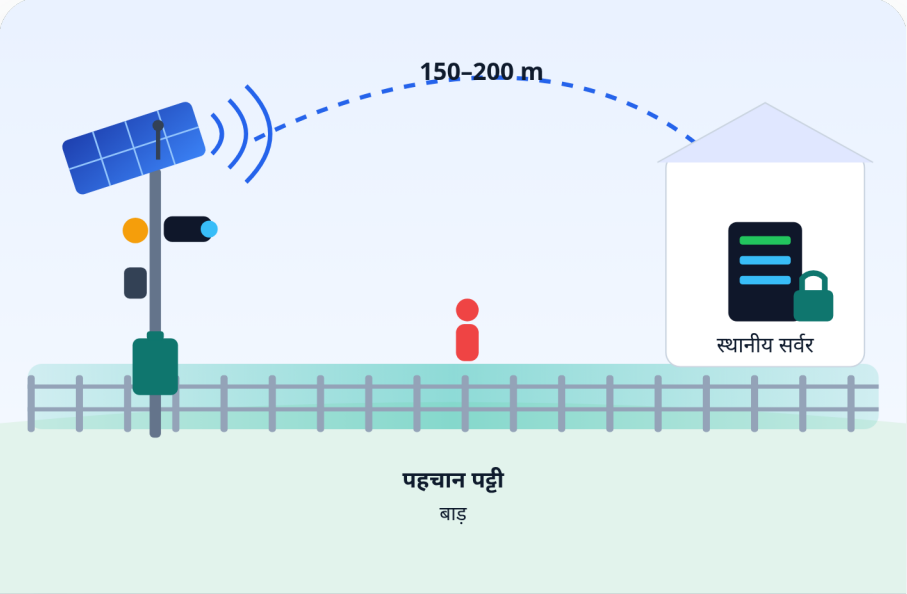
आवासीय परिसर के साझा क्षेत्र की सुरक्षा

CLARYEL Perimetro

साझा क्षेत्र के लिए स्वायत्त बुद्धिमान सुरक्षा प्रणाली की परियोजना

बाड़ के साथ एक ही स्वायत्त बुद्धिमान वीडियो निगरानी बिंदु। सारा डेटा केवल हमारे पास, परिसर के भीतर, एन्क्रिप्टेड रूप में रहता है: कोई क्लाउड नहीं, कोई तृतीय-पक्ष सेवा नहीं, सब कुछ केवल स्थानीय।

- केवल स्थानीय
- एन्क्रिप्टेड
- कोई क्लाउड नहीं
- हर अलार्म पर तुरंत लॉक



मूल सिद्धांत

सब कुछ हमारे पास रहता है — परिसर के भीतर

सभी चित्र, घटनाओं की क्लिप और लॉग केवल भवन के भीतर, परिसर में स्थित स्थानीय सर्वर पर संग्रहीत होते हैं।

सारी जानकारी एन्क्रिप्टेड रूप में संग्रहीत और प्रेषित की जाती है।

किसी भी अलार्म पर सारी जानकारी तुरंत लॉक की जा सकती है: आर्काइव तक पहुँच बंद हो जाती है और घटना की क्लिप बदलाव और हटाए जाने से सुरक्षित हो जाती हैं।

कोई क्लाउड नहीं और कोई तृतीय-पक्ष सेवा नहीं: कृत्रिम बुद्धिमत्ता द्वारा प्रसंस्करण और संग्रहण केवल स्थानीय रूप से होता है।

- भवन में स्थानीय सर्वर
- एन्क्रिप्शन
- तुरंत लॉक
- कोई क्लाउड नहीं
- कोई तृतीय-पक्ष सेवा नहीं



कैमरे का विकल्प

Wi-Fi संकेतों द्वारा पहचान: कोई चित्र नहीं, कोई पहचान नहीं

- कोई कैमरा नहीं
- कोई चित्र नहीं
- कोई पहचान नहीं
- केवल स्थानीय

कैमरे के विकल्प के रूप में बाड़ के साथ दो Wi-Fi उपकरण लगाए जा सकते हैं, निगरानी वाले हिस्से के प्रत्येक छोर पर एक।

दोनों उपकरणों के बीच Wi-Fi संकेत के कच्चे डेटा (उसके परिवर्तनों, जिन्हें CSI — Channel State Information कहा जाता है) से प्रणाली पट्टी में चल रहे लोगों की रूपरेखा निकालती है, बिना किसी चित्र के और बिना यह पहचाने कि वे कौन हैं।

