



UNIONE EUROPEA
Fondo europeo di sviluppo regionale



REPUBBLICA ITALIANA



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA



COMUNE DI SUNI PROVINCIA DI ORISTANO

POR FESR 2014-2020 - INTERVENTO “REALIZZAZIONE DI RETI PER LA SICUREZZA DEL CITTADINO E DEL TERRITORIO – FASE 2”

PROGETTO DEFINITIVO - ESECUTIVO

RELAZIONE TECNICA GENERALE

I Progettisti

Ing. Carlo Pisanu

Il Responsabile del Procedimento

Ing. Francesca Campus

Ing. Emanuele Tendas

Ing. Luisa Mameli

Elab.

A

Rev.00 del 07-01-2020

Sommario

1. INTRODUZIONE	1
2. NORMATIVA DI RIFERIMENTO	2
3. FINALITA' DEL PROGETTO	4
4. SOLUZIONE PROGETTUALE.....	6
4.1. Backbone Wireless	6
4.2. Caratteristiche Telecamere IP	7
4.3. Centro di Controllo	8
5. SITI DI INTERESSE	11
6. IMPIANTI.....	14
6.1. Alimentazioni Elettriche.....	14
6.2. Conduitture	14
6.3. Pali	15
7. CONNESSIONE ALLA RTR	16
7.1. La Rete Telematica Regionale	16
7.2. Il Sistema Regionale Centralizzato di Monitoraggio	16
8. NORME PER LE AZIONI DI INFORMAZIONE E DI COMUNICAZIONE	19
9. INTEGRAZIONE DEI SISTEMI PERIFERICI DI VIDEOSORVEGLIANZA CON IL SISTEMA CENTRALE SCNTT	21
9.1. Requisiti Fondamentali.....	22
9.2. Gestione Rilevamenti	23
10. TRATTAMENTO DEI DATI PERSONALI	26
10.1. Conservazione e Sicurezza delle Riprese.....	28
10.2. Il Decreto n.101 del 10 Agosto del 2018.....	29
10.3. A EDPB – DRAFT LINEE GUIDA 3/2019 SULLA VIDEOSORVEGLIANZA	30
11. SERVIZIO DI MANUTENZIONE E GARANZIA	35
12. QUADRO ECONOMICO DEI LAVORI	36

1. INTRODUZIONE

Con Determinazione n°71 Prot. 902 del 18.02.2019 del Direttore del Servizio dell'Assessorato degli Affari Generali, Personale e Riforma della Regione Sardegna sono stati approvati, ai sensi dell'art. 12 dell'Avviso Pubblico relativamente al finanziamento POR FESR 2014-2020 - Obiettivo Tematico 2 – Azione 2.2.2 - Intervento "Rete per la Sicurezza del Cittadino e del Territorio. Reti Sicurezza - Fase 2", i finanziamenti al comune di Suni per un importo pari a Euro 40'000.

Il presente progetto definitivo - esecutivo sviluppa una parte del progetto di fattibilità tecnica ed economica, che prevedeva l'installazione di **n.21 telecamere Bullet e n.5 con sistema lettura targhe** e l'insieme di tutti gli apparati necessari per sorvegliare diverse zone "sensibili" all'interno del centro abitato di Suni, oltre che le principali zone di accesso.

Per questioni legate alle risorse finanziarie disponibili, non sarà possibile eseguire la totalità dei lavori; per questo, il presente intervento svilupperà tecnicamente la porzione di rete e di apparati rientranti nell'importo del finanziamento predetto. Verranno comunque descritte e rappresentate graficamente tutte le zone da videosorvegliare con le rispettive telecamere.

Tutte le telecamere del progetto definitivo - esecutivo, rispettano le posizioni del precedente progetto di fattibilità tecnica ed economica che ha avuto il parere favorevole da parte della Prefettura di Nuoro, N° Protocollo 0071784 del 16/12/2019.

2. NORMATIVA DI RIFERIMENTO

- Decreto Legislativo 18 aprile 2016, n. 50 Codice dei Contratti pubblici di Lavori, Servizi, Forniture;
- Decreto Legislativo n. 81 del 9 aprile 2008, Testo unico in materia di salute e sicurezza sul lavoro;
- Direttiva del Ministero degli Interni sui sistemi di videosorveglianza in ambito comunale, N. 558/SICPART/421.2/70/224632 del 02/03/2012;
- Norma EN 62676-1-1, EN 62676-1-2, EN 62676-2-1, EN 62676-2-2 EN 62676-2-3, EN 62676-3, EN 62676-4, CEI EN 62676-1-1 (Requisiti generali di sistema), CEI EN 62676-4 (Linee guida di applicazione), CEI UNI EN 16763 (CEI 79-94) "Servizi per i sistemi di sicurezza antincendio e i sistemi di sicurezza";
- EDPB – Draft Linee Guida 3/2019 sulla videosorveglianza, Guidelines 3/2019 on processing of personal data through video devices
- Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
- Regolamento UE n. 2016/679 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;
- Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. n. 101 del 10 agosto 2018, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- D.Lgs. 18/05/2018, n. 51 recante: "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio."
- art. 54 del D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni;
- decalogo del 29 novembre 2000 promosso dal Garante per la protezione di dati personali;
- circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/A/471;

- D.L. 23 febbraio 2009, n. 11, recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori", ed in particolare dall'art. 6;
- "Provvedimento in materia di videosorveglianza" emanato dal garante per la protezione dei dati personali in data 8 aprile 2010.
- REGOLAMENTO (UE) N. 1303/2013 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 dicembre 2013 recante disposizioni comuni sul Fondo europeo di sviluppo regionale, sul Fondo sociale europeo, sul Fondo di coesione, sul Fondo europeo agricolo per lo sviluppo rurale e sul Fondo europeo per gli affari marittimi e la pesca e disposizioni generali sul Fondo europeo di sviluppo regionale, sul Fondo sociale europeo, sul Fondo di coesione e sul Fondo europeo per gli affari marittimi e la pesca, e che abroga il regolamento (CE) n. 1083/2006 del Consiglio; art. 115, art.116, art.117 e relativi allegati.
- REGOLAMENTO DI ESECUZIONE (UE) N. 821/2014 DELLA COMMISSIONE, del 28 luglio 2014, recante modalità di applicazione del regolamento (UE) n. 1303/2013 del Parlamento europeo e del Consiglio per quanto riguarda le modalità dettagliate per il trasferimento e la gestione dei contributi dei programmi, le relazioni sugli strumenti finanziari, le caratteristiche tecniche delle misure di informazione, di comunicazione e di visibilità per le operazioni e il sistema di registrazione e memorizzazione dei dati, in particolare art. 5.

3. FINALITA' DEL PROGETTO

I sistemi di videosorveglianza rappresentano un valido strumento d'ausilio per le forze dell'ordine nelle attività di controllo del territorio urbano. L'applicazione di sistemi di ripresa introduce nuovi metodi di intervento fornendo differenti possibilità di utilizzo, tra le quali riportiamo:

- Controllo e visualizzazione da remoto di un evento
- Ricostruzione dell'evento tramite l'analisi delle immagini archiviate
- Deterrenza contro atti vandalici
- Analisi selettiva e rilevamento di un evento con segnalazione automatica in remoto
- Controllo del traffico
- Rilevamento meteorologico

L'utilizzo di sistemi di videosorveglianza ha garantito negli ultimi anni differenti e decisivi risultati nelle attività di prevenzione degli eventi di microcriminalità nei territori urbani. Il livello di prestazione di questi sistemi si è evoluto nel tempo con l'introduzione di nuove tecnologie sia dal punto di vista delle unità di ripresa delle immagini che da quello di trasmissione ed archiviazione delle stesse.

Scopo di questo documento è la descrizione del Progetto di un Sistema di Videosorveglianza finalizzato alla sicurezza urbana integrata nell'area del Comune di Suni (Or).

Il progetto intende realizzare un sistema di videosorveglianza di spazi pubblici per consentire la registrazione di scenari atti a supportare le forze di polizia nell'attività di prevenzione e contrasto delle illegalità, soprattutto per soddisfare l'esigenza dei cittadini di una più diffusa ed efficace salvaguardia dei beni pubblici e privati e di ripristino delle condizioni di sicurezza.

