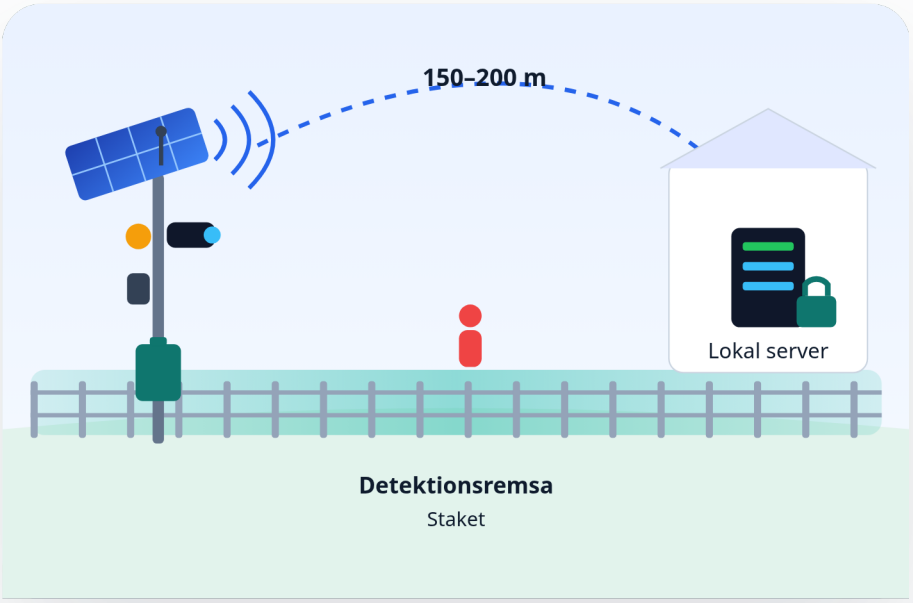
SÄKERHET FÖR DET GEMENSAMMA OMRÅDET

CLARYEL Perimetro

Projekt för ett autonomt intelligent säkerhetssystem för det gemensamma området

En enda autonom intelligent kamerapunkt längs staketet. Alla data stannar endast hos oss, på fastigheten, i krypterad form: inga moln, inga tredjepartstjänster, allt endast lokalt.

- Endast lokalt
- Krypterat
- Inget moln
- Omedelbar låsning vid varje larm



GRUNDPRINCIP

Allt stannar hos oss — på fastigheten

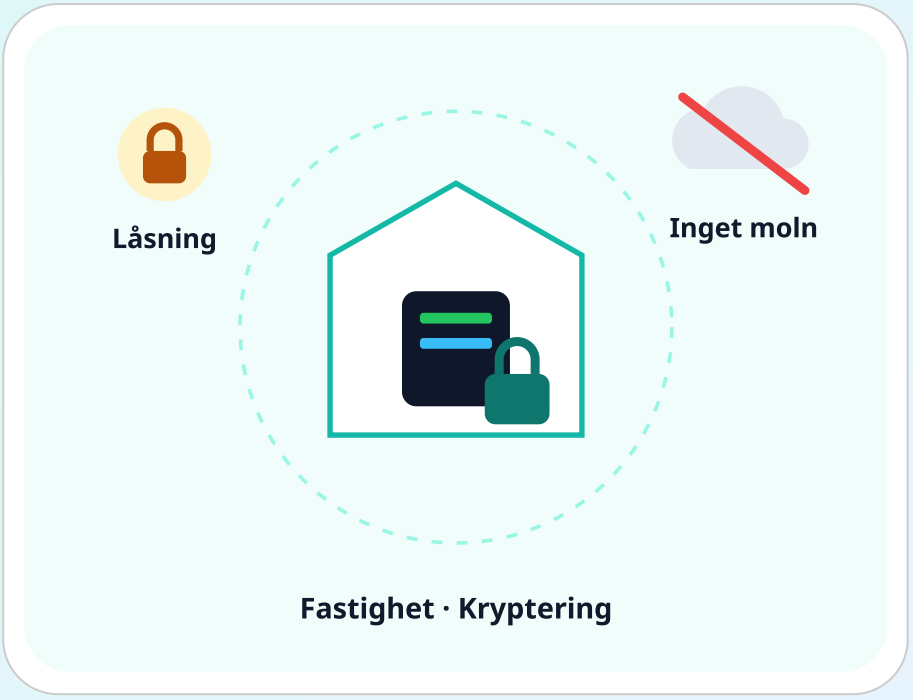
Alla bilder, händelseklipp och loggar lagras endast på den lokala servern i byggnaden, på fastigheten.

