nello scenario analizzato si sono cominciati ad affacciare problemi relativi alla sicurezza digitale. Perché dunque questo problema è legato proprio alla nascita delle smart city, e non è invece presente nella stessa maniera nelle città non smart? Banale sarebbe rispondere, semplicemente, che all'interno della smart city la tecnologia è l'elemento caratterizzante, e che proprio per questo motivo, quanto più aumenta la presenza di tecnologia nella quotidianità, tanto più è accresciuto il bisogno di cybersicurezza.

Per rispondere a questa domanda, però, in modo più preciso, ci si deve chiedere innanzitutto cosa renda una città "smart", cosa si intenda per smartness, e, ancora di più, come questa smartness possa essere legata al concetto/fenomeno di sicurezza.

Per smartness si intende un processo tecnico, tecnologico e sociale che tramite l'utilizzo delle TIC sia rivolto alla ricerca di soluzioni ottimali (De Santis *et al.*, 2014). Basandosi su questa definizione la smart city coniuga l'integrazione della tecnologia nell'ambiente naturale aumentando l'efficacia in ogni ambito del suo funzionamento al fine di raggiungere uno sviluppo sostenibile ed aumentare la qualità della vita dei propri cittadini. Allo stesso modo una *Smart Safe City* è una città che grazie all'integrazione dei due fattori appena

citati, tecnologia e sostenibilità, aumenta l'efficacia nei campi della sicurezza al fine di ridurre qualsiasi tipo di minaccia (digitale) che possa incrinare la qualità della vita dei propri cittadini.

Proprio nel momento in cui le città divengono più intelligenti, le persone possono soffrire di una serie di minacce a causa delle applicazioni smart city (Zhang *et al.*, 2017), poiché la tecnologia diventa sempre più integrata nelle attività quotidiane e nelle infrastrutture della città, facendo emergere nuove preoccupazioni. Il ruolo dell'informazione nella città porta all'attenzione come questa sia gestita, posseduta e controllata da oggetti tecnologici e come questa non sia una preoccupazione periferica. Le informazioni raccolte da sistemi intelligenti e non adeguatamente controllate possono aprire la strada alla divulgazione di dati sensibili. I requisiti di sicurezza e privacy, tra cui riservatezza, integrità, non disconoscibilità, disponibilità e controllo degli accessi dovrebbero essere soddisfatti nelle informazioni e nelle comunicazioni, così come nei mondi fisici (Zhang *et al.*, 2017).

3. Paradosso e fiducia nella smart city

Rattoppare un sistema strutturalmente insicuro e che fatichi a mantenere livelli di sicurezza essenziali ai cittadini si rivelerà molto costoso a lungo termine. Gli investimenti in sicurezza si dovrebbero, quindi auspicabilmente basare su misure preventive che aumentino la fiducia nell'intero sistema. Cosa dunque si intende in questo caso quando si parla di fiducia? Sebbene come detto le accezioni della fiducia siano innumerevoli, tante quante, almeno, le definizioni che si possono dare di sicurezza, tenendoci il più possibile ad un livello generico, la fiducia si esplicita in una *prospettiva di auto-rinforzo* (Curcuruto, Mariani e Lippert, 2009, p. 256) che pone l'attenzione su due movimenti salienti: un primo movimento di conferma (trust) e un secondo movimento di disconferma (mistrust) delle aspettative. In altre parole la fiducia si traduce nell'attesa di un comportamento della controparte, che però sia facilmente prevedibile, coordinato e collaborativo (Dwyer *et al.*, 1987). Risulta così particolarmente notevole come, nell'ambito della fiducia, a ricoprire un ruolo importante è la dimensione dell'esperienza progressiva nel tempo (Blomqvist, 1997),

dal momento in cui la creazione e distruzione delle aspettative si sviluppa in un arco di tempo t_0/t_1.

Ci si trova in questo modo davanti ad una società tecnologica che fa ricorso a degli accorgimenti per non tradire le aspettative dei propri cittadini e di conseguenza, per garantire loro fiducia. È evidente come la dimensione della fiducia a essere messa sotto la lente di ingrandimento nel binomio tra smartness e privacy, sia la dimensione sistemica/istituzionale che pone al centro del ragionamento il rapporto tra l'attore sociale e l'organizzazione sociale nel suo insieme.