यह तकनीक घरों के भीतर पहले से अध्ययन की जा रही है: उदाहरण के लिए, कार्नेगी मेलन विश्वविद्यालय का शोध “DensePose From WiFi” केवल Wi-Fi संकेतों से कमरे में मौजूद लोगों की आकृतियाँ पुनर्निर्मित करता है। हम इसे बाहर, बाड़ के साथ लागू करने का प्रस्ताव करते हैं।

प्रणाली केवल उपस्थिति, गति की दिशा और एक अनाम आकृति का पता लगाती है। प्रसंस्करण स्थानीय सर्वर पर एन्क्रिप्टेड रूप में होता है, जैसा पूरी परियोजना में है, और वही चेतावनियाँ सक्रिय करता है: प्रकाश, ध्वनि संदेश और निवासियों को सूचनाएँ।

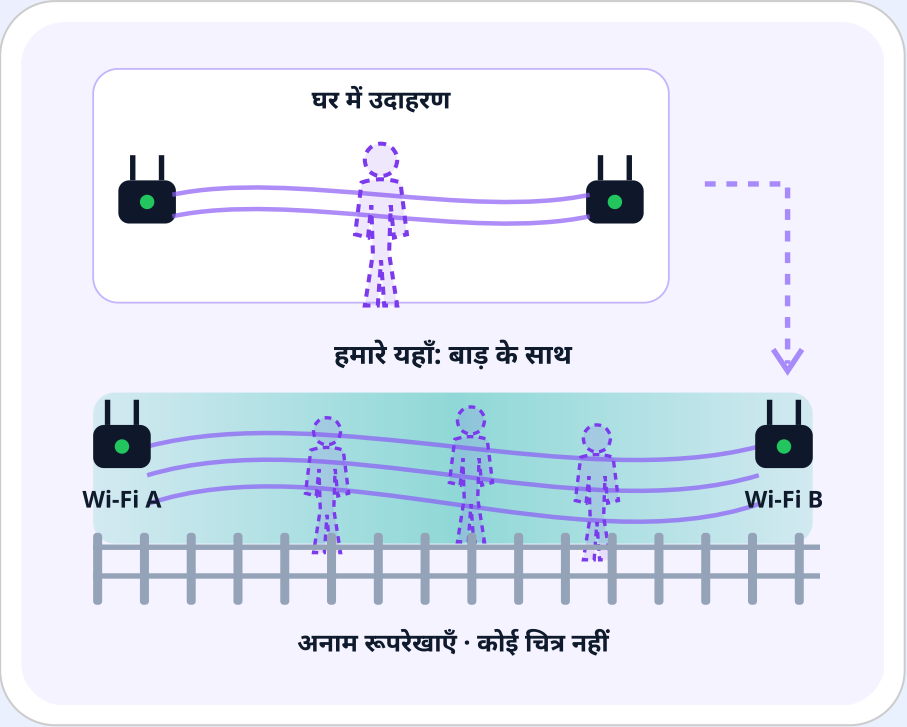
कानूनी पहलू — DPO या सलाहकार के साथ सत्यापित किया जाना है

Wi-Fi द्वारा पहचान कोई चित्र या वीडियो नहीं लेती: इसलिए यह वीडियो निगरानी प्रणाली नहीं है, और वीडियो निगरानी के विशिष्ट नियम (उदाहरण के लिए कैमरों के लिए Garante द्वारा निर्धारित सूचना बोर्ड) इस रूप में लागू नहीं होते।

फिर भी GDPR लागू रहता है यदि डेटा किसी पहचाने गए या पहचाने जा सकने वाले व्यक्ति से संबंधित हो सकता है (GDPR का अनुच्छेद 4, बिंदु 1)। इसलिए प्रणाली को केवल अनाम उपस्थिति और रूपरेखा संसाधित करने के लिए बनाया गया है, बिना पहचान के, केवल स्थानीय रूप से और एन्क्रिप्टेड रूप में।

इस आकलन की पुष्टि स्थापना से पहले DPO या सलाहकार के साथ की जानी चाहिए और यह कोई कानूनी गारंटी नहीं है।

घर के भीतर उदाहरण: "DensePose From WiFi", कार्नेगी मेलन विश्वविद्यालय (arXiv) ↗



01

परियोजना का उद्देश्य

परिसर के साझा क्षेत्र की बाड़ के साथ बुद्धिमान वीडियो निगरानी का एक ही स्वायत्त बिंदु स्थापित करने का प्रस्ताव है।

यह प्रणाली संभावित अनधिकृत घुसपैठ का पता लगाने, घुसपैठियों को चेतावनी देने और निवासियों को तुरंत सूचित करने के लिए बनाई गई है।