All information lagras och överförs i krypterad form.

Vid varje larm kan all information låsas omedelbart: åtkomsten till arkivet stängs och händelseklippen skyddas mot ändring och radering.

Inga moln och inga tredjepartstjänster: bearbetning med artificiell intelligens och lagring sker endast lokalt.

- Lokal server i byggnaden
- Kryptering
- Omedelbar låsning
- Inget moln
- Inga tredjepartstjänster



ALTERNATIV TILL KAMERAN

Detektion med Wi-Fi-signaler: inga bilder, ingen identifiering

- Ingen kamera
- Inga bilder
- Ingen identifiering
- Endast lokalt

Som alternativ till kameran kan två Wi-Fi-enheter installeras längs staketet, en i vardera änden av den övervakade sträckan.

Ur rådata från Wi-Fi-signalen mellan de två enheterna (dess variationer, kända som CSI — Channel State Information) härleder systemet konturerna av personer som rör sig i remsan, utan någon bild och utan att identifiera vilka de är.

Tekniken studeras redan inomhus i bostäder: forskningen ”DensePose From WiFi” vid Carnegie Mellon University återskapar till exempel silhuetterna av personer i ett rum med enbart Wi-Fi-signaler. Vi föreslår att den används utomhus, längs staketet.

Systemet upptäcker endast närvaro, rörelseriktning och en anonym silhuett. Bearbetningen sker krypterat på den lokala servern, precis som i resten av projektet, och utlöser samma varningar: ljus, röstmeddelande och aviseringar till de boende.

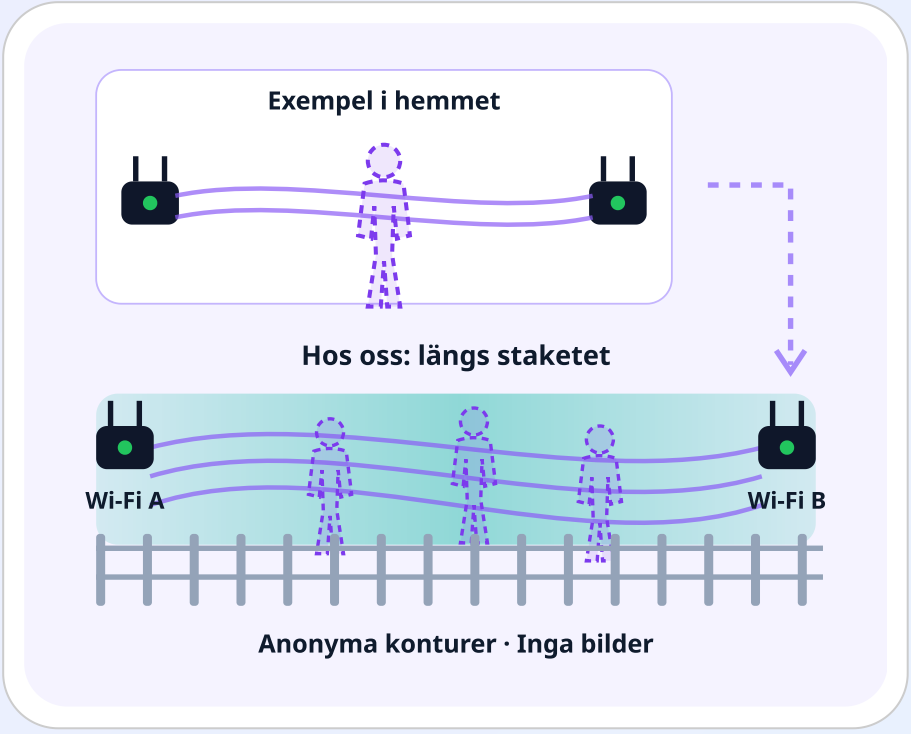
Rättsliga aspekter — ska kontrolleras med dataskyddsombudet (DPO) eller en rådgivare

Wi-Fi-detektion fångar inga bilder eller video: det är därför inte ett kameraövervakningssystem, och de särskilda reglerna om kameraövervakning (till exempel den informationsskylt som Garante anger för kameror) gäller inte som sådana.