Af-*fidarsi* quindi alla tecnologia in una società, oramai a spinta digitale, vuol dire con-*fidare* nel fatto che le proprie aspettative non saranno disattese dalle istituzioni, che giocano un doppio ruolo: da una parte sono il soggetto in capo al quale pende il dovere di protezione dei cittadini; dall'altra parte invece, sono il principale obiettivo di attacco alla sicurezza, proprio perché incubatore dei dati fornitegli dai cittadini stessi, per i motivi più vari.

In generale, il modo in cui gli ordinamenti reagiscono a situazioni che mettono a dura prova la fiducia e quindi la sicurezza dei cittadini, sia essa relativa alla condivisione dei dati, così anche fisica, si concreta nel ricorso a interventi di carattere emergenziale che limitano e comprimono le tradizionali libertà negative. Sebbene negli ultimi due anni si riconosce come i Paesi europei abbiano deciso di intervenire, parimenti al Patriot Act americano, per prevenire e controllare le sfide poste dalle ICT (Rubechi, 2016) e per colmare il gap tra Paesi europei e Paesi americani. Il tema della sicurezza, infatti, in questo caso, riguarda, come si è già precedentemente visto, la cybersecurity «da intendere non come mero obiettivo di "difesa" (riduzione del numero e dell'impatto degli attacchi informatici), ma come nuovo obiettivo di safety» (Gaspari, 2018, p. 101) tale da auspicare una ubiquitous city, una città onnipresente con un continuo controllo dei cittadini.

Da un lato, quindi, una città intelligente, per mandare autonomamente avanti le sue strutture, raccoglie su vasta scala dati sensibili, dall'altra parte, invece, elabora queste informazioni, manipolando e incidendo sulla vita delle persone. Proprio a causa di queste imperfezioni, la smart city diminuisce la sua presa sui cittadini, minandone la fiducia, non incoraggiando l'uso delle sue soluzioni tecnologiche.

Una città intelligente basandosi sui big data è vulnerabile alla perdita di informazioni sia per problemi interni (che l'efficienza dei sistemi dovrebbe impedire), sia da parte di aggressori esterni. Le informazioni sulla privacy di un cittadino all'interno della città intelligente possono condividere dati sulla posizione, sull'assistenza sanitaria, sull'identità, sullo stile di vita e così via. Proprio per questo, senza sufficienti protezioni nell'ambito della sicurezza e della privacy, gli utenti potrebbero rifiutarsi dall'accettare la smart city, che rimarrebbe solamente vicina ad un'idea futuristica (Zhang *et al.*, 2017, p. 123), nel senso che, qualora l'utente non registri il quantum di fiducia necessaria, non sarà spinto a credere e ad accettare la smart city.

Gli utenti della città intelligente parteciperanno ad essa solamente nel momento in cui verrà raggiunta la soglia personale di privacy e sicurezza. Questo vuol dire che ognuno degli utenti all'interno della città parteciperà alla vita della città in tempi e modi diversi, avendo differenti livelli di bisogni e quindi di riconoscimento di privacy e sicurezza. Per soddisfare la maggior parte dei cittadini, la città intelligente dovrebbe lavorare per stabilire la fiducia computazionale all'interno della rete. Con il termine "fiducia computazionale" ci si riferisce ad una fiducia numericamente calcolabile tanto da definire i livelli di fiducia che circondano le interazioni nella tecnologia dell'informazione che sono fondamentali per facilitare le interazioni e la cooperazione attraverso mezzi digitali. Stabilire la fiducia all'interno della rete intelligente fornirà la necessaria garanzia per le interazioni tra pari ed in più faciliterà l'incentivo di tutte le parti a rispettare le leggi della città intelligente. Per raggiungere il massimo dell'efficienza, e della sicurezza, allora, una città intelligente si affiderà all'automazione, a sistemi di intelligenza artificiale che gestiranno gran parte dei servizi, anche quelli di privacy.

Alla luce di quanto detto fino ad ora, sembrerebbe dunque necessario chiedersi cosa succederebbe se il sistema di automazione fosse compromesso. Senza adeguate soluzioni di emergenza le città intelligenti potrebbero mettere in pericolo cittadini e infrastrutture, proprio perché le informazioni veicolate e protette da quei sistemi di automazione, sarebbero molteplici e talmente tanto specifiche, da poter arrecare danni superiori a quelli immaginati. Dal momento in cui una rete intelligente, come abbiamo più volte visto, è per definizione interconnessa, «le dimensioni della sicurezza e della privacy avrebbero effetti a

cascata su tutto il sistema sociale» (Zhang *et al.*, 2017, p. 123, trad. nostra).