परियोजना के मूल सिद्धांत:

01

निजी जीवन में न्यूनतम हस्तक्षेप।

02

बाड़ के साथ केवल एक संकरी पट्टी की निगरानी।

03

कृत्रिम बुद्धिमत्ता द्वारा पूरी तरह स्थानीय चित्र प्रसंस्करण।

04

कोई अनिवार्य क्लाउड सेवा नहीं।

05

प्रेषित और संग्रहीत जानकारी का एन्क्रिप्शन।

06

निवासियों को स्वचालित चेतावनियाँ और सूचनाएँ।

07

कानून प्रवर्तन से शीघ्र संपर्क की संभावना।

02

वीडियो निगरानी की सीमा और निजता की सुरक्षा

कैमरा केवल साझा क्षेत्र के पूर्व-निर्धारित हिस्से की ओर, सीधे बाड़ के साथ, लक्षित होगा।

चित्र के वे सभी हिस्से जिनमें पड़ोसी निजी भूखंड, खिड़कियाँ, बालकनियाँ और निगरानी क्षेत्र के बाहर के अन्य स्थान दिख सकते हैं, अपारदर्शी काले मास्क से पूरी तरह ढके जाएँगे।

मास्किंग सीधे कैमरे में, वीडियो स्ट्रीम के प्रेषण या रिकॉर्डिंग से पहले की जाती है।

इसके अलावा, सॉफ़्टवेयर में एक संकरी पहचान पट्टी निर्धारित की जाती है। कृत्रिम बुद्धिमत्ता इस क्षेत्र के बाहर की वस्तुओं का विश्लेषण नहीं करेगी।

प्रणाली में चेहरा पहचान, विशिष्ट व्यक्तियों की पहचान, वाहनों की ट्रैकिंग या निवासियों के दैनिक जीवन का अवलोकन शामिल नहीं है।



03

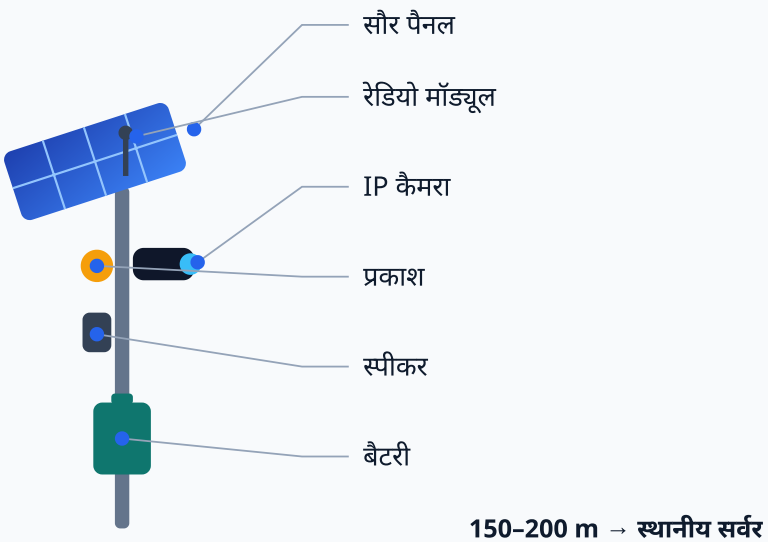
स्वायत्त उपकरण

दूरस्थ नोड में IP कैमरा, सौर पैनल, बैटरी, वायरलेस संचार मॉड्यूल, चेतावनी प्रकाश और एक छोटा स्पीकर होगा।

स्थानीय सर्वर तक अनुमानित दूरी 150–200 मीटर है।

चित्र एक सुरक्षित वायरलेस लिंक के माध्यम से भवन के भीतर स्थित सर्वर तक भेजा जाएगा।

प्रणाली बाहरी इंटरनेट पर निर्भर नहीं होगी। इंटरनेट की आवश्यकता केवल स्थानीय नेटवर्क के बाहर सूचनाएँ भेजने और कानून प्रवर्तन से संभावित संपर्क के लिए होगी।



04

स्थानीय कृत्रिम बुद्धिमत्ता

स्थानीय सर्वर पर कंप्यूटर विज़न का एक विशेष एल्गोरिद्म चलेगा।

प्रारंभिक योजना के अनुसार चित्र का विश्लेषण प्रति सेकंड दो फ़्रेम पर होगा, आवश्यकता होने पर दर बढ़ाने की संभावना के साथ।