GDPR gäller dock fortfarande om uppgifterna kan avse en identifierad eller identifierbar person (artikel 4.1 GDPR). Därför är systemet utformat för att endast behandla anonym närvaro och konturer, utan identifiering, endast lokalt och i krypterad form.

Denna bedömning måste bekräftas med dataskyddsombudet eller en rådgivare före installationen och utgör ingen juridisk garanti.

Exempel i en bostad: ”DensePose From WiFi”, Carnegie Mellon University (arXiv) ↗



01

Projektets syfte

Vi föreslår att en enda autonom punkt för intelligent kameraövervakning installeras längs staketet runt fastighetens gemensamma område.

Systemet ska upptäcka möjligt obehörigt intrång, varna inkräktare och snabbt informera de boende.

Projektets grundprinciper:

01

Minimalt intrång i privatlivet.

02

Övervakning av endast en smal remsa längs staketet.

03

Helt lokal bildbearbetning med artificiell intelligens.

04

Inga obligatoriska molntjänster.

05

Kryptering av överförd och lagrad information.

06

Automatiska varningar och aviseringar till de boende.

07

Möjlighet att snabbt kontakta polisen.

02

Begränsning av kameraövervakningen och skydd av privatlivet

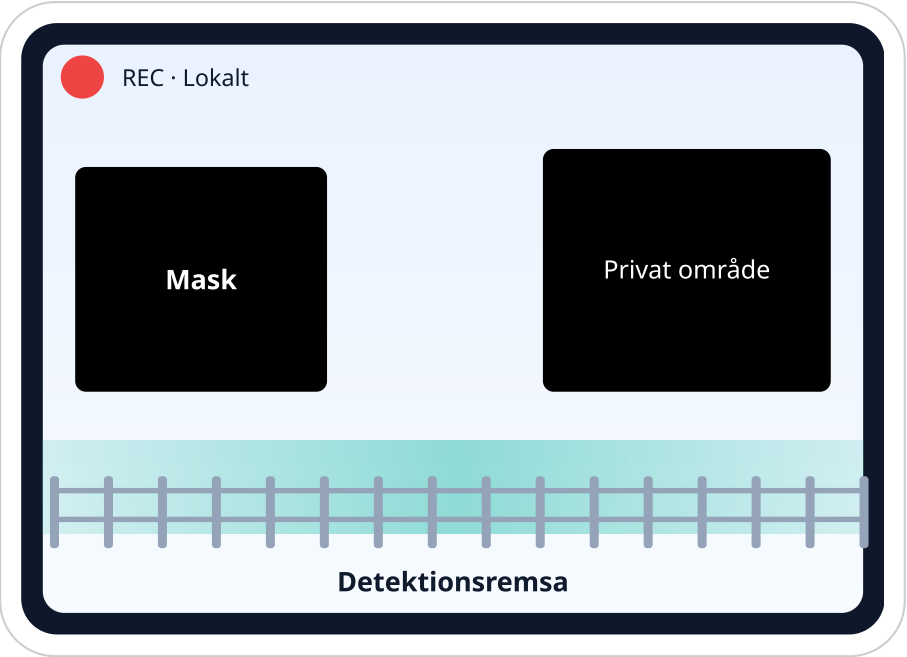
Kameran riktas uteslutande mot en förutbestämd del av det gemensamma området direkt längs staketet.

Alla delar av bilden som kan visa angränsande privata tomter, fönster, balkonger och andra utrymmen utanför den övervakade zonen täcks helt med ogenomskinliga svarta masker.

Maskeringen görs direkt i kameran, innan videoströmmen överförs eller spelas in.

Dessutom definieras en smal detektionsremsa i programvaran. Den artificiella intelligensen analyserar inte objekt utanför detta område.

Systemet omfattar inte ansiktsigenkänning, identifiering av specifika personer, fordonsövervakning eller observation av de boendes vardag.



