

<p>UNI/PdR xxx:2018</p>	<p>Sicurezza urbana - Quadro normativo, terminologia e modelli applicativi per pianificare, progettare, realizzare e gestire soluzioni di sicurezza urbana</p>
<p>Sommario</p>	<p>La presente prassi di riferimento è una linea guida che intende:</p> <ul style="list-style-type: none"> • contribuire alla definizione e all'adozione di un linguaggio comune da parte di tutti i soggetti operanti a vario titolo nel settore della sicurezza urbana; • fornire una panoramica delle prescrizioni nazionali, europee ed internazionali relative alla sicurezza urbana; • proporre modelli applicativi di riferimento per pianificare, progettare, realizzare e gestire soluzioni di sicurezza urbana. <p>Il documento è destinato ad essere utilizzato dagli operatori del settore quali la pubblica amministrazione, le forze dell'ordine, i "security manager", i "product manager", gli ingegneri, i progettisti, gli urbanisti, i giuristi, gli avvocati, i consulenti, gli installatori e cittadini, quando si trovano a confrontarsi con problematiche di 'Sicurezza Urbana' in aree e luoghi pubblici e privati.</p>
<p>Data</p>	<p>2018-07-20</p>

Avvertenza

Il presente documento è un progetto di Prassi di Riferimento (UNI/PdR) sottoposta alla fase di consultazione, da utilizzare solo ed esclusivamente per fini informativi e per la formulazione di commenti.

Il processo di elaborazione delle Prassi di Riferimento prevede che i progetti vengano sottoposti alla consultazione sul sito web UNI per raccogliere i commenti del mercato: la UNI/PdR definitiva potrebbe quindi presentare differenze rispetto al documento messo in consultazione.

Questo documento perde qualsiasi valore al termine della consultazione, cioè il: 4 settembre 2018.

UNI non è responsabile delle conseguenze che possono derivare dall'uso improprio del testo dei progetti di Prassi di Riferimento in consultazione.

PREMESSA

La presente prassi di riferimento UNI/PdR XX:2018 non è una norma nazionale, ma è un documento pubblicato da UNI, come previsto dal Regolamento UE n.1025/2012, che raccoglie prescrizioni relative a prassi condivise all'interno del seguente soggetto firmatario di un accordo di collaborazione con UNI:

FOIM - Fondazione Ordine Ingegneri Provincia di Milano

Via Pergolesi, 25

20124 Milano

La presente prassi di riferimento è stata elaborata dal Tavolo “Mappatura scenario sicurezza urbana” condotto da UNI, costituito dai seguenti esperti:

Nome Cognome 1 – Project Leader (organizzazione xyz)

Nome Cognome 2 (organizzazione yz)

Nome Cognome 3 (organizzazione xyz)

Nome Cognome 4 (organizzazione y)

Nome Cognome 5 (organizzazione xz)

Nome Cognome 6 (organizzazione z)

La presente prassi di riferimento è stata ratificata dal Presidente dell'UNI il xx xxxx 2018.

Le prassi di riferimento, adottate esclusivamente in ambito nazionale, rientrano fra i “prodotti della normazione europea”, come previsti dal Regolamento UE n.1025/2012, e sono documenti che introducono prescrizioni tecniche, elaborati sulla base di un rapido processo ristretto ai soli autori, sotto la conduzione operativa di UNI.

Le prassi di riferimento sono disponibili per un periodo non superiore a 5 anni, tempo massimo dalla loro pubblicazione entro il quale possono essere trasformate in un documento normativo (UNI, UNI/TS, UNI/TR) oppure devono essere ritirate.

Chiunque ritenesse, a seguito dell'applicazione della presente prassi di riferimento, di poter fornire suggerimenti per un suo miglioramento è pregato di inviare i propri contributi all'UNI, Ente Nazionale Italiano di Unificazione, che li terrà in considerazione.

SOMMARIO

0	INTRODUZIONE	4
1	SCOPO E CAMPO DI APPLICAZIONE	6
2	PRINCIPIO	6
3	ELENCO RIFERIMENTI NORMATIVI E LEGISLATIVI.....	7
4	GLOSSARIO E RIFERIMENTI TERMINOLOGICI	10
5	SCENARIO DI RIFERIMENTO	17
5.1	SICUREZZA URBANA E CITTÀ SOSTENIBILE	17
5.2	SICUREZZA URBANA E SCENARIO DI RIFERIMENTO LEGISLATIVO	19
5.2.1	LEGGE N. 48 DEL 18 APRILE 2017	19
5.2.2	LINEE GENERALI PER LE POLITICHE PUBBLICHE DELLA SICUREZZA INTEGRATA	23
6	LINEE DI SVILUPPO DELLA SICUREZZA URBANA.....	24
6.1	GENERALITÀ	24
6.2	SICUREZZA URBANA E TECNOLOGIA	25
6.3	FORMAZIONE E SVILUPPO DELLE COMPETENZE	26
6.4	FAVORIRE LE PARTNERSHIP	26
6.5	SOSTENIBILITÀ FINANZIARIA DEI PROGETTI DI SICUREZZA URBANA.....	26
7	IMPLEMENTAZIONE DELLE SOLUZIONI DI SICUREZZA URBANA	27
7.1	GENERALITÀ	27
7.2	PROPOSTE DI SICUREZZA URBANA PER LO SVILUPPO SOSTENIBILE DELLE CITTÀ	27
7.3	VALUTAZIONE DEI PROGETTI DI SICUREZZA URBANA.....	28
7.4	INTERVENTI PER LA SICUREZZA URBANA.....	28
7.4.1	METODOLOGIA DI ATTUAZIONE DEGLI INTERVENTI	30
7.4.2	VERIFICA DELLE AZIONI INTRAPRESE E LORO VALUTAZIONE	30
7.5	SINTESI DEL RAPPORTO TECNICO UNI CEN/TR 14383-2:2010	32
7.5.1	GENERALITÀ	32
7.5.2	ORGANISMO RESPONSABILE DELLA PIANIFICAZIONE URBANISTICA	32
7.5.3	CONTENUTI E PROCESSO	35

7.6	SORVEGLIANZA SPONTANEA	38
7.6.1	GENERALITÀ	38
7.6.2	NUMERO UNICO DI EMERGENZE (NUE).....	38
7.6.3	SORVEGLIANZA SPONTANEA AUTOMATICA	38
7.6.4	APPLICAZIONE YOUPOL.....	40
7.6.5	EENA - SEGNALAZIONE SPONTANEA E SEGNALAZIONE AUTOMATIZZATA	40
7.6.6	HELP POINT FERROVIENORD	41
APPENDICE A - MESSA IN SICUREZZA DI PROMENADE DES ANGLAIS, NIZZA		42
APPENDICE B - SISTEMA DI VIDEOSORVEGLIANZA DELLA CITTA' DI VENEZIA		44
APPENDICE C - ESEMPIO DI ILLUMINAZIONE INTELLIGENTE E VIDEOSORVEGLIANZA: STATUA DEL CRISTO REDENTORE A RIO DE JANEIRO, BRASILE		46
APPENDICE D - CASO APPLICATIVO REALE DI SORVEGLIANZA DELLA RETE FERROVIENORD		47
BIBLIOGRAFIA.....		49

0 INTRODUZIONE

Oggi la sicurezza è tra le maggiori preoccupazioni dei cittadini ed uno dei temi più spesso ricorrenti nei media, con particolare risalto alla sicurezza urbana.

Essere liberi di condurre la propria vita senza essere vittima di crimine, di violenza, di atti intimidatori o di paure è un diritto fondamentale scritto nella Dichiarazione Universale dei Diritti dell'Uomo (art. 3). Tale libertà non è soltanto importante per migliorare la qualità della vita di ogni cittadino, ma lo è soprattutto per lo sviluppo sostenibile delle città.

La sicurezza urbana contribuisce a creare un ambiente favorevole alla crescita economica nel quale possono essere assicurati servizi efficaci e nel quale si creano i presupposti per la riduzione della povertà e dell'esclusione sociale.

La necessità di sicurezza è antichissima ed è stato uno dei motivi che ha spinto gli esseri umani, nel corso dell'evoluzione a riunirsi in conglomerati urbani sempre meglio difesi, prima da terrapieni, poi da mura e fossati, con accessi ben difendibili e controllabili.

L'ampliarsi delle città fino a diventare città-stato costituiva una formidabile difesa da nemici esterni, ma l'accumularsi di molte persone in uno spazio relativamente ristretto ha portato a problemi nuovi, quali ad esempio il traffico, l'approvvigionamento idrico, i rifiuti urbani. Inoltre, la densità di popolazione ed abitazioni ha aumentato man mano il rischio ed i danni dovuti ad eventi come gli incendi o criminalità.

Questo ha portato fin dai tempi antichi a sviluppare metodologie, infrastrutture ed istituzioni che oggi sono considerate anche componenti della sicurezza urbana, quali la pianificazione delle città, le reti fognarie, i vigili del fuoco.

Oggi che l'urbanizzazione è altissima ed in crescita costante, sia i problemi che le contromisure si sono moltiplicati e questa tendenza sta subendo un'ulteriore accelerazione man mano che le città si attrezzano per diventare 'smart cities'.

Una 'smart city' si può definire una città in grado di migliorare la qualità dei servizi e della vita per coloro che vi abitano o vi si recano, grazie all'uso intelligente di tecnologie avanzate; tra queste sono preponderanti le tecnologie dell'informazione e della telecomunicazione.

Una 'smart city' è il risultato di servizi, infrastrutture ed oggetti interconnessi.

Una città non nasce 'smart' ma lo diviene gradualmente, con l'evoluzione e l'integrazione dei suoi componenti.

Come esempio possiamo prendere l'illuminazione urbana: possiamo ottimizzare il livello di illuminazione per risparmiare energia elettrica, avere la segnalazione dei guasti in tempo reale, per facilitare la programmazione degli interventi, supplire temporaneamente al deficit di illuminazione incrementando la potenza delle lampade limitrofe, misurare ed archiviare i parametri fondamentali per successive analisi. Poi, nella stessa infrastruttura possiamo aggiungere telecamere, sensori di rilevazione di traffico, ricarica di veicoli elettrici, ecc.

Più i processi vengono integrati ed ottimizzati, più la città potrà essere efficiente ed essere considerata 'smart', ma integrazione significa complessità ed interdipendenza tra i servizi. Più i sistemi sono interconnessi più è probabile che un malfunzionamento o una vulnerabilità di un componente causi problemi o danni ad altri componenti o all'intero sistema. Più i sistemi sono accessibili da Internet, più sono esposti ad azioni criminose di hackers.

In una 'smart city' un malfunzionamento, per esempio nella gestione "intelligente" del traffico, non solo può creare disagi significativi a tutta la popolazione, ma può generare anche gravi pericoli per l'incolumità fisica.

Pertanto, nella pianificazione urbana, ed ancora di più se si vuole andare nella direzione delle 'smart cities', si deve tener conto delle esigenze di sicurezza fin dalle prime fasi della progettazione, perché aggiungerle in fase di implementazione ha costi e complessità molto più elevati, costi che diventano proibitivi se si tenta di aggiungerle ad opera già completata.

È doveroso precisare che al termine italiano sicurezza corrispondono due parole inglesi: "security" e "safety".

La presente prassi di riferimento tratta esclusivamente della sicurezza intesa come security; trattare anche della sicurezza in termini di "safety" avrebbe coinvolto troppi aspetti, quali le emergenze e la protezione civile, che meritano un'ampia trattazione. D'altronde la sicurezza "security" costituisce spesso, come effetto collaterale desiderabile, un'efficace prevenzione di eventi che possono minare la "safety".

Le tecnologie abilitanti sono comuni alle due accezioni di "sicurezza".

La presente prassi di riferimento intende dare un contributo alla comprensione ed all'attuazione della sicurezza urbana riunendo e classificando in un contesto organico la casistica dei problemi e delle soluzioni.

A questo proposito vengono proposti alcuni esempi di buone pratiche nelle Appendici A, B, C e D.

1 SCOPO E CAMPO DI APPLICAZIONE

La presente prassi di riferimento è una linea guida che intende:

- contribuire alla definizione e all'adozione di un linguaggio comune da parte di tutti i soggetti operanti a vario titolo nel settore della sicurezza urbana;
- fornire una panoramica delle prescrizioni nazionali, europee ed internazionali relative alla sicurezza urbana;
- proporre modelli applicativi di riferimento per pianificare, progettare, realizzare e gestire soluzioni di sicurezza urbana.

Il documento è destinato ad essere utilizzato dagli operatori del settore quali la pubblica amministrazione, le forze dell'ordine, i "security manager", i "product manager", gli ingegneri, i progettisti, gli urbanisti, i giuristi, gli avvocati, i consulenti, gli installatori e cittadini, quando si trovano a confrontarsi con problematiche di 'Sicurezza Urbana' in aree e luoghi pubblici e privati quali:

- strutture residenziali pubbliche o private (condomini, residence, hotel);
- infrastrutture per i servizi di trasporto (aeroporti, porti, stazioni, interporti);
- strutture per servizi e terziario (uffici, scuole, università, ospedali);
- centri e distretti commerciali (centri commerciali, supermercati, retail);
- strutture per il tempo libero (musei, centri espositivi, stadi, cinema, poli culturali);
- spazi pubblici e privati delimitati (piazze, viali, parchi tematici).

Il documento tiene conto della compresenza di tecnologia (soluzioni per controllo accessi, varchi, videosorveglianza, ecc.) e servizi (es. vigilanza privata, stazionamento forze dell'ordine), finalizzati alla prevenzione di atti criminosi e della vulnerabilità dei siti riconducibili alle loro proprietà attuali o precedenti di ordine simbolico, politico, e/o religioso.

2 PRINCIPIO

La presente prassi di riferimento si propone di definire le linee guida per pianificare, progettare, realizzare e gestire soluzioni di sicurezza urbana.

A tal fine il documento fornisce:

- un quadro dei più significativi riferimenti legislativi e normativi nazionali, europei ed internazionali relativi alla sicurezza urbana;
- un glossario e riferimenti terminologici;
- la mappatura del contesto che caratterizza lo scenario di riferimento della sicurezza urbana;
- le linee di sviluppo della sicurezza urbana;

- implementazione delle soluzioni di sicurezza urbana;
- esempi di modelli applicativi per pianificare, progettare, realizzare e gestire soluzioni di sicurezza urbana.