Il sistema di videosorveglianza ha quindi l'obiettivo di "integrare" le azioni di carattere strutturale, sociale e di controllo del territorio da parte degli organi di polizia.

Nello specifico la realizzazione e la gestione del sistema di videosorveglianza è finalizzata a:

- ✓ Prevenire fatti criminosi attraverso un'azione di deterrenza che la presenza di telecamere è in grado di esercitare;
- ✓ Sorvegliare in presa diretta zone che di volta in volta presentano particolari elementi di criticità o in concomitanza di eventi rilevanti per l'ordine e la sicurezza pubblica;
- ✓ Favorire la repressione degli stessi fatti criminosi qualora avvengano nelle zone controllate dalle telecamere ricorrendo alle informazioni che il sistema sarà in grado di fornire;
- ✓ Rassicurare i cittadini attraverso una chiara comunicazione sulle zone sorvegliate.

Il progetto deve consentire la sua realizzazione attraverso uno sviluppo scalare sulla base delle necessità che emergeranno nel corso del tempo.

L'archivio dei dati registrati costituisce, inoltre, per il tempo di conservazione successivamente stabilito, un patrimonio informativo per le finalità di polizia giudiziaria con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati.

La finalità del Progetto è quella di realizzare un sistema di videosorveglianza che preveda l'installazione di telecamere nei punti di maggiore passaggio, individuati in relazione alle possibili vie di fuga, così distribuite:

- Principali vie d'accesso al territorio del Comune di Suni;
- Aree interne alla suddetta area di maggior interesse: Piazze, Parcheggi, Edifici di particolare rilevanza Storico-Culturale-Sportivo.

Di seguito saranno individuati i punti di installazione delle telecamere, che potranno essere naturalmente modificati ed integrati nel tempo in relazione a diverse e sopravvenute esigenze.

Nell'ambito del sistema di videosorveglianza che si intende realizzare, l'Amministrazione, deciderà se implementare o meno il sistema in modo più capillare sull'intero territorio comunale secondo interventi definiti per successive fasi.

4. SOLUZIONE PROGETTUALE

La soluzione tecnologica ingegnerizzata prevede un sistema di videosorveglianza distribuito composto da tre elementi fondamentali:

- Backbone Wireless
- Telecamere IP dislocate su territorio
- Centro di Governo

4.1. **BACKBONE WIRELESS**

Il Backbone Wireless rappresenta la dorsale digitale sulla quale instradare il traffico dati acquisito dalle telecamere e successivamente inviato verso il server di videosorveglianza centralizzato.

Dovrà essere realizzata una rete altamente performante con topologia Point-to-Point (PtP) sfruttando la banda trasmissiva libera ISM (Industrial Scientific & Medical), detta anche banda collettiva, dei 5 Ghz. (Hiperlan - 5,42-5,78 GHz). L'insieme delle PtP (Point-to-Point) saranno realizzate attraverso l'uso di apparati business class e costituirà dunque la topologia di rete precedentemente citata.

La dorsale dovrà contare su una capacità trasmissiva in linea con i più recenti standard tecnologici (IEEE 802.11ac) in termini di trasmissione radio e si avvarrà di tutte le feature proprie dello stesso. Lo standard 802.11ac prevede una velocità trasmissiva reale che si attesta attorno ai 450 Mbit/sec. e garantisce una retro compatibilità con tutti i precedenti draft dello standard quali l'802.11a, b e g. La feature sfruttata per raggiungere tale capacità trasmissiva viene identificata col nome di MIMO (Multiple-Input-Multiple-Output) che consente l'utilizzo di più antenne in contemporanea sia per la trasmissione che per la ricezione delle informazioni, aggregando più flussi di dati e moltiplicando dunque per n volte la velocità trasmissiva di base.

Gli apparati radio previsti, conformi alle norme vigenti in termini di EMC (Electromagnetic Compatibility), dovranno essere terminati, così come le telecamere, su un dispositivo di switching manageable dedicato che dovrà supportare la funzionalità Power over Ethernet (PoE – IEEE802.3af) e dovrà essere in grado di fornire connettività e alimentazione per ciascuna delle telecamere previste attraverso un numero congruo di porte ethernet.

4.2. CARATTERISTICHE TELECAMERE IP

Le telecamere saranno di due tipologie. Una tipologia è utilizzata per sorvegliare l'ambiente circostante a una media-bassa distanza mentre l'altra tipologia è atta ad effettuare la lettura targhe degli automezzi in transito. Entrambe dovranno rispettare i requisiti minimi indicati dalle *Linee Guida RAS*.

Le telecamere con finalità di **sorveglianza degli scenari**, saranno prodotte da leader riconosciuto sul panorama mondiale della videosorveglianza su IP.

Le caratteristiche minime di questi apparecchi devono essere:

- **Telecamere Bullet/dome fixed:** Compatibilità ONVIF; Sensore 1/2.5" CMOS (4:3), Ottica 3.6mm/F2.0, Illuminazione minima 0,01/F2.0 (color) - 0,01 F1.2 (IR), Day/night ICR, Massima distanza IR 30m, Compressione video H265, Risoluzione 5 Mpixel (2592 x 1944), Frame rate 50/60fps@10800P, Multi-streaming 2/3 streams, Analisi video: Tripwire, intrusion, Scene change, Abandoned/missing e Face detection, Micro SD, Grado di protezione IP67, Temperatura di esercizio ~ -30°C ~ +-+ 50 °C.
- **Telecamere Bullet/dome varifocal:** Compatibilità ONVIF, Sensore 1/3" CMOS 4 Mp, Ottica 3,3-12 mm /F1.4 motorized, Illuminazione minima 0,05 Lux /F1.4 (color) 0Lux /F1.4 (IR), Day/night ICR, Massima distanza IR 50 m, Compressione video H.264/H.265/MPEG4/MJPEG, Risoluzione 4 Mpixel (2688x1520), Frame rate 50/60fps@1080P, Multi-streaming 2/3 streams, Analisi video (Tripwire, intrusion, Scene change, Abandoned/missing e Face detection), Micro SD, Grado di protezione IP67, Temperatura di esercizio ~ -30°C ~ +50°C.
- **Telecamera speed dome:** Compatibilità ONVIF, Sensore 1/2.8" CMOS, Ottica 5-129 mm (optical zoom), Illuminazione minima 0.05Lux/F1.4 (color) - 0Lux /F1.4 (IR), IR; Massima distanza IR (328ft) 150 Mt; Compressione video H265, Risoluzione 3 Mp (2048 x 1536), Frame rate 30fps@1.3M/720P, Multi-streaming 3 streams, Analisi video: Tripwire, intrusion, Abandoned/missing e Face detection; Micro SD, Grado di protezione IP67, Temperatura di esercizio -10 / +50.

L'alta qualità delle immagini e le funzionalità proprie dei sistemi "day&night" e "motion-detection", renderanno le telecamere individuate, fisse, ideali per un monitoraggio

costante h24, 7 giorni su 7 in qualsiasi condizione di luce e/o meteo grazie anche agli illuminatori all'infrarosso.

Ciascuna delle telecamere dovrà essere classificata IP67. A corredo, integrati, ove previsto, dovrà prevedere la fornitura di un illuminatore infrarossi al fine di garantire una maggiore qualità video per le aree prossime agli apparati in zone poco illuminate.

Le **telecamere per lettura targhe** dovranno avere le seguenti caratteristiche minime: Compatibilità ONVIF, Sensore 1/1.8" progressive CCD CMOS, Ottica 4 ~ 8mm, Risoluzione 3 Mpixel (2048 x1536) a 25Fps, Illuminazione minima 0.002Lux/F1.2 (color), Day/night ICR, Eventi: Lettura targhe europee fino a -180km/h, Compressione video H265, Frame rate 60fps@10800P, Grado di protezione IP66, Temperatura di esercizio ~ -40°C ~ +80°C. Completa di software di riconoscimento lettura targhe ANP.

