

Ms.WEAS per la prevenzione del crimine urbano. Idee per migliorare la protezione della propria persona

Vittoria Porta, Ardalán Mehraram

20 Dicembre 2019

Indice

1	Introduzione	2
2	Come nasce l'idea di Ms.WEAS	2
2.1	I <i>competitor</i> presenti sul mercato internazionale	3
3	Le caratteristiche di Ms.WEAS: come è fatto	3
3.1	Value proposition	4
3.1.1	Il modello di business basato su una piattaforma	4
4	La creazione di una <i>crime map online</i>	5
4.1	Devianza e previsione: le teorie sociologiche a sostegno della prevedibilità delle azioni criminose.	6
4.2	L'origine della <i>crime map</i>	6
4.3	Il <i>crime mapping</i> oggi.	7
4.3.1	Il caso italiano	8
4.4	I limiti al <i>crime mapping</i> e possibili miglioramenti	8
5	Tra tecnologia, etica e tutela della <i>privacy</i>	9
5.1	Il questionario	9
5.1.1	I risultati	10
5.2	Etica, <i>privacy</i> e innovazione: riflessioni	12
5.3	La geolocalizzazione e la biometria: utilizzo e regolamentazione	13
5.3.1	Il riconoscimento facciale	14
6	Conclusioni	15

1 Introduzione

Immaginate come sarebbe vivere in un mondo senza crimini, o meglio, come sarebbe vivere in un mondo in cui i crimini possono essere previsti ancor prima che i criminali abbiano la possibilità di commetterli. In molti potrebbero pensare che si stia parlando di fantascienza, ma i dipartimenti di polizia che utilizzano l'analisi predittiva per la prevenzione del crimine sono attivi nelle nostre città ormai da diversi anni.

Il progetto è volto ad analizzare l'idea innovativa della creazione di un dispositivo portatile in grado di segnalare un qualsiasi tipo di aggressione direttamente alle forze dell'ordine ed agli utenti oltre al desiderio di migliorare il tema della sicurezza personale.

Nel primo capitolo viene discusso come nasce l'idea di Ms.WEAS e le sue caratteristiche, con un *focus* sui principali *competitor* presenti sul mercato internazionale.

Successivamente vengono analizzate le caratteristiche e le funzionalità del dispositivo in sé, fornendo un'idea concreta su come sviluppare la parte *hardware*.

Il terzo capitolo si preoccupa di analizzare la costruzione della mappa del crimine, cominciando con uno studio della letteratura sul tema, fino ad arrivare ai *tools* che oggigiorno vengono utilizzati dalle forze dell'ordine come strumenti di visualizzazione dei reati. Una particolare attenzione viene data ai limiti del suo utilizzo e ai miglioramenti che Ms.WEAS offre.

L'ultimo affronta il tema della *privacy* dal punto di vista etico e legale, prendendo spunto dai risultati ottenuti da un questionario *online*.

2 Come nasce l'idea di Ms.WEAS

Oggigiorno, le città sono in continua espansione. Assistiamo con un ritmo sempre più rapido ad un ampliamento dell'area urbana, che diventa mano a mano un grosso sistema di centri abitati interconnessi. Pertanto, urge implementare delle nuove tecnologie che siano in grado di proteggere e affiancare il cittadino, che spesso si ritrova ad essere

insicuro a percorrere le strade del proprio quartiere.

Realmente parlando è impossibile pensare che chiunque venga costantemente seguito da una guardia del corpo e d'altra parte, risulta difficile essere completamente fiduciosi nel sistema di tutela dell'incolumità del cittadino offerto dalle forze dell'ordine.

In un mondo governato dalle ICT's, si sta tentando di trovare una soluzione efficace, in grado di proteggere le vittime e intervenire tempestivamente in caso di aggressione. In un mondo costantemente connesso è ancora molto difficile riuscire ad "attirare l'attenzione" in caso di pericolo e a lanciare un allarme che non rimanga inascoltato dalla comunità. Secondariamente, è complicato gestire il panico della vittima che subisce un' aggressione, ad esempio al giorno d'oggi, esistono diverse applicazioni *mobile* che si occupano di effettuare una chiamata di emergenza qualora ce ne fosse bisogno, ma rendono l'utente dipendente dallo *smartphone* e da tutti i problemi che ne derivano: *bugs*, difficoltà nel recuperare il dispositivo e tremori causati dalla sensazione di paura.

L'idea di Ms.WEAS nasce dal desiderio di creare un apparecchio unico, indipendente e automatico, come un *wearable*, capace di comprendere il tentativo di un' aggressione. Esso è composto da un insieme di sensori, ognuno con una propria funzionalità: chiamata di emergenza, registrazione di suoni e immagini, geolocalizzazione...

"Il mercato *hi-tech* da polso sta vivendo uno dei momenti più floridi con la vendita di *smartwatch* che sfiora più del 29% nel secondo trimestre del 2019. Le consegne dei dispositivi *hi-tech* che si portano al polso sono cresciute del 28,8% su base annua, arrivando a quota 34,2 milioni di unità" ¹. Ms.WEAS potrebbe dunque entrare a far parte di un mercato in crescita, con la differenza che il suo obiettivo è finalizzato alla protezione dell'incolumità di chiunque lo indossi; è un vero e proprio dispositivo anti-aggressione.

In conclusione è possibile affermare che per sviluppare una tecnologia nuova e che sia innovativa, occorre: rendere il dispositivo portatile indipendente dallo *smartphone*; renderlo indossabile in ogni si-

¹Fonte dei dati: <https://www.digitalic.it/economia-digitale/smartwatch-e-smartband-mercato-2019>

tuazione ed evitare che abbia un display. Queste caratteristiche renderebbero Ms.WEAS uno strumento completamente differente dagli *wearables* attualmente in commercio.

2.1 I *competitor* presenti sul mercato internazionale

Per sviluppare l'idea concreta che sta alla base del progetto, è stato necessario compiere un'analisi di mercato per comprendere quali sono le aziende concorrenti attualmente attive nell'arena internazionale.

Le prime cinque aziende mondiali per la produzione di dispositivi tecnologici da polso sono: Xiaomi, Apple, Huawei, Fitbit e Samsung che detengono il 65,7% del mercato.²

Oltre ai grandi colossi della tecnologia, sono presenti alcuni *brand* e *start-up* che si occupano nello specifico di sicurezza personale, ad esempio E24WOMAN, che durante quest'anno ha dato vita ad un prototipo di bracciale, composto da un sensore che rileva il tentativo di aggressione e un modulo *GSM* per le chiamate di emergenza collegato a un tasto di allarme. E' possibile effettuare tre tipi di chiamate: alle forze dell'ordine; all'ambulanza e al soccorso stradale che verranno gestite da una centrale operativa privata la quale le distribuirà ai servizi competenti. Lo strumento pensato dalla *start-up*, non ancora sul mercato, ha il vantaggio di essere indipendente dall'uso dello *smartphone*, ma la centrale operativa privata potrebbe avere un alto costo di gestione.

SHECALL è vincitrice di diversi premi per *start-up*, finanziata da Amazon e ha sperimentato l'idea di uno strumento rivolto soprattutto ad un pubblico femminile. Il dispositivo è dipendente dallo *smartphone*, poiché invia l'allarme solo tramite SMS alle persone selezionate dall'utente e non è in grado di visualizzare autonomamente le forze dell'ordine. Anch'esso non è ancora in vendita.