La prassi di riferimento si completa con Appendici esemplificative in cui è stato proposto un elenco di buone pratiche messe in atto in alcune città e da alcune organizzazioni:

- Appendice A – Messa in sicurezza della ‘Promenade des Anglais’, Nizza, Francia
- Appendice B – Sistema di videosorveglianza della città di Venezia
- Appendice C – Esempio di illuminazione intelligente e videosorveglianza: statua del Cristo Redentore a Rio de Janeiro, Brasile
- Appendice D – Caso applicativo reale di sorveglianza della rete FERROVIENORD

3 ELENCO RIFERIMENTI NORMATIVI E LEGISLATIVI

Regolamento (UE) n.1025/2012, del Parlamento Europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le Direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le Direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n.1673/2006/CE del Parlamento europeo e del Consiglio

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

D.Lgs 30 giugno 2003, n. 196 ‘Codice in materia di protezione dei dati personali’

D.Lgs 9 aprile 2008, n. 81 ‘Testo coordinato con il D.lgs. 3 agosto 2009’, n. 106 - Testo unico sulla salute e sicurezza sul lavoro

D.Lgs 15 dicembre 2017, n. 223 Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea e della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d’informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell’informazione

Decreto del Ministro dell’Interno del 5 agosto 2008 ‘Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione’

Legge 24 luglio 2008, n. 125 Conversione in legge, con modificazioni, del decreto-legge 23 maggio 2008, n. 92, recante misure urgenti in materia di sicurezza pubblica

Legge 18 aprile 2017, n. 48 - Disposizioni urgenti in materia di sicurezza delle città

UNI/TS 11291-11-1:2014 Sistemi di misurazione del gas - Dispositivi di misurazione del gas su base oraria - Parte 11-1: Generalità

UNI EN 13201 Illuminazione stradale

UNI EN 14383-1:2006 Prevenzione del crimine - Pianificazione urbanistica e progettazione edilizia - Parte 1: Definizione dei termini specifici

UNI EN ISO 9001 Sistemi di gestione per la qualità

UNI EN ISO 19011 Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale

UNI EN ISO 14031:2013 Gestione ambientale - Valutazione delle prestazioni ambientali - Linee guida

UNI EN ISO 22600-1:2014 Informatica medica - Gestione privilegiata e controllo di accesso - Parte 1: Gestione politica e visione d'insieme

UNI EN ISO 22311:2015 Sicurezza della società - Videosorveglianza - Compatibilità tra contenuti digitali di videoregistrazioni

UNI EN ISO 22300:2018 Sicurezza e resilienza - Vocabolario

UNI CEN ISO/TS 14265:2013 Informatica sanitaria - Classificazione dei requisiti per la gestione delle informazioni sanitarie personali

UNI CEI EN ISO 14971:2012 Dispositivi medici - Applicazione della gestione dei rischi ai dispositivi medici

UNI CEI ISO 7498-2 :1993 Sistemi per l'elaborazione delle informazioni. Interconnessione di sistemi aperti (OSI). Modello di riferimento di base. Architettura di sicurezza

UNI CEI ISO/IEC 29100:2015 Tecnologie informatiche - Tecniche per la sicurezza - Quadro di riferimento per la privacy

UNI CEN/TR 14383-2:2010 Prevenzione del crimine - Pianificazione urbanistica e progettazione edilizia - Parte 2: Pianificazione urbanistica

UNI ISO 31000 Gestione del rischio - Principi e linee guida

ISO 8468:2007 Ships and marine technology - Ship's bridge layout and associated equipment - Requirements and guidelines

ISO 19092:2008 Financial services - Biometrics - Security framework

ISO 22320:2011 Societal security - Emergency management - Requirements for incident response

ISO 22315:2014 Societal security - Mass evacuation - Guidelines for planning

ISO 22397:2014 Societal security - Guidelines for establishing partnering arrangements

ISO 37120:2014 Sustainable development of communities - Indicators for city services and quality of life

ISO 18435-3:2015 Industrial automation systems and integration - Diagnostics, capability assessment and maintenance applications integration - Part 3: Applications integration description method

ISO 37100:2016 Sustainable cities and communities - Vocabulary

ISO 37101:2016 Sustainable development in communities - Management system for sustainable development- Requirements with guidance for use

ISO 6707-1:2017 Buildings and civil engineering works - Vocabulary General terms

ISO/DTS 22375 Security and resilience - Guidelines for complexity assessment process to improve security and resilience

ISO/TS 27790:2009 Health informatics - Document registry framework

ISO/TS 12911:2012 Framework for building information modelling (BIM)

ISO/TR 25743:2010 Lifts (elevators) - Study of the use of lifts for evacuation during an emergency

ISO/TR 17522:2015 Health informatics - Provisions for health applications on mobile/smart Devices

ISO/TR 22351:2015 Societal security - Emergency management - Message structure for exchange of information

ISO/IEC 7816-13:2007 Identification cards - Integrated circuit cards - Part 13: Commands for application management in a multi-application environment

ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity

ISO/IEC 2382:2015 Information technology - Vocabulary

ISO/IEC 27033-1:2015 Information technology - Security techniques - Network security - Part 1: Overview and concepts

ISO/IEC 30134-1:2016 Information technology - Data centres - Key performance indicators - Part 1: Overview and general requirements

ISO/IEC 38505-1:2017 Information technology - Governance of IT - Governance of data - Part 1: Application of ISO/IEC 38500 to the governance of data

ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary

ISO/IEC TR 20547-5:2018 Information technology - Big data reference architecture - Part 5: Standards roadmap

4 GLOSSARIO E RIFERIMENTI TERMINOLOGICI

Il presente punto riporta un glossario che raccoglie una serie di riferimenti terminologici utili a favorire l'adozione e la diffusione di un linguaggio comune nel settore della sicurezza urbana.

4.1 application (applicazione): Strutture, elementi di dati e moduli di programma necessari per eseguire una funzionalità specifica.

[ISO/IEC 7816-13:2007, punto 4.1]

4.2 area commerciale: Area adibita ad attività commerciali.

4.3 area industriale: Area riservata ad attività industriali.

4.4 area residenziale: Insieme di abitati, costituiti da unità individuali o di caseggiati, in un'area circoscritta.

[UNI EN 14383-1:2006, punto 3.20]

4.5 autenticazione: Azione che verifica l'identità dichiarata di un'entità.

Esempio: La convalida di un'identità dichiarata di un utente può essere effettuata verificando alcune conoscenze, chiavi o proprietà segrete associate a tale utente, ad esempio una password, una chiave SSL, una chiave privata PGP o una firma manoscritta.

[ISO/IEC 2382:2015, punto 2126251]

4.6 autorizzazione: Autorizzazione ad effettuare determinate operazioni o ad utilizzare determinati metodi o servizi.

[UNI CEN ISO/TS 14265:2013, punto 2.3]

NOTA L'autorizzazione viene concessa confrontando i diritti di accesso dell'utente convalidato con l'azione/i richieste dall'utente su un oggetto, ad esempio per leggere e modificare il contenuto di un oggetto.

4.7 disponibilità: Proprietà di essere accessibile e utilizzabile su richiesta da parte di un soggetto autorizzato.

[ISO/IEC 27000:2018, punto 3.7]

4.8 barriera: Limite simbolico, fisico o elettronico imposto allo scopo di creare separazioni tra una determinata area e i suoi dintorni. Es road blocker, dissuasori, tyre killer, ecc.

[UNI EN 14383-1:2006, punto 3.6]

4.9 benchmark: Test appositamente studiato per valutare le prestazioni di un dispositivo o l'efficacia di un processo tecnico o di uno strumento finanziario in rapporto a uno standard di riferimento.

4.10 big data: Ampi set di dati - principalmente nelle caratteristiche di volume, varietà, velocità e/o variabilità - che richiedono un'architettura scalabile per un'efficiente memorizzazione, manipolazione e analisi.

[ISO/IEC TR 20547-5:2018, punto 3.1.1]

4.11 building information modelling (BIM): Rappresentazione digitale condivisa delle caratteristiche fisiche e funzionali di qualsiasi oggetto costruito, compresi edifici, ponti, strade, impianti di processo, ecc.

[ISO/TS 12911:2012, punto 3.1]

NOTA Il BIM non è solo un CAD 3D, né una nuova applicazione tecnologica. Il BIM è essenzialmente il valore che genera la collaborazione attraverso l'intero ciclo di vita di un asset, sostenuta dalla creazione, raccolta e scambio di modelli 3D condivisi e di dati intelligenti e strutturati ad essi collegati.

4.12 building management system: Sistema in grado di prendere decisioni intelligenti sulla base delle informazioni che gli sono trasmesse.

[ISO/TR 25743:2010, punto 2.1]

4.13 centrale di monitoraggio: Locale pubblico o privato, dotato di personale a orario continuato, che agisce alla ricezione a distanza di segnali di allarme da sistemi automatici antintrusione o di rivelazione incendio.

[UNI EN 14383-1:2006, punto 3.25]

4.14 Comitato Metropolitano: Costituito da: Prefetto, Sindaco metropolitano, Sindaci Comuni Città metropolitana. [così come disposto dalla Legge 18 aprile 2017, n. 48.]

4.15 confidentiality (confidenzialità): Proprietà che le informazioni non sono rese disponibili o divulgate a persone, entità o processi non autorizzati. Caratteristica che impedisce che le informazioni siano rese disponibili o divulgate a persone, entità o processi non autorizzati.

[ISO/IEC 27000:2018, punto 3.10]

4.16 controllo degli accessi: Insieme di tecniche, mezzi, procedure, che permettono la gestione di livelli di accesso e eventualmente la tracciabilità dell'accesso stesso ad un luogo o ad aree sensibili predefinite di tale luogo in una gamma che va dal divieto di accesso, all'accesso libero.

[UNI EN 14383-1:2006, punto 3.1]

NOTA Il controllo degli accessi può essere meccanico, umano, elettronico o una combinazione di questi sistemi.

4.17 controllore informale: Individuo (non appositamente formato per la difesa di altri civili) che utilizza, nel corso delle sue attività quotidiane, la propria presenza e le proprie capacità di

osservazione come deterrente nei confronti di comportamenti criminali, e che riferisce eventuali episodi alle autorità competenti, per favorirne l'intervento.

[UNI EN 14383-1:2006, punto 3.21]

4.18 controllore professionale (professional guardian): Soggetto formato e autorizzato per la protezione di persone o beni da reati e per la prevenzione della commissione di reati.

[UNI EN 14383-1:2006, punto 3.30]

NOTA Nella terminologia italiana tale soggetto è chiamato Agente di pubblica sicurezza, Operatore di sicurezza privata.

4.19 cyber security: Meccanismi e processi posti in essere per garantire l'integrità del funzionamento dei sistemi informatici, proteggendo le loro operazioni da interventi dolosi o involontari. Si intendono i controlli e le azioni che si usano per proteggere il cyber spazio, sia civile che militare, dalle minacce insite o che possano danneggiare i network interdipendenti e le strutture informatiche. La cyber security mira a preservare l'accessibilità e l'integrità delle reti e dell'infrastruttura e la confidenzialità delle informazioni ivi contenute.

NOTA Esempi di interventi dolosi o involontari includono intercettazioni, trojan, virus e worm, phishing, interruzione di servizio, rootkit e keylogger.

4.20 data centre: Struttura, o gruppo di strutture, dedicate alla sistemazione, all'interconnessione e al funzionamento centralizzati delle apparecchiature informatiche e di telecomunicazione di rete che forniscono servizi di memorizzazione, elaborazione e trasporto dei dati, nonché di tutte le strutture e infrastrutture di distribuzione dell'energia e di controllo ambientale, con i necessari livelli di resilienza e sicurezza necessari per fornire la disponibilità del servizio auspicata.

[ISO/IEC 30134-1:2016, punto 3.1.4]

4.21 data network: Rete in cui i circuiti di dati ed eventualmente gli impianti di commutazione consentono la comunicazione di dati tra apparecchiature terminali di dati.

[ISO/IEC 2382:2015, punto 2124424]

4.22 dati biometrici: Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

4.23 denial of service (DoS): Impossibilità di accesso autorizzato a una risorsa di sistema o del ritardo nelle operazioni e nelle funzioni del sistema, con conseguente perdita di disponibilità per gli utenti autorizzati.

[ISO/IEC 27033-1:2015, punto 3.9]

4.24 dissuasore: Costituito da un pistone a scomparsa esso può comprendere sia elementi meccanici, sia l'elettronica di potenza necessaria a movimentare l'attuatore oltre che alcuni sensori/attuatori quali spire induttive sia davanti che dietro il dissuasore, un sensore vibrofonico, un semaforo stradale (con luci rosso e verde).

4.25 DOC (Design Out of Crime): , Riduzione di criminalità e disordine e dell'insicurezza soggettiva attraverso la pianificazione urbanistica e la progettazione edilizia.
[UNI CEN/TR 14383-2]

4.26 drone o SAPR (SAPR) : Sistema Aeromobile a Pilotaggio Remoto:, sistema costituito da un mezzo aereo (aeromobile a pilotaggio remoto) senza persone a bordo, utilizzato per fini diversi da quelli ricreativi e sportivi, e dai relativi componenti necessari per il controllo e comando (stazione di controllo) da parte di un pilota remoto.
[Ente Nazionale per l'Aviazione Civile (ENAC)- Regolamento 'Mezzi aerei a pilotaggio remoto'- Edizione 2 del 16 luglio 2015, Emendamento 3 del 24 marzo 2017]

4.27 edificio: Costruzione che ha, tra i suoi scopi principali, quello di fornire riparo ai suoi occupanti o oggetti contenuti, ed è solitamente confinato e progettato per essere eretto permanentemente in un sito.
[ISO 6707-1:2017, punto 3.1.1.3]

4.28 effrazione: Introduzione intenzionale in una proprietà privata che causa danni materiali.
[UNI EN 14383-1:2006, punto 3.7]

4.29 garante protezione dati personali: Autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675) - che ha attuato nell'ordinamento giuridico italiano la direttiva comunitaria 95/46/CE . La materia della protezione dati personali è oggi disciplinata dal GDPR Regolamento europeo 679/2016.

4.30 hacking: Accedere intenzionalmente a un sistema informatico senza l'autorizzazione dell'utente o del proprietario.
[ISO/IEC 27032:2012 punto 4.25]

NOTA Ai fini della presente prassi di riferimento si considera soltanto l'hacking malevolo

4.31 illuminazione urbana: Installazioni luminose fisse che hanno lo scopo di fornire buona visibilità agli utenti delle aree pubbliche di traffico esterne, durante le ore di buio, per contribuire allo scorrimento, alla sicurezza del traffico e alla sicurezza pubblica.
[Serie UNI EN 13201 'Illuminazione stradale']

4.32 information security: Tutela della riservatezza, dell'integrità e della disponibilità delle informazioni; inoltre, possono essere coinvolte anche altre proprietà quali l'autenticità, la responsabilità, l'impossibilità di disconoscere e l'affidabilità. Es: chiave per la cifratura o il rilevamento di manomissioni, autorizzazioni di accesso per la lettura e la scrittura di oggetti, tracce di controllo per le modifiche ai dati.
[ISO 19092:2008, punto 4.35]

4.33 integrità: Proprietà di accuratezza e completezza.
[ISO/IEC 27000:2018, punto 3.36]

4.34 interoperabilità: Capacità di un sistema di scambiare dati con altri sistemi di differenti tipi e/o provenienti da differenti fabbricanti. [UNI/TS 11291-11-1:2014, 3.1.2]. È un prerequisito per l'intercambiabilità.

4.35 intercambiabilità: Capacità di sostituire un dispositivo con un altro senza ridurre le funzionalità originali e senza malfunzionamenti o perdita di efficienza del sistema complessivo.
[UNI/TS 11291-11-1:2014, 3.1.1.]