Garanzia di compatibilità per la realizzazione dell'interconnessione del sistema al centro **SCNTT** (Sistema Centralizzato Nazionale Targhe e Transiti) di Napoli.

4.3. CENTRO DI CONTROLLO

Sarà disponibile, presso i locali dell'Amministrazione (Municipio), il Locale Tecnologico dove eseguire l'installazione fisica, la configurazione e la messa in esercizio nelle macchine server, dell'armadio e del gruppo di continuità.

La piattaforma e il tipo di gestione/archiviazione sono garantiti da un sistema NVR (Digital Video Recorder) di tipo Embedded in contenitore installabile a rack 19" 2U con pannello frontale Easy Flip Down per l'inserimento dei dischi da frontale, supporta sistema operativo linux di tipo ridondato. Supporto sino a 64 ingressi IP (ONVIF o SDK di terze parti), risoluzione dei canali IP sino a 12Mpixel, banda totale massima in ingresso 320Mbps (200Mbps con RAID abilitato). Supporto doppia scheda di rete Ethernet 1Gbps configurabile in modalità multi indirizzo oppure load balancing oppure fail over. Supporto sino a 128 stream in rete (320Mbps). e della piattaforma di archiviazione dati adibite ad ospitare il software di gestione dell'intera infrastruttura. L'insieme di tutti questi elementi rappresenterà il vero e proprio Centro di Governo della soluzione di videosorveglianza.

Supporto sino a 4HDD SATA + DVD R/W oppure 8HDD SATA senza DVD R/W da 6TB cadauno inseribili su slitta dal pannello frontale. Supporta 1 HDD esterno su porta eSATA. Supporta la gestione proprietaria in gruppi degli HDD con la possibilità di effettuare la

registrazione ridondata delle telecamere su più di un disco e supporta la gestione degli array di dischi in modalità RAID1, 5, 0, 10.

Il sistema NVR dovrà essere completo di software riconoscimento lettura targhe ANP, gestione completa di tutte le telecamere installate, Sistema di video management VMS tipo "MILESTONE xprotect" o similare. È inoltre prevista l'installazione di un software di controllo in remoto da installare nella stazione dei Carabinieri e di collegamento al sistema informativo della Questura locale per il check in tempo reale delle targhe segnalate.

Caratteristiche minime:

- ✓ 1 ingresso audio, canale voice talk, 2 uscite audio, 2 uscita video HDMI (di cui una a risoluzione 4K e una in risoluzione FullHD), 2 uscite video VGA (sino a risoluzione FullHD). 16 ingressi allarme per gestione allarmi, 4 uscite relè, porta RS485 e RS232, porta RS485 per tastiera opzionale, 1 porta eSATA, 2 porte USB ver 2.0, 1 porta USB ver 3.0.
- ✓ funzione hot spare N+1;
- ✓ funzione ANR per il ripristino della registrazione effettuata a bordo telecamera;
- ✓ funzione transcoded playback per la riproduzione da remoto della registrazione con frame rate e risoluzione inferiore;
- ✓ webserver Internet Explorer® Firefox® Chrome®; la soluzione proposta garantisce la gestione delle mappe grafiche;
- ✓ SDK proprietario per la centralizzazione su client di terze parti. Include applicazioni proprietarie per iOS, Android® e Windows Phone8®. Supporta integrazione su terze parti per mezzo di API proprietarie, protocollo CGI. Compatibile con lo Standard ONVIF ver 2.2 profilo S e standard CGI, PSIA. La soluzione proposta comprende un alimentatore interno 110-240Vac e dispone di 2 schede di rete Ethernet auto adattanti 10/ 100/ 1000M.
- ✓ SO embedded base linux di tipo ridonato per incrementare la sicurezza e la stabilità del sistema;
- ✓ Funzionalità hot spare di tipo N+1 che prevede l'utilizzo di un NVR di tipo hot standby in soccorso automatico in caso di guasto di uno degli N NVR in normale esercizio;

- ✓ Funzionalità della codifica del canale zero che permette di visualizzare da remoto in un unico stream video sino a 16 telecamere contemporaneamente in 16 riquadri;
- ✓ Playback automatico a velocità normale in corrispondenza di eventi filtrati e a velocità 16x in assenza di eventi filtrati;
- ✓ Funzionalità transcoded playback per la riproduzione da remoto della registrazione ad un frame rate e risoluzione inferiori rispetto a quella della registrazione;
- ✓ Funzionalità ANR per il ripristino della registrazione a bordo NVR della registrazione effettuata a bordo telecamera a seguito di disconnessione e successiva riconnessione di una telecamera IP;
- ✓ Visualizzazione in live con 25/32/36/64 riquadri sul monitor collegato all'uscita video. Supporta la funzione click and drag nella finestra di visualizzazione live per regolare automaticamente l'ordine delle telecamere visualizzate;
- ✓ livello di accesso multiutente protetto da password;
- ✓ gestione evoluta di eventi quali motion detection face detection, intrusion detection, virtual plane traversing, allarme perdita fuoco, allarme telecamera spositonata e di associare delle correlazioni agli eventi;
- ✓ maschere di privacy, allarme tamper e video loss;
- ✓ log file filtrabile per data/ora e per tipologia di evento (operazioni, allarmi ed eventi) su due livelli di filtro;
- ✓ tag sulla registrazione e permette di effettuare il playback per tag;
- ✓ zoom digitale durante il live ed il playback;
- ✓ snapshot manualmente per mezzo di un'icona disponibile sull'interfaccia di live e di playback;
- ✓ importare ed esportare la configurazione delle telecamere IP collegate per mezzo di un file in formato exel;
- ✓ la gestione di mappe grafiche;
- ✓ SDK proprietario per la centralizzazione su client di terze parti;
- ✓ applicazioni proprietarie per iOS, Android® e Windows Phone8®;
- ✓ integrazione su terze parti per mezzo di API proprietarie, protocollo CGI.

Webserver Internet Explorer® Firefox® Chrome®.

5. SITI DI INTERESSE

Di seguito si elencano i siti di interesse oggetto d'intervento secondo le richieste e le modalità espresse dall'Amministrazione comunale di Suni.

Il sistema di videosorveglianza distribuito prevede la realizzazione del centro di controllo all'interno del Municipio, lo sviluppo della maggior parte della struttura di rete-radio prevista per i collegamenti e l'installazione **n. 3 telecamere Bullet** e **n.2 telecamere lettura targhe** dislocate nei seguenti spazi ed edifici pubblici.

Elenco telecamere e posizioni incluse nel finanziamento RAS (n°3 telecamere bullet e n.2 telecamere lettura targhe):

Municipio:

- n°1 switch POE 8 porte Gb
- n°3 Ponte radio 5Ghz
- n°1 telecamere Bullet

Scuola Elementare:

- n°1 switch POE 8 porte Gb
- n°2 Ponte radio 5Ghz
- n°1 telecamere Bullet

Scuola Media:

- n°1 switch POE 8 porte Gb
- n°1 Ponte radio 5Ghz
- n°1 telecamere Bullet

Biblioteca - Ludoteca:

- n°1 switch POE 8 porte Gb
- n°2 Ponte radio 5Ghz

Ingresso Macomer:

- n°1 switch POE 8 porte Gb
- n°1 Ponte radio 5Ghz
- n°1 telecamere lettura targhe
- n°1 Alimentatore di switching con carica batterie integrato

Ingresso Circonvallazione nord - direzione Bosa:

- n°1 switch POE 8 porte Gb

- n°1 Ponte radio 5Ghz
- n°1 telecamere lettura targhe
- n°1 Alimentatore di switching con carica batterie integrato

Sono indicati inoltre i punti da videosorvegliare che non rientrano all'interno dei finanziamenti RAS di cui l'Amministrazione ha fatto richiesta e che potranno essere integrati con successivi interventi.