In materia di *app mobile* è stata sviluppata *SECURE ITALY*, un'applicazione in grado di gestire le chiamate di emergenza tramite una centrale operativa. Ha un grande potere di mercato, ma non

offre nessun tipo di dispositivo *wearable*.

Infine, il colosso italiano che opera nel settore elettronico e della sicurezza, Beghelli, ha ideato un apparecchio dal nome *SALVAVITAGO WRIST-BAND*, che si presenta sotto forma di bracciale salvavita. Il dispositivo è dipendente dallo *smartphone*, che viene accoppiato tramite bluetooth e la chiamata di allarme viene attivata premendo un tasto sul bracciale.

Concludendo, è possibile affermare che tutti i prototipi fin'ora idealizzati hanno in comune l'idea di tutelare le vittime da una possibile aggressione e tentano di semplificare l'atto della chiamata di emergenza inserendo l'opportunità di inviare l'allarme premendo solo un bottone. Alcuni di questi si presentano come dispositivi indossabili, il che è comprensibile, soprattutto se si pensa ai trend tecnologici in voga al giorno d'oggi. Ciò che non viene preso in considerazione è la potenzialità di creare una vera e propria rete di utenti, che formino una *community* per una città più sicura.

3 Le caratteristiche di Ms.WEAS: come è fatto

A seguito dello studio effettuato sui prototipi idealizzati dai *competitor*, si è giunti all'idealizzazione di un dispositivo in grado di racchiudere tutte le migliori peculiarità delle tecnologie presenti: dovrà essere un *wearable* elegante non ingombrante e facile da indossare.

Il nome del progetto è Ms.WEAS (acronimo di *We Are Safe*) che vuole indicare la volontà di essere al sicuro, di essere protetti da una "supereroina" che accompagna ogni cittadino in qualsiasi occasione. "Noi siamo al sicuro" rende l'idea di unione tra le persone tramite un *network* connesso che si preoccupa di aiutare gli altri utenti e di migliorare il lavoro dei poliziotti.

Il progetto si compone di due parti, in primo luogo, una componente *hardware*, ovvero il dispositivo in sé; in secondo luogo, una componente *software*, supportata da un'interfaccia *mobile*, la quale fornisce un ulteriore servizio fondamentale: la visualizzazione di una mappa del crimine in tempo reale

² *ibidem*

costruita con i dati raccolti dai dispositivi degli utenti.

Per quanto riguarda il lato *hardware* questo è composto da:

- un sensore d'urto: il chip viene attivato ogni qual volta venga rilevato un urto inconsueto (il microcircuito è già presente negli strumenti di sussidio agli anziani). Dal momento dell'attivazione il dispositivo sarà in grado di effettuare una chiamata di allarme entro 15 secondi dall'urto, fuorché l'utente stesso non disattivi la funzione.
- un sensore di impronte digitali: l'equivalente di un tasto fisico, che avrà la funzione di disattivare l'allarme e impostare i diversi livelli.
- un allarme sonoro: quando viene rilevata l'aggressione il dispositivo emetterà suoni dissuasivi.
- un registratore ambientale: questo chip ha una funzione di scatola nera, ovvero restituisce i dati riguardanti l'aggressione che potranno poi essere utilizzati come prove durante un eventuale processo e potranno migliorare i procedimenti burocratici di denuncia da parte degli agenti di polizia.
- GPS/GSM: al momento dell'aggressione il dispositivo attiverà la localizzazione dell'utente visibile a tutta la *community*.
- uno standard bluetooth: permette di accoppiare il proprio bracciale allo *smartphone*.

In questo modo è stato possibile ipotizzare uno strumento che sia indipendente dallo *smartphone* (nell'eventualità che l'utente non ne possieda uno o abbia la batteria scarica) e che riesca ad agire comunque autonomamente. Inoltre, l'utente sarà in grado di impostare il grado di controllo del sensore d'urto in base al tipo di percorso che andrà ad affrontare: ad esempio, nel caso in cui l'utente si senta poco sicuro potrà attivare il controllo massimo, il quale renderà più sensibile il sensore e scatterà al primo urto non calcolato; contrariamen-

te l'utente potrà selezionare il controllo minimo, il quale prevede l'attivazione manuale dell'allarme.

La parte *software* viene sviluppata in correlazione allo sviluppo dell'interfaccia che visualizza la mappa del crimine *online*, aggiornata in tempo reale: al momento dell'aggressione sarà raffigurata l'icona direttamente sulla mappa disponibile a tutti gli utenti e ciò permetterà alla vittima di essere collegata con tutta la comunità.

L'utente tramite una *chat* inserita nell'interfaccia della mappa potrà essere in grado di recensire la strada che sta percorrendo, in modo da segnalare situazioni sospette.

Ulteriori sviluppi potrebbero comprendere l'eventualità di suggerire all'utente il percorso più sicuro da intraprendere data la destinazione desiderata, tramite una raccolta di dati e tecniche di analisi predittiva (*machine learning*, capaci di comprendere il livello di pericolosità di ogni strada su base storica).

3.1 Value proposition

In sintesi vengono esposti i punti di forza dello strumento presentato in questo paper: in primo luogo, è un progetto di (*business platform based*, poiché caratterizzato da una visione prettamente (*social* la quale richiede una comunità di utenti vasta per funzionare nel modo ottimale. Se il modello dà il risultato desiderato sarà possibile tagliare i costi di gestione di una centrale operativa privata, poiché gli utenti della comunità saranno in grado aiutare la vittima in tempo reale.

Secondariamente, la creazione di una (*crime map* aggiornata in tempo reale tramite i dati raccolti dai dispositivi).

3.1.1 Il modello di business basato su una piattaforma

Un *business model platform based* o conosciuto anche come *MSP multi sided platform*, viene definito come un insieme di "tecnologie, prodotti o servizi che creano valore principalmente consentendo interazioni dirette tra due o più gruppi di clienti o partecipanti³"

³<https://www.innovationtactics.com/platform-business-model-complete-guide/>

Solitamente, le interazioni avvengono tra la parte del mercato che rappresenta l'offerta e la parte della domanda e in questo caso le piattaforme non fanno altro che favorire l'incontro tra le parti e migliorare lo scambio del bene o del servizio.

La forza di questo tipo di modello di business risiede nel fatto che le tecnologie digitali permettono ad attori diversi, interni ed esterni all'organizzazione, di creare e consumare valore attraverso una piattaforma che li metta in comunicazione. Colui che possiede la piattaforma rende possibile l'utilizzo della propria tecnologia per creare prodotti o servizi nuovi e per aprire canali di comunicazione. Questo modello porta ad un cambiamento che è ora legato "alla capacità di attrarre entrambe le tipologie di utenti, chi crea e chi consuma innovazione, dando vita a un "effetto rete" che alimenti il circolo virtuoso su cui si basa il successo di una piattaforma"⁴.

Lo strumento presentato in questo progetto è costituito da una parte software che si basa sulla creazione di una mappa del crimine *online* supportata da una *community*.

L'ecosistema in cui si sviluppa la parte software del progetto formato dall'interazione di due protagonisti fondamentali: gli *users*, ovvero i normali cittadini che segnalano gli atti criminosi e le forze dell'ordine, che possono visualizzare gli avvisi in tempo reale.