Proprio per questo è necessario che le smart city, nel momento in cui utilizzano un'intelligenza artificiale, mantengano anche un sovrintendente umano nel caso in cui debbano essere adottate delle misure di emergenza. Nell'eterna lotta tra uomo e macchina, risulta essere proprio la razionalità e resilienza umana, in questo caso, a salvare la sicurezza, e, di pari passo, la fiducia.

Poiché le vulnerabilità della privacy e della sicurezza sono amplificate dall'interconnettività della città intelligente, la fiducia degli utenti nel sistema può essere più facilmente scossa. Ciò è significativo poiché, come già detto, la fiducia dell'utente nel sistema è necessaria per l'adozione e la funzionalità delle smart city. Senza la piena partecipazione dell'abitante alla rete intelligente, le città intelligenti non possono offrire l'efficienza e la qualità della vita tanto ricercate. Inoltre, la potenziale conoscenza che le città intelligenti possono scoprire, con i loro ricchi set di dati e il pionerismo tecnologico, andrebbe persa. Quando la smart city non è protetta, ciò significa che servizi essenziali come sicurezza pubblica, governo, sanità e infrastrutture non sono protetti e questo porrà un serio problema di sicurezza generale. Si nota come, alla luce di quanto precedentemente scritto, security, safety e privacy non debbano e non possano essere trascurati quando si parla di smart city, poiché motore della fiducia dei cittadini nei dispositivi smart. Nonostante la fiducia (Giddens, 1994; Gambetta, 1989) non sia materiale al pari degli incentivi economici, rimane comunque la cartina al tornasole dei sistemi smart. Obiettivo principale della smart city permarrà sempre quello di interfacciarsi con i propri cittadini di modo tale che il fenomeno smart non rimanga solo un fenomeno ma diventi ideologia, ispiri nuovi valori e condizioni positivamente le ruotine quotidiane degli attori sociali.

Ebbene, sembrerebbe presentarsi sulla scena una nuova categoria concettuale, quella della "sostenibilità informatica", secondo la quale l'esigenza di sicurezza all'interno della smart city risponda a logiche sia immediate, sia di lungo periodo, parimenti alla sostenibilità tout court (Cohen, 2017; Donolo, 2003). Se una città può essere definita sostenibile quando «le sue condizioni di produzione non distruggono nel tempo le condizioni della sua riproduzione» (Yigitcanlar e Kamruzzaman, 2018, p. 123) allo stesso modo, la sostenibilità informatica all'interno della città dovrebbe garantire la sicurezza che la stessa abbia di

riprodursi alle medesime condizioni. Questo vuol dire che la sicurezza risulta essere elemento nativo e caratterizzante delle nuove città smart, dal momento che incrementa la fiducia del cittadino nei sistemi smart e che, come nei paragrafi precedenti si è visto, è il motore della creazione della smart city.

4. Conclusioni

Analizzate dunque le diverse accezioni della sicurezza che hanno disegnato un quadro concettuale necessario per poter parlare del binomio esistente tra la città smart e la cyber sicurezza, si è visto cosa voglia dire trattare l'argomento cybersicurezza in relazione alla smart city. È risultato difatti arduo riuscire a sciogliere il paradosso che la smart city porta con sé, perché come noto, la smart city basa la sua "smartness" soprattutto sull'utilizzo delle ICT. Tali tecnologie, per loro natura, sebbene divengano obsolete con il passare degli anni, non muoiono mai, sono sempre la base per creare dell'altro tecnologico. Questo eterno riuso del tecnologico, se da un lato protegge da problemi già verificati, dall'altro, di pari passo all'innovazione (altra importante causa), crea nuovi bias che producono nuovi problemi, nuovi comportamenti devianti. Ad ogni nuovo comportamento deviante, poi, si associa un nuovo problema di sicurezza, costringendo, dunque, la calibrazione della stessa, ogni volta che si verifichi ciò che è stato appena descritto. La presenza, quindi, di problemi di sicurezza ha dimostrato come le sfide della sicurezza delle città intelligenti vadano oltre le singole vulnerabilità tecnologiche. Le pressioni economiche provenienti dalle risorse limitate presenti nelle città possono ostacolare gli sforzi per il mantenimento della sicurezza, dal momento in cui le sfide di sicurezza all'interno del contesto cittadino smart non sono statiche bensì dinamiche, e possono moltiplicarsi nel tempo (Sen *et al.*, 2013).