03

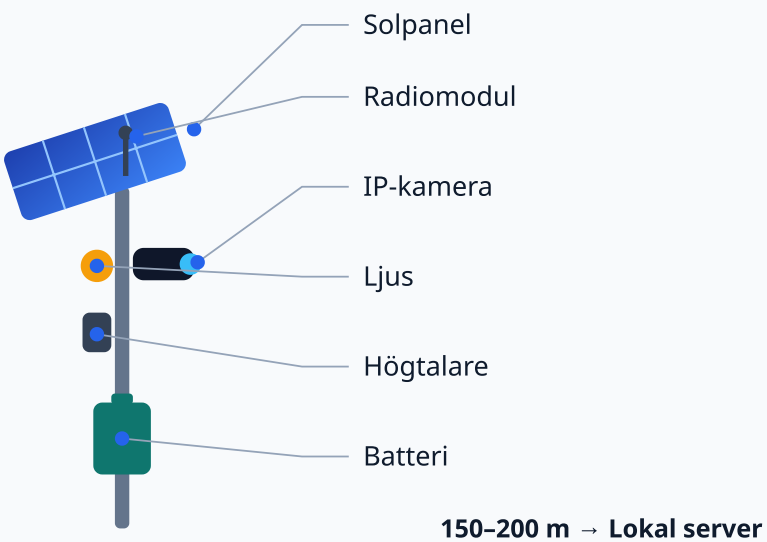
Autonom utrustning

Den fristående noden utrustas med en IP-kamera, en solpanel, ett batteri, en modul för trådlös kommunikation, ett varningsljus och en liten högtalare.

Det förväntade avståndet till den lokala servern är 150–200 meter.

Bilden överförs via en säker trådlös länk till en server inne i byggnaden.

Systemet är inte beroende av externt internet. Internetåtkomst behövs endast för att skicka aviseringar utanför det lokala nätverket och för eventuell kontakt med polisen.



04

Lokal artificiell intelligens

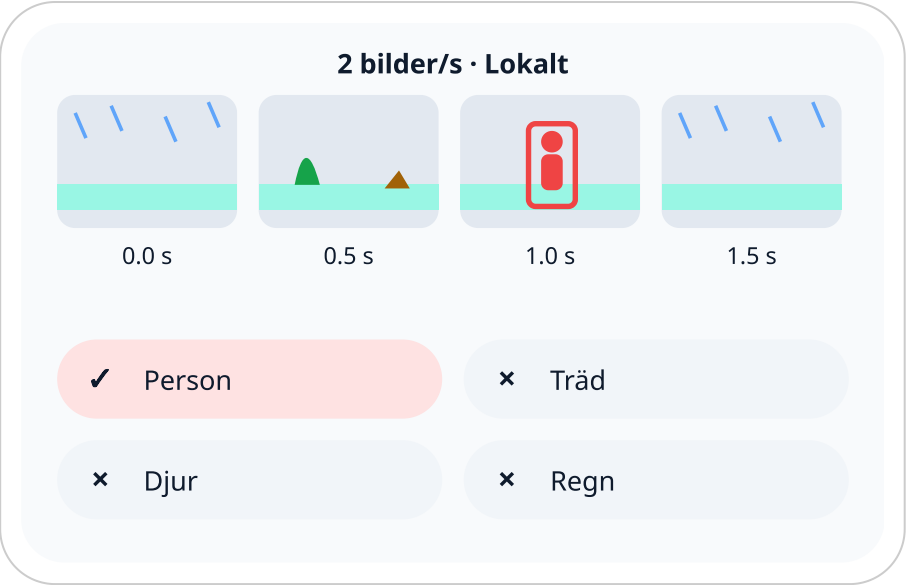
En specialiserad algoritm för datorseende körs på den lokala servern.

Den preliminära planen är att analysera bilden med två bilder per sekund, med möjlighet att öka frekvensen vid behov.

Systemet skiljer människor från rörelser hos träd, buskar, djur, regn och andra naturliga förändringar i bilden.

Varningar utlöses endast när en person bekräftats i den definierade zonen.

Dessutom kan rörelseriktning, passage av en virtuell gräns och tid i den övervakade remsan analyseras.