4.36 Internet of Things (IoT): Infrastruttura globale per la società dell'informazione che consenta servizi avanzati grazie all'interconnessione di elementi (fisici e virtuali) basati sulle tecnologie dell'informazione e della comunicazione interoperabili esistenti ed in evoluzione.
[ISO/IEC 38505-1:2017, punto 3.6]

4.37 monitoraggio: Atto di verificare periodicamente le attrezzature e l'ambiente al fine di rilevare eventuali cambiamenti.
[ISO 8468:2007, punto 3.1.36]

4.38 ontologia: Definizione esplicita e consensuale di concetti di un dominio applicativo, indipendente dall'uso dei concetti stessi.
[ISO 18435-3:2015, 3.1]

4.39 open data: Contenuti o dati che sono disponibili per essere utilizzati, riutilizzati e ridistribuiti, eventualmente soggetti all'obbligo di attribuire correttamente la fonte degli stessi.[<http://opendefinition.org/>]

4.40 patti per la sicurezza urbana: Patti sulla sicurezza urbana, che prefetti e sindaci sottoscrivono con lo scopo di individuare congiuntamente gli interventi necessari per la sicurezza urbana, come previsto dalla legge 18 aprile 2017, n. 48.

4.41 Personally Identifiable Information [PII]: Qualsiasi informazione che possa essere utilizzata per identificare l'utente cui tali informazioni si riferiscono in modo univoco oppure che sia o possa essere direttamente o indirettamente collegata all'utente (PII).

4.42 physical security: Misure utilizzate per garantire la protezione fisica delle risorse contro le minacce deliberate e accidentali.
[UNI CEI ISO 7498-2:1989, punto 3.3.41]

4.43 pianificazione urbanistica: Gestione complessiva dell'ambiente urbano che ha come scopo la progettazione dello spazio urbano e la pianificazione organica delle modificazioni del territorio incluso nella città o collegato con essa.

4.44 policy: Insieme di obblighi giuridici, politici, organizzativi, funzionali e tecnici per la comunicazione e la cooperazione.
[UNI EN ISO 22600-1:2014, punto 3.13]

4.45 predictive analytics (analisi predittiva): Tecniche statistiche e analitiche utilizzate per sviluppare modelli di previsione di eventi o comportamenti futuri.

NOTA La forma di questi modelli predittivi varia a seconda del comportamento o dell'evento che stanno predicendo. La maggior parte dei modelli predittivi genera un punteggio che indica la probabilità che il comportamento o l'evento dato si verifichi.

4.46 privacy: Libertà da intrusioni nella vita privata o negli affari privati di una persona quando tali intrusioni derivano dalla raccolta e dall'uso indebiti o illeciti di dati che la riguardano.
[ISO/TS 27790:2009, punto 3.56]

4.47 privacy breach: Evento per cui le informazioni di identificazione personale sono trattate in violazione di uno o più requisiti di tutela della privacy.
[UNI CEI ISO/IEC 29100:2015, punto 2.13]

4.48 privacy principles: Insieme dei valori condivisi che disciplinano la protezione della vita privata delle informazioni di identificazione personale (PII) quando vengono trattate da sistemi di tecnologia dell'informazione e della comunicazione.
[UNI CEI ISO/IEC 29100:2015 punto 2.18]

4.49 processo: Insieme di attività correlate o interagenti che trasformano input in output.
[ISO/IEC 27000:2018, punto 3.54]

4.50 resilienza (resilience): Capacità di assorbimento (dei cambiamenti) e di adattamento in un ambiente in evoluzione.
[UNI EN ISO 22300:2018, punto 3.192]

NOTA 1 Una città è resiliente se ha sviluppato la capacità di assorbire possibili shock e pone l'accento sulla sua economia sociale e sulle sue infrastrutture per essere in grado di conservare le sue funzioni, strutture, organizzazioni e identità. [<http://www.resilientcity.org>]

NOTA 2 Una componente essenziale della resilienza è la flessibilità (agility), ovvero la capacità di anticipare, prepararsi, riconfigurarsi e rispondere agli eventi in tempo utile. [<http://www.resilientcity.org>]

4.51 sicurezza (safety): Essere esenti da rischi inaccettabili.
[UNI CEI EN ISO 14971:2012, punto 2.24]

4.52 scala di prestazione (o di benchmark): Riferimento rispetto al quale viene confrontato il benchmark.

4.53 SDK (Software Development Kit): Fornitura delle informazioni tecniche di componenti hardware/software per sviluppi di terza parte.

4.54 separatore di sicurezza: Materiale resistente, trasparente o opaco, per la sicurezza di persone e/o beni.
[UNI EN 14383 -1:2006, punto 3.40]

4.55 sicurezza integrata: Insieme degli interventi assicurati dallo Stato, dalle regioni, dalle province autonome di Trento e Bolzano e dagli enti locali, nonché da altri soggetti istituzionali, al fine di concorrere, ciascuno nell'ambito delle proprie competenze e responsabilità, alla promozione e all'attuazione di un sistema unitario e integrato di sicurezza per il benessere delle comunità territoriali.
[Legge 18 aprile 2017, n. 48.]

4.56 sicurezza urbana: Bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione, anche urbanistica, sociale e culturale, e recupero delle aree o dei siti degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione della cultura del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile [...], di cui alla Legge 18 aprile 2017, n. 48.

4.57 sistema di registrazione: Apparati per la registrazione e conservazione dei filmati.

4.58 sistemi integrati di videosorveglianza: Sistemi che collegano telecamere tra soggetti diversi, sia pubblici che privati, o che consentono la fornitura di servizi di videosorveglianza in remoto da parte di società specializzate mediante collegamento telematico ad un unico centro [Ministero Interno: Circolare n. 558/SICPART/421.2/70/224632 'Sistemi di videosorveglianza in ambito comunale' del 2 marzo 2012]

4.59 sistemi intelligenti (di riconoscimento): Sistemi dotati di software che permettono l'associazione di immagini a dati biometrici o in grado di riprendere e registrare automaticamente comportamenti od eventi anomali e segnalarli (es. motion detection).

4.60 sistema di videosorveglianza: Sistema composto da telecamere, sistemi di videoregistrazione, di trasmissione e di visualizzazione.

4.61 sistemi di sorveglianza tecnologicamente avanzati: Sistemi dotati di software di analisi video per il monitoraggio attivo con invio di allarmi automatici a centrali delle FFPP (Forze di Polizia) o di Istituti di vigilanza privata convenzionati (di cui alla Legge 18 aprile 2017, n. 48).

4.62 Smart city: Città che:

- accresce continuamente il ritmo con cui incrementa la sostenibilità e la resilienza, migliorando sostanzialmente il metodo di coinvolgimento della società;
- perfeziona continuamente il modo in cui si realizza la collaborazione e i metodi di leadership;
- accresce l'integrazione tra discipline e sistemi urbani;
- ricorre all'utilizzo dei dati e delle tecnologie al fine di trasformare i servizi e la qualità della vita sia per le persone all'interno della città che per quelle con essa coinvolte (residenti, imprese, visitatori).

[ISO Technical Management Board Strategic Advisory group Smart Cities, giugno 2015]

4.63 spazio interno: Spazio collocato all'interno di un edificio.

[UNI EN 14383-1:2006, punto 3.47]

4.64 spazio periferico: Territorio e vicinato che circondano uno o più luoghi.

[UNI EN 14383-1:2006, punto 3.28]

4.65 spazio perimetrico: Spazio immediatamente adiacente ad un edificio (dai confini alla struttura dell'edificio, accessi compresi).

[UNI EN 14383-1:2006, punto 3.27]

4.66 stazione centrale di controllo (Control room): Locale pubblico o privato, dotato di personale fisso, che riceve e gestisce le segnalazioni di allarme da sistemi antintrusione, di rivelazione incendi e di dati tecnici degli edifici; per la progettazione e la selezione del personale di tale centrale sono richieste norme specifiche.

[UNI EN 14383-1:2006, punto 3.12]

4.67 target hardening: Difesa dei possibili obiettivi di criminalità e disordine.

5 SCENARIO DI RIFERIMENTO

5.1 SICUREZZA URBANA E CITTÀ SOSTENIBILE

Se definiamo l'ambiente come "l'insieme di condizioni, sociali, culturali e morali, nel quale una persona si trova e sviluppa la propria personalità" appare evidente che la sicurezza urbana sia uno dei principali requisiti per la sostenibilità.

Trattare la questione della sicurezza rafforza il diritto alla vita privata e la protezione della sicurezza pubblica, nonché la prevenzione e la gestione dei rischi nelle comunità.

La norma ISO 37101 in riferimento alle strategie, piani e progetti che una organizzazione deve elaborare e valutare per un sistema di gestione che miri allo sviluppo sostenibile di una comunità, propone degli esempi relativi agli aspetti di 'safety e security' collegati con i 6 obiettivi di sostenibilità della norma: attrattività; conservazione e miglioramento dell'ambiente; resilienza; uso responsabile delle risorse; coesione sociale e benessere.

Il tema della sicurezza inoltre emerge tra gli aspetti importanti da considerare nello sviluppo sostenibile delle comunità e deve basarsi su una strategia che abbia un approccio olistico, così come rappresentato nella Figura 1.

Non esiste una misura assoluta per la sostenibilità, essendo una caratteristica tipicamente territoriale, che può essere definita basandosi sul confronto tra aree differenti, oppure tra il confronto della stessa area in intervalli di tempo definiti. È necessario quindi individuare alcuni "indicatori di sostenibilità", attraverso i quali sia possibile ottenere un giudizio del tipo e della direzione dello sviluppo di un determinato processo di trasformazione, sia a livello urbano che territoriale. Tali parametri sono indici per definire e valutare, in forma non complessa e sintetica, il grado di crescita/regresso da un obiettivo di sviluppo sostenibile, mediante la valutazione quantitativa di alcune grandezze ritenute significative.

Nel lungo periodo l'attenzione è stata posta sulla sostenibilità urbana.

In tal modo gli indicatori hanno guadagnato grande evidenza tra gli strumenti di analisi, supporto tecnico/metodologico, comunicazione, di decisioni politiche dirette alla sostenibilità locale.

Oltre ai diversi sistemi di misurazione di fattori chiave per la sostenibilità su scala locale, sono stati sviluppati indicatori promossi non solo da organizzazioni internazionali come UNCS¹, AEA², EUROSTAT³, OCSE⁴ e ISO⁵, ma derivanti anche dalle esperienze di monitoraggio e valutazione della performance di piani di gestione sostenibile, maturate a livello urbano, dalle autorità locali competenti.

Gli indicatori di sostenibilità hanno quindi lo scopo di: informare, comunicare e sensibilizzare la comunità locale sul problema della sostenibilità, predisporre, un insieme di strumenti tecnici capaci di supportare, accompagnandolo, il processo di monitoraggio del grado di crescita o regresso dall'obiettivo dello sviluppo sostenibile.

Un indicatore di sostenibilità è efficace, quando evidenzia in modo semplice un andamento tendenziale rispetto all'obiettivo individuato e presenta la caratteristica di essere interpretabile rispetto ad un benchmark di riferimento, inoltre:

1. è facile da misurare;
2. è credibile;
3. è affidabile;
4. deve essere riconosciuto dalle istituzioni nazionali ed internazionali competenti.

Lo sviluppo sostenibile non può essere realizzato senza che i governi, le comunità locali e i singoli cittadini si adoperino per rispondere in modo idoneo e articolato alle principali sfide della sostenibilità.

Trattare di sicurezza urbana significa anche considerare la dimensione della criminalità. La criminalità oggi investe tutto il territorio urbano, non concentrandosi più in specifici quartieri; la minaccia viene avvertita da tutti i cittadini, non solo da quelli delle zone più disagiate. Desto inoltre sempre maggiore preoccupazione la diffusione di quella che può essere definita "area grigia dell'illegalità", caratterizzata da piccola criminalità, accattonaggio a volte aggressivo, muri deturpati da graffiti, prostituzione, ecc.

Per quanto concerne l'indicatore relativo alla sicurezza urbana, definito quale "il grado in cui le persone soffrono per la mancanza di sicurezza urbana"⁶, sono individuati quali elementi da considerare:

- l'unità di misura "Sicurezza Urbana equivalente (USeq)" pari alla percentuale totale della popolazione seriamente colpita dalla criminalità;
- l'orientamento delle politiche che devono essere indirizzate alla promozione della sicurezza urbana con lo scopo di ridurre e idealmente eliminare le aggressioni;
- la necessità di indicatori secondari per la stima della percentuale totale di infortuni irreversibili a lungo termine;

¹ UNCS¹ :Commissione per lo Sviluppo Sostenibile delle Nazioni Unite

² AEA :Agenzia Europea per l'Ambiente

³ EUROSTAT : Ufficio Statistico dell'Unione Europea

⁴ OCSE -:Organizzazione per la Cooperazione e lo Sviluppo Economico

⁵ ISO : International Organization for Standardization

⁶ Fondazione Europea per il miglioramento delle condizioni di vita e di lavoro (Eurofound)

- la componente di dati intesa come percentuale di persone vittime di attacchi;
- la composizione dell'indicatore pari alla percentuale totale della popolazione colpita dai due precedenti fattori.

Un indicatore può essere a priori assegnato a ciascun tema di policy. La varietà della natura e dell'ampiezza dei temi di policy determina la necessità di varietà degli indicatori da proporre.



Fig. 1 - Composizione delle politiche urbane ed indicatori di performance⁷

Per politiche di sicurezza urbana si intende “la sperimentazione di azioni volte a ridurre l’insicurezza del vivere quotidiano nelle città, anche nella sua dimensione percettiva e anche con riferimento a fenomeni diversi da quelli penalmente sanzionati. Caratteristiche queste che definiscono le politiche di sicurezza come politiche (...) i cui attori istituzionali sono, oltre allo Stato, anche gli altri livelli di governo territoriale e, in particolare, i comuni”.⁸

5.2 SICUREZZA URBANA E SCENARIO DI RIFERIMENTO LEGISLATIVO

5.2.1 LEGGE N. 48 DEL 18 APRILE 2017

Nel contesto italiano il Decreto-Legge 20 febbraio 2017 n.14 ‘Disposizioni urgenti in materia di sicurezza delle città’, convertito con modificazioni, dalla Legge n. 48 del 18 aprile 2017, pubblicata nella Gazzetta Ufficiale n. 93 del 21 aprile 2017, si pone l’obiettivo di “Prevenire i

⁷ Figura tratta da: Voula Mega and Jørn Pedersen, Urban Sustainability Indicators, 1998, pag.10

⁸ Amendola G., Città, criminalità, paure. Sessanta parole chiave per capire e affrontare l’insicurezza urbana, Liguori, Napoli, 2008.

fenomeni di criminalità organizzata diffusa e di promuovere legalità e rispetto del decoro urbano”.

Di seguito le misure più rilevanti.

5.2.1.1 SICUREZZA INTEGRATA

Si definisce sicurezza integrata l'insieme degli interventi assicurati dallo Stato, dalle Regioni, dalle Province autonome di Trento e Bolzano e dagli Enti locali, nonché da altri soggetti istituzionali, al fine di concorrere, ciascuno nell'ambito delle proprie competenze e responsabilità, alla promozione e all'attuazione di un sistema unitario e integrato di sicurezza per il benessere delle comunità territoriali.

Alcuni esempi di buone pratiche relative alla sicurezza urbana integrata sono descritti nelle Appendici A e B.