Tutti coloro che possiedono il *wearable* anti aggressione, potranno, da una parte, tramite la piattaforma visualizzabile *online*, segnalare qualsiasi tipo di crimine, accedendo con il proprio profilo; dall'altra, il braccialetto segnalerà automaticamente l'aggressione in tempo reale.

Così facendo il numero di *users* attivi della comunità saranno in grado di fornire dati continuamente aggiornati e visualizzabili, in stile puramente *social*.

Le forze dell'ordine saranno in grado, dai loro centri di controllo, di visualizzare la mappa e le segnalazioni dei cittadini e ciò permetterebbe:

1. Uno smaltimento più efficiente delle chiamate ai centralini di pronto intervento.
2. Segnalazioni più veloci e indipendenza dal telefono cellulare.

3. Interventi delle forze dell'ordine mirati, rapidi e coordinati.
4. Possibilità di avere sotto controllo una panoramica digitale delle zone a più alto rischio criminoso.

Ulteriori studi potrebbero portare all'implementazione del dispositivo tramite la possibilità di immagazzinare i dati che lo strumento raccoglie (per mezzo dei sensori, ad esempio) e di depositarli in un cloud. In questo modo le informazioni raccolte potrebbero essere direttamente disponibili come prove utilizzabili durante un ipotetico processo o semplicemente all'atto della denuncia del fatto criminoso.

Ciò comporterebbe una sostanziale semplificazione e velocizzazione della burocrazia.

4 La creazione di una *crime map online*

La componente *software* del progetto prevede la creazione di un sistema di mappatura del crimine online aggiornato in tempo reale con i dati derivanti dalle segnalazioni di atti criminosi dagli utenti. La costruzione e visualizzazione di mappe che segnalano atti devianti all'interno di un'area urbana è sempre stato di fondamentale aiuto alla polizia: a partire da una semplice cartina della città appesa nell'ufficio del capo delle indagini, su cui venivano segnalate le aree a maggior rischio con una puntina in metallo; fino ad arrivare alla raffigurazione di una mappa digitale. Questo passaggio è stato permesso dall'attento lavoro degli agenti incaricati di raccogliere i dati relativi alle denunce, e di trascriverli all'interno di dataset strutturati. Questo lavoro ha consentito lo sviluppo di vere e proprie tecniche e modelli predittivi statistici in grado di prevedere con la maggiore accuratezza possibile, le azioni criminose.

Si sviluppa in questo modo il concetto di *crime mapping* che è l'analisi della distribuzione spaziale di reati attraverso l'applicazione di tecniche statistico-geografiche che permettono una mappatura innovativa/

⁴<https://www.zerounoweb.it/cio-innovation/sono-platform-based-i-modelli-di-business-sostenibili-per-gestire->

patura e una tematizzazione fatta sulla base di considerazioni criminologiche.⁵

4.1 Devianza e previsione: le teorie sociologiche a sostegno della prevedibilità delle azioni criminose.

Lo sviluppo della *crime science* fonda le sue radici nelle diverse teorie sociologiche della devianza, da quella che riconduce i comportamenti criminosi alle caratteristiche fisiche e biologiche degli individui, fino ad arrivare alla “teoria della tensione” di Robert Merton.

Un ulteriore passo avanti nella comprensione della devianza è stato fatto grazie a due studiosi della scuola di Chicago, Clifford Shaw e Henry McKay, i quali svilupparono la teoria della sotto cultura che si inserisce nella corrente della criminologia ambientale.

Nel 1929 condussero un'imponente ricerca sociale a Chicago dividendo in cinque zone concentriche la città, calcolarono “il tasso di delinquenza”, ovvero il rapporto fra il numero degli autori di reati residenti in un'area e il totale della popolazione della stessa. Notarono come il valore del tasso diminuisse man mano che ci si allontanava dal centro città. A distanza di tempo i valori non subivano cambiamenti, nonostante il ricambio di generazione. Sostennero allora che in alcuni quartieri vi erano norme e valori favorevoli a certe forme di devianza e questo patrimonio culturale veniva trasmesso ai nuovi arrivati tramite la formazione di bande e piccoli gruppi.⁶

Successivamente è stata proposta la teoria della *routine activity theory*⁷ che si focalizza sullo spazio e sulle condizioni in cui si realizza un'azione criminosa.

Poiché si compia un reato devono verificarsi tre condizioni in un determinato momento e luogo: deve essere presente un “bersaglio” adatto; non deve essere presente un “controllore” idoneo determinato a prevenire l'evento criminale e deve essere presente un “potenziale aggressore” motiva-

to a compiere l'atto criminale.⁸

La teoria porta alla luce considerazioni interessanti riguardo i soggetti coinvolti in un reato e sottolinea come infatti, i bersagli, ovvero le vittime, abbiano molto spesso delle caratteristiche comuni e come i potenziali aggressori agiscono razionalmente e preliminarmente facendo considerazioni riguardo al luogo e al bersaglio da colpire.

E' importante sottolineare questo punto, poiché la mappa del crimine ha il compito di visualizzare le zone ad alto rischio di delinquenza e a sostegno di quest'ultima teoria si afferma che la criminalità non si estende in modo uniforme su tutta l'area urbana, ciò comporta la comparsa di cosiddette aree calde ad alto rischio di delittuosità *hot spots*, che emergono a diverse ore del giorno e in diversi giorni della settimana.

Facendo leva su questo concetto vengono elaborati i fondamenti dei metodi di polizia predittiva e viene dunque giustificato il motivo per cui sia essenziale la creazione di una mappa urbana digitale che visualizzi i crimini in tempo reale.

4.2 L'origine della *crime map*.

L'origine della costruzione della mappa del crimine risale circa al XIX secolo ed è da ricercarsi nello studio portato avanti da tre scienziati esperti in criminologia, Guerry; Quelet e Mayhew.

Nella sua opera “*Statistica morale*”, Guerry, ha prodotto una “cartografia sociale della criminalità”, accoppiando i dati demografici alle statistiche dei reati, creando così una mappa dei atti criminali commessi nei diversi dipartimenti francesi. Successivamente, Mayhew, percorrendo i quartieri più poveri di Londra e intervistando gli abitanti, ha classificato il territorio trasportando i risultati su una mappa urbana.

Quello di Mayhew risulta essere così, il primo e vero lavoro di *crime mapping* con la connotazione odierna.⁹

⁵A.Ummarino, *Una introduzione ai software per il crime mapping*, p.148

⁶Bagnasco A, Barbagli M, Cavalli A, *Corso di sociologia*, 2012, p. 190

⁷La teoria delle attività routinarie è stata sviluppata da Felson, M. and R.V. Clarke nel 1998

⁸<https://www.fisu.it/2017/05/08/teoria-delle-attivita-routinarie-2/>

⁹I. Fasolino, F.Coppola, M.Grimaldi, *La sicurezza urbana degli insediamenti. Azioni e tecniche per il piano urbanistico*, 2018

Durante i primi anni del novecento anche gli esponenti della scuola di Chicago, dopo aver proposto la "teoria della sotto cultura" hanno elaborato un modello di mappa del crimine, prendendo come esempio quelle sviluppate dai loro predecessori. Essi hanno circoscritto una zona urbana sulla quale hanno calcolato il tasso di delinquenza e hanno poi rappresentato il risultato della loro indagine attraverso quattro mappe differenti, in base ai casi, ai tassi di delinquenza, mappe radiali e mappe zonali, mostrando la distribuzione geografica dei reati nell'area interessata.