प्रणाली लोगों को पेड़ों, झाड़ियों, जानवरों, बारिश और चित्र में अन्य प्राकृतिक परिवर्तनों की गति से अलग पहचानेगी।

चेतावनियाँ केवल तभी सक्रिय होंगी जब निर्धारित क्षेत्र में किसी व्यक्ति की पुष्टि हो।

इसके अलावा, गति की दिशा, आभासी सीमा पार करना और निगरानी पट्टी में बिताया गया समय भी विश्लेषित किया जा सकता है।



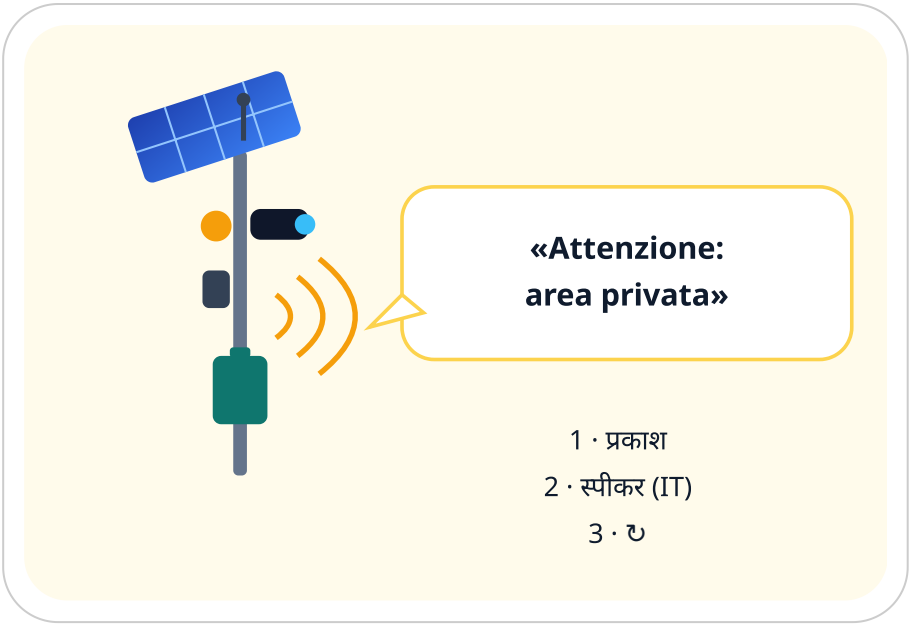
05

स्थल पर स्वचालित चेतावनी

जब कोई व्यक्ति संरक्षित क्षेत्र में दिखाई देता है, तो प्रणाली ये कर सकेगी:

1. चेतावनी प्रकाश जलाना।
2. इतालवी भाषा में एक ध्वनि संदेश चलाना कि व्यक्ति निजी संपत्ति पर है।
3. आवश्यकता होने पर निर्धारित सीमाओं के भीतर चेतावनी दोहराना।

आवाज़, संचालन के घंटे और सक्रियण की शर्तें इस तरह निर्धारित की जाएँगी कि निवासियों को न्यूनतम असुविधा हो।



06

सभी निवासियों को सूचनाएँ

सभी इच्छुक निवासी बिना कोई फ़ोटो या वीडियो भेजे अपने मोबाइल फ़ोन पर सूचनाएँ प्राप्त कर सकेंगे।

उदाहरण के लिए:

> **“ध्यान दें! बाड़ के निगरानी वाले हिस्से पर एक व्यक्ति का पता चला है। प्रणाली ने चेतावनी सक्रिय कर दी है।”**

सामान्य सूचनाएँ प्राप्त करने के लिए निवासियों को कैमरे या आर्काइव तक पहुँच की आवश्यकता नहीं होगी।

सूचनाओं की सदस्यता स्वैच्छिक होगी। प्रत्येक प्रतिभागी संदेश प्राप्त करना बंद कर सकेगा।

प्रणाली प्रशासक केवल प्राप्तकर्ताओं की सूची और सूचना सेटिंग्स का प्रबंधन करेगा।

संदेश प्रतिभागियों के संपर्क डेटा की सुरक्षा संबंधी आवश्यकताओं के अनुसार भेजे जाएँगे।



07

पुष्टि की गई घुसपैठ पर प्रतिक्रिया

एक अतिरिक्त उच्च अलर्ट मोड की योजना है।

यह तब सक्रिय हो सकता है जब प्रणाली संभावित घुसपैठ के संकेतों की एक श्रृंखला का पता लगाए, उदाहरण के लिए:

- किसी व्यक्ति ने बाड़ की निर्धारित सीमा पार की है।
- वह भीतरी क्षेत्र की ओर बढ़ता जा रहा है।
- वह ऐसे क्षेत्र में है जहाँ सामान्यतः लोग नहीं गुज़रते।
- कई फ़्रेमों के विश्लेषण से घटना की पुष्टि होती है।

इस स्थिति में प्रणाली स्वचालित रूप से एक वीडियो क्लिप सहेज सकेगी और निवासियों को तत्काल सूचना भेज सकेगी।

पुलिस से संपर्क की संभावना

तकनीकी संरचना कानून प्रवर्तन के लिए एक स्वचालित संदेश तैयार करने की अनुमति देती है।

पुष्टि की गई घुसपैठ की स्थिति में प्रणाली तैयार कर सकेगी:

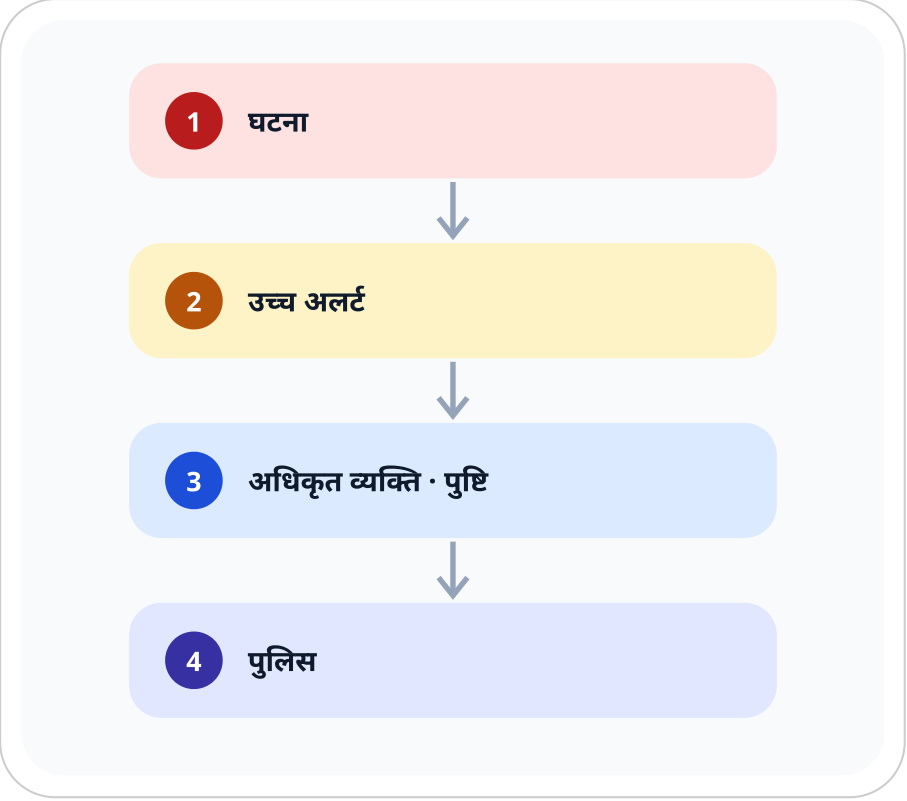
- इतालवी में एक ध्वनि संदेश, जिसमें पता, घटना की प्रकृति और पता चलने का समय हो।
- कुछ चित्र या एक छोटी वीडियो क्लिप।
- घटना के स्थान की जानकारी।
- परिसर के अधिकृत प्रतिनिधि का संपर्क विवरण।

आपात स्थितियों के लिए अधिकृत व्यक्ति के माध्यम से पुलिस को त्वरित कॉल की योजना है।

भविष्य में जानकारी और चित्र ईमेल, सुरक्षित इलेक्ट्रॉनिक चैनल या किसी अन्य आधिकारिक रूप से सहमत संचार माध्यम से भेजे जा सकते हैं।

सीधे पुलिस को पूरी तरह स्वचालित सूचना केवल तभी संभव है जब उपयुक्त आधिकारिक रूप से सहमत सहयोग प्रक्रिया मौजूद हो। उसके सहमत होने तक कॉल और चित्रों का प्रेषण अधिकृत व्यक्ति की पुष्टि के बाद होगा।

यह तकनीकी त्रुटियों या झूठे अलार्म के कारण होने वाली अनुचित सूचनाओं से बचने के लिए आवश्यक है।



डेटा संग्रहण और पहुँच प्रबंधन

सब कुछ केवल स्थानीय रूप से, परिसर के भीतर, एन्क्रिप्टेड रूप में रहता है। किसी भी अलार्म पर जानकारी तुरंत लॉक की जा सकती है। कोई क्लाउड नहीं और कोई तृतीय-पक्ष सेवा नहीं।