5.2.1.2 SICUREZZA URBANA

L'art. 4 del provvedimento legislativo introduce la definizione di sicurezza urbana (punto 3, definizione 4.56 della presente prassi di riferimento), sulla scia del Decreto del Ministero dell'Interno del 5 agosto 2008.

Lo stesso articolo individua alcune aree di intervento volte a promuovere la sicurezza urbana:

- riqualificazione e recupero delle aree o dei siti degradati;
- eliminazione dei fattori di marginalità e di esclusione sociale;
- prevenzione della criminalità, in particolare di tipo predatorio;
- promozione della cultura del rispetto e della legalità;
- affermazione di più elevati livelli di coesione sociale e convivenza civile.

5.2.1.3 PATTI PER L'ATTUAZIONE DELLA SICUREZZA URBANA

La legge istituisce i Patti sulla sicurezza urbana che Prefetti e Sindaci sottoscrivono con lo scopo di individuare congiuntamente gli interventi necessari per la sicurezza urbana.

In particolare, in attuazione dell'art. 2 della legge 48/2017 “Linee generali per la promozione della sicurezza integrata”, il Governo, le Regioni, e le Province autonome e gli Enti locali, in sede di Conferenza unificata, hanno approvato l'accordo sulle linee generali delle politiche pubbliche per la promozione della sicurezza integrata.

È opportuno richiamare nella presente prassi di riferimento come nel delineare queste politiche pubbliche la Conferenza Unificata abbia citato espressamente la normazione tecnica; in particolare nel settimo capitolo relativo all'inclusione sociale, tra le iniziative che abbiano l'obiettivo del miglioramento della qualità della vita e della riqualificazione socio-culturale delle aree e dei distretti “insofferenza” è stata citata la pianificazione urbanistica che “potrà valorizzare i criteri di sicurezza urbana” così come definiti dal rapporto tecnico UNI CEN/TR 14383-2, al quale viene dato ampio risalto nel punto successivo della presente prassi.

5.2.1.4 COMITATO METROPOLITANO

La Legge prevede anche la costituzione di un Comitato metropolitano presieduto congiuntamente dal Prefetto e dal Sindaco metropolitano: per azioni di analisi, valutazione e confronto sui temi di sicurezza urbana inerenti al territorio della città metropolitana.

5.2.1.5 STRUMENTI E OBIETTIVI PER L'ATTUAZIONE DI INIZIATIVE CONGIUNTE

All'art. 7 viene previsto che possano essere individuati specifici obiettivi per l'incremento dei servizi di controllo del territorio e per la sua valorizzazione.

Sotto il profilo del sostegno strumentale, finanziario e logistico possono concorrere enti pubblici, anche non economici, e soggetti privati, ferma restando la finalità pubblica degli interventi. Soggetti privati quali Enti gestori di edilizia residenziale, amministratori di condomini, imprese anche individuali, associazioni di categoria, consorzi o comitati, possono proporre progetti per la messa in opera di sistemi di sorveglianza tecnologicamente avanzati, dotati di software di analisi video per il monitoraggio attivo con invio di allarmi automatici a centrali delle forze di polizia o di istituti di vigilanza privata convenzionati. A tale scopo i Comuni possono deliberare detrazioni fiscali in favore dei soggetti che assumono a proprio carico gli oneri di investimento e di gestione dei sistemi.

5.2.1.6 DASPO URBANO

Il Daspo urbano, si può attivare contro chi:

- impedisce la libera accessibilità o la fruizione di aree e infrastrutture pubbliche;
- viene trovato in stato di ubriachezza;
- compie atti contrari alla pubblica decenza o esercita il commercio o l'attività di parcheggiatore abusivo.

È prevista una sanzione amministrativa da 100 a 300 euro e l'allontanamento.

La reiterazione delle condotte incriminate, consente al questore di disporre, con un provvedimento motivato, per un periodo da 6 mesi a 2 anni, un vero divieto di accesso all'area o all'infrastruttura in questione.

5.2.1.7 ARRESTO IN FLAGRANZA DIFFERITA

Risulta possibile l'arresto nel caso di violenza alle persone o alle cose, in occasione o durante manifestazioni pubbliche. La flagranza differita⁹ scatta solo per i casi in cui è obbligatorio l'arresto, ed entro 48 ore dal fatto. Inoltre, deve essere disponibile una documentazione video o fotografica del reato.

⁹ È considerato in stato di flagranza anche colui che, sulla scorta di documentazione video fotografica dalla quale emerge chiaramente il fatto, ne risulta autore, sempre che l'arresto sia effettuato non oltre il tempo necessario alla sua identificazione e, comunque, entro le 48 ore dal fatto. Tali disposizioni sono efficaci dalla data di entrata in vigore della legge di conversione fino al 30 giugno 2020 (art. 10, comma 6-*quater* D.L. 20 febbraio 2017, n. 14 convertito, con modificazioni, dalla legge n. 48/17 del 18 aprile 2017, G.U. n. 93 del 21 aprile 2017).

5.2.1.8 OCCUPAZIONE ABUSIVA E ARBITRARIA DI IMMOBILI

Tale fenomeno illecito è diventato nel corso degli anni particolarmente diffuso nelle grandi città, specie in relazione agli alloggi di proprietà pubblica.

L'art. 11 della legge interviene nella materia: il Prefetto, sentito il Comitato provinciale per l'ordine e la sicurezza pubblica, impartisce disposizioni al fine di prevenire, in riferimento al numero degli immobili occupati illecitamente da sgomberare, il pericolo di possibili turbative per l'ordine e la sicurezza pubblica e per assicurare il concorso della Forza pubblica all'esecuzione di provvedimenti dell'Autorità Giudiziaria concernenti i medesimi immobili.

L'articolo prevede che l'uso della forza pubblica per lo sgombero degli immobili illegalmente occupati, debba tenere in conto alcune differenti priorità, vale a dire:

- la situazione dell'ordine e della sicurezza pubblica nei territori interessati;
- i rischi [prevedibili] per l'incolumità e la salute pubblica;
- i diritti dei proprietari degli immobili occupati;
- i livelli assistenziali che devono essere in ogni caso garantiti dalle regioni ed enti locali a chi versando in stato di bisogno ne abbia diritto.

5.2.1.9 MISURE DI CONTRASTO AI PARCHEGGIATORI ABUSIVI

Per i parcheggiatori abusivi, sono previste multe rilevanti, da un minimo di 1.000 ad un massimo di 3.500 euro. Se nell'illecita attività sono stati coinvolti dei minori, o nei casi di reiterazione, la sanzione raddoppia. Viene comunque comminata la sanzione accessoria della confisca delle somme percepite.

5.2.1.10 MISURE DI CONTRASTO DELLO SPACCIO DI SOSTANZE STUPEFACENTI

Art. 13: il questore potrà disporre per motivi di sicurezza e nei confronti di soggetti condannati con sentenza definitiva o confermata in appello nell'ultimo triennio per reati di produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope, il divieto di accesso nei locali pubblici o aperti al pubblico in cui sono stati commessi gli atti illeciti.

Il divieto in questione non può avere una durata inferiore a un anno né superiore a cinque e può riguardare anche lo stazionamento dei soggetti raggiunti dal provvedimento nelle immediate vicinanze degli stessi locali.

5.2.1.11 MISURE DI CONTRASTO AI "WRITERS" [GRAFFITARI]

Con l'art. 16 del decreto, infine, si integra la formulazione dell'art. 639 Codice Penale.

Con l'obiettivo di combattere il fenomeno dilagante del deturpamento e imbrattamento di cose altrui (monumenti, muri di edifici, mezzi di trasporto pubblici o privati, ecc.), si prevede che "con la sentenza di condanna a carico dei trasgressori, il giudice può subordinare l'applicazione della sospensione condizionale della pena all'obbligo di ripristino e ripulitura dei luoghi oggetto dell'illecito". La stessa misura è adottata per i casi di recidività del medesimo reato.

Qualora non sia possibile mandare ad effetto tali misure, che impongono l'effettuazione di operazioni fisiche, al fine della concessione del beneficio può essere disposto da parte del giudice: l'obbligo di sostenere le spese di ripristino o di rimborsare quelle già sostenute o in alternativa, con il consenso del condannato, la prestazione di attività, utili per la collettività e non retribuite, per un periodo definito, comunque non superiore alla durata della pena sospesa, secondo quanto verrà indicato nella sentenza di condanna.

5.2.2 LINEE GENERALI PER LE POLITICHE PUBBLICHE DELLA SICUREZZA INTEGRATA

In riferimento all'art. 2 del Decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48 sono state approvate le 'Linee generali per le politiche pubbliche della sicurezza integrata', che rappresentano il quadro di riferimento nella materia.

Tali linee guida sono rivolte prioritariamente a coordinare, per lo svolgimento di attività di interesse comune, l'esercizio delle competenze dei soggetti istituzionali coinvolti, anche con riferimento alla collaborazione tra le Forze di polizia e la Polizia locale nei seguenti settori d'intervento:

- scambio informativo tra Polizia locale e Forze di Polizia presenti sul territorio per gli aspetti di interesse comune, ferme restando le rispettive attribuzioni istituzionali;
- interconnessione a livello territoriale delle sale operative della Polizia locale con le sale operative delle Forze di polizia;
- regolamentazione dell'utilizzo in comune dei sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività soggette a rischio;
- aggiornamento professionale integrato per operatori della Polizia locale e delle Forze di polizia.

Qui di seguito sono riportati alcuni punti delle Linee che riprendono azioni già descritte come facenti parte delle strategie di gestione della sicurezza e che beneficiano dell'innovazione tecnologica sia al riguardo dell'interscambio informativo dei dati, sia dell'accesso al CED Interforze da parte delle Polizie locali.

In senso esteso si richiama qui la sorveglianza spontanea e quindi si sintetizzano i riferimenti principali per l'utilizzo di informazioni inviate "spontaneamente" dai cittadini o da sensori presenti sul territorio.

Le Linee generali per le politiche pubbliche della sicurezza integrata delineano i seguenti aspetti:

- coinvolgimento dei Comuni negli accordi per la promozione della sicurezza integrata e nei progetti e iniziative ivi previsti: lo Stato e le Regioni possono concludere specifici accordi per la promozione della sicurezza integrata in attuazione delle Linee generali.

I Comuni interessati alla realizzazione di specifiche progettualità e iniziative contenute nell'accordo sono previamente coinvolti. Rappresentanti dei Comuni capoluogo e degli altri Enti locali interessati o coinvolti nelle specifiche progettualità partecipano, di volta in volta, ai tavoli tecnici, attivati dagli accordi, che verificano lo stato di attuazione e di avanzamento dei progetti.

- interscambio informativo dei dati: i Prefetti forniscono ai Sindaci dei Comuni capoluogo e delle Città metropolitane i dati in forma statistica sull'andamento della delittuosità, con cadenze periodiche.
- accesso al CED Interforze per le Polizie Locali: è prevista una massimizzazione delle opportunità di accesso al CED Interforze per consentire alla Polizia Locale di sfruttare le possibilità di consultazione e inserimento dei dati previste dall'attuale ordinamento. Le Regioni possono prevedere progetti e interventi per sostenere, anche finanziariamente, l'attivazione di collegamenti al CED da parte delle Polizie locali dei Comuni più interessati ai fenomeni di criminalità diffusa o dei Comuni con più limitate capacità di spesa.
- interconnessione delle sale operative della Polizia Locale e delle Forze di polizia: gli accordi potranno promuovere l'adozione di misure di sostegno nei confronti dei Comuni per l'implementazione di interventi di adeguamento tecnologico delle centrali esistenti o per la creazione di nuove ed incentivi per il passaggio a sistemi di conduzione in comune delle sale operative delle Polizie municipali che, soprattutto nei Comuni di più contenute dimensioni, rappresentano il volano per il definitivo passaggio o consolidamento della gestione associata delle funzioni e dei compiti di Polizia Locale.
- formazione integrata della Polizia Locale con le Forze di Polizia (*punto 6 dell'Accordo¹⁰*): è previsto un aggiornamento congiunto con il personale delle Forze di Polizia che verte non solo sulle materie più "tradizionali" ma anche su argomenti più attuali in virtù dell'evoluzione del quadro normativo e giurisprudenziale. Fondamentale è la distinzione dell'aggiornamento diretto al personale addetto al servizio di Polizia municipale rispetto a quello rivolto ai Dirigenti di servizio. Le Regioni possono sostenere finanziariamente le attività di formazione.

6 LINEE DI SVILUPPO DELLA SICUREZZA URBANA

6.1 GENERALITÀ

Il documento propone una riflessione su diversi aspetti relativi allo sviluppo di progetti di sicurezza urbana.

¹⁰ Linee generali delle politiche pubbliche per la sicurezza integrata (art. 2 del decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48)- Allegato A, Accordo sulle linee generali delle politiche pubbliche per la promozione della sicurezza integrata, punto 6.

In particolare sono considerati i seguenti elementi:

- tecnologia
- formazione e sviluppo delle competenze
- partnership
- sostenibilità finanziaria

6.2 SICUREZZA URBANA E TECNOLOGIA

L'utilizzo sempre più diffuso di nuove tecnologie, tra cui nuove modalità di rilevazione e raccolta dei dati, registrazione, identificazione, monitoraggio ed il noto tema della digitalizzazione, fusione e analisi dei dati, sta cambiando la struttura tecnica delle nostre città, che stanno divenendo "digitali" e "intelligenti". L'innovazione digitale contribuisce a connettere e fondere il vivere democratico con il bisogno di sicurezza urbana.

La tecnologia per la sicurezza urbana è un mezzo funzionale ad un approccio basato preminentemente sulla prevenzione.

La tecnologia non deve limitarsi a fornire nuovi strumenti per proteggere e controllare, ma anche a favorire la trasparenza (dati disponibili, possibilità di controllare la bontà degli interventi, ecc.), la partecipazione e responsabilizzazione dei cittadini, nonché servire anche al miglioramento dei servizi e della governance.

La tecnologia fornisce nuovi strumenti agli Enti e alle Autorità coinvolte nei processi di sicurezza urbana che, anche per le recenti disposizioni legislative hanno l'obbligo di essere parte di una strategia complessiva e multi-canale per la sicurezza urbana che deve avere l'obiettivo di affrontare in modo adeguato le diverse cause dell'insicurezza e non si riduca ad una mera gestione tecnica del rischio presumibile.

Tali strumenti possono anche contribuire a promuovere una prevenzione del crimine basata sull'evidenza dei fatti analizzabili, attraverso una migliore conoscenza dell'effettiva situazione locale di reale insicurezza e della percezione di insicurezza.

L'utilizzo di tecnologie per la sicurezza urbana non è esente da rischi, in particolare in termini etici e di rischio di possibili violazioni di diritti fondamentali.

Così come nel caso di altri strumenti di sicurezza urbana, occorre stabilire se le tecnologie previste per l'uso sono efficaci, facilmente utilizzabili e se giustificano l'investimento da operare.

Va inoltre affrontato il problema intrinseco della sorveglianza medesima. Infatti, anche se non sono tecnologie di sorveglianza diretta, molti di questi sistemi producono di per sé sorveglianza in modo indiretto. La posta in gioco non è solo un fatto di privacy poiché tocca anche la sfera dell'inclusione sociale e delle libertà di pensiero, di coscienza, di religione, di espressione, di associazione, ecc.