Questa venne poi analizzata e correlata ai fattori ambientali capaci di favorire i comportamenti devianti.¹⁰

La previsione e la classificazione, risultano dunque essere entrambi concetti fondamentali nella scienza comportamentale, criminologica e infine nel processo decisionale in materia di giustizia penale.

La previsione è importante per prevenire i problemi relativi ai comportamenti devianti, mentre, la classificazione, si basa sul raggruppamento di persone in classi che sono simili e vicine tra loro. E' usata per cercare di raggiungere il massimo livello di omogeneità tra gruppi e massimo livello di eterogeneità tra gruppi differenti.

La classificazione in criminologia viene utilizzata in riferimento a un metodo di categorizzazione di soggetti "tipo"; mentre la previsione si riferisce ad una valutazione di certi comportamenti futuri attesi da parte di una persona ¹¹.

4.3 Il *crime mapping* oggi.

La costruzione e la visualizzazione delle mappe avviene oggi, tramite i GIS, strumenti di analisi e rappresentazione geografica (Geographic Information System).

Essi permettono l'acquisizione, registrazione, analisi, visualizzazione, restituzione, condivisione e presentazione di informazioni derivanti da dati geografici.

Tutte gli episodi a livello internazionale in ambito di polizia predittiva che sono stati sperimentati

¹⁰ *ibidem*

¹¹ M. Tonry, *Prediction and Classification: Legal and Ethical Issues*, in Crime and Justice, Vol. 9, Prediction and Classification: Criminal Justice Decision Making (1987)

fino ad ora condividono un modello che prevede la visualizzazione dei reati tramite una mappa urbana. In particolare le stesse mostrano le zone ad alto rischio di criminalità e permettono agli agenti di pattugliare le aree più efficientemente.

Le *crime maps* non sono strumenti utili solo alle forze dell'ordine, bensì anche ai cittadini, i quali devono e possono essere informati circa il rischio che potrebbero correre frequentando determinati quartieri a determinate ore del giorno.

Esistono infatti, aziende come CrimeMapping.com, CrimeReports e RAIDS Online che offrono prestazioni di mappatura urbana del crimine online: tramite questi servizi i cittadini sono in grado di controllare online quali sono le aree e i quartieri più a rischio e modificare il proprio comportamento evitando i punti caldi.

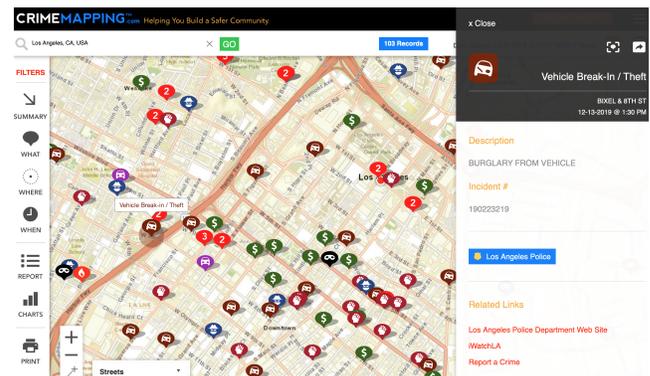


Figura 1: Crimemapping della città di Los Angeles, CA

La figura 1 mostra la schermata della mappa di *CrimeMapping.com* e come si può notare viene segnalata la localizzazione di tutti i crimini relativi alla zona selezionata con in allegato una descrizione della tipologia di reato.

Il sito è stato sviluppato da TriTech Software System con lo scopo di aiutare i poliziotti a fornire informazioni sulle attività criminali dei diversi quartieri. Come si può leggere dal loro sito, "il nostro obiettivo è aiutare i dipartimenti di polizia a ridurre il crimine attraverso una cittadinanza meglio informata". ¹²

I dati vengono raccolti sistematicamente tramite diverse agenzie grazie al sistema di registrazione di

ogni dipartimento e vengono poi visualizzate tramite l'interfaccia web, i dati sono sempre verificati e anonimizzati, al fine di garantire la protezione della *privacy*.

D'altro canto, per esempio, Spot Crime (un altro sito di *crimemapping online*), utilizza i dati dei reati su una base cartografica fornita da Google Maps. Le mappe sono interattive e intuitive e forniscono anch'esse i dettagli dell'azione criminosa, sia attraverso una simbologia, sia tramite una scheda informativa.

Come si è potuto comprendere fin'ora le esperienze più significative sono state registrate negli Stati Uniti e in Inghilterra, dove lo strumento di mappatura è utilizzato frequentemente, sia dalle forze di polizia, sia dai cittadini.

4.3.1 Il caso italiano

In Italia, la pratica di mappatura del crimine è ancora poco diffusa, per l'appunto sono state costruite e messe a disposizione dei cittadini solo due mappe: la prima è stata elaborata dal Sole24ore, dopo una raccolta dei dati relativi alle denunce dell'anno precedente. Sulla mappa viene visualizzata la distribuzione dei reati per provincia e viene realizzata una classificazione delle azioni criminose in base alla loro tipologia.

In secondo luogo, sono state fornite ai cittadini delle mappe di natura puntuale, create utilizzando lo strumento Google MyMaps che fornisce la localizzazione e una breve descrizione dell'accaduto. Purtroppo questa mappa non è disponibile per tutte le città italiane.

D'altro canto è stato sviluppato a Milano il primo *software* italiano di polizia predittiva, dal nome KeyCrime on lo scopo principale di ridurre il numero di rapine nelle farmacie della città metropolitana del Nord Italia.

Il modello di previsione dei crimini che è stato realizzato, tenta di ricercare le serie criminali, partendo dall'assunto teorico che spiega come i criminali abbiano dei comportamenti abituali, i quali rendono le loro azioni future parecchio prevedibili.

Il software esamina circa 11.000 bits di informazioni circa le rapine (data, ora, luogo, tipo di attività commerciale colpita...), circa i criminali (età stima-

ta, altezza, struttura corporea, colore dei capelli, della pelle, caratteristiche del vestiario...), circa le armi utilizzate durante il colpo (modello, marca, tipo di arma...) e circa il veicolo utilizzato dal criminale.¹³

Tutte le rapine vengono visualizzate sulla mappa e categorizzate in base al loro grado di similarità, e a seguito dell'analisi delle caratteristiche comuni, il modello esegue una previsione sulla farmacia che ha più probabilità di essere vittima del prossimo attacco. La mappa non risulta essere disponibile e consultabile ai cittadini.

4.4 I limiti al *crime mapping* e possibili miglioramenti

Per quanto riguarda il caso italiano, uno dei limiti principali, rispetto alle esperienze britanniche e statunitensi, risiede nel fatto che non esiste una sufficiente disponibilità di dati e ciò condiziona fortemente il risultato finale di una buona visualizzazione. Le informazioni utilizzate per la costruzione della mappa, vengono solamente dedotte dagli articoli giornalistici e denunce fatte agli agenti; inoltre la mappatura del territorio non viene fatta sistematicamente, ma solo di anno in anno. Non risulta essere un problema solamente circoscritto al caso italiano, ovvero la quantità e la qualità dei dati disponibili è un problema che si riferisce a tutte le mappe del crimine che vengono create dalle forze di polizia, oltre al fatto che l'attendibilità dei risultati prodotti è fortemente condizionata dalle competenze di chi si appropria ad un'analisi di questo tipo.