वीडियो स्ट्रीम का प्रसंस्करण बाहरी कृत्रिम बुद्धिमत्ता सेवाओं के बिना स्थानीय सर्वर पर होगा।

पूरी वीडियो स्ट्रीम की निरंतर रिकॉर्डिंग की योजना नहीं है। आवश्यकता होने पर पता चली घटनाओं से संबंधित छोटी क्लिप सहेजी जाएँगी।

प्रारंभिक प्रस्ताव के रूप में, सामान्य रिकॉर्डिंग 24 घंटे बाद स्वचालित रूप से हटा दी जाएँगी। किसी विशिष्ट घटना को लंबे समय तक रखना उचित आवश्यकता होने पर अनुमत है, उदाहरण के लिए कानून प्रवर्तन को सामग्री सौंपने के लिए।

चित्रों तक पहुँच केवल विशेष रूप से नामित व्यक्तियों को दी जाती है।

सामान्य निवासियों को लिखित सूचनाएँ मिलती हैं, लेकिन कैमरे तक पहुँच नहीं।

आर्काइव तक हर पहुँच सिस्टम लॉग में दर्ज की जाती है।



09

आवश्यक स्वीकृतियाँ

कार्यान्वयन के लिए निम्नलिखित प्रक्रिया प्रस्तावित है:

पहला चरण — निवासियों के साथ चर्चा।

परियोजना के तकनीकी विवरण का प्रकाशन और टिप्पणियों का संग्रह।

दूसरा चरण — प्रशासन के साथ सहमति।

परिसर प्रशासक को प्रणाली का विवरण, कैमरे की स्थिति की योजना, निगरानी क्षेत्र की सीमा का आरेख और डेटा प्रसंस्करण के नियम प्राप्त होते हैं।

तीसरा चरण — आम सभा का निर्णय।

साझा क्षेत्र में उपकरण की स्थापना को इतालवी नागरिक संहिता के अनुच्छेद 1122-ter और 1136 के अनुसार मतदान के लिए रखा जाता है।

चौथा चरण — संचालन नियमों का निर्माण।

परिसर को डेटा नियंत्रक नामित किया जाता है। आवश्यकता होने पर सीमित अधिकारों वाला एक तकनीकी संचालक नियुक्त किया जाता है।

पहुँच, संग्रहण अवधि, निवासियों को सूचित करने की प्रक्रिया और वीडियो रिकॉर्डिंग के उपयोग के नियम स्वीकृत किए जाते हैं।

वीडियो निगरानी के अनिवार्य सूचना बोर्ड लगाए जाते हैं।

पाँचवाँ चरण — प्रायोगिक संचालन।

आवश्यक अनुमतियाँ मिलने के बाद एक ही प्रायोगिक बिंदु स्थापित किया जाता है। पहचान की विश्वसनीयता, झूठे अलार्म, लिंक की गुणवत्ता, बिजली आपूर्ति और सूचनाओं की जाँच की जाती है।

कानून प्रवर्तन को सीधे संदेश भेजने पर संबंधित सेवाओं के साथ अलग से विचार किया जाता है।

निष्कर्ष

प्रस्तावित प्रणाली एक स्वायत्त बुद्धिमान सुरक्षा स्थापना है, जो केवल साझा क्षेत्र के एक सीमित हिस्से की निगरानी के लिए है।

इसका कार्य निवासियों पर नज़र रखना नहीं, बल्कि बाड़ के माध्यम से संभावित घुसपैठ का समय पर पता लगाना, घुसपैठिए को चेतावनी देना और निवासियों को सूचित करना है।

कृत्रिम बुद्धिमत्ता द्वारा स्थानीय प्रसंस्करण, सीमित दृश्य क्षेत्र, निजी क्षेत्रों की भौतिक मास्किंग और वीडियो रिकॉर्डिंग तक मुक्त पहुँच का अभाव निजता की उच्च स्तरीय सुरक्षा सुनिश्चित करने वाले हैं।

भविष्य में प्रणाली को कानून प्रवर्तन के साथ त्वरित सहयोग के साधनों से पूरक बनाया जा सकता है।

परियोजना को चरणबद्ध रूप से, एक ही प्रायोगिक बिंदु से शुरू करके, और केवल आवश्यक स्वीकृतियों के बाद लागू करने का इरादा है।