6.3 FORMAZIONE E SVILUPPO DELLE COMPETENZE

Lo sviluppo delle competenze in materia di sicurezza urbana è una necessità che le Istituzioni dovrebbero favorire, incoraggiando la formazione di professionisti della sicurezza urbana con l'ausilio delle università, scuole superiori e gli altri istituti di formazione, elaborando con il settore educativo ed il settore professionale criteri di validazione e di qualificazione professionale.

6.4 FAVORIRE LE PARTNERSHIP

Un elemento di crescita della sicurezza urbana consiste nell'azione delle istituzioni per favorire le partnership tra diversi soggetti (istituzioni medesime, Enti e pubbliche autorità, enti del terzo settore, privati, industria, ecc.).

Nel caso specifico, dopo l'identificazione degli obiettivi occorre individuare gli elementi occorrenti al loro raggiungimento, inclusa la necessità di indicare un ruolo chiaro per ognuno dei partners, incoraggiando la formazione e garantendo il corretto funzionamento delle partnership.

6.5 SOSTENIBILITÀ FINANZIARIA DEI PROGETTI DI SICUREZZA URBANA

La sostenibilità finanziaria dei progetti di sicurezza urbana è, dopo la progettazione, il principale elemento da tenere in considerazione per il raggiungimento degli obiettivi.

Assicurare la sostenibilità finanziaria dei programmi deve essere un impegno valutato a priori, pena il mancato raggiungimento degli obiettivi o, peggio, la dissoluzione delle iniziative di prevenzione pianificate.

A ciò si può arrivare:

1. controllando la destinazione delle risorse disponibili;
2. stabilendo e mantenendo un giusto equilibrio tra gli schemi di prevenzione del crimine e gli altri sistemi posti in essere al fine di prevenire con la maggiore efficacia ottenibile i comportamenti illegali;
3. intervenendo con chiarezza nel quadro delle responsabilità assegnate per il finanziamento, la pianificazione gli aspetti di coordinamento delle iniziative riguardanti le misure preventive contro i comportamenti illegali ed illeciti;
4. promuovendo la partecipazione della collettività alle misure che mirano ad assicurare la sostenibilità finanziaria (es. crowdfunding);
5. presentando progetti che possano rientrare tra le forme di sostegno finanziario previste dalla Legge 48/2017 all'art. 7, della quale verranno descritti gli aspetti salienti al successivo punto 8.2.

7 IMPLEMENTAZIONE DELLE SOLUZIONI DI SICUREZZA URBANA

7.1 GENERALITÀ

Nel processo di implementazione delle soluzioni di sicurezza urbana, il documento propone un riferimento al ruolo delle norme tecniche, alle competenze professionali della figura del progettista, ai processi di valutazione dei progetti e degli interventi, alla metodologia, alla verifica e valutazione delle azioni intraprese. Inoltre, il presente punto contiene una sintesi del rapporto tecnico UNI CEN/TR 14383-2:2010, che fornisce linee guida sui metodi per valutare il rischio di crimini e/o la paura del crimine e le misure, le procedure ed i processi volti a ridurre questi rischi.

7.2 PROPOSTE DI SICUREZZA URBANA PER LO SVILUPPO SOSTENIBILE DELLE CITTÀ

Uno spazio urbano privo di barriere fisiche e mentali, atto alla combinazione di usi e funzioni che lo rendono vitale non può essere frutto di solo design ambientale: è necessario che la comunità locale che ne fruisce sviluppi una forte rete di legami sociali e interpersonali. Un tessuto comunitario forte unito a un senso di “appartenenza territoriale” può essere efficace in termini di prevenzione del crimine.

In questo contesto, per la parte progettuale, un aiuto fondamentale può venire dalle norme tecniche disponibili.

La mancata rispondenza di un progetto a una norma tecnica di riferimento riconosciuta, solitamente comporta problemi e specifiche responsabilità del progettista incaricato.

Nel contesto della sicurezza urbana bisogna evitare che un progetto architettonico o urbano si rilevi carente o, peggio, inadatto in termini “prestazionali” rispetto alla medesima o se una volta realizzato inneschi dinamiche di rischio sociale.

Il progettista sarebbe investito di un’ ulteriore responsabilità che riguarda l’individuazione di strumenti più idonei e strategie di riduzione del crimine non facilmente individuabili, specie se non standardizzate, dovendosi adattare ai diversi contesti territoriali e locali di riferimento.

La valutazione di impatto sulla sicurezza dei progetti architettonici ed urbani, in tema di sicurezza urbana, comporta il possesso di una serie di specifiche competenze (in architettura, sociologia, urbanistica, criminologia, psicologia, economia, ecc.).

Si potrebbe prevedere la nascita di una nuova figura professionale che potrebbe definirsi come “coordinatore della sicurezza urbana in fase di progettazione”, tenendo già conto che ciò costituirebbe un onere, di natura economica, per il committente, sia esso pubblico, che privato ed evitando che un percorso valutativo sui progetti di sicurezza urbana possa diventare una pura pratica formale.

Un aiuto potrebbe arrivare dalla metodologia BIM e l’adozione di una specifica comune pratica per procedure condivise che consenta ai fornitori ed ai committenti di conseguire progetti di

sicurezza urbana adottabili con pratiche trasparenti, comparabili nei servizi e con garanzie sulla qualità dei dati, dei costi e dei tempi di esecuzione.

Un'iniziativa è stata recentemente adottata dal CNI (Consiglio Nazionale Ingegneri) con l'emanazione delle "Linee guida per il coordinatore della sicurezza in fase di progettazione". Le linee guida che sono correlate all'esecuzione di attività connesse al D.Lgs. 81/08, focalizzano in modo sintetico e sistematico una serie di obblighi e azioni, risultando un valido strumento di riferimento per coloro a cui sono dirette.

7.3 VALUTAZIONE DEI PROGETTI DI SICUREZZA URBANA

Per la valutazione dei progetti di sicurezza urbana si dovrebbero tenere in conto alcune indicazioni:

- 1) l'oggetto della valutazione deve essere chiaramente definito;
- 2) bisogna evitare di considerare come un risultato acquisito quanto è stato messo in opera. Ad esempio, non si può considerare un indicatore di valutazione l'intervento di installazione di un determinato numero di telecamere. Bisogna invece valutare gli effetti prodotti dall'installazione delle telecamere nel tempo;
- 3) nella valutazione di un progetto bisogna essere obiettivi e oggettivi, utilizzando per la valutazione riferimenti standard riconosciuti (es. norme tecniche, prassi di riferimento, ecc.);
- 4) gli obiettivi e modalità di realizzazione per il progetto di sicurezza urbana devono essere fissati a priori, non è corretto cercarli a posteriori se il progetto non li ha fissati con chiarezza in precedenza;
- 5) il confronto tra il "prima" e il "dopo" l'esecuzione dell'intervento ha una notevole importanza. In particolare, il monitoraggio del fenomeno del "dislocamento" (spostamento di un comportamento indesiderato dall'area di intervento a una differente area/località) o il "*contagio positivo*" (allargamento spontaneo degli effetti dell'intervento ad aree o a destinatari diversi da quelli inizialmente considerati).
- 6) considerate le specificità di ogni intervento (ogni intervento di sicurezza urbana è in generale fine a se stesso, considerate le molteplici variabili che intervengono nel processo), bisogna evitare di adeguare i risultati ottenuti in un determinato contesto ipotizzando, la trasferibilità del modello, mentre vada valorizzata l'esperienza che può essere comunque trasferita in una buona pratica neutra e generalizzata o in una "case history".

Se le risorse a disposizione per un progetto di valutazione sono limitate, è preferibile concentrarsi sulla valutazione di ambiti specifici dell'intervento più importanti dal punto di vista strategico.

7.4 INTERVENTI PER LA SICUREZZA URBANA

È compito di chi pianifica gli interventi favorire un processo che comprenda almeno:

- 1) un'analisi sistematica dei comportamenti illegali, le loro cause e concause, i fattori di rischio e il loro impatto sul territorio;
- 2) un piano esecutivo per mandare a effetto interventi mirati, caratterizzati da razionalità, efficacia, e avvalorati da entità capaci di perorare/propugnare la causa (media, social, ecc.);
- 3) lo sviluppo della forma d'approccio più idonea, la cui concezione dovrà dar modo di adattare, con la massima flessibilità, gli interventi alle situazioni identificate come problematiche e al contesto territoriale, particolarmente a livello locale.
In particolare, le pubbliche autorità dovrebbero favorire i programmi che riguardano la salute, il lavoro, l'educazione scolastica e l'abitazione, incoraggiando così le attività che rimedino alla marginalizzazione e all'esclusione che spesso sono l'acqua di coltura per l'insorgere di comportamenti asociali e violenti.
Non sono estranee a questa visione le strategie di regolazione dei conflitti e le iniziative di educazione e di sensibilizzazione dei cittadini per favorire una cultura della legalità e della tolleranza nel rispetto della multiculturalità.

La pianificazione degli interventi dovrebbe comprendere almeno le seguenti azioni:

1. la redazione di una matrice del rischio atta a descrivere la probabilità di accadimento dei fattori di rischio nel sito oggetto di indagine che includa almeno i seguenti aspetti:
 - furti interni ed esterni;
 - rapina;
 - intrusione;
 - attacchi vandalici;
 - danneggiamenti;
 - rischi ambientali (contaminazioni);
 - esondazioni;
 - incendi;
 - attacchi terroristici;
 - sequestro di persona;
 - rischi reputazionali.

La matrice dovrebbe indicare, per ciascuno dei fattori sopra descritti, il grado di probabilità (alto, medio, basso);

2. Un piano di mitigazione del rischio consequenziale alla redazione della matrice, atto a mandare ad effetto interventi mirati, caratterizzati da razionalità ed efficacia e adeguatamente comunicati ai cittadini attraverso i media;
3. L'indicazione delle possibili soluzioni urbanistiche, tecnologiche e di servizi in funzione delle caratteristiche territoriali e locali del sito oggetto di indagine.

7.4.1 METODOLOGIA DI ATTUAZIONE DEGLI INTERVENTI

La migliore forma di prevenzione è quella basata sul rilevamento oggettivo del contesto.

Si deve pertanto:

1. promuovere un approccio multidisciplinare nella pianificazione degli interventi di sicurezza urbana, laddove questo favorisca la partecipazione di competenze utili a innalzare l'efficacia delle soluzioni adottate;
2. favorire l'organizzazione schematica, la classificazione e la sintesi delle conoscenze colmando le lacune esistenti;
3. mettere a frutto le conoscenze acquisite assicurando il monitoraggio costante dei risultati ottenuti e la loro condivisione in un'ottica di sicurezza integrata tenendo conto dei bisogni manifestati dalla collettività;
4. favorire la messa a punto e l'adozione di un sistema di banche dati per supportare in modo più fattivo ed efficace la gestione della prevenzione delle attività illegali, inclusa la realizzazione di indagini quali-quantitative sulla percezione generale dei fenomeni di illegalità diffusa;
5. aggiornare, anche attraverso gli output delle suddette banche dati, le mappe del rischio favorendo l'adozione di contromisure per scongiurare la ripetizione di azioni illegali.

7.4.2 VERIFICA DELLE AZIONI INTRAPRESE E LORO VALUTAZIONE

I sistemi di monitoraggio e la misurazione sono strumenti coerenti e sinergici per la verifica delle azioni intraprese e una migliore comprensione in termini di valutazione.

La raccolta dei dati rilevanti è un asse portante del sistema di verifica e valutazione.

Occorre inoltre tenere conto dei sistemi di raccolta dati ed eventuale reportistica.

Le misurazioni fanno riferimento a quei processi strutturati di raccolta di dati significativi, condotti tramite i relativi indicatori, interpretati sulla base degli esiti ed utili a misurare e dare evidenza all'efficacia (o meno) delle azioni intraprese.

Qualunque attività deve essere legata a controllare nel tempo il grado di avanzamento delle azioni definite nel piano, al fine di verificarne la realizzazione secondo il cronoprogramma definito; ciò consente peraltro di intervenire con azioni a supporto, per esempio aumentando le risorse, qualora si avesse evidenza che il cronoprogramma non fosse rispettato.

Il sistema di monitoraggio e misurazione deve essere in grado di:

- identificare carenze nell'applicazione dei requisiti (di legge e altri);
- disporre di un cruscotto di indicatori idonei ed appropriati, definiti rispetto agli aspetti specifici trattati nell'ambito dei temi fondamentali e capace di restituire agli stakeholder interni ed esterni una fotografia accurata, completa e comprensibile del contributo che le azioni intraprese hanno dato a favore della sicurezza urbana e delle ricadute che ne

sono derivate sui diversi portatori di interesse e sull'ambiente;

governare il processo di attuazione, controllo e raccolta dati in modo da valorizzare la sinergia tra funzioni (Legge n. 48 del 18 aprile 2017), la razionalizzazione dell'impegno e la condivisione dei risultati;

- verificare l'implementazione delle azioni intraprese, garantendo il rispetto dei tempi.

La seguente tabella indica le possibili criticità nella verifica delle azioni intraprese e loro valutazione.

<p>Individuazione degli indicatori chiave</p>	<p>Non si identificano indicatori ma elementi qualitativi non misurabili e quantificabili.</p> <p>Non sono chiari e semplici per i portatori d'interesse.</p> <p>È necessaria un'attenzione progressiva, costante e sistematica</p>	<p>Impossibilità di rendere conto con la "dittatura delle cifre", anche se gli indicatori sono rilevati i portatori d'interesse non li comprendono. La lista è troppo limitata</p>
<p>Monitoraggio della performance</p>	<p>Non si assegna una persona al monitoraggio</p> <p>Le frequenze non sono idonee</p>	<p>Di fatto nessuno svolge monitoraggio.</p> <p>Farlo in ritardo significa sostenere i costi senza ottenere risultati</p>
<p>Mancanza di Interrelazioni fra i soggetti interessati (vedi Legge 18 aprile 2017, n. 48)</p>	<p>Non c'è sinergia tra i soggetti interessati</p>	<p>Si lavora su binari paralleli, producendo in forme diverse gli stessi dati utili per la verifica delle azioni intraprese.</p> <p>I dati non possono essere utilizzati in forma aggregata.</p>

Nel presente documento vengono suggeriti precisi indicatori, tuttavia, poiché è utile e prioritario rispetto alle attività di reporting utilizzare indicatori per la verifica delle azioni intraprese e per la loro valutazione, si suggerisce di utilizzare indicatori che siano:

- rilevabili periodicamente (es. con cadenza annuale);
- completi, quindi riferiti a tutte le attività poste in essere, con livelli di approfondimento selettivi, perché la rilevazione deve essere anche agile e facilmente fruibile e quindi non sempre può concentrarsi su aspetti di dettaglio;
- finalizzati a consentire di leggere i risultati anche da un punto di vista esterno;
- affidabili, cioè basati su dati e informazioni oggettive, attendibili e verificabili, acquisite attraverso un sistema di rilevazione metodologicamente corretto;
- che consentano di mantenere il collegamento tra quanto già fatto e quanto previsto fare in futuro, aiutando a leggere i risultati sia in termini di andamento, sia a consuntivo, in modo da definire le priorità di intervento per i periodi successivi;

- aperti e volutamente sottoposti al giudizio e al dialogo, utilizzabili in termini di comunicazione e di base per la discussione di merito;
- specifici e dedicati, in funzione della tipologia dell'organizzazione, sia essa pubblica, privata, profit, non-profit, di dimensione differente, ecc. in modo da avere una visione il più possibile efficace e completa.