Trattandosi di eventi criminali, le maggiori fonti di dati sono le forze dell'ordine e per questo motivo è possibile incappare in pratiche di "polizia sporca", ovvero, condotte viziate e comportamenti illeciti immorali e tendenziosi da parte degli agenti che influiscono direttamente sull'efficacia dei modelli. Si tratta di azioni discriminatorie da parte dei poliziotti verso una determinata etnia, gruppo religioso o cultura, che viene segnalata come pericolosa.

Conseguentemente, il quartiere dove questa si stanza risulta essere zona a rischio criminalità elevata e i dati che vengono raccolti durante i pattugliamenti o in seguito a qualche reato possono essere manipolati allo scopo di incrementare il pre-

¹²<https://www.crimemapping.com>

giudizio razziale.

La redazione di report alterati distorcono la metodologia con cui i dati vengono raccolti e provocano la creazione di modelli basati su dati cosiddetti sporchi (*dirty data*).

Dal momento che modelli vengono costruiti sulla base di dati sporchi i risultati ottenuti condurranno ad un'analisi sempre più difettosa. I pregiudizi razziali che potrebbero essere insiti negli algoritmi dei software di polizia predittiva sono stati a lungo al centro di numerose critiche: secondo diverse organizzazioni gli algoritmi predittivi incoraggierebbero le pattuglie a dirigersi verso comunità minoritarie con conseguenze discriminatorie per gli individui appartenenti a quella minoranza.

Un' accusa di discriminazione è stata indirizzata al dipartimento di polizia di New York durante l'utilizzo del programma di *predictive policing* COMPSTAT: il progetto ha portato ad un drastico calo della criminalità, ma allo stesso tempo sono sorte numerose denunce sia in riguardo alle pressioni esercitate dagli agenti al fine di raccogliere dati sugli arresti, sia riguardanti l'impatto su alcune comunità minoritarie.¹⁴

Un ulteriore ostacolo che deve essere tenuto in considerazione, è che le mappe online che sono state costruite fin'ora, si limitano a "rappresentare il passato", senza la capacità di individuare prontamente nuovi trend e hanno quindi, una capacità predittiva scarsa.¹⁵ Il progetto di Ms.WEAS si pone come obiettivo la costruzione di una mappa che sia disponibile per tutti i cittadini e che mostri i dati delle aggressioni in tempo reale. I dati che vengono raccolti dai braccialetti potranno essere immediatamente visualizzabili sulla mappa e non sarà più necessario aspettare che venga fatta denuncia alle forze competenti.

Tramite la comunità online, sarà inoltre disponibile uno spazio di condivisione dedicato agli utenti, i quali potranno segnalare le condizioni delle strade in cui si trovano.

5 Tra tecnologia, etica e tutela della *privacy*

Per affrontare i potenziali limiti etici che una tecnologia come Ms.WEAS potrebbe incontrare, lo studio ha richiesto una raccolta di dati tramite un questionario anonimo a risposte guidate sotto forma di un foglio Google SpreadSheet. L'obiettivo di indagine è stato, da una parte, analizzare la percezione della popolazione riguardo la sicurezza nei luoghi pubblici; dall'altra, è stata verificata l'ipotetica volontà di acquisto del braccialetto anti-aggressione.

5.1 Il questionario

Il questionario sottoposto alla popolazione riportava come di seguito:

1. Sei un/una?
 - Uomo
 - Donna
2. Quanti anni hai?
 - Meno di 18
 - 18-25
 - 26-34
 - Più di 35
3. Qual è la tua occupazione?
 - Studente
 - Studente-lavoratore
 - Lavoratore
 - Disoccupato
4. Dove vivi?
 - Grande città (>200.000 abitanti)
 - Media città (80.000-200.000)
 - Piccola città o paese (<80.000)
5. Quanto ti senti al sicuro ad uscire da sola/o alla sera?
 - Molto al sicuro
 - Abbastanza al sicuro

¹³Mastrobuoni G, *Crime is Terribly Revealing: Information Technology and Police Productivity*, 2014, p.9

¹⁴A.G. Ferguson, *Predictive policing and reasonable suspicion*, 2012, p.323

- Poco al sicuro
 - Per niente al sicuro
6. Sei mai stato/a vittima di un'aggressione/furto?
- Sì
 - No
7. Hai mai assistito ad un'aggressione/furto?
- Sì
 - No
8. Se si hai fatto qualcosa per aiutare la vittima?
- Sì
 - No
9. Utilizzeresti un dispositivo (bracciale) in grado di segnalare un tentativo di aggressione/furto?
- Sì
 - No
10. Che importanza dai alle seguenti caratteristiche in relazione ad un bracciale di sicurezza personale? (1 = Poco importante, 5 = Molto importante)
- Design
 - Prezzo
 - Localizzazione
 - Possibilità di registrare suoni e immagini
 - Segnalazione di crimini in tempo reale
 - Possibilità di essere aiutato e aiutare in grado di aggressione/furto
 - Chiamate di emergenza
11. Quanto saresti disposto a pagare per un servizio come quello descritto?
- <di 50 €
 - 50 €- 99€
 - 100€-150€
 - >150€

12. Acquistaresti questo bracciale per te o per un conoscente?
- Sì
 - No

5.1.1 I risultati

Sono state raccolte in due mesi di indagine (ottobre 29- dicembre 6, 2019), n. 316 risposte al questionario online. 185 risposte sono state inviate da donne e 131 risposte da uomini. I risultati ottenuti (vd. figura 2 e 3) mostrano che la maggior parte delle persone che hanno risposto al questionario sono giovani (range 18-25 anni), ovvero il 54,7% della popolazione totale. Il 41,8% della popolazione vive in una città con meno di 80.000 abitanti, il 32,5% in una grande città con più di 200.000 abitanti e il restante 25,7% in una città di medie dimensioni.