Elenco telecamere e posizioni non incluse nel finanziamento RAS (n°18 telecamere bullet e n°3 telecamere lettura targhe):

Scuola Elementare:

- n°1 telecamera Bullet

Scuola Media:

- n°1 telecamera Bullet

Scuola Materna:

- n°1 telecamera Bullet

Biblioteca - Ludoteca:

- n°2 telecamere Bullet

Mercato comunale:

- n°2 telecamere Bullet

Giardini pubblici:

- n°2 telecamere Bullet

Centro sociale - Guardia medica:

- n°2 telecamere Bullet

Cimitero:

- n°1 telecamere Bullet

Eco-centro -Campi sportivi:

- n°2 telecamere Bullet

Centro Servizi:

- n°2 telecamere Bullet

Centro Servizi Parco Archeologico:

- n°2 telecamere Bullet

Ingresso Circonvallazione sud:

- n°1 telecamere lettura targhe

Ingresso Pozzomaggiore:

- n°1 telecamere lettura targhe

Ingresso Tinnura:

- n°1 telecamere lettura targhe

6. IMPIANTI

La valutazione progettuale riguardante la parte Impiantistica generale, i servizi e le opere necessarie al corretto funzionamento dell'Infrastruttura di videosorveglianza, nello specifico riguarda:

- le alimentazioni elettriche dei dispositivi
- le condutture
- i pali

6.1. ALIMENTAZIONI ELETTRICHE

Relativamente alle alimentazioni elettriche e le relative condutture, si prevede, per ogni telecamera la realizzazione di un collegamento diretto con uno switch di rete posto all'interno dell'edificio di competenza o comunque nelle vicinanze del sito, con il quale la telecamera verrà alimentata grazie alla tecnologia POE IEEE 802.3 AF.

In alcuni casi potrà essere necessario ricorrere al montaggio delle telecamere su pali dell'illuminazione pubblica esistenti, in alternativa al montaggio a parete. La motivazione di tale scelta ricade nella possibilità, mediante pali opportunamente posizionati, di ottimizzare l'inquadratura, la qualità di ripresa e di ridurre il numero complessivo di telecamere.

Laddove non sia presente una alimentazione elettrica continua, l'alimentazione elettrica sarà derivata dall'impianto di illuminazione pubblica con integrazione diurna mediante Kit Batteria che dovrà avere un tempo di ricarica inferiore a 6 ore e una durata a pieno carico, in caso di blackout, maggiore di 40 ore.

6.2. CONDUTTURE

Le condutture dove necessarie dovranno essere realizzate in tubazione a vista in PVC, di diametro non inferiore a 20 mm con scatole di derivazione ogni 25/30m, i raccordi dovranno rispettare una classificazione IP adeguata all'ambiente.

Le linee di alimentazione dovranno essere realizzate con conduttore multipolare Fg16 Om1 o equivalente con una sezione di fase non inferiore a 2,5 mmq, aumentandone la sezione in funzione del carico.

Gli scavi ove presenti dovranno eseguirsi con mezzo meccanico e con sezione 200X500.

Gli impianti dovranno essere realizzati secondo la buona regola dell'arte e in conformità a tutte le leggi e regolamenti in vigore.

6.3. PALI

I pali per il supporto delle unità di ripresa, dove non sia possibile utilizzare quelli già esistenti, dovranno essere realizzati in materiale ferroso zincato a caldo spessore adeguato all'altezza e diametro di cima non inferiore a 60mm, altezza 10 metri fuori terra.

I plinti di adeguata dimensione dovranno essere realizzati a getto, sul posto, previa verifica da parte dell'amministrazione.

7. CONNESSIONE ALLA RTR

La rete locale di videosorveglianza sarà realizzata in modo che sia possibile l'integrazione e l'interoperabilità con la **Rete Telematica Regionale** che, tramite il sistema centralizzato, deve essere in grado di monitorare, visionare, trasferire, in tempo reale, flussi video provenienti dalle reti locali di videosorveglianza dei beneficiari, nel rispetto delle norme sulla privacy e secondo i protocolli di sicurezza, standard tecnologici e disposti per legge e, ove necessario, mediante la stipula di opportune e/o necessarie convenzioni con gli enti preposti alla sicurezza.

7.1. LA RETE TELEMATICA REGIONALE

La **Rete Telematica Regionale (RTR)** è l'infrastruttura di proprietà della Regione al servizio dell'Amministrazione regionale, dei suoi Enti e Agenzie, e delle Aziende sanitarie per le esigenze di connettività dati e voce.

La soluzione tecnica che la RTR adotta è costituita da un Backbone in fibra ottica, con nodi dislocati presso le città capoluogo di provincia, punto di raccolta per le esistenti reti metropolitane, che sfrutta tecnologie trasmissive DWDM per il Backbone, IP/MPLS per le sedi periferiche non direttamente interconnesse in fibra ottica e Gigabit Ethernet per le MAN. Attualmente interconnette circa 500 sedi nell'intero territorio ed è in corso di estensione. La RTR adotta il TCP/IP come protocollo standard.

Nelle sedi dove è presente il centro stella delle reti di videosorveglianza locali, sarà attivato un punto di accesso alla RTR. Sarà cura dell'Amministrazione Regionale predisporre un piano di indirizzamento IP armonizzato con quella della RTR.

7.2. IL SISTEMA REGIONALE CENTRALIZZATO DI MONITORAGGIO

Per le esigenze e gli scopi sopra descritti l'amministrazione regionale (RAS) utilizza un sistema di gestione video digitale (DVMS – Digital Video Management System), in grado di inter operare, monitorare gestire i flussi dei sistemi di videosorveglianza locali.

Per garantire l'interoperabilità tra dispositivi, è necessario l'utilizzo di protocolli standard. Attraverso il proprio DVMS, la RAS, deve poter comunicare, interagire e gestire l'hardware di sorveglianza associato al progetto, pertanto è necessario che il DVMS sia uno strumento di alta qualità in grado di operare con gli eterogenei sistemi di videosorveglianza locali, indipendente da brand e costruttori. Dovrà infatti essere

garantita la raggiungibilità da parte del DVMS, attraverso la RTR, di tutti gli apparati (videoserver e/o telecamere) del sistema di videosorveglianza locali.

Pertanto l'infrastruttura di comunicazione locale dovrà garantire l'apertura delle porte di rete per il transito di tutti i protocolli utilizzati dal DVMS. La Regione al fine di garantire la massima interoperabilità e massima compatibilità, ha optato per la scelta di un DVMS conforme altresì allo standard de facto ONVIF1 e PSIA2, che definiscono una serie di specifiche e accordi tra i produttori sul mercato.

La suddetta interoperabilità si attua concretamente tramite la standardizzazione di:

- protocolli di comunicazione IP: definisce il protocollo comune per lo scambio di informazioni tra dispositivi video di rete tra cui rilevamento dei dispositivi automatici, streaming video e metadati intelligenza.
 - rilevamento dei dispositivi;
 - assegnazione degli indirizzi IP;
 - controllo e configurazione dei dispositivi remoti;
 - protocolli dei flussi audio-video;
 - visualizzazione e registrazione dei flussi audio-video.

La piattaforma DVMS è in grado di realizzare l'integrazione con le reti di videosorveglianza di terze parti anche attraverso la disponibilità di API (Application Programming Interface) sviluppate ad hoc.

Il DVMS RAS dispone di un'interfaccia video in uscita conforme a ONVIF che abilita l'integrazione standardizzata e sicura e assicura l'interoperabilità video completa in installazioni multi-fornitore, fornendo supporto per l'accesso a video live e registrati e la capacità di controllare remotamente le telecamere PTZ (Pan/Tilt/Zoom).

Il DVMS supporta la ricezione, la memorizzazione e l'esportazione dei metadati secondo il formato ONVIF, inclusi i metadati derivanti da sistemi di video analisi residenti a bordo camera e dati di localizzazione dai sistemi mobili.

Adotta lo standard Ethernet TCP/IP e supporta la gestione e la federazione di installazioni con versioni di software anche di release diverse. Fornisce una soluzione avanzata di monitoraggio del sistema, che include la ricezione di notifiche per Allarmi/avvisi per tipologia di oggetto e oggetto singolo, generati da qualsiasi componente del sistema, e avvisi di ritenzione video predittivo.