7.5 SINTESI DEL RAPPORTO TECNICO UNI CEN/TR 14383-2:2010

7.5.1 GENERALITÀ

Il rapporto tecnico UNI CEN/TR 14383-2:2010 'Prevenzione del crimine - Pianificazione urbanistica e progettazione edilizia' fornisce delle linee guida sui metodi per valutare il rischio di crimini e/o la paura del crimine e le misure, le procedure e i processi volti a ridurre questi rischi.

Tenuto conto delle considerazioni generali e degli obiettivi descritti, al fine di declinare degli strumenti operativi utilizzabili dai vari soggetti interessati, si è ritenuto opportuno richiamare alcuni contenuti dell'UNI CEN/TR 14383-2.

Nella stesura della presente prassi di riferimento, oltre a rimandare a tale rapporto per la valutazione dei contenuti di dettaglio, si suggeriscono alcune integrazioni conseguenti l'innovazione tecnologica e le recenti normative introdotte in Italia.

L'UNI CEN/TR 14383-2 considera contemporaneamente "contenuti" e "processo":

- I contenuti rispondono alla domanda: quali strategie e misure possono essere implementate per prevenire e ridurre i problemi di criminalità e disordine in un determinato contesto.
- Il processo risponde alla domanda: come seguire un procedimento efficace ed efficiente, nel quale gli interessati scelgano le strategie e le misure più efficaci e fattibili per prevenire e ridurre i problemi di criminalità e disordine, da loro stessi individuati.

Contenuti e processo sono dettagliati nel Rapporto tecnico, ma prima di consultarli occorre valutare una serie di questioni preliminari che riguardano:

- l'individuazione dell'area (contesto): DOVE
- il problema della criminalità e del disordine: COSA
- i soggetti coinvolti/ interessati: CHI

7.5.2 ORGANISMO RESPONSABILE DELLA PIANIFICAZIONE URBANISTICA

Esistono numerosi modelli di riferimento per integrare le politiche di prevenzione di criminalità e disordine nella pianificazione urbanistica: dagli accordi di partenariato privi di un soggetto-guida formale, ai progetti diretti dalla polizia, a quelli fondati sul ruolo centrale delle amministrazioni locali. Ogni volta che si ha a che fare con strumenti che regolano la pianificazione urbanistica e la progettazione edilizia, dovrebbe essere presente un organismo democraticamente eletto che governi, direttamente o indirettamente, il processo di

pianificazione, di costruzione o di gestione del territorio. Nel Rapporto tecnico ci si riferisce a questo organismo come "Organismo Responsabile".

L'Organismo Responsabile può essere sia l'amministrazione locale, sia un gruppo di professionisti della pianificazione incaricato dalle autorità locali, regionali o nazionali, oppure un comitato dirigente interdisciplinare. Se la varietà degli interessati è considerevole, l'approccio è semplice e si basa su tre domande:

- **dove:** identificazione dell'esatta ubicazione dell'area (attraverso coordinate, definizione dei confini, utilizzo dei codici postali, ecc.) e della tipologia dell'area; l'area può essere una struttura urbana (edifici e strade) esistente o un'area nuova da progettare;
- **cosa:** individuazione generale e preliminare dei problemi di criminalità e disordine esistenti nell'area o dei problemi potenziali che possono verificarsi in futuro nella nuova area e della propensione della stessa area ad attrarre comportamenti antisociali e a generare insicurezza soggettiva;
- **chi:** identificazione degli interessati da coinvolgere per una definizione più dettagliata e approfondita dei problemi di criminalità e disordine e per l'implementazione delle misure di prevenzione e contrasto.

7.5.2.1 IDENTIFICAZIONE DELL'AREA: DOVE

È importante definire se l'area di intervento è di un nuovo impianto (per cui esiste solo il progetto) o se si tratta di un insediamento esistente. Le differenze sono infatti di vasta portata:

- **progettazione di nuova area/ nuovo progetto:** i fattori di criminalità e disordine e insicurezza soggettiva possono essere valutati solo basandosi su teorie o utilizzando esperienze tratte da quartieri e progetti molto simili per condizioni di progettazione e di contesto, questo tipo di analisi di criminalità e disordine dovrebbero essere chiamate "valutazioni predittive di sicurezza in un nuovo contesto urbano" dei problemi che potrebbero presentarsi in futuro nell'area, una volta realizzati gli interventi;
- **riqualificazione di area esistente:** i fattori di criminalità e disordine e insicurezza soggettiva possono essere analizzati nel concreto, attraverso, per esempio, i dati su criminalità e disordine registrata, le inchieste, le indagini sulla sicurezza, la raccolta delle esperienze e delle opinioni di residenti o dei fruitori della zona, degli esperti (agenti di polizia, gestori dei negozi, ecc.), l'osservazione diretta, le interviste a vittime e autori di reato, ecc.; questo genere di analisi delle condizioni di criminalità e disordine si può chiamare "diagnosi di sicurezza in un contesto urbano esistente" (valutazione dei problemi presenti in un'area urbana esistente ben definita).

7.5.2.1.1 CONTESTI NUOVI E GIÀ ESISTENTI

Nuovo contesto urbano	Contesto urbano esistente
Esiste solo il progetto	Tutto è già presente: persone, edifici, strade, ecc.

Progetto per un nuovo contesto	Progetto per la riqualificazione, il completamento, ecc.
Strumento: Diagnosi predittiva di sicurezza in un nuovo contesto urbano (vedere appendice A del rapporto tecnico UNI CEN/TR 14383-2)	Strumento: Diagnosi di sicurezza in un contesto urbano esistente (vedere appendice B del rapporto tecnico UNI CEN/TR 14383-2)

È importante in questa fase che i soggetti interessati e l'Organismo responsabile adottino strumenti per effettuare diagnosi di sicurezza diverse a seconda che il contesto urbano sia esistente o di progetto; il rapporto tecnico UNI CEN/TR 14383-2 riporta utili indicazioni nelle Appendici A e B citate nel precedente schema.

7.5.2.2 IDENTIFICAZIONE DEL PROBLEMA: COSA

Dopo aver definito l'area di studio, la domanda successiva riguarda l'individuazione dei problemi di criminalità e disordine esistenti (diagnosi di sicurezza in un contesto urbano esistente) o dei problemi di sicurezza che possono verificarsi in futuro nella nuova area oggetto di intervento (diagnosi predittiva di sicurezza in un nuovo contesto urbano).

I problemi da prendere in considerazione possono essere piuttosto diversificati: dall'insicurezza soggettiva, ai comportamenti antisociali, ai reati più gravi. Le valutazioni, basate sulle informazioni strutturali e socioeconomiche e sui dati relativi a criminalità e disordine, permetteranno di individuare tali problemi.

Le appendici A e B dell'UNI CEN/TR 14383-2 anzi citate danno alcune indicazioni per la "diagnosi di sicurezza in un contesto urbano esistente" e la "diagnosi predittiva di sicurezza in un nuovo contesto urbano", specificando le informazioni che possono essere utilizzate per tali valutazioni.

Per la definizione del problema da affrontare vengono distinti i comportamenti criminali (reati e non) e comportamenti antisociali o conflitti minori.

Un approfondimento, contenuto nell'appendice C dell'UNI CEN/TR 14383-2, riguarda l'insicurezza soggettiva ed il senso di disagio rispetto all'ambiente circostante, tenendo conto che l'insicurezza soggettiva è una reazione emotiva, difficile da misurare. In parte è dovuta a fattori di carattere generale (comportamento dei media, violenza nei film, insicurezza sociale ed economica) legati non alla dimensione locale, ma a scenari più ampi.

La pianificazione, l'urbanistica e la progettazione edilizia non possono intervenire direttamente su questo genere di paura, anche se un ambiente non ansiogeno può contribuire positivamente a ridurla.

Inoltre, viene approfondita la propensione di un luogo ad attrarre comportamenti criminali antisociali e a generare insicurezza soggettiva.

Molti studi hanno dimostrato che esiste una forte correlazione tra azioni criminose, comportamenti antisociali e le caratteristiche dell'ambiente costruito. L'insicurezza soggettiva e il senso di insicurezza o di disagio sono fortemente connessi con il carattere dell'ambiente. Anche allo scopo di analizzare questa correlazione, è necessario identificare, misurare e

valutare gli specifici fattori dell'ambiente fisico che permettono il realizzarsi di questo genere di correlazioni.

7.5.2.3 GLI INTERESSATI: CHI

Si possono identificare tre categorie di interessati:

- proprietari e committenti;
- specialisti che portano la loro esperienza al progetto;
- residenti e utilizzatori.

Si ritiene qui utile dettagliare la seconda delle categorie che riguarda:

7.5.2.3.1 SPECIALISTI CHE PORTANO LA LORO ESPERIENZA AL PROGETTO

I principali professionisti che possono contribuire al processo di pianificazione (in un'ottica di sicurezza) sono:

- pianificatori e progettisti: urbanisti, architetti, paesaggisti, ingegneri del traffico e dei trasporti, ingegneri civili;
- forze di polizia e servizi di sicurezza professionali: operatori di prevenzione di criminalità e disordine, operatori dei servizi di supporto alle vittime, agenzie e consulenti privati, compagnie di assicurazione;
- operatori sociali: assistenti sociali, mediatori dei conflitti, operatori di supporto per i gruppi marginali, operatori di supporto per le dipendenze da droghe;
- sociologi, psicologi, ricercatori.

Il ruolo di questi specialisti è puramente quello di fornitori di servizi dopo l'attuazione del progetto, possono essere assunti dai gestori e dai proprietari.

Appare utile sottolineare il coinvolgimento, tra gli specialisti, delle forze di polizia e dei servizi di sicurezza professionali. In proposito viene riportato nel punto 5.3 del presente documento relativo alle "Linee generali per la promozione della sicurezza integrata" un approfondimento sulle recenti disposizioni legislative introdotte in Italia.

7.5.3 CONTENUTI E PROCESSO

Una volta data risposta a queste tre domande, è possibile avviare il percorso decisionale rispetto a:

- quali siano le azioni possibili, necessarie e praticabili;
- in che modo tali azioni possono essere attuate ed eseguite.

Al punto 5 (linee guida di progettazione), l'UNI CEN/TR 14383-2 fornisce indicazioni relative alla prima domanda e al punto 6 (processo) presenta un metodo di aiuto e supporto alla creazione di un processo efficace di implementazione, esecuzione e valutazione.

In particolare, l'UNI CEN/TR 14383-2 propone utili suggerimenti sui contenuti e sui processi.

In merito ai contenuti si sofferma sulle strategie di pianificazione e progettazione urbanistiche e sulle strategie di gestione.

In particolare, viene introdotto il tema della creazione di una densità urbana adeguata a permettere vitalità e sorveglianza spontanea del territorio (si veda il punto 7.5 del documento); Vengono inoltre suggeriti contenuti specifici per le Strategie di gestione.

Le strategie di gestione in materia di prevenzione di criminalità e disordine riguardano:

- il “target hardening” (rendere gli obiettivi meno “facili” per gli autori di reato);
- la manutenzione;
- il controllo (pattugliamento, videosorveglianza);
- le regole (di condotta del pubblico negli spazi pubblici);
- la disponibilità di attrezzature per gruppi particolari,
- la comunicazione (di messaggi informativi e regole di condotta per il pubblico).

In pratica nessuna area urbana si gestisce completamente da sola: la maggior parte di esse necessita di un certo grado di controllo e manutenzione di tipo professionale.

Le strategie di gestione possono prevedere l'intervento di figure professionali e sono finalizzate a supportare e a incoraggiare la sorveglianza spontanea e il senso di appartenenza dei residenti e dei visitatori. Il coinvolgimento di soggetti esterni non significa però l'esclusione dei residenti da questo genere di funzione: le strategie di gestione presuppongono un certo livello di autogestione, che può però passare ad un livello superiore con l'aiuto di professionisti.

Le strategie di gestione hanno una maggiore importanza in aree in cui già esistono problemi di criminalità e disordine su cui è necessario intervenire. In tali casi, la portata degli interventi di pianificazione e disegno urbano può essere limitata e sono quindi necessarie strategie di gestione per creare le condizioni per un'azione completa ed efficace.

L'UNI CEN/TR 14383-2 si conclude con i processi analizzando e schematizzando in particolare il processo per le politiche di prevenzione e di riduzione di criminalità e disordine e dell'insicurezza soggettiva attraverso la progettazione e la gestione urbana.

Viene quindi schematizzato il seguente, diagramma di flusso.

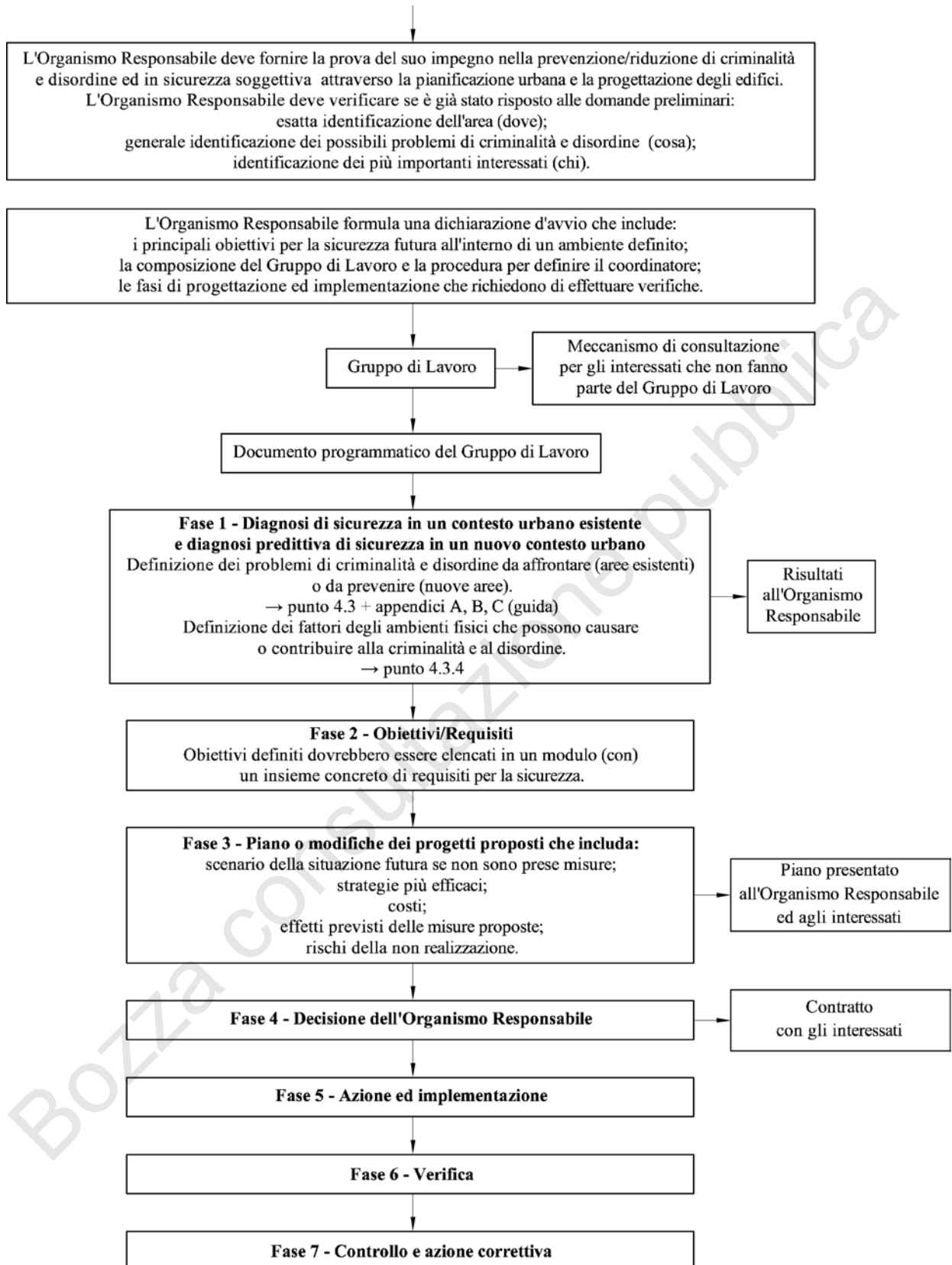


Figura 2 :UNI CEN/TR 14383-2 - Schema di processo

7.6 SORVEGLIANZA SPONTANEA

7.6.1 GENERALITÀ

Nell'ambito dell'integrazione dei dati si evidenzia l'utilizzo di informazioni che giungono spontaneamente dal territorio.