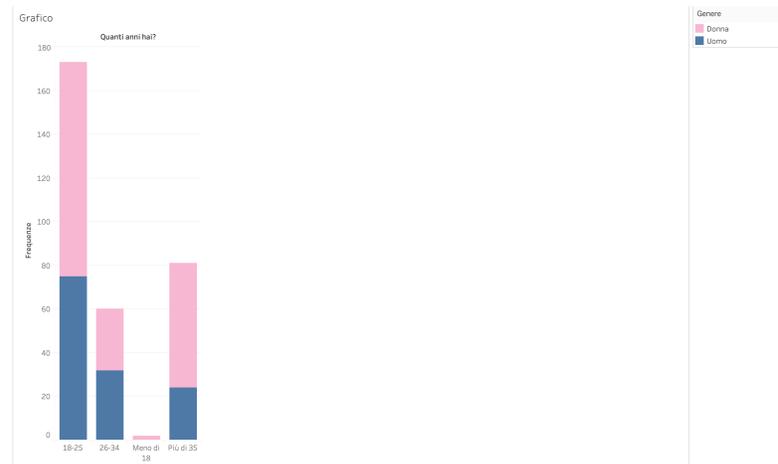


Figura 2

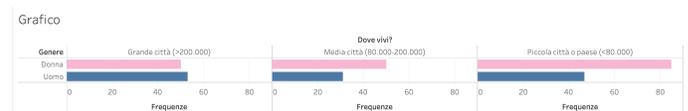


Figura 3

Per avere uno sguardo più preciso e completo su tutta la distribuzione della popolazione la figura 4 visualizza la variabile genere, l'età e il luogo. I risultati sono diversi tra loro e questo mette in luce l'eterogeneità complessiva del campione. Nel range 18-25 anni il genere femminile viene distri-

buito in modo abbastanza omogeneo tra tutte e tre le modalità di risposte relative alla domanda “dove vivi”; registrando i record più alti per la prima e la terza modalità di risposta; per quanto riguarda il genere maschile invece, la frequenza più alta viene registrata per la prima modalità di risposta. I risultati ottenuti riguardo al range 26-34 anni, ovvero il 19 % della popolazione, sono piuttosto omogenei sia per quanto riguarda la distribuzione del genere sia per il dove vivi. Successivamente sono stati registrati solo due record di donne con meno di 18 anni, che vivono in una piccola città. Infine, sono state registrate un numero sostanziale di risposte dal genere femminile con più di 35 anni che vive in una piccola realtà.

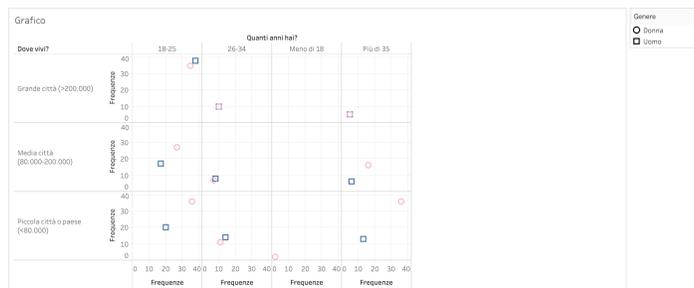


Figura 4

Sono poi state registrate le frequenze rispetto all'occupazione della popolazione, il 33,8% ha dichiarato di essere un lavoratore; mentre il 41,4% è uno studente.

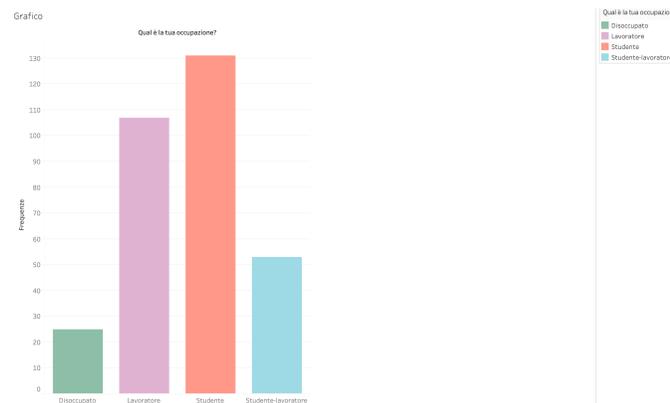


Figura 5

Nella seconda parte del questionario vengono pro-

poste delle domande a risposta multipla con l'obiettivo di interrogare la popolazione circa il tema dell'incolumità personale.

La figura 6 mostra la percezione della sicurezza durante le ore serali.



Figura 6

Dal grafico si evince che il 9,7% delle donne non si sente per niente al sicuro ad uscire da sole durante le ore serali e notturne, mentre per quanto riguarda il genere maschile, solo due osservazioni hanno scelto questa modalità di risposta: il 37,3% delle donne dice di sentirsi poco al sicuro contro il 6,1% degli uomini.

E' evidente che il 49,2% di donne e il 67,2% degli uomini si sentono “abbastanza sicuri” ad uscire da soli durante le ore serali e notturne, mentre solo il 3,8% delle donne si sente "molto al sicuro" contro un 25,2% degli uomini.

Le domande seguenti riguardano in particolare gli episodi di aggressione e furto.

La figura 7 mostra omogeneità di risposta secondo il genere per quanto riguarda la prima risposta e si evince che la maggior parte della popolazione non è mai stata vittima diretta di un'aggressione o di un furto. Allo stesso modo, la maggior parte della popolazione non risulta nemmeno aver mai assistito ad una scena di violenza, d'altra parte, però gli uomini più sovente assistono ad un'aggressione. Tra coloro poi che hanno assistito direttamente ad una scena di violenza, rispettivamente il 68,5 % degli uomini e il 62,5% delle donne hanno provato ad aiutare la vittima in qualche modo.

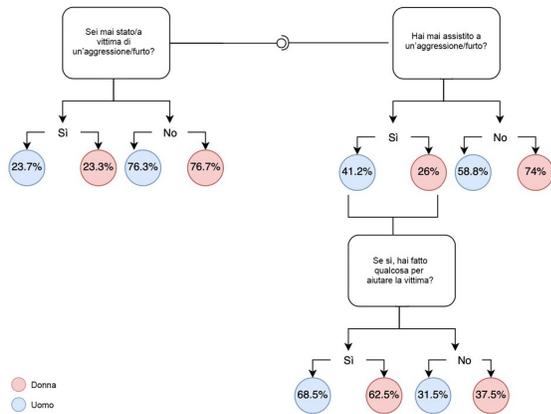


Figura 7

L'ultima parte del questionario propone alcune domande più specifiche riguardo allo strumento Ms.WEAS.

Alla domanda "Utilizzeresti un dispositivo dispositivo (bracciale) in grado di segnalare un tentativo di aggressione/furto?", la figura 8 mostra come l'81,3% della popolazione ha risposto positivamente.

Nella visualizzazione vengono riportate sia le risposte alla domanda n. 9 sia le risposte alla domanda n.6, entrambe filtrate per il genere.

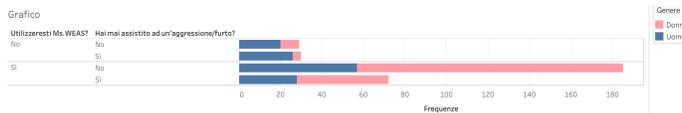


Figura 8

Infine è stato costruito un grafico che rappresenta, tramite degli istogrammi, le preferenze nelle caratteristiche del dispositivo.

la figura 9 mostra come sia il prezzo sia il design del dispositivo siano di marginale interesse, mentre ciò che è davvero importante per la popolazione è la possibilità di essere localizzati e la possibilità di effettuare chiamate di emergenza.

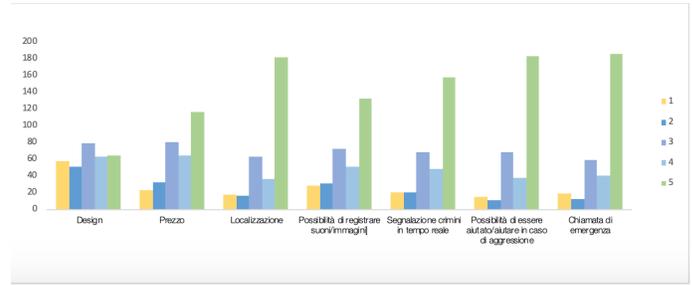


Figura 9

5.2 Etica, *privacy* e innovazione: riflessioni

A seguito dello studio circa le caratteristiche del dispositivo; i possibili competitor già affermati sul mercato e la raccolta dati sulla popolazione, sono sorte diverse questioni etiche su cui riflettere e che non possono essere ignorate.