Il software del sistema DVMS consente l'archiviazione ottimizzate di registrazioni video e audio. Il DVMS è conforme alla normativa vigente sulla privacy, rispetta le direttive del Ministero dell'Interno, normative CEI EN 50132-1 (CEI 79-70) Sistemi di allarme Sistemi di videosorveglianza per applicazioni di sicurezza. Supporta tutti i protocolli standard. Algoritmi di compressione H.264/H.265, MJPEG, MPEG-4ASP, MxPEG, Zipstream, protocollo di comunicazione unicast, multicast, SNMP, supporto IPV6.

8. NORME PER LE AZIONI DI INFORMAZIONE E DI COMUNICAZIONE

Il periodo di **Programmazione 2014-2020** richiede, ai diversi protagonisti coinvolti nell'attuazione degli interventi, un impegno congiunto per rafforzare la consapevolezza sulle opportunità a disposizione, sull'utilizzo delle risorse pubbliche e sui cambiamenti che anche la **Regione Sardegna** sta operando lungo il percorso di crescita intelligente, sostenibile e inclusiva.

Gli interventi finanziati dal "Fondo europeo di sviluppo regionale POR FESR 2014-2020 della Regione Sardegna" devono seguire la **Circolare N.2** sulle **Linee Guida per le azioni di informazione e di comunicazione**.

Le Linee Guida per le azioni di informazione e di comunicazione nascono per offrire una panoramica esaustiva su quanto previsto dai regolamenti europei su un tema estremamente rilevante, al fine di agevolare e semplificare l'applicazione dell'ampio sistema di regole comunitarie dalle quali dipende l'ammissibilità degli interventi alla rendicontazione ovvero la revoca dei finanziamenti concessi.

Nella programmazione 2014-2020 del POR FESR Sardegna i **Beneficiari** dei finanziamenti hanno un ruolo di primo piano perché sono chiamati, insieme **all'Autorità di Gestione**, a promuovere i progetti finanziati e a dare evidenza ai cambiamenti avvenuti grazie alle risorse comunitarie.

A partire dal momento in cui il progetto viene finanziato dal POR FESR Sardegna 2014-2020, il Beneficiario è tenuto ad avviare tutte le azioni di comunicazione necessarie per dare evidenza al sostegno finanziario ricevuto. Tali obblighi si differenziano in base **all'entità del sostegno finanziario pubblico ricevuto**, (inferiore o superiore a 500.000 euro); **e alla fase in cui si trova il progetto**: se il progetto è in una fase di esecuzione **l'azione informativa** sarà **temporanea**, se è concluso sarà **permanente**.

Il presente finanziamento risulta inferiore a 500.000 Euro. I Beneficiari, ossia i **Comuni**, devono provvedere, sia durante l'esecuzione che dopo il suo completamento, all'esposizione di un poster con informazioni sul progetto (formato minimo A3), che indichi il sostegno finanziario dell'Unione, da collocare in un luogo facilmente visibile al pubblico. L'emblema dell'Unione Europea, il riferimento al fondo, il nome del progetto e l'obiettivo principale dell'operazione dovranno occupare almeno il 25% dell'area del poster.

Inoltre, durante l'attuazione del progetto, il Beneficiario informa il pubblico sul sostegno ottenuto dai fondi inserendo nel proprio sito web una breve descrizione, di 1.000 caratteri circa, del progetto per cui ha ottenuto il sostegno finanziario. Nella descrizione vanno inseriti le finalità, i risultati attesi e, successivamente, i risultati raggiunti.

Queste disposizioni fanno riferimento alla normativa europea riguardante la Programmazione 2014-2020:

- Il Regolamento (UE) n. 1303/2013 del Parlamento europeo e del Consiglio del 17 dicembre 2013.

Il Regolamento di esecuzione (UE) n. 821/2014 della Commissione del 28 luglio 2014.

9. INTEGRAZIONE DEI SISTEMI PERIFERICI DI VIDEOSORVEGLIANZA CON IL SISTEMA CENTRALE SCNTT

Con la circolare del Dipartimento per la pubblica sicurezza del Ministero dell'interno n. 1065 del 12 gennaio 2018, viene richiesto il collegamento dei sistemi periferici di videosorveglianza per la lettura targhe al centro Scntt di Napoli.

Il “**Sistema Centralizzato Nazionale Targhe e Transiti**”, è un progetto del ministero dell'interno volto a far confluire tutti i transiti rilevati da telecamere di lettura targhe verso il centro elaborazione di Napoli. Questo sistema ha lo scopo di:

- Acquisire e distribuire ai sistemi periferici le liste nazionali delle targhe rubate (lista A1), di quelle segnalate dagli uffici di polizia (lista C) e di quelle non revisionate (lista A2) solo per i sistemi periferici della Polizia Stradale;
- Realizzare un'unica Banca Dati per tutti i transiti registrati dei sistemi periferici di videosorveglianza;
- Implementare meccanismi di correlazione e propagazione tra sistemi degli allarmi relativi alle targhe segnalate (lista C);
- Fornire servizi tramite interfaccia Web agli Uffici al fine di effettuare ricerche sui transiti, segnalare le targhe (lista C) e visionare gli allarmi di propria competenza;
- Fornire statistiche, report

Il collegamento SCNTT richiede l'installazione di un server aggiuntivo in questura, collegato a un software che sia in grado di comunicare con il centro elaborazione di Napoli.

Gli uffici territoriali (Amministrazione Comunale, Prefettura, Questura, ecc.) dovranno farsi carico della realizzazione del sistema **LPR** (License Plate Recognition), il sistema server per la lettura targhe, e richiedere l'interconnessione al sistema **SCNTT**.

Lo scambio di informazioni previsto nell'integrazione è di tipo bidirezionale ed è costituito dalle seguenti entità:

- **Gestione Liste** (SCNTT → LPR): provvede all'aggiornamento delle liste A1, A2 e C (Hot List) verso i sistemi LPR.
- **Gestione Rilevamenti** (LPR → SCNTT): provvede all'invio a SCNTT dei transiti e degli allarmi (lista C) registrati nei varchi installati nel territorio.

La comunicazione tra i sistemi avverrà tramite i metodi esposti dal servizio web denominato SCNTT del CEN di Napoli e quelli esposti dai servizi web dei singoli LPR. Questo scambio avviene attraverso due meccanismi:

- Web Services dando così la possibilità di utilizzare i protocolli normalmente in uso in internet (HTTP, XML, SMTP ecc) e garantendo l'interoperabilità con le piattaforme più disparate.;
- Repliche Oracle ove possibile.

I flussi generati per lo scambio dei dati devono essere criptati (SSL) con l'utilizzo di un certificato digitale fornito dal N.O.C.

9.1. REQUISITI FONDAMENTALI

Il sistema SCNTT invierà ai sistemi LPR gli aggiornamenti delle liste A1, A2, e C utilizzando un loro servizio web ed esporrà a sua volta dei servizi per ricevere i rilevamenti (transiti ed allarmi) dai sistemi LPR.

I sistemi LPR che si interfaceranno al SCNTT dovranno rispettare i seguenti requisiti:

- Le informazioni che vengono inviate al sistema centrale devono essere complete e rispettare i criteri di obbligatorietà espressi nelle presenti specifiche.
- Il sistema LPR deve aver ottenuto un proprio certificato dalla Certification Authority del sistema SCNTT per poter gestire l'autenticazione HTTPS. Il certificato verrà fornito da SCNTT in modalità offline insieme all'id e al nome con i quali il sistema viene registrato in SCNTT e alle credenziali di accesso. La chiave privata fornita dovrà essere utilizzata per attivare il protocollo https per i messaggi SOAP che arrivano dal sistema centrale.
- Oltre al riconoscimento del certificato il sistema LPR, nell'invocare i metodi esposti dal SCNTT, dovrà utilizzare le credenziali rilasciate dall'amministrazione all'atto della sua registrazione. (Credential). Ad ogni messaggio SOAP inviato verso il SCNTT il campo PassKey dovrà essere firmato digitalmente con la stessa chiave privata inviata. In particolare il campo Credential.PassKey deve contenere la firma SHA1withRSA in Base64 della PassKey.
- Tutte le richieste di colloquio fra i sistemi avverranno dopo aver effettuato l'autenticazione del sistema richiedente al fine di verificare l'effettiva

autorizzazione e per garantire la sicurezza dei dati trasmessi e la non-ripudiabilità ovvero che né il mittente né il destinatario possano negare di aver trasmesso o ricevuto un messaggio.