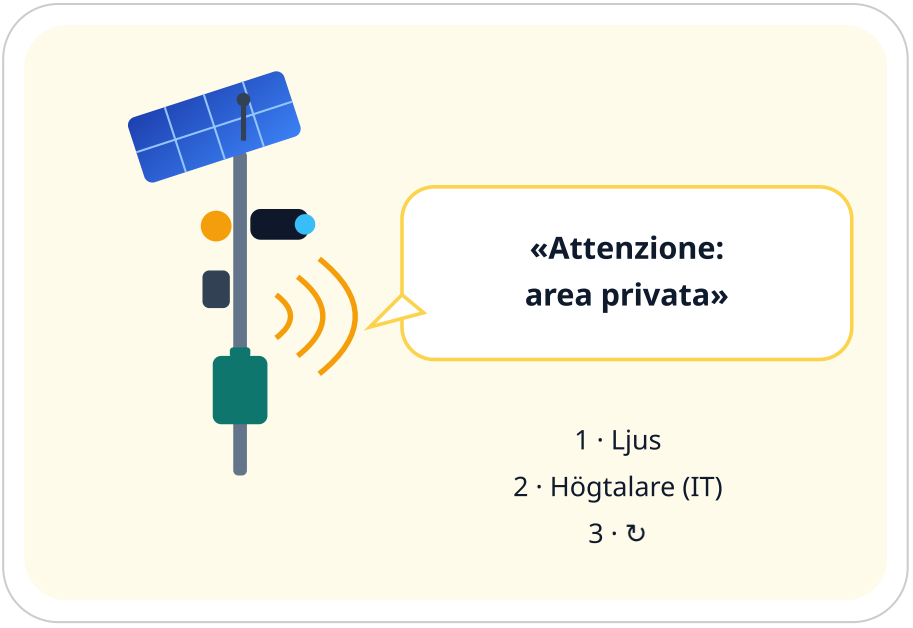
05

Automatisk varning på plats

När en person dyker upp i den skyddade zonen kan systemet:

1. Tända ett varningsljus.
2. Spela upp ett röstmeddelande på italienska om att personen befinner sig på privat område.
3. Vid behov upprepa varningen inom de fastställda gränserna.

Volym, drifttider och aktiveringsvillkor ställs in så att störningar för de boende minimeras.



06

Aviseringar till alla boende

Alla intresserade boende kan få aviseringar i mobilen utan att några foton eller videobilder skickas.

Till exempel:

> **”Obs! En person har upptäckts på den övervakade delen av staketet. Systemet har aktiverat en varning.”**

De boende behöver ingen åtkomst till kameran eller arkivet för att få vanliga aviseringar.

Prenumeration på aviseringar är frivillig. Varje deltagare kan sluta ta emot meddelanden.

Systemadministratören hanterar endast mottagarlistan och aviseringsinställningarna.

Meddelanden skickas i enlighet med kraven på skydd av deltagarnas kontaktuppgifter.



07

Reaktion vid bekräftat intrång

Ett ytterligare läge för förhöjt larm planeras.

Det kan aktiveras om systemet upptäcker en följd av tecken på möjligt intrång, till exempel:

- En person har passerat den definierade gränsen vid staketet.
- Personen fortsätter röra sig mot det inre området.
- Personen befinner sig i en zon där människor normalt inte passerar.
- Händelsen bekräftas genom analys av flera bilder.

I så fall kan systemet automatiskt spara ett videoklipp och skicka en brådskande avisering till de boende.

Möjlighet att kontakta polisen

Den tekniska arkitekturen gör det möjligt att förbereda ett automatiskt meddelande till polisen.

Vid ett bekräftat intrång kan systemet förbereda:

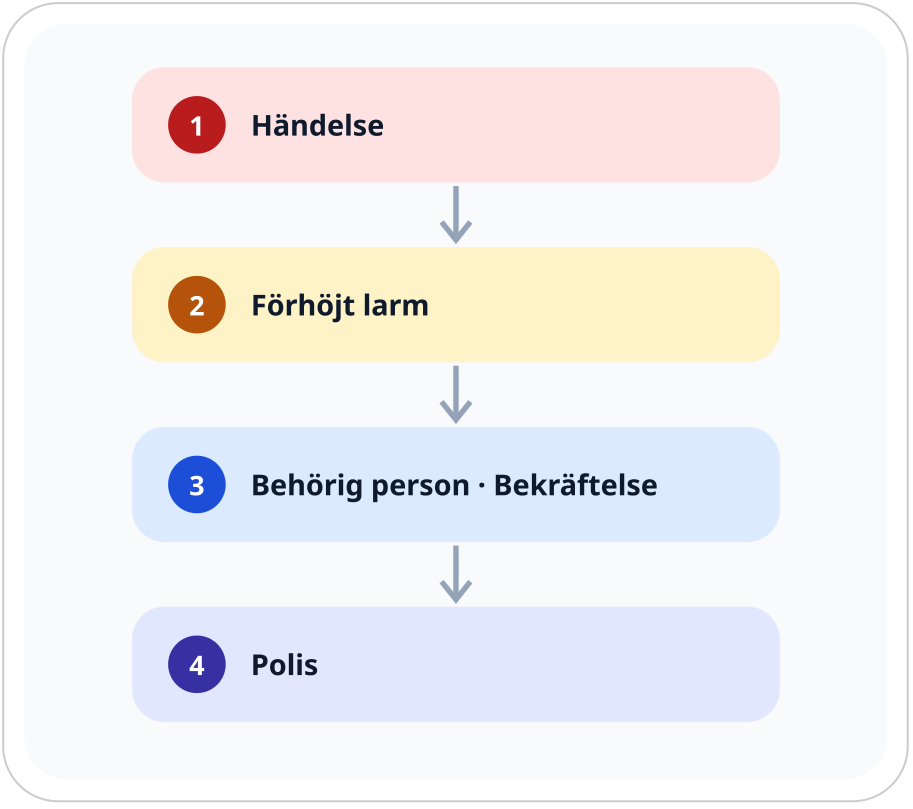
- Ett röstmeddelande på italienska med adress, händelsens art och tidpunkt för upptäckten.
- Några bilder eller ett kort videoklipp.
- Information om var händelsen inträffade.
- Kontaktuppgifter till fastighetens behöriga företrädare.

I nödsituationer planeras ett snabbt samtal till polisen via en behörig person.

I framtiden kan information och bilder överföras via e-post, en säker elektronisk kanal eller ett annat officiellt överenskommet kommunikationsmedel.

Helt automatisk anmälan direkt till polisen är möjlig endast om ett lämpligt officiellt överenskommet samarbetsförfarande finns. Tills det har överenskommits sker samtalet och överföringen av bilder efter bekräftelse av en behörig person.

Detta är nödvändigt för att undvika obefogade anmälningar orsakade av tekniska fel eller falsklarm.



Datalagring och åtkomsthantering

Allt stannar endast lokalt, på fastigheten, i krypterad form. Vid varje larm kan informationen låsas omedelbart. Inga moln och inga tredjepartstjänster.

Videoströmmen bearbetas på den lokala servern utan externa tjänster för artificiell intelligens.

Kontinuerlig inspelning av hela videoströmmen planeras inte. Vid behov sparas korta klipp som rör upptäckta händelser.

Som ett preliminärt förslag raderas vanliga inspelningar automatiskt efter 24 timmar. Längre lagring av en viss händelse är tillåten vid ett motiverat behov, till exempel för att lämna material till polisen.

Åtkomst till bilder ges endast till särskilt utsedda personer.

Vanliga boende får skriftliga aviseringar men ingen åtkomst till kameran.

All åtkomst till arkivet registreras i systemloggen.



09

Nödvändiga godkännanden

Följande förfarande föreslås för genomförandet:

Steg ett — diskussion med de boende.

Publicering av projektets tekniska beskrivning och insamling av synpunkter.

Steg två — överenskommelse med förvaltningen.

Fastighetsförvaltaren får systembeskrivningen, planen för kamerans placering, schemat som begränsar den övervakade zonen och reglerna för databehandling.

Steg tre — beslut av stämman.

Installationen av utrustning i det gemensamma området sätts till omröstning i enlighet med artiklarna 1122-ter och 1136 i den italienska civillagen.

Steg fyra — upprättande av driftregler.

Fastigheten utses till personuppgiftsansvarig. Vid behov utses en teknisk operatör av systemet med begränsade befogenheter.

Regler för åtkomst, lagringstider, förfarandet för att avisera de boende och användningen av videoinspelningar godkänns.

De obligatoriska informationsskyltarna om kameraövervakning sätts upp.

Steg fem — experimentell drift.

Efter att nödvändiga tillstånd erhållits installeras en enda experimentell punkt. Detektionens tillförlitlighet, falsklarm, länkkvalitet, strömförsörjning och aviseringar kontrolleras.

Att skicka meddelanden direkt till polisen behandlas separat med de berörda myndigheterna.

Sammanfattning

Det föreslagna systemet är en autonom intelligent säkerhetsinstallation avsedd uteslutande för övervakning av en begränsad del av det gemensamma området.