Nel mondo interconnesso in cui viviamo oggi, dove il progresso tecnologico cresce molto rapidamente, ogni novità sembra venir accolta con entusiasmo e troppo spesso accettata senza la necessaria valutazione.

Si prenda come esempio il questionario sopra riportato: la tecnologia lì presentata non esiste ancora, ma è stato sufficiente idealizzarla nella mente della popolazione per ricevere consensi. La sola idea di un qualcosa di tecnologicamente nuovo e avanzato è bastato per riscuotere un grande successo. Per esempio, la stra grande maggioranza della popolazione ha acconsentito a condividere ininterrottamente la propria posizione e a inviare i propri dati ad un centro di analisi, non ben specificato.

Le persone hanno poca percezione del valore dei dati e delle informazioni, forse perché troppo volatili e immateriali, forse perché sembrano di poco conto, e non ci si rende conto che invece, essi costituiscono la nostra vera essenza.

Il peso della *privacy* quando si parla di innovazione sembra passare in secondo piano, tanto che non ci si domanda mai "chi" sia colui che attenta all'integrità di questo diritto.

Lo studioso Lyon dice che per sua natura la società dell'informazione è una società sorvegliata¹⁶.

te monitorata come mai prima era successo nella storia". D. Lyon, La società sorvegliata. *Tecnologie di controllo della vita quotidiana*, 2002 p. 1.

¹⁵F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, p.254

¹⁶Le società che per le loro procedure amministrative e di controllo dipendono dalle tecnologie della comunicazione e dell'informazione sono società sorvegliate. Gli effetti di ciò sono percepibili nella vita quotidiana, la quale è strettamen-

Già nel suo saggio del 1997¹⁷, Lyon aveva messo in guardia i suoi lettori dalla sempre maggiore invadenza da parte della società dei consumi nella vita quotidiana delle persone.

Il tema principale del progetto riguarda la sicurezza personale nell'ambito urbano, che è un contesto comunitario, e risulta quindi necessario chiedersi come mantenere l'equilibrio tra libertà e sicurezza, da una parte e tutela del diritto di non violazione della propria persona e il controllo, dall'altra. Più si cerca di allargare il campo della libertà di circolazione e della libertà d'azione degli individui più si è obbligati a intensificare i meccanismi di sicurezza che hanno il compito di garantire questi stessi movimenti e azioni. Nel momento in cui diviene tecnologicamente possibile tenere sotto controllo un numero sempre maggiore di persone tramite le tecnologie elettroniche ed informatiche la libertà sembra scomparire.

Si è passati dal termine "sorveglianza", al termine "dataveglanza"¹⁸: non è più necessario infatti, disporre di uno strumento materiale per controllare le persone, bensì basta incrociare istantaneamente i dati riguardanti un soggetto tramite tecniche di *computer matching* per arrivare ad avere un controllo sul suo comportamento, sui suoi spostamenti e sulle sue transazioni quotidiane.

Da ciò risulta che le tecnologie sembrano funzionare meglio dell'occhio umano in quanto a controllo delle azioni della popolazione intera, per questo motivo vengono implementate ad un ritmo dinamico strumenti in grado di riconoscere e schedare i volti della gente e di localizzare la loro posizione in tempo reale.

La stessa tecnologia pensata in questo progetto possiede queste funzioni e la popolazione a cui è stata presentata, non solo sembra aver accettato il compromesso di cedere parte della propria libertà, bensì le ritiene di fondamentale importanza.

Il punto cruciale è questo: i comuni cittadini hanno fiducia nella tecnologia, forse perché non dispongono di informazioni precise e quindi accettano le misure che gli vengono proposte, oppure perché ammalati dall'idea che le cose possano funzionare

in un modo migliore. Entrambe queste situazioni aumentano esponenzialmente il potere che gli strumenti hanno e di conseguenza anche di coloro che li creano e li possiedono e se usati in modo errato, ovvero, senza il rispetto dei diritti fondamentali, ci ritroveremmo davanti ad una soluzione eticamente scorretta. E' proprio per questo motivo che invece di sperare che i dati vengano trattati in maniera etica, è necessario costruire dei veri e propri sistemi che implicino l'etica nel processo di trattamento stesso: è il principio dell' *ethics by design*.¹⁹

5.3 La geolocalizzazione e la biometria: utilizzo e regolamentazione

Il dispositivo presentato nel paper, si compone di due funzionalità che necessitano di ulteriori considerazioni: il GPS/GSM integrato nello strumento e la possibilità di scattare immagini.

La possibilità che l'individuo che vive in una società moderna ha di essere localizzato cambia la natura dei rapporti personali e dei rapporti tra uomo e tecnologia, viene infatti messo in discussione il rispetto per i valori fondamentali per l'autonomia della persona e la Carta dei Diritti Fondamentali dell'Unione Europea inizia proprio con l'affermazione solenne dell'inviolabilità della dignità umana.²⁰

La geolocalizzazione è l'identificazione della posizione geografica di un dispositivo connesso o meno alla rete Internet, secondo diverse tecniche, quali, ad esempio il GPS che è basato sui segnali radio ottenuto da satelliti artificiali in orbita attorno alla Terra. I servizi di geolocalizzazione dovrebbero essere integrati in un nucleo di norme valide e coordinati con le libertà e i diritti delle persone, purtroppo una regolamentazione ancora non esiste.

Urge un'elaborazione di regole che valgano a rendere sostenibile il processo innovativo della tecnologia, affidandosi una fonte legislativa che non sia "monocentrica", bensì a un "policentrismo di fonti"²¹. Tutti i paesi interessati alla soluzione

dicembre 2019

²⁰Carta dei Diritti Fondamentali dell'Unione Europea, 2000, Art.1

¹⁷D. Lyon, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, 1997

¹⁸F.Domenicali, *Esiste una "filosofia della sorveglianza?"*, p.2

¹⁹<https://www.vice.com/it/article/4xn9bn/etica-importanza-per-futuro-tecnologia> ultimo accesso: 19

del problema, dovrebbero essere in grado di promulgare leggi comuni, così da auto disciplinarsi in materia. "Si realizza in tal modo quel moderno processo regolatore, frutto della convergenza di molteplici fonti normative, che si definisce come *coregulation*"²².

L'azione di sorveglianza prevede in sé il tentativo di identificare un soggetto attraverso il confronto tra le immagini acquisite da strumenti come una telecamera e quelle contenute negli archivi delle forze dell'ordine. Il confronto delle immagini, e quindi la possibilità di acquisirne ulteriori tramite dispositivi in grado di scattare fotografie richiede una regolamentazione legale.

Il dispositivo dell'art. 96 Legge sulla protezione del diritto d'autore del codice penale italiano dice chiaramente che "il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa".