- Ogni anomalia che si verifichi durante l'esecuzione dei metodi richiesti dagli sistemi LPR sarà segnalata da SCNTT.
- Ogni anomalia che si verifichi durante l'esecuzione dei metodi richiesti dal sistema SCNTT sarà segnalata dall'LPR.
- Il sistema LPR dovrà inviare a SCNTT l'anagrafica delle telecamere di rilevazione indicando, oltre una breve descrizione, la loro esatta ubicazione unitamente ai varchi a cui afferiscono, secondo lo schema indicato nel presente documento di specifiche. Inoltre dovrà garantire aggiornamenti in tempo reale nel caso di variazioni utilizzando l'apposita funzione esposta dal SCNTT.
- Il sistema LPR deve avere un servizio web (LPR) che esponga i metodi descritti nel presente documento e che colloqui con il SCNTT secondo il protocollo https/SOAP (ver. 1.2). altresì il webservice deve pubblicare i wsdl forniti dall'ufficio N.O.C.
- Il collegamento con il sistema SCNTT è consentito esclusivamente con sistemi LPR ubicati presso Uffici di P.S., attestati su rete Interpolizia in fibra ottica.

9.2. GESTIONE RILEVAMENTI

Il singolo sistema LPR invia costantemente i transiti e gli allarmi, generati dai propri apparati. Nel caso un transitò abbia generato un allarme (lista C) il sistema provvederà ad inviarlo in tempo reale a SCNTT.

Per "dato" di un transitò/allarme si intende l'insieme dei metadati (numero di targa, data ed ora del rilevamento, ecc.) unitamente alle seguenti immagini (file.jpg):

1. immagine completa del veicolo rilevata dalla telecamera ed elaborata dall'OCR (obbligatoria);
2. immagine completa del veicolo a colori (solo nel caso di allarmi).

Per i transiti la foto a colori di cui al punto 2 non deve essere inviata ma solo resa disponibile tramite apposito servizio dell'LPR.

Il sistema LPR periodicamente (ritardo massimo 30 min.) invia i transiti a SCNTT che provvederà ad archiviare i dati e le immagini.

La modalità di trasmissione utilizzerà il web service esposto dal SCNTT utilizzando il protocollo SOAP su https. Prima dell'invio dei transiti è necessario aver effettuato l'inserimento delle anagrafiche dei lettori. Per transito da inviare è da intendersi il rilievo fotografico del passaggio del veicolo rilevato da un lettore targhe. Nel caso il lettore effettui più rilievi fotografici per un singolo passaggio del veicolo rilevato dal lettore, ad SCNTT deve essere inviato un solo transito per passaggio.

La chiave univoca che identifica il singolo transito per ogni rilevatore (DetectId) è data dalla combinazione dei campi **PlateNumber** e **TransitDateTime**.

Per garantire l'unicità dei nomi delle immagini utilizzare deve essere utilizzata la seguente nomenclatura: **NAAAAMMGGHHMMSSRT.jpg** con:

- **N** indica il numero di targa
- **AAAAMMGGHHMMSS**: indica la data/ora del rilevamento
- **R** indica l'id del rilevatore
- **T** indica la tipologia:
 - **L** immagine OCR
 - **F** immagine a colori

L'immagine OCR di tipo **L** inviata dovrà essere completa, ovvero dovrà essere visibile l'intero contesto scenico e dovrà avere una risoluzione minima tale da consentire, per fini giudiziari, una lettura della targa a occhio nudo.

L'immagine di tipo **F** inviata dovrà essere, come per il tipo **L**, completa, ovvero dovrà essere visibile l'intero contesto scenico, ma a colori, in modo da consentire il riconoscimento del colore e del veicolo.

Per ottimizzare i tempi di trasferimento e minimizzare l'occupazione della banda, poiché per ogni telecamera sono attesi in media un elevato numero di transiti giornalieri, il sistema SCNTT non deve ricevere dai sistemi LPR le immagini di contesto (F), che nel singolo record rappresentano l'attributo di dimensione maggiore (fino 200 KB). Una volta che il sistema LPR ha preparato i transiti da inviare li trasferisce al CEN attraverso l'invocazione del metodo *updateTransits* esposto dal web service SCNTT.

Il Sistema SCNTT acquisisce i transiti provenienti dalla periferia e li memorizza per 15 giorni. In questo lasso di tempo i dati relativi ai transiti saranno accedibili, tramite un servizio web oriented, dagli operatori della Polizia di Stato opportunamente autorizzati. In casi particolari (richiesta dell'Autorità Giudiziaria) è possibile scaricare i dati per metterli a disposizione delle competenti autorità secondo modalità che assicurino la integrità dei dati e il rispetto della normativa sulla privacy.

Per questioni legate alle risorse finanziarie non è possibile realizzare l'interconnessione tra il sistema di videosorveglianza progettato e il centro SCNTT di Napoli, ma i sistemi realizzati nel presente intervento, sono compatibili con la rete di interconnessione sopracitata che potrà essere integrata con il reperimento di ulteriori risorse economiche.

10. TRATTAMENTO DEI DATI PERSONALI

Presso i locali dell'Amministrazione (Municipio), sarà allestito il locale tecnologico dove eseguire l'installazione fisica, la configurazione e la messa in esercizio nelle macchine server, dell'armadio e del gruppo di continuità.

Il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza attivati nel territorio comunale è disciplinato con apposito regolamento approvato con deliberazione del Consiglio Comunale.

L'accesso ai dati sarà consentito al sindaco e ai suoi delegati, e inoltre sarà realizzato un collegamento in remoto per cui sarà possibile, per la stazione dei Carabinieri accedere direttamente al server.

Le normative recenti hanno attribuito specifici compiti ai Sindaci, in materia di pubblica incolumità e sicurezza urbana. A tali fini, l'art. 1 della Legge n. 38/2009, di conversione del D. L. n. 11/2009, ha previsto che "per la tutela della sicurezza urbana i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico", con conservazione delle immagini per un periodo massimo di sette giorni (art. 6, commi 7 e 8). Anche la legge n. 48/2017, di conversione del D.L. n. 14/2017, in materia di sicurezza urbana integrata, potenzia l'intervento degli enti territoriali e la collaborazione tra le forze di polizia statali e locali e riconosce l'utilità, al fine di contrastare la criminalità diffusa e predatoria, tutelare l'arredo urbano, il verde pubblico e i parchi cittadini, della videosorveglianza, incentivandone l'utilizzo anche da parte dei privati mediante misure fiscali.

Col provvedimento dell'8 aprile 2010, il Garante della Privacy detta disposizioni relative alla videosorveglianza nella sicurezza urbana e nel deposito di rifiuti; disposizioni che riguardano indubbiamente anche il fototrappolaggio, riconducibile alla categoria della videosorveglianza.

Tale provvedimento sarà sostituito con la definitiva adozione delle linee guida 3/2019 pubblicate in settembre 2019 dal Comitato Europeo per la protezione dei dati (EDPB). Riguardo alla sicurezza urbana, al punto 5.1. del provvedimento summenzionato, il Garante stabilisce che "... sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di

tutelare la sicurezza urbana". Inoltre, auspica che anche nelle ipotesi in cui le attività di videosorveglianza siano assimilabili alla tutela della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati (ipotesi in cui l'informativa potrebbe essere omessa, come ci ricorda il punto 3.1.1) "l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui".

Per il deposito dei rifiuti, al punto 5.2 del provvedimento il Garante ammette l'uso dei sistemi di videosorveglianza solo in caso di inefficacia o impossibilità di sistemi alternativi e sia per quanto riguarda le disposizioni sanzionate amministrativamente che per quelle di natura penale.

Nel rispetto del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 e delle sopracitate sopravvenute normative e regolamenti, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, deve essere approvato in Consiglio Comunale un tale regolamento che deve:

- individuare gli impianti di videosorveglianza di proprietà del Comune o da esso gestiti;
- definire le caratteristiche e le modalità di utilizzo degli impianti di videosorveglianza;
- disciplinare gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza.