+

सुधार के प्रस्ताव

नीचे निवासियों और प्रशासन के साथ चर्चा के लिए CLARYEL के प्रस्ताव हैं। ये स्वीकृत परियोजना का हिस्सा नहीं हैं और कानूनी राय नहीं हैं: प्रत्येक प्रस्ताव की जाँच प्रशासक के साथ और आवश्यकता होने पर डेटा संरक्षण विशेषज्ञ के साथ की जानी चाहिए।

चर्चा हेतु प्रस्ताव · 1

डेटा संरक्षण प्रभाव आकलन

स्थापना से पहले प्रभाव आकलन (DPIA, GDPR का अनुच्छेद 35) करें और उसका दस्तावेज़ीकरण करें, या लिखित रूप में बताएँ कि इस मामले में इसकी आवश्यकता क्यों नहीं है।

चर्चा हेतु प्रस्ताव · 2

निवासियों और राहगीरों को जानकारी

वीडियो निगरानी के लिए Garante Privacy के मॉडल के अनुसार सूचना बोर्ड लगाएँ और GDPR के अनुच्छेद 13 के अंतर्गत पूर्ण सूचना तैयार करें, वीडियो निगरानी पर Garante और EDPB के मार्गदर्शन को ध्यान में रखते हुए।

चर्चा हेतु प्रस्ताव · 3

लिखित संग्रहण नीति

नियमों में तय करें: डिफ़ॉल्ट रूप से 24 घंटे, अनुमत अपवादों की सूची, विस्तार का निर्णय कौन लेता है और विस्तारित रिकॉर्डिंग कैसे हटाई जाती है।

चर्चा हेतु प्रस्ताव · 4

शांत घंटे और स्पीकर की सीमाएँ

रात में केवल प्रकाश या कम आवाज़, प्रति घटना दोहराव की अधिकतम संख्या और चेतावनियों के बीच विराम।

चर्चा हेतु प्रस्ताव · 5

छेड़छाड़ और खराबी की निगरानी

यदि कैमरा ढका या हिलाया जाए, चित्र बदल जाए, नोड ऑफ़लाइन हो जाए या बैटरी कम हो, तो प्रशासक को अलग सूचनाएँ।

चर्चा हेतु प्रस्ताव · 6

नोड की “धड़कन” की निगरानी

नोड नियमित रूप से सर्वर को संकेत भेजता है कि वह काम कर रहा है; संकेत न मिलने पर प्रशासक को संदेश मिलता है।

चर्चा हेतु प्रस्ताव · 7

लिंक और संग्रहण की सुरक्षा

रेडियो लिंक का एन्क्रिप्शन (उदाहरण के लिए WPA3 और WireGuard टनल), क्लिप का एन्क्रिप्टेड संग्रहण, एक्सेस लॉग, कैमरा फ़र्मवेयर अपडेट और फ़ैक्टरी पासवर्ड बदलना।

चर्चा हेतु प्रस्ताव · 8

दो व्यक्तियों की उपस्थिति में पहुँच

क्लिप देखना और निर्यात करना केवल दो नामित व्यक्तियों की उपस्थिति में, लॉग में दर्ज करके।

चर्चा हेतु प्रस्ताव · 9

शुरुआत से पहले मास्क की जाँच

प्रणाली शुरू करने से पहले निवासियों को लगाए गए मास्क वाला एक फ़्रेम दिखाएँ और उसे सभा के कार्यवृत्त में संलग्न करें; कैमरे के हर पुनः समायोजन के बाद दोहराएँ।

चर्चा हेतु प्रस्ताव · 10

प्रायोगिक चरण के मापदंड

झूठे अलार्म और छूटी हुई पहचान दर्ज करें, “जारी रखें / जारी न रखें” के मानदंड पहले से तय करें और सभा को रिपोर्ट प्रस्तुत करें।

चर्चा हेतु प्रस्ताव · 11

सूचना चैनल

सूचनाएँ स्थानीय सर्वर पर बनती हैं और उनमें केवल लिखित संदेश होता है, बिना चित्रों के; सभा वितरण का तरीका चुनती है, तृतीय-पक्ष क्लाउड सेवाओं के बिना विकल्पों को प्राथमिकता देते हुए; कोई भी कभी भी सदस्यता छोड़ सकता है।

चर्चा हेतु प्रस्ताव · 12

डेटा न्यूनीकरण

कोई चेहरा पहचान नहीं, कोई नंबर प्लेट पढ़ना नहीं, कोई ऑडियो रिकॉर्डिंग नहीं; केवल वही रखें जो विशिष्ट घटना के लिए आवश्यक हो।