Certamente, si può affermare che, alla luce di quanto detto, a preoccupare maggiormente all'interno della città smart è l'accezione della cyber sicurezza come *privacy,* dal momento che l'enorme quantità di dati personali generati e diffusi dalle TIC, unita alla capacità di «archiviarli, organizzarli e correlarli traendo dai medesimi […] nuovi dati e nuove informazioni, consente, infatti, una profilazione assai precisa tanto dei singoli individui

quanto dei gruppi sociali» (Orofino, 2018, p. 82). Per affrontare adeguatamente le sfide poste dal mantenimento della privacy individuale, il livello di privacy dovrebbe essere quantificato e mappato. Una volta compiuto questo processo è fondamentale che le organizzazioni comunichino tra loro per proteggere al meglio tutte le informazioni che viaggiano nella rete. Questo perché, essendo la smart city un sistema di oggetti tecnologicamente intelligenti e ben collegati, la sicurezza generale è intrinsecamente più difficile rispetto alla protezione dei singoli.

La sfida che si presenta, più che tecnologica, sembra essere, dunque, etica e chiama in causa nuovi diritti ancora non normati. Basti pensare che solamente nel Giugno 2019 si è dato vita al Cybersecurity Act (Commissione Europea, 2009), il Regolamento Europeo in materia, appunto, di sicurezza dello spazio del bit, che punta a rafforzare la resilienza dell'Unione agli attacchi informatici, ma che rende anche permanente l'ENISA (l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione).

Una sfida, come già accennato, etica, che chiama in causa anche categorie sociologiche sempre attuali come quella della fiducia sistemica/istituzionale. Si è osservato, difatti, come la fiducia, al pari della sicurezza, sia l'elemento che permette alla smart city di continuare a sopravvivere, e, ancora di più, l'elemento che permette di poter far diventare ideologia le logiche smart. Senza la fiducia dei cittadini, per quanto il cambiamento verso la smartness possa essere già in atto passivamente, questo non si avrà invece in modo attivo, partecipativo e interiorizzato. Difatti, senza la partecipazione e l'interiorizzazione si tratterà solo di un cambiamento parziale e non interiorizzato. In questa chiave appare evidente come «esiste la necessità di una maggiore sperimentazione e formalizzazione per stabilire una maggiore comprensione del concetto di fiducia nei contesti socio-organizzativi contemporanei secondo una prospettiva socio-tecnica che sappia interpretare sia l'insieme delle relazioni sociali che i processi di interazione con le strutture tecnologiche» (Curcuruto, Mariani e Lippert, 2009, p. 257). In altre parole, una maggiore comprensione di ciò che Giddens (1994) chiama "fidatezza nei sistemi astratti", ovvero un tipo di fiducia che non si basa sul patto non scritto tra due soggetti, di rispetto reciproco delle aspettative, ma che si basa, invece, sulla "fiducia nei sistemi esperti" cioè su una fiducia orientata verso la competenza, che, per sua intrinseca natura, è efficienza. Una fiducia che, per certi versi,

diventa fede quando l'altro al quale dare la propria fiducia sia un altro tecnologico, inconoscibile nelle sue versioni più complesse.

In definitiva, dunque, la domanda che ci si dovrebbe porre quando ci si trova davanti alla gestione della sicurezza della città da parte di attori tecnologici è, tanto antica, quanto estremamente attuale: chi controlla il controllore? Una domanda già posta nella VI Satira da Giovenale, che, essendo vissuto nei primi decenni dopo la nascita di Cristo, non avrebbe potuto conoscere la cybersicurezza, ma che tinteggia il problema a monte di tutta la questione: chi o quali modi si potrebbero inventare per provare a risolvere i possibili danni arrecati da coloro che la sicurezza la dovrebbero gestire e garantire? La risposta non sembra potersi incardinare in questo breve saggio, che ha solamente voluto fornire una chiave di lettura, seppur ridotta, sull'ambito della sicurezza all'interno delle smart city, senza voler in alcun modo contrastare con le altre chiavi di lettura. Ma certamente è proprio nella risposta a quella domanda, declinandola nel classico binomio che oppone l'uomo alla macchina, che si potrebbe provare a trovare una definitiva soluzione ad un problema che oramai affligge in larga parte le città smart.