Il regolamento comunale garantisce che il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza gestiti dal Comune e collegati alle centrali di controllo ubicate presso le sedi del Comando di Polizia locale, della Questura e del Comando provinciale dei Carabinieri si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento. L'utilizzo degli impianti di videosorveglianza comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video che, in relazione ai luoghi di installazione

delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area interessata.

Il trattamento dei dati personali si svolge nel pieno rispetto dei principi di liceità, finalità, necessità e proporzionalità, sanciti dal Codice.

In attuazione dei principi di liceità e finalità, il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza è effettuato dal Comune esclusivamente per lo svolgimento delle funzioni istituzionali.

In attuazione del principio di necessità, gli impianti di videosorveglianza ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

In attuazione del principio di proporzionalità e dei criteri di pertinenza e non eccedenza, gli impianti di videosorveglianza sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

Il Comune è titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza pubblici. A tal fine il Comune è rappresentato dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.

10.1. CONSERVAZIONE E SICUREZZA DELLE RIPRESE

Le riprese possono essere conservate fino a 24 ore, termine che può essere elevato in caso di esigenze che giustifichino l'ulteriore conservazione in relazione a giorni di festività o chiusura di uffici o esercizi, nonché nel caso in cui si debba ottemperare ad una specifica richiesta investigativa dell'autorità giudiziaria. Per i Comuni la conservazione è possibile fino a "sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione") ai sensi dell'art. 6, DL 23 febbraio 2009, n. 11. Per andare oltre i 7 giorni occorrono situazioni eccezionali, previo controllo da parte del Garante, o specifiche richieste dell'autorità giudiziaria.

Occorre predisporre le misure minime di sicurezza, in particolare i dati devono essere conservati in modo da garantire la perdita, la distruzione anche accidentale e soprattutto l'accesso di persone non autorizzate agli stessi (eventualmente predisponendo modalità di cifratura dei dati). Inoltre, devono essere predisposte misure organizzative per la cancellazione dei dati alla scadenza, o dei dati non più necessari.

Gli interessati, cioè i soggetti ripresi, devono poter accedere alle riprese che li riguardano e verificare le modalità di utilizzo dei dati raccolti. L'illiceità delle riprese comporta non solo l'inutilizzabilità delle registrazioni, ma anche il provvedimento di blocco e divieto di trattamento dei dati, da parte del Garante. In casi estremi si possono configurare anche reati penali.

10.2. IL DECRETO N.101 DEL 10 AGOSTO DEL 2018

In Italia il quadro normativo in materia di tutela dei dati personali è disciplinato dal Regolamento Europeo sulla Privacy e dal Codice Privacy novellato dal Decreto Legislativo 101/2018.

L'impianto normativo è regolamentato su 2 livelli:

1. il primo, rappresentato da una norma di fonte superiore, quella "Europea" (il GDPR entrato in vigore il 25 maggio 2018), cui tutti gli Stati Membri dell'Unione devono indistintamente uniformarsi;
2. il secondo, rappresentato dal Codice per la protezione dei dati personali (codice della privacy Dlgs 196/2003) e dal Decreto legislativo n.101/2018 emanato il 10 agosto 2018 ed entrato in vigore il 19 settembre 2018.

Nell'adeguamento al Nuovo Regolamento europeo, il Decreto attuativo 101/2018, se da un lato non introduce novità rilevanti in merito a temi quali l'informativa ed il consenso regolamentati dal GDPR (ad eccezione di alcune disposizioni sui minori, sugli studenti, sul trattamento di dati genetici, biometrici e sanitari), dall'altro, detta ed introduce invece rilevanti modifiche riguardanti le sanzioni, i diritti dell'interessato, l'utilizzabilità dei dati acquisiti in violazione delle disposizioni, l'attribuzione al Garante di poteri più forti e compiti ulteriori, le modalità di attuazione del GDPR per le micro, piccole e medie imprese, i servizi dell'informazione e i minori, i codici deontologici, le

regole di condotta, il trattamento di "categorie particolari di dati" per finalità di ricerca scientifica, fini statistici, ricerca storica e di rilevante interesse pubblico.

In questo nuovo contesto tutto è demandato all'Autorità Garante di "controllo" per la protezione dei dati; spetterà a tale Organismo armonizzare le nuove disposizioni garantendo un minimo di certezza ad operatori, manager di azienda, professionisti e Pubblica Amministrazione.

10.3. A EDPB – DRAFT LINEE GUIDA 3/2019 SULLA VIDEOSORVEGLIANZA

Il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato il 10 giugno 2019 le linee-guida sulla videosorveglianza che chiariscono in quali termini il regolamento generale sulla protezione dei dati si applichi al trattamento dei dati personali quando si utilizzano dispositivi video, e mirano a garantire l'applicazione coerente del GDPR in materia. Le linee-guida riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti. Per quanto concerne questi ultimi, le linee-guida si concentrano sulle norme relative al trattamento di categorie particolari di dati. Altre tematiche affrontate nel documento riguardano, tra l'altro, la liceità del trattamento, l'applicabilità dei criteri di esclusione relativi ai trattamenti in ambito domestico e la divulgazione di filmati a terzi.

La materia della videosorveglianza era disciplinata da un provvedimento del Garante italiano dell'8 aprile 2010. Ora, a seguito della piena operatività del Gdpr, occorre aggiornare la disciplina.

Le normative recenti hanno attribuito specifici compiti ai Sindaci, in materia di pubblica incolumità e sicurezza urbana. A tali fini, l'art. 1 della Legge n. 38/2009, di conversione del D. L. n. 11/2009, ha previsto che "per la tutela della sicurezza urbana i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico", con conservazione delle immagini per un periodo massimo di sette giorni (art. 6, commi 7 e 8). Anche la legge n. 48/2017, di conversione del D.L. n. 14/2017, in materia di sicurezza urbana integrata, potenzia l'intervento degli enti territoriali e la collaborazione tra le forze di polizia statali e locali e riconosce l'utilità, al fine di contrastare la criminalità diffusa e predatoria, tutelare l'arredo urbano, il verde pubblico e i parchi cittadini, della

videosorveglianza, incentivandone l'utilizzo anche da parte dei privati mediante misure fiscali.

Col provvedimento dell'8 aprile 2010, il Garante della Privacy detta disposizioni relative alla videosorveglianza nella sicurezza urbana e nel deposito di rifiuti; disposizioni che riguardano anche il fototrappolaggio, riconducibile alla categoria della videosorveglianza.

Tale provvedimento sarà sostituito con la definitiva adozione delle linee guida 3/2019 pubblicate in settembre 2019 dal Comitato Europeo per la protezione dei dati (EDPB). Riguardo alla sicurezza urbana, al punto 5.1. del provvedimento summenzionato, il Garante stabilisce che " ... sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana". Inoltre, auspica che anche nelle ipotesi in cui le attività di videosorveglianza siano assimilabili alla tutela della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati (ipotesi in cui l'informativa potrebbe essere omessa, come ci ricorda il punto 3.1.1) "l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui".

Per il deposito dei rifiuti, al punto 5.2 del provvedimento il Garante ammette l'uso dei sistemi di videosorveglianza solo in caso di inefficacia o impossibilità di sistemi alternativi e sia per quanto riguarda le disposizioni sanzionate amministrativamente che per quelle di natura penale.

Anche il fototrappolaggio pone l'esigenza, al pari di altri sistemi di trattamento dei dati, di tutelare la privacy e proteggere i dati raccolti. L'attivazione del dispositivo, se finalizzata ad attività di ricerca scientifica, di osservazione faunistica di polizia amministrativa, comporta, innanzi tutto, gli obblighi d'informativa con cartelli posti prima del raggio d'azione della telecamera, secondo le prescrizioni degli artt. 13 e 14 del Reg. U.E. 2016/679. Anche per finalità di sicurezza e protezione dei beni, nonché prevenzione di furti, se l'area è pubblica o accessibile al pubblico, i cartelli informativi sono necessari; se l'area è privata è sufficiente solo l'autorizzazione del proprietario.