Il primo aspetto della sorveglianza spontanea, nella progettazione urbanistica, è quello di agevolare i cittadini nel farsi parte attiva e diligente nel migliorare lo stato di benessere collettivo in un determinato contesto urbano.

Un secondo aspetto riguarda le possibilità offerte dalle attuali tecnologie di consentire l'invio di segnalazioni alle Forze di Polizia in merito ad accadimenti che possono apparire minacciosi per la sicurezza propria od altrui.

Il documento elenca qui di seguito alcuni esempi di sorveglianza spontanea:

- Numero Unico di Emergenze;
- sorveglianza spontanea automatica;
- applicazione YouPol;
- EENA- Segnalazione spontanea e segnalazione automatizzata;
- Help Point Ferroviennord

7.6.2 NUMERO UNICO DI EMERGENZE (NUE)

Il sistema di gestione unificata delle chiamate di emergenza è un sistema che porta l'informazione relativa ad un qualche tipo di emergenza, rilevata in modi eterogenei, ad un ente autorizzato e competente ad avviare l'azione successiva.

La modalità base è la chiamata telefonica. Un secondo metodo è il messaggio telefonico che, se inviato a mezzo di un'apposita APP, consente la geo-localizzazione precisa (es. esperienza AREU).

Per dettagli ci si può riferire, tra gli altri, al documento della European Emergency Number Association (EENA) "Public safety digital transformation: the Internet of Things and emergency services"¹¹, che si pone l'obiettivo di individuare diverse modalità di trattamento di informazioni rese disponibili dalle innovazioni tecnologiche.

7.6.3 SORVEGLIANZA SPONTANEA AUTOMATICA

Il concetto base di sorveglianza spontanea automatica potrebbe essere esteso anche ad informazioni generate automaticamente che devono giungere al giusto ente competente.

¹¹ Public Safety Digital Transformation: The Internet of Things (IoT) and Emergency Services, European Emergency Number Association (EENA), 3 marzo 2016

L'esistenza di infrastrutture per la gestione del Numero Unico Emergenze permette, ad esempio, di automatizzare l'invio di segnalazioni di emergenza in modalità M2M (Machine to Machine).

Un esempio recente è quello dell'installazione di dispositivi di chiamata d'emergenza "eCall", in grado di allertare automaticamente i servizi di soccorso in caso d'incidente stradale, su tutti i nuovi modelli di auto e furgoni leggeri dal 31 marzo 2018, secondo le norme approvate dal Parlamento europeo.

Un altro esempio è costituito da una videocamera intelligente che è sostanzialmente un dispositivo che mette in posizione ON una diagnostica di potenziale allarme (evento) e la rende disponibile ad un apparato che trasmette il messaggio in modo che un sistema possa inoltrarlo all'ente che può/deve analizzarne il contenuto ed eventualmente avviare un'azione in loco.

In tal modo l'utilizzo del sensore (nel caso specifico videocamera) spinge (push) l'informazione oltre a rimanere comunque a disposizione per essere "interrogata" in modalità "pull".

Il documento dell'EENA citato al punto 7.5.1, riporta dei suggerimenti, alcuni dei quali elencati qui di seguito, per chi si accinge a valutare progetti di gestione di allarmi automatici.

- Un elemento chiave consiste nel capire preventivamente come gestire le moli di dati ed eseguire le analisi per prevenire extra costi causati dalle moltitudini di sorgenti di informazioni e dall'enorme numero di elementi e flussi;
- Comprendere come applicare alla gestione delle emergenze le tecnologie già esistenti in ambito commerciale (es. i contact center multicanale) per prendere decisioni sulla priorità degli allarmi e consentire ai sistemi automatici di superare i picchi che si osservano durante i principali eventi e incidenti;
- Esaminare i metodi per ottimizzare il numero di PSAP (Public Safety Answering Point) laddove sussistano molti PSAP di piccole dimensioni. Ciò consentirà l'introduzione di nuovi servizi per i cittadini in modo più efficiente e controllato;
- Considerare più alternative per fornire efficienza operativa e proporre soluzioni finanziariamente ragionevoli; ad esempio, dovrebbero essere agevolati i centri più grandi che hanno iniziato a costruire competenze ed esperienza per gestire i nuovi servizi. In questo contesto, è necessario valutare PSAP virtuali e distribuzioni basate su cloud;
- Effettuare analisi di valutazione del rischio in termini di prospettive tecniche (sicurezza) e operative (gestione del cambiamento);

Si raccomanda di impostare la strategia di implementazione delle nuove tecnologie e di sviluppo dei nuovi servizi tenendo presenti i seguenti suggerimenti:

- individuare quali sarebbero gli utenti ed i gruppi target per i nuovi sistemi di allarmistica automatica basati su Internet. Iniziare con le comunità piccole e chiuse per acquisire esperienza, prima di aprire le funzionalità ad altri insiemi più complessi quali:
 - scuole e università, a causa dell'elevato numero di persone interessate da un problema di sicurezza;
 - edifici pubblici e istituzioni come biblioteche, edifici amministrativi e siti con una grande quantità di lavoratori e visitatori;

- luoghi che ospitano eventi sportivi e culturali;
- industrie speciali come i trasporti (stazioni ferroviarie, aeroporti);
- infrastrutture critiche (petrolio e gas, energia, ecc.)
- Quali informazioni e media si vogliono trattare e gestire?
Si dovrebbe iniziare con quelli più semplici da gestire (ad esempio caricamento di immagini da fotocamere smartphone, posizioni GPS che tracciano il percorso seguito da un escursionista disperso).
- Indirizzare e spingere la strategia verso il tipo di comunicazione originata automaticamente che dovrebbe essere introdotta nel sistema. Questa decisione favorisce ed abilita al pieno utilizzo delle "chiamate automatiche" non originate dall'uomo:
 - l'eCall europeo è un esempio di percorso iniziato su spinta obbligatoria in questo nuovo contesto. Occorre monitorare e consolidare gli insegnamenti chiave che si traggono dall'esperienza di implementazione di eCall.
- Iniziare valutando i casi d'uso documentati in applicazioni Next Generation 112 (ad esempio video, testo in tempo reale);
- Se si desidera aprire i servizi di emergenza per allarmi di applicazioni o dispositivi originati da terze parti, è necessario fornire interfacce e API ben strutturate per consentire agli sviluppatori di terze parti di creare App per dispositivi intelligenti o sviluppare funzioni in dispositivi connessi che possono generare allarmi nei PSAP.
Si pensi ad una piattaforma di certificazione nazionale per consentire la connettività solo per dispositivi e applicazioni certificati.

7.6.4 APPLICAZIONE YOUPOL

La nuova App della Polizia di Stato denominata "YouPol"¹², già attiva nelle città di Roma, Milano e Catania dal novembre scorso, sarà operativa anche nelle restanti città capoluogo di regione.

L'App ha lo scopo di permettere a tutti, giovani e adulti, di interagire con la Polizia di Stato, consentendo l'invio di segnalazioni di episodi di bullismo o di spaccio di sostanze stupefacenti. Come descritto nel video di presentazione, con l'App si potranno denunciare fatti di cui si è testimoni diretti (anche mediante foto o immagini acquisite sul proprio dispositivo) ovvero notizie di cui si è appreso in forma immediata (link, pagine web, ricezione messaggi, informazioni orali, ecc.).

L'applicativo è scaricabile su tutti gli smartphone e tablet che utilizzano Android e Ios, e consente di interagire con la polizia inviando immagini o segnalazioni scritte direttamente alle sale operative delle questure, anche se il segnalante si trova in una provincia diversa.

L'utente avrà anche la possibilità di effettuare una chiamata di emergenza alla sala operativa della provincia nella quale si trova, utilizzando un pulsante ben visibile di colore rosso

7.6.5 EENA - SEGNALAZIONE SPONTANEA E SEGNALAZIONE AUTOMATIZZATA

In riferimento alle possibilità di segnalazione spontanea e di segnalazione automatizzata, al fine di valutarne l'efficacia nei diversi scenari di progettazione, pianificazione e gestione della sicurezza urbana, si rimanda per approfondimenti al documento EENA 'What Internet

¹² Informazione tratta dal portale Internet della Polizia di Stato, 8 febbraio 2018

Companies can do in Emergency and Crisis situations¹³ in cui viene prodotto un “case study” esemplificativo. Questo “case study” nasce con la collaborazione di Autorità Pubbliche e Organizzazioni e offre una panoramica su come applicazioni e tecnologie disponibili possano essere d'aiuto per fronteggiare emergenze e situazioni di crisi.

7.6.6 HELP POINT FERROVIENORD

Sulla rete FERROVIENORD sono installati dei dispositivi di videotelefonia, denominati Help Point, dislocati nei vari spazi di stazione (biglietteria, atrio, ascensori, ecc..) e lungo le linee ferroviarie (passaggi a livello o gallerie ferroviarie).

Hanno un design molto funzionale con tre tasti e un cartello su come utilizzare il dispositivo.

Il primo tasto serve per richiedere informazioni relative alla circolazione ferroviaria, mettendo il viaggiatore direttamente in contatto con il personale FERROVIENORD.

Il secondo serve per l'intervento sanitario e il terzo per l'intervento della polizia: questi ultimi mettono in comunicazione con il Posto Centrale di Vigilanza (PCV) di FERROVIENORD, che gestisce la richiesta in funzione delle informazioni che riceve.

Tutte le chiamate sono registrate, sia video che audio, in modo da tracciare le comunicazioni avvenute.

¹³ What Internet Companies can do in Emergency and Crisis situations, European Emergency Number Association (EENA 112), 21 novembre 2017

APPENDICE A - MESSA IN SICUREZZA DI PROMENADE DES ANGLAIS, NIZZA

In riferimento al punto 5.4.1 del documento di prassi, si riporta il caso applicativo reale di sicurezza urbana integrata

Obiettivi del progetto*

1. Mettere in sicurezza 4km di marciapiede del lungomare di Nizza (Promenade des Anglais) in relazione al potenziale transito di veicoli in movimento, non autorizzati e guidati da soggetti con intenzioni omicide
2. Realizzare un sistema di controllo e di gestione generale degli accessi al marciapiede, regolamentandone al contempo i transiti
3. Attuare interventi migliorativi del paesaggio urbano installando soluzioni il più possibile 'embedded', anche grazie all'integrazione con il nuovo verde, piantumato con finalità di camouflage
4. Migliorare la coesistenza dei transiti pedonali e dei transiti con bici

Tipologia di committenza: Pubblica

Valore complessivo: € 28 MLN

Data di esecuzione: 2016-2017

Tipologie di soluzioni installate

- ✓ 287 dissuasori fissi
- ✓ 48 dissuasori amovibili
- ✓ 28 dissuasori a scomparsa
- ✓ Barriere semovibili in occasione di eventi pubblici
- ✓ 2 km. Di cavi d'acciaio del diametro di 22mm

Principali criticità e soluzioni adottate

1. *Proteggere la pista ciclabile lungo l'intero percorso con soluzioni esteticamente gradevoli e poco visibili.* Sono stati installati cavi d'acciaio del diametro di 22mm supportati da pali. Per assicurare un effetto camouflage sono stati piantati 300 nuovi alberi. Rif.Fig.2
2. *Mantenere la fluidità di circolazione del traffico veicolare nonostante la restrizione di alcuni punti di accesso.* E' stata parzialmente modificata la circolazione sia dei veicoli privati, sia dei mezzi di trasporto pubblico cittadino (autobus). Rif. Fig.2

Note integrative*

La municipalità di Nizza (Città Metropolitana) aveva pianificato il progetto prima dell'attentato terroristico del luglio 2016. Si trattava di un progetto di riqualificazione generale del lungomare. Successivamente a questa data lo ha revisionato per rafforzare il sistema di gestione del rischio e implementare le soluzioni di sicurezza.

Gli studi preliminari per la seconda versione del progetto sono durati tre mesi. I lavori sono durati complessivamente un anno. I varchi veicolari, il cui accesso è controllato dai dissuasori a scomparsa, sono controllati a distanza da un control room. I dissuasori si abbassano tutti i

gironi dalle ore 4 alle ore 8.30 per consentire il transito dei mezzi di rifornimento HORECA alle stazioni balneari presenti nel tratto chiuso (Fig.1).

Nella seconda versione del progetto è stato introdotto un sistema di lettura targhe, inizialmente non previsto, in grado di monitorare i transiti lungo 4 km di carreggiata. Inoltre sono stati inseriti nuovi impianti di videosorveglianza, integrati con quelli preesistenti.