La questione da affrontare non riguarda solamente l'uso improprio di immagini, ma anche di altri dati biometrici che i sensori del dispositivo idealizzato in questo progetto potrebbero rilevare ed elaborare. Si parla di dati biometrici quando ci si riferisce a dati personali che si ricavano da caratteristiche fisiche o comportamentali uniche e identificative di ciascuna persona fisica. Fanno parte di questa categoria di dati, ad esempio, le impronte digitali, la specifica conformazione fisica della mano o del volto, dell'iride o della retina e il timbro e la tonalità della voce.²³

Dal momento che all'art. 9 del GDPR viene vietato un qualsiasi tipo di trattamento compiuto mediante l'uso di dati biometrici intesi a identificare in modo univoco una persona fisica; e considerando come trattamento una qualsiasi operazione, compiuta con o senza l'ausilio di processi automatizzati, come la raccolta e la registrazione[...]; si potrebbe affermare che l'utilizzo di un dispositivo con un sensore integrato capace di elaborare dati biometrici di una persona terza, non sia previsto dalla normativa.

D'altro canto il dispositivo dell'art. 266 del Codice di procedura penale permette "l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile [...]"²⁴, solo se vi è fondato motivo di ritenere che ivi

si stia svolgendo un'attività criminosa".

Le regolamentazioni sopra indicate destano diversi dubbi circa la legalità dell'utilizzo di sensori di questo tipo, e sembra dunque esserci un vuoto interpretativo che è difficile colmare. L'innovazione tecnologica disegna progressivamente un nuovo quadro di diritti civili, modifica le relazioni tra le persone, introduce dei "dilemmi etici" ai quali occorre trovare delle risposte per contribuire efficacemente allo sviluppo della società; allo stesso modo per non venire sopraffatti dal cambiamento sono necessarie delle nuove norme che regolamentino l'utilizzo di strumenti tecnologici innovativi.

5.3.1 Il riconoscimento facciale

Il riconoscimento facciale è una tecnica di intelligenza artificiale utilizzata in biometria per identificare l'identità di una persona dall'immagine del suo volto.

Il riconoscimento avviene tramite l'elaborazione dei dati di immagini digitali che vengono raccolti da un sensore (quale, fotocamera, videocamera, webcam, telecamera di sorveglianza...).

L'utilizzo di queste tecniche ormai è oggetto di studio da diversi anni e sono sempre state al centro di proteste a causa del loro poco rispetto del diritto di privacy. Fece scandalo la tecnica pervasiva di sorveglianza messa in atto a Tampa per la finale del Super Bowl nel 2001, durante la quale vennero scannerizzati di 100 000 volti di spettatori americani e confrontati con i database della polizia contenenti i volti di terroristi, criminali e ricercati.

Gli spettatori non ne furono informati se non dopo l'accaduto.

Facendo riferimento al riconoscimento facciale sotto questo punto di vista si rischia di ricadere in una visione Orwelliana dello stato e della società, quando, al contrario, queste tecniche risultano essere molto utili quando si parla di sicurezza personale.

Se il dispositivo presentato in questo progetto avesse la possibilità attraverso una fotocamera impiantata direttamente nel *wearable*, oppure attraverso la fotocamera dello *smartphone* di scattare un'immagine del volto dell'aggressore sarebbe possibile utilizzare tecniche di riconoscimento del volto.

Gli algoritmi sviluppati in questo campo sono sva-

²²A cura di G.Rasi, *Innovazioni tecnologiche e privacy*, p.26

²²*ibidem*

²³Art. 4 GDPR, 2018

riati, ad esempio il "PCA (Principal Component Analysis) che è un algoritmo in grado di isolare e rappresentare le componenti tipiche di un insieme di dati, utilizzato principalmente nel *pattern recognition*"²⁵. L'algoritmo ha riportato un grande successo proprio perché è in grado di evidenziare i tratti più significativi di un volto, e quindi di caratterizzarlo, in modo tale da renderlo unico e diverso da tutti gli altri volti.

Dal momento che questa tecnica massimizza le peculiarità dei volti, prestando attenzione ai minimi particolari, purtroppo presta attenzione anche ai difetti dell'immagine e quindi in caso di scarsa luminosità non riesce a performare bene.

Idealmente parlando, la situazione ottimale si potrebbe raggiungere quando, il dato di immagine raccolto dal sensore del dispositivo venisse immediatamente elaborato dall'algoritmo e reso disponibile alle forze dell'ordine tramite il software.

del prodotto.

6 Conclusioni

Lo studio si è concretizzato con l'idealizzazione di uno strumento che sia in grado di migliorare la sicurezza personale nei luoghi urbani. Da una possibile realizzazione del dispositivo, passando in rassegna i principali competitor presenti sul mercato, si è cercato di analizzare quali possono essere le modifiche e le implementazioni più adatte a rendere il congegno più funzionale.

L'idea di creare una visione *social*, è risultato essere uno degli elementi principali per creare una comunità più solidale e attenta al tema della sicurezza.

E' stata poi analizzata la possibilità di creare una mappa del crimine disponibile per tutti i cittadini, aggiornata con i dati in tempo reale e che fornisca, dunque, informazioni vere e precise sugli eventi criminosi nei vari quartieri della città. Questa idea è innovativa, dal momento che non ne esistono ancora online, oggi giorno.

Nell'ultima parte sono state analizzate varie problematiche relative all'etica e alla regolamentazione legale, circa l'utilizzo di alcuni sensori del dispositivo che rilevano la geolocalizzazione e che registrano i dati biometrici.

Ulteriori ricerche potrebbero comprendere l'elaborazione di un *business plan*, per la realizzazione

²⁴Art. 4 GDPR, 2018

Bibliografia

Bagnasco A, Barbagli M, Cavalli A, Corso di sociologia, 2012

F. Domenicali, Esiste una "filosofia della sorveglianza?"

D. Lyon, L'occhio elettronico. Privacy e filosofia della sorveglianza, 1997

I. Fasolino, F. Coppola, M. Grimaldi, La sicurezza urbana degli insediamenti. Azioni e tecniche per il pianourbanistico, 2018

Mastrobuoni G, Crime is Terribly Revealing: Information Technology and Police Productivity, 2014

F. Pizzetti, Intelligenza artificiale, protezione dei dati personali e regolazione

G. Rasi, Innovazioni tecnologiche e privacy

M. Tonry, Prediction and Classification: Legal and Ethical Issues, in Crime and Justice, Vol. 9, Prediction and Classification: Criminal Justice Decision Making (1987)

A. Ummarino, Una introduzione ai software per il crimemapping.

Sitografia

<https://www.digitalic.it/economia-digitale/smartwatch-e-smartband-mercato-2019> ultimo accesso 18 dicembre 2019

<https://www.fisu.it/2017/05/08/teoria-delle-attivita-routinarie-2/> ultimo accesso 18 dicembre 2019

<https://www.vice.com/it/article/4xn9bn/etica-importanza-per-futuro-tecnologia> ultimo accesso: 19 dicembre 2019

<https://www.crimemapping.com> ultimo accesso: 19 dicembre 2019

<https://www.innovationtactics.com/platform-business-model-complete-guide/>

<https://www.zerounoweb.it/cio-innovation/sono-platform-based-i-modelli-di-business-sostenibili-per-gestire-linnovazione/> <https://amslaurea.unibo.it/11855/1/mbacci092916.pdf>

²⁵<https://amslaurea.unibo.it/11855/1/mbacci092916.pdf>