I predetti cartelli dovranno riportare:

- identità e dati di contatto del titolare e/o responsabile del trattamento

- finalità e base giuridica del trattamento
- periodo di conservazione delle immagini o criteri per determinare tale periodo
- diritto di accesso dell'interessato ai propri dati
- altre informazioni, di cui agli artt. 13 e 14 predetti

Naturalmente, non potendo tutte le informazioni elencate agli artt. 13 e 14 Reg. U.E. 2016/679 essere contenute in un cartello, dovrà essere indicato un modo semplice e diretto affinché gli interessati possano reperire le informazioni prescritte (numero telefonico, sito web, indirizzo dell'ente che ha posizionato la fototrappola, etc.).

Pertanto, è opportuno che il Comune, per maggior chiarezza ed uniformità di prassi, disciplini sempre con un regolamento dettagliato l'intera fase delle procedure di posizionamento degli apparecchi, di accertamento delle fattispecie, di verbalizzazione dell'illecito, di estrapolazione dei dati, di visione dei fotogrammi, di conservazione e altro.

Nell'ipotesi di riprese effettuate nel corso di indagini di polizia giudiziaria, la disciplina cambia. Il trattamento dei dati nelle attività di p.g., infatti, a livello europeo non ricade nell'ambito del GDPR (acronimo che individua il reg. U.E. 2016/679), bensì della direttiva 2016/680; la direttiva è fonte normativa che obbliga i destinatari (gli Stati) a raggiungere una determinata finalità con i mezzi giuridici che essi ritengono più utili ed opportuni. In Italia, la direttiva summenzionata è stata attuata con D. Lgs. 51/2018, che riguarda il trattamento dei dati effettuati dalle autorità pubbliche a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Con riferimento a quanto sopra esposto, nel corso di indagini di p.g. che si avvalgono dell'utilizzo di fototrappole, l'informativa può essere omessa (Punto 3.1.1 del Provvedimento del Garante dell'8 aprile 2010); l'incaricato (ossia, colui che esegue materialmente le operazioni di trattamento dei dati) deve rivestire necessariamente la qualifica di cui all'art. 57 c.p.p.; le immagini vanno conservate per il tempo prescritto dall'art. 10 del D.P.R. n. 15 del 15.01.2018, che distingue diversi periodi per differenti fattispecie di reato (peraltro, anche nel caso di infrazioni amministrative accertate, le immagini vanno conservate oltre il termine dei 7 giorni sopra riferito, in quanto entrano in altro procedimento).

Inoltre, il titolare e il responsabile del trattamento dei dati sono destinatari di obblighi di sicurezza, per la protezione dei dati, di cui all'art. 25 del D. Lgs. 51/2018 e al capo V del D.P.R. n. 15/2018; sulla base dei predetti articoli, a titolo puramente indicativo, si può

suggerire che la fototrappola sia posizionata in contenitori antifurto oppure chiusa con lucchetti a cavo (came-lock); che venga impostata una password che impedisca a chi non è autorizzato di cambiare la configurazione all'apparecchio, et cetera.

Tuttavia, le misure di sicurezza possono essere innumerevoli: infatti, in base al principio di accountability, che informa tutta la recente normativa sulla protezione dei dati, titolari e responsabili sono tenuti ad adottare tutte le misure adeguate alla protezione, siano esse di natura tecnica che organizzativa; in caso di trattamento illecito dei dati, infatti, l'onere di provare che esso è avvenuto per caso fortuito ed imprevedibile spetta proprio al titolare e/o al responsabile; diversamente, gli stessi saranno sanzionati e tenuti al risarcimento del danno eventualmente prodotto dal trattamento illecito dei dati.

Per questo, sui sistemi di videosorveglianza è buona norma condurre, con l'ausilio dei fornitori dei servizi di installazione e gestione, una Valutazione di impatto che analizza in maniera dettagliata l'ambito, le modalità, le misure di sicurezza e i rischi per le libertà e i diritti delle persone fisiche.

Con riferimento alle succitate linee guida 3/2019 si richiama l'attenzione sui contenuti innovativi rispetto al provvedimento del Garante del 2010.

Il modello a tinte UE espone più informazioni di quelle contenute nel modello attualmente in uso: richiede anche i dati di contatto del Responsabile della protezione dei dati, un elenco sintetico dei diritti dell'interessato e il codice QR e l'indicazione delle modalità per avere le altre informazioni non presenti sul cartello.

Le linee guida del Comitato europeo, per le quali la consultazione pubblica, preliminare alla adozione definitiva, si è chiusa il 9 settembre 2019, propongono un facsimile diverso, in quanto corredato da un maggior numero di informazioni.

Con riferimento alla procedura di informativa agli interessati, viene confermata la struttura a due livelli: informativa sintetica e informativa completa e, quindi, prima un cartello e, poi, altre fonti per le informazioni ulteriori.

Quanto al cartello, le linee guida in esame richiedono che sia posizionato nei pressi della telecamera, così da far capire all'interessato che sta per essere ripreso, e tendenzialmente ad altezza della persona, ma, ovviamente, senza dare la posizione esatta.

Il contenuto del cartello deve riportare le informazioni essenziali, quali lo scopo del trattamento, l'identità del titolare del trattamento, i diritti previsti dal Gdpr. Sono da

inserire anche i dati di contatti del Dpo (Data protection officer, responsabile protezione dati) o un riferimento al legittimo interesse del titolare o di terze parti. Bisogna inserire nel cartello anche un rinvio al secondo livello dell'informativa e a come ottenerlo.

Il cartello deve indicare se i dati sono trasferiti fuori UE e il periodo di conservazione: in mancanza, è implicito e l'interessato può dedurre che si tratta di riprese senza conservazione o trasmissione dei dati a terzi.

Nel cartello ci deve essere un riferimento alle modalità per trovare l'informativa al secondo livello: un codice QR o un sito internet.

L'informativa completa deve essere disponibile anche con modalità alternative alla rete, come fogli informativi o recapiti telefonici.

L'informativa di secondo livello può essere facilmente disponibile, ad esempio, mediante fogli informativi allo sportello dell'ente o poster o affissioni presso una sede del titolare.

Oltre a ciò, le linee guida suggeriscono di inserire l'ubicazione le telecamere attive sulle mappe disponibili online collegate alla relativa informativa.

11. SERVIZIO DI MANUTENZIONE E GARANZIA

Servizi di manutenzione dei sistemi dovrà comprendere almeno: la manodopera necessaria per effettuare gli interventi di ripristino in garanzia e le operazioni di manutenzione preventiva; i materiali di consumo per sostituzione di componenti non soggetti ad usura; l'impiego dei mezzi necessari per l'esecuzione dei lavori (scale o piattaforme aeree).

I Servizi di Manutenzione avranno inizio dal giorno successivo al collaudo dell'impianto (Certificato di regolare esecuzione) e per una durata complessiva di 5 anni.

Tutte le apparecchiature, oggetto dell'appalto, dovranno essere mantenute con gli SLA (Service Level Agreement) di seguito descritti:

- Tempi di intervento: entro 8 ore lavorative successive alla richiesta di intervento.
- Per il mantenimento in efficienza del sistema, dovranno prevedersi 2 visite durante l'anno per la manutenzione programmata ordinaria.
- Tutte le componenti fornite dovranno essere garantite 2 anni dalla data di consegna.

12. QUADRO ECONOMICO DEI LAVORI

QUADRO ECONOMICO DEI LAVORI		
	PER LAVORI	
A1	Importo lavori soggetti a ribasso d'asta	€ 28 326,90
A2	Oneri per la sicurezza non soggetti a ribasso d'asta	€ 705,36
A	IMPORTO COMPLESSIVO DEI LAVORI	€ 29 032,26
	SOMME A DISPOSIZIONE DELL'AMMINISTRAZIONE	
B1	IVA sui lavori al 22%	€ 6 387,10
B2	Spese tecniche incluse INARCASSA (4%) e IVA (22%)	€ 4 000,00
B3	Incentivi al RUP 2%	€ 580,65
B	TOTALE SOMME A DISPOSIZIONE	€ 10 967,74
A+B	IMPORTO COMPLESSIVO DEI LAVORI	€ 40 000,00