* Fonte: Direction de l'Infrastructure et de la Circulation, Services Espaces Publics et Voiries- METROPOLE COTE D'AZUR

Figura 1- Vista panoramica

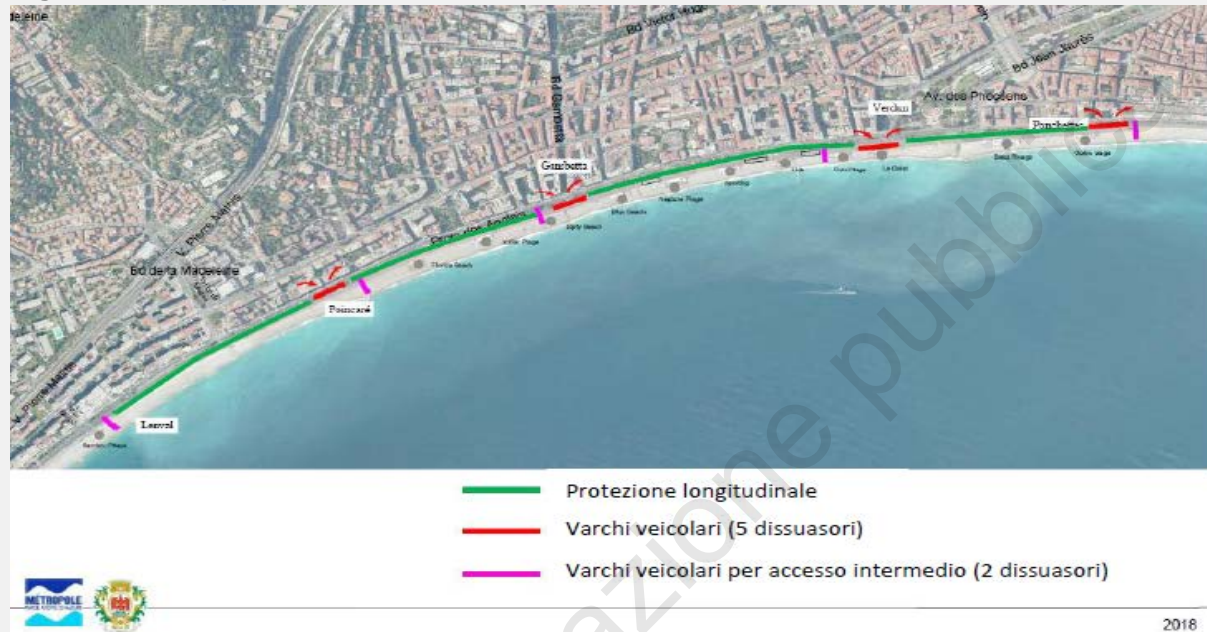


Figura 2- Carreggiata



APPENDICE B - SISTEMA DI VIDEOSORVEGLIANZA DELLA CITTA' DI VENEZIA

In riferimento al punto 5.4.1 del documento di prassi, ove si è introdotto il tema della sicurezza urbana integrata, si riporta il caso applicativo del sistema di videosorveglianza della città di Venezia.

Obiettivi del progetto:

1. Sorvegliare i palazzi storici del centro cittadino (in particolare: Piazza S. Marco, Piazza Ferretto ed il Ponte di Rialto);
2. Incrementare la sicurezza per i cittadini ed i turisti;
3. Efficientare i costi di gestione;
4. Sostituire il sistema analogico di videosorveglianza con un sistema IP basato su rete

Tipologia di committenza: Pubblica

Valore complessivo: n.d

Data di esecuzione: 2012 -2018 (Revamping ed implementazione progressiva del sistema)

Tipologie di soluzioni installate

- ✓ Software di gestione per le control room
- ✓ Monitor full HD per le control room
- ✓ Camere HD 8 e16 MP
- ✓ Network Video Recorder
- ✓ Analogue Video Encoder

Principali criticità e soluzioni adottate

1. *Conversione in HD dei sistemi di videosorveglianza analogici installati in precedenza (60 videocamere), al fine di assicurare l'uniformità dell'alta definizione del flusso di immagini.*

La conversione è resa possibile dall'utilizzo di encoder per la migrazione del sistema esistente verso un sistema IP basato su rete. Il sistema analogico presentava infatti due principali criticità: i lunghi tempi di ricerca delle immagini e il livello di dettaglio fornito dalle stesse (es. primi piani in una piazza affollata), livello ritenuto non sufficientemente adeguato. Infine, non erano rari i malfunzionamenti e la conseguente impossibilità di utilizzare immagini indispensabili a scopo di indagine.

2. *Implementazione delle funzioni di storage dei NVR.* Questo problema è stato risolto installando NVR in grado di ottemperare a due esigenze: adeguato spazio di registrazione e mantenimento dell'alta definizione - e dunque della qualità complessiva delle immagini registrate.

Note integrative

L'installazione del nuovo sistema di videosorveglianza presso la città di Venezia è stato avviato nel 2012. La prima fase ha previsto la conversione, nella piattaforma, di tutte le videocamere

IP esistenti. In una seconda fase sono state installate nuove videocamere da 16MP nelle zone ritenute strategiche. Da allora il sistema è stato progressivamente sia arricchito (con l'introduzione di nuove videocamere e componenti hardware) sia implementato a livello di software di gestione. Per monitorare le zone più estese e ritenute più critiche dal punto di vista della sicurezza urbana sono state installate videocamere da 30 MP.

In Piazza S. Marco le due videocamere installate sono 'esteticamente' bene integrate e posizionate sotto le arcate del campanile. La prima videocamera assicura la visuale in direzione della banchina del molo, mentre la seconda copre l'area in direzione dell'Ala Napoleonica del Museo Correr.

Ad oggi il sistema di videosorveglianza è composto da 200 videocamere.

Il Comune e le Forze dell'Ordine evidenziano come il revamping del sistema abbia consentito di acquisire due principali vantaggi. Il primo è la sicurezza di poter recuperare, in poco tempo e in alta definizione immagini necessarie alle indagini (senza limiti di volume in termini di storage: il sistema assicura la registrazione in alta definizione H24 per almeno sette giorni). Il secondo è l'abbattimento dei costi di manutenzione (le videocamere sono meno, ma più evolute tecnologicamente) e di risorse (i venditori abusivi, ad esempio, possono essere individuati e direttamente identificati da una persona attraverso la piattaforma di gestione e senza necessariamente pattugliare il territorio interessato).

Figura 1 e 2- Dettagli del sistema di videosorveglianza a Venezia



APPENDICE C - ESEMPIO DI ILLUMINAZIONE INTELLIGENTE E VIDEOSORVEGLIANZA: STATUA DEL CRISTO REDENTORE A RIO DE JANEIRO, BRASILE

Il rifacimento dell'impianto di illuminazione della statua del Cristo Redentore a Rio de Janeiro è un esempio di come l'uso intelligente dell'illuminazione urbana e delle tecnologie connesse può avere un impatto anche sulla sicurezza urbana.

Il sistema non solo illumina la statua, creando a richiesta effetti altamente spettacolari, ad esempio vestire il Redentore con colori della bandiera biancoceleste per commemorare il Bicentenario dell'Indipendenza dell'Argentina, ma permette di gestire in maniera intelligente e sicura sia l'illuminazione che le telecamere di sorveglianza dell'area circostante.

L'azienda incaricata dell'Illuminazione del Cristo, in occasione del rifacimento dell'impianto, ha deciso di dotarsi di un sistema (fornito da un'azienda italiana) di telegestione e telecontrollo, che consenta di ottimizzare l'utilizzo e la manutenzione dei 340 proiettori LED, da 56 watt cadauno, e delle telecamere.

I benefici sono stati valutati nel 64% di riduzione atti di criminalità ed oltre il 20% di risparmio manutentivo, il che significa anche maggior continuità di servizio.

Il sistema di telecontrollo permette sia la gestione che la diagnostica in tempo reale dell'illuminazione e delle telecamere da internet o da smartphone.

Il sistema si basa sulle onde convogliate, sfruttando così per la trasmissione dei dati un'infrastruttura già esistente, cioè la rete elettrica.

Questo, oltre a garantire risparmi di installazione e di manutenzione, dà una notevole sicurezza sia dal punto di vista fisico, essendo normalmente le reti elettriche ben protette sia da eventi accidentali che dolosi, che dal punto di vista informatico, dato il quadro di comando è il solo punto accessibile da Internet, pertanto è da proteggere con la massima cura.

APPENDICE D - CASO APPLICATIVO REALE DI SORVEGLIANZA DELLA RETE FERROVIENORD

In riferimento al punto 7.5 della prassi di riferimento, ove si è introdotto il tema delle strategie di gestione, si riporta il caso applicativo reale di sorveglianza con guardie itineranti nelle stazioni della rete FERROVIENORD.

FERROVIENORD è il gestore dell'Infrastruttura della rete ferroviaria di proprietà della Regione Lombardia. Con 331 km di linee e 125 stazioni, da sempre soffre di problemi legati alla micro-criminalità, spaccio e atti vandalici; con il progressivo impresenziamento degli impianti, l'azienda ha dovuto affrontare con maggiore impegno il problema della sicurezza dei viaggiatori e delle infrastrutture. Il processo di innovazione è partito agli inizi degli anni duemila ed è in continua evoluzione grazie alle nuove tecnologie disponibili sul mercato.

Di seguito viene esposto il processo di innovazione che ha coinvolto FERROVIENORD.

Antecedentemente al 2005, ogni stazione disponeva di un sistema di allarme antintrusione collegato ad un ponte radio bidirezionale proprio che, in caso di allarme, inviava un segnale alla centrale operativa dell'istituto di vigilanza privato che ne deteneva la competenza. L'istituto, in autonomia, provvedeva ad inviare una propria pattuglia per gli accertamenti in loco. A FERROVIENORD veniva, al termine dell'intervento, rilasciato un rapporto di servizio cartaceo con i dettagli dell'operazione. Analogo discorso per il sistema di videosorveglianza: le telecamere installate in ogni stazione risultavano essere visibili da locale, in quanto collegate ad un videoregistratore collocato nella stessa.

Nel 2008 FERROVIENORD ha creato il Posto Centrale di Vigilanza (PCV) – organo unico e accentrato in cui avviene quotidianamente la gestione della security. In esso sono remotizzati gli impianti anti-intrusione e i sistemi di videosorveglianza (ivi compresi quelli installati negli impianti elevatori – ascensori, rampe e scale mobili – in servizio pubblico) dell'intera rete.

Per il pronto intervento rimaneva la criticità di dover dipendere in egual modo dalle centrali operative dei singoli istituti di vigilanza, con tempi di attesa che variavano in funzione della disponibilità delle pattuglie presenti in quel momento sul territorio. L'agente giunto in loco, per comunicare con FERROVIENORD doveva necessariamente passare attraverso la propria centrale operativa. La creazione del PCV ha permesso di fare in modo che l'operatore in turno possa redigere, a seguito di intervento o di evento, un rapporto di servizio standardizzato in formato digitale recapitato automaticamente e in tempo reale a FERROVIENORD.

Dall'anno 2016, in virtù di una diversa filosofia societaria –orientata verso la sicurezza nelle stazioni ferroviarie – è stato impostato un nuovo concetto di security che prevede la presenza di guardie denominate “dinamiche”. Gli agenti in servizio, automuniti e dislocati in punti strategici della rete, a seguito di chiamata da parte del PCV hanno la possibilità di recarsi in tempi brevi in ognuna delle stazioni di propria competenza territoriale. Per mezzo del PCV, la comunicazione tra FERROVIENORD e guardie è così divenuta diretta; inoltre gli agenti che effettuano questo tipo di servizio in maniera continuativa, acquisiscono progressivamente una conoscenza degli spazi e delle dotazioni presenti nelle stazioni potendo agire in maniera più autonoma, rapida e professionale, aumentando la qualità del servizio reso e riducendo ulteriormente i tempi di intervento.

In conclusione, si è passati da una fase in cui FERROVIENORD veniva semplicemente messa a conoscenza al termine degli eventi (a volte anche in maniera piuttosto approssimativa) ad una fase in cui, grazie all'istituzione del posto centrale (PCV), l'azienda è direttamente protagonista nella risoluzione degli eventi critici, anche in situazioni dove è necessario l'ausilio

di altre strutture interne (reparti manutentivi, personale addetto alla gestione della circolazione ferroviaria, personale addetto al decoro delle stazioni). Il lavoro di remotizzazione e degli apparati e delle informazioni, unito alla presenza sul territorio delle guardie dinamiche, ha permesso di ridurre notevolmente i tempi di intervento, di aumentare la qualità del servizio di security e di aumentare, infine, la sicurezza dei viaggiatori e del patrimonio aziendale.

Bozza consultazione pubblica

BIBLIOGRAFIA

- [1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)
- [2] Legge Urbanistica Statale 17 agosto 1942, n. 1150 come modificata ed integrata da: legge 21 dicembre 1955, n. 1354; legge 6 agosto 1967, n. 765; legge 19 novembre 1968, n. 1187; legge 1° giugno 1971, n. 291; legge 22 ottobre 1971, n. 865; legge 28 gennaio 1977, n. 10; d.l. 23 gennaio 1982, n. 9, convertito in legge 25 marzo 1982, n.94; legge 28 febbraio 1985, n. 47; d.l. 23 aprile 1985, n. 146, convertito in legge 21 giugno 1985, n. 298; legge 24 marzo 1989, n. 122; legge 17 febbraio 1992, n. 179.
- [3] Ministero Interno: Direttiva 28 luglio 2017 'Modelli organizzativi per garantire alti livelli di sicurezza in occasione di manifestazioni pubbliche'.
- [4] Ministero Interno: Circolare n.558/SICPART/421.2/70/224632 'Sistemi di videosorveglianza in ambito comunale' del 2 marzo 2012
- [5] Ministero Interno: Piattaforma della videosorveglianza integrata e allegato documento tecnico. Circolare n. 558/SICPART/421.2/70/224632 'Sistemi di videosorveglianza in ambito comunale', 2 marzo 2012
- [6] Ministero Interno: Circolare n.558/A/421.2/70/195960 'Sistemi di videosorveglianza, Sollecito ad ANCI a sensibilizzare i Comuni, 6 agosto 2010
- [7] Ministero Interno: Circolare 'Linee guida videosorveglianza', 8 febbraio 2005
- [8] CONFERENZA UNIFICATA DEL 24.01.2018: Accordo tra il Governo le Regioni e gli Enti locali ai sensi dell'articolo 9 comma 2 lett. c) del decreto legislativo 28 agosto 1997 n. 281 finalizzato alla determinazione delle linee generali delle politiche pubbliche per la promozione della sicurezza integrata ai sensi dell'articolo 2 del decreto legge 20 febbraio 2017 n. 14 convertito con modificazioni dalla legge 18 aprile 2017 n. 48. [Repertorio Atti n. 4/CU del 24/01/2018]
- [9] Circolare CNI n.117/XIX 'Linee guida per il coordinatore della sicurezza in fase di progettazione', 27 settembre 2017
- [10] Garante per la protezione dei dati personali: Provvedimento in materia di videosorveglianza - 8 aprile 2010 [Gazzetta Ufficiale nr. 99 del 29 aprile 2010]
- [11] CEI EN 62676-1-1:2014 Sistemi di videosorveglianza per applicazioni di sicurezza Parte 1-1: Requisiti di sistema – Generalità
- [12] UNI/PdR 4:2013 'Servizi di integrazione dei sistemi audio, video e controlli (AVC) - Requisiti di progettazione, installazione, configurazione, taratura, programmazione e verifica tecnica'

- [13] European Emergency Number Association (EENA 112), 'What Internet Companies can do in Emergency and Crisis situations', 21 novembre 2017
- [14] European Emergency Number Association (EENA 112), 'Public Safety Digital Transformation: The Internet of Things (IoT) and Emergency Services', 3 marzo 2016
- [15] Garante per la protezione dei dati personali: Vademecum 'Il Condominio e la privacy', 2013
- [16] ANCI, Linee guida per i comuni in materia di videosorveglianza alla luce del provvedimento Garante privacy, 8 Aprile 2010
- [17] Garante per la protezione dei dati personali, 'Videosorveglianza - Provvedimento generale', 29 aprile 2004

Bozza consultazione pubblica