Dess uppgift är inte att övervaka de boende, utan att i tid upptäcka ett möjligt intrång genom staketet, varna inkräktaren och informera de boende.

Lokal bearbetning med artificiell intelligens, ett begränsat synfält, fysisk maskering av privata områden och avsaknaden av fri åtkomst till videoinspelningar ska säkerställa en hög nivå av integritetsskydd.

I framtiden kan systemet kompletteras med medel för snabbt samarbete med polisen.

Projektet ska genomföras stegvis, med början i en enda experimentell punkt, och endast efter nödvändiga godkännanden.



+

Förbättringsförslag

Nedan följer CLARYEL:s förslag för diskussion med de boende och förvaltningen. De ingår inte i det godkända projektet och utgör inte ett juridiskt utlåtande: varje förslag bör kontrolleras med förvaltaren och vid behov med en dataskyddsexpert.

FÖRSLAG FÖR DISKUSSION · 1

Konsekvensbedömning avseende dataskydd

Före installationen genomföra och dokumentera en konsekvensbedömning (DPIA, artikel 35 GDPR), eller skriftligen förklara varför den inte krävs i detta fall.

FÖRSLAG FÖR DISKUSSION · 2

Information till boende och förbipasserande

Sätta upp informationsskylten enligt Garante Privacys mall för kameraövervakning och förbereda den fullständiga informationen enligt artikel 13 GDPR, med hänsyn till Garantes och EDPB:s vägledning om kameraövervakning.

FÖRSLAG FÖR DISKUSSION · 3

Skriftlig lagringspolicy

Fastställa i reglerna: 24 timmar som standard, listan över tillåtna undantag, vem som beslutar om förlängning och hur en förlängd inspelning raderas.

FÖRSLAG FÖR DISKUSSION · 4

Tysta timmar och högtalargränser

På natten endast ljus eller sänkt volym, ett högsta antal upprepningar per händelse och en paus mellan varningarna.

FÖRSLAG FÖR DISKUSSION · 5

Övervakning av sabotage och fel

Separata aviseringar till administratören om kameran täcks över eller flyttas, bilden ändras, noden går offline eller batteriet håller på att ta slut.

FÖRSLAG FÖR DISKUSSION · 6

Övervakning av nodens ”hjärtslag”

Noden skickar regelbundet en signal till servern om att den fungerar; uteblir signalen får administratören ett meddelande.

FÖRSLAG FÖR DISKUSSION · 7

Skydd av länk och lagring

Kryptering av radiolänken (till exempel WPA3 och en WireGuard-tunnel), krypterad lagring av klipp, åtkomstlogg, uppdatering av kamerans firmware och byte av fabrikslösenorden.

FÖRSLAG FÖR DISKUSSION · 8

Åtkomst med två personer

Visning och export av klipp endast i närvaro av två utsedda personer, med registrering i loggen.

FÖRSLAG FÖR DISKUSSION · 9

Kontroll av maskerna före driftstart

Visa de boende en bild med maskerna tillämpade och bifoga den till stämmoprotokollet före driftstart; upprepa efter varje justering av kameran.

FÖRSLAG FÖR DISKUSSION · 10

Mått för den experimentella fasen

Registrera falsklarm och missade upptäckter, komma överens i förväg om kriterier för ”fortsätta / inte fortsätta” och presentera en rapport för stämman.

FÖRSLAG FÖR DISKUSSION · 11

Aviseringskanaler

Aviseringarna skapas på den lokala servern och innehåller endast ett skriftligt meddelande, utan bilder; stämman väljer leveranssätt och föredrar alternativ utan molntjänster från tredje part; vem som helst kan avregistrera sig när som helst.

FÖRSLAG FÖR DISKUSSION · 12

Dataminimering

Ingen ansiktsigenkänning, ingen avläsning av registreringsskyltar, ingen ljudinspelning; endast det som behövs för den specifika händelsen sparas.

FÖRSLAG FÖR DISKUSSION · 13

Vinterautonomi

Kontrollera energireserven hos solpanelen och batteriet under korta, mulna dagar och fastställ i förväg hur noden beter sig när batteriet är lågt.

FÖRSLAG FÖR DISKUSSION · 14

Placering av skyltar

Skyltarna placeras före ingången till den filmade zonen och är väl synliga både dag och natt.