Bibliografia

Braun T., Fung B.C.M., Iqbal F., Shah B. (2018). Security and Privacy Challenges. *Sustainable Cities and Society,* 39: 499. DOI: 10.1016/j.scs.2018.02.039.

Battistelli F., Paci M. (2008). Sicurezza e insicurezza nella società contemporanea. *Sociologia e ricerca sociale*, 85: 5.

Bauman Z. (2005). *Fiducia e Paura nella città*. Milano: Mondadori.

Bauman Z. (2006). *Paura liquida*. Roma: Laterza.

Blomqvist K. (1997). The Many Faces of Trust. *Scandinavian Journal Management* 13, 3: 271. DOI: 10.1016/S0956-5221(97)84644-1.

Castel R. (2011). *L'insicurezza sociale. Che significa essere protetti?* Torino: Einaudi.

Cohen S. (2017). *The Sustainable City.* New York: Columbia University Press.

Commissione Europea (2019). *The EU Cybersecurity Act*. Testo disponibile all'indirizzo

web: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (11/04/2020)

Curcuruto M., Mariani M.G., Lippert S.K. (2009). La fiducia nei sistemi informatici. Contributo alla validazione italiana di un modello. *Psicologia sociale*, 2: 255. DOI: 10.1482/30126

De Santis R., Fasano A., Mignolli N., Villa A. (2014). Il fenomeno smart cities. *Rivista Italiana di Economia Demografia e Statistica*, 68, 1: 143.

Donolo C. (2003). *Il distretto sostenibile. Governare i beni comuni per lo sviluppo.* Milano: FrancoAngeli.

Elmaghraby A.S., Losavio M.M. (2014). Cyber Security Challenges in Smart Cities: Safety, Security and Privacy. *Journal of Advance Research*, 5, 4: 491. DOI: 10.1016/j.jare.2014.02.006.

Gambetta D. (1989). *Le strategie della fiducia.* Torino: Einaudi.

Garfinkel H. (1963). A Conception of and Experiment with "Trust" as a Condition of Stable Concerned Action. In Harvey O.J., a cura di, *Motivation and Social Interaction. Cognitive Determinants.* New York: The Ronald Press.

Gaspari F. (2018). *Smart city. Agenda urbana multilivello e nuova cittadinanza amministrativa*. Napoli: Editoriale Scientifica.

Giddens A. (1994). *Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo*. Bologna: il Mulino.

Giffinger R., Fertner C., Karmar H., Kalasek R., Pichler-Milanovic N., Meijers E. (2007). *Smart cities. Ranking of European medium sized cities.* Testo disponibile all'indirizzo web: http://www.smart-cities.eu/download/smart_cities_final_report.pdf (11/04/2020).

Harvey D. (1998). *L'esperienza urbana*. Milano*:* Il Saggiatore.

Hollands R. (2008). Will the Real Smart City Stand Up? Intelligent, Progressive, or Entrepreneurial? *City,* 12, 3: 303. DOI: 10.1080/13604810802479126.

Lacinák M., Ristvej J. (2017). Smart City Safety and Security. *Procedia Engineering,* 192: 522. DOI: 10.1016/j.proeng.2017.06.090.

Malinowsky B. (1976). *Freedom and Civilization*. Santa Barbara: Greenwood Press.

Maneri M. (2013). Si fa presto a dire «sicurezza». Analisi di un oggetto culturale. *Etnografia e ricerca qualitativa,* 2: 283. DOI: 10.3240/74120.

Maslow A. (1954). *Motivation and Personality.* New York: Harper & Row Publishing.

Orofino M. (2018). Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione. *MediaLaws*, 2: 82. Testo disponibile all'indirizzo web: http://www.medialaws.eu/wp-content/uploads/2019/05/RDM-2-2018.pdf (11/04/2020).

Rubechi M. (2016). Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi). *Federalismi.it*, 30 novembre. Testo disponibile all'indirizzo web: https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=32831&dpath=document&dfile=30112016143102.pdf (11/04/2020).

Warren S.D., Brandeis L. D. (2015). *The Right to Privacy*. New Orleans: Quid Pro LLC.

Yigitcanlar T., Kamruzzaman M. D. (2018). Does Smat City Policy Lead to Sustainability of Cities? *Land Use Policy*, 73: 49. DOI: 10.1016/j.landusepol.2018.01.034.

Zhang K., Ni J., Yang K., Liang X., Ren J., Shen X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, 55, 1: 122. DOI: 10.1109/MCOM.2017.1600267CM.