FÖRSLAG FÖR DISKUSSION · 15

Regelbunden översyn

Regelbundet, till exempel en gång om året, presentera en rapport för stämman om systemets drift, zoninställningarna och lagringstiderna.

FÖRSLAG FÖR DISKUSSION · 16

Rapportmall för polisen

Ett formulär som förberetts i förväg: datum och tid, sträcka, beskrivning, klipp, kontakt till den behöriga företrädaren, vem som bekräftade händelsen och när.

?

Vanliga frågor

Kommer kameran att filma fönster, balkonger och privata tomter?

Nej. Dessa delar av bilden täcks med ogenomskinliga svarta masker direkt i kameran, före överföring och inspelning. Den artificiella intelligensen analyserar endast en smal remsa längs staketet.

Vem kan titta på videon?

Endast särskilt utsedda personer. De boende får skriftliga aviseringar utan foton eller video och har ingen åtkomst till kameran eller arkivet. Varje åtkomst till arkivet loggas.

Var lagras data och hur länge?

Endast på den lokala servern på fastigheten, i krypterad form, utan moln eller tredjepartstjänster. Det finns ingen kontinuerlig inspelning: korta händelseklipp raderas, som ett preliminärt förslag, automatiskt efter 24 timmar; längre lagring endast vid ett motiverat behov.

Kan jag avstå från aviseringar?

Ja. Prenumerationen är frivillig och du kan sluta ta emot meddelanden när som helst.

Hur är det med falsklarm?

Systemet skiljer människor från träd, buskar, djur och regn, och varningar utlöses endast när en person bekräftats. Polisen kontaktas endast efter bekräftelse av en behörig person. Falsklarm kontrolleras under den experimentella fasen.

Kommer systemet att känna igen ansikten eller registreringsskyltar?

Nej. Projektet omfattar inte ansiktsigenkänning, identifiering av specifika personer eller fordonsövervakning.

Vad kommer det att kosta?

Kostnaden har ännu inte fastställts. Den diskuteras separat, efter att de tekniska lösningarna har stämts av med de boende och förvaltningen.

§

Rättsliga hänvisningar

Officiella källor som är användbara för diskussionen. Länkarna är endast informativa och ersätter inte professionell rådgivning.

Förordning (EU) 2016/679 (GDPR) — officiell version ↗ — https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
Särskilt artikel 13 (information) och artikel 35 (konsekvensbedömning).

Italiensk dataskyddslag — lagstiftningsdekret 196/2003 ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196
Normattiva, gällande version.

Italienska civillagen, artikel 1122-ter — kameraövervakning av gemensamma delar ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1122ter
Normattiva.

Italienska civillagen, artikel 1136 — stämmans beslutförhet och besluts giltighet ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1136
Normattiva.

Garante Privacy — Kameraövervakning ↗ — https://www.garanteprivacy.it/temi/videosorveglianza
Temasida från den italienska dataskyddsmyndigheten.

Garante Privacy — Vanliga frågor, vägledning och skyltmall för kameraövervakning ↗ — https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9496574
Vägledning om förenklad information (skylt) och lagringstider.

EDPB — Riktlinjer 3/2019 om behandling av personuppgifter med videoenheter ↗
— https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it
Europeiska dataskyddsstyrelsen.

Lokalt sammanhang

Fastigheten ligger i kommunen Fino Mornasco (provinsen Como). De organ som anges nedan är möjliga motparter för samordning: projektet förutsätter inga redan ingångna avtal med dem.

I alla nödsituationer gäller alltid det europeiska nödnumret 112.

Kommunen Fino Mornasco ↗ — https://www.comune.finomornasco.co.it/
Kommunförvaltning och lokal polis (Polizia Locale): samordning om lokala regler och skyltar.

Arma dei Carabinieri ↗ — https://www.carabinieri.it/
Den lokalt behöriga stationen: ett möjligt överenskommet förfarande för anmälningar.

✉

Ditt förslag eller din kommentar

Projektets första steg är diskussion med de boende. Berätta vad som kan förbättras och vad som väcker frågor eller tvivel.

Eller kontakta oss direkt

CLARYEL Perimetro — Detta är ett projekt för diskussion med de boende och fastighetens förvaltning. Det kan genomföras först efter nödvändiga godkännanden.

Innehållet är endast informativt och utgör inte juridisk rådgivning.