चर्चा हेतु प्रस्ताव · 13

सर्दियों में स्वायत्तता

छोटे, बादल वाले दिनों में सौर पैनल और बैटरी के ऊर्जा भंडार की जाँच करें और पहले से तय करें कि बैटरी कम होने पर नोड कैसे व्यवहार करेगा।

चर्चा हेतु प्रस्ताव · 14

बोर्डों की स्थिति

बोर्ड रिकॉर्डिंग क्षेत्र के प्रवेश से पहले लगाए जाते हैं और दिन और रात दोनों में स्पष्ट रूप से दिखाई देते हैं।

चर्चा हेतु प्रस्ताव · 15

आवधिक समीक्षा

नियमित रूप से, उदाहरण के लिए वर्ष में एक बार, सभा को प्रणाली के संचालन, क्षेत्र सेटिंग्स और संग्रहण अवधियों पर रिपोर्ट प्रस्तुत करें।

चर्चा हेतु प्रस्ताव · 16

पुलिस के लिए रिपोर्ट का प्रारूप

पहले से तैयार एक फ़ॉर्म: तिथि और समय, हिस्सा, विवरण, क्लिप, अधिकृत प्रतिनिधि का संपर्क, घटना की पुष्टि किसने और कब की।

?

अक्सर पूछे जाने वाले प्रश्न

क्या कैमरा खिड़कियों, बालकनियों और निजी भूखंडों को रिकॉर्ड करेगा?

नहीं। चित्र के ये हिस्से प्रेषण और रिकॉर्डिंग से पहले सीधे कैमरे में अपारदर्शी काले मास्क से ढके जाते हैं। कृत्रिम बुद्धिमत्ता केवल बाड़ के साथ एक संकरी पट्टी का विश्लेषण करती है।

वीडियो कौन देख सकता है?

केवल विशेष रूप से नामित व्यक्ति। निवासियों को बिना फ़ोटो या वीडियो के लिखित सूचनाएँ मिलती हैं और उन्हें कैमरे या आर्काइव तक पहुँच नहीं होती। आर्काइव तक हर पहुँच दर्ज की जाती है।

डेटा कहाँ और कितने समय तक रखा जाता है?

केवल परिसर में स्थानीय सर्वर पर, एन्क्रिप्टेड रूप में, बिना क्लाउड या तृतीय-पक्ष सेवाओं के। निरंतर रिकॉर्डिंग नहीं होती: घटनाओं की छोटी क्लिप, प्रारंभिक प्रस्ताव के रूप में, 24 घंटे बाद स्वचालित रूप से हटा दी जाती हैं; लंबा संग्रहण केवल उचित आवश्यकता होने पर।

क्या मैं सूचनाएँ बंद कर सकता हूँ?

हाँ। सदस्यता स्वैच्छिक है और आप कभी भी संदेश प्राप्त करना बंद कर सकते हैं।

झूठे अलार्म का क्या?

प्रणाली लोगों को पेड़ों, झाड़ियों, जानवरों और बारिश से अलग पहचानती है, और चेतावनियाँ केवल व्यक्ति की पुष्टि होने पर सक्रिय होती हैं। पुलिस से संपर्क केवल अधिकृत व्यक्ति की पुष्टि के बाद किया जाता है। झूठे अलार्म की जाँच प्रायोगिक चरण में की जाती है।

क्या प्रणाली चेहरे या नंबर प्लेट पहचानेगी?

नहीं। परियोजना में चेहरा पहचान, विशिष्ट व्यक्तियों की पहचान या वाहनों की ट्रैकिंग शामिल नहीं है।

इसकी लागत कितनी होगी?

लागत अभी तय नहीं हुई है। निवासियों और प्रशासन के साथ तकनीकी समाधानों पर सहमति के बाद इस पर अलग से चर्चा की जाएगी।

§

कानूनी संदर्भ

चर्चा के लिए उपयोगी आधिकारिक स्रोत। लिंक केवल जानकारी के लिए हैं और पेशेवर सलाह का स्थान नहीं लेते।

विनियम (EU) 2016/679 (GDPR) — आधिकारिक संस्करण ↗ — https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
विशेष रूप से अनुच्छेद 13 (सूचना) और अनुच्छेद 35 (प्रभाव आकलन)।

इतालवी व्यक्तिगत डेटा संरक्षण संहिता — विधायी डिक्री 196/2003 ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196
Normattiva, वर्तमान संस्करण।

इतालवी नागरिक संहिता, अनुच्छेद 1122-ter — साझा भागों पर वीडियो निगरानी प्रणालियाँ ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1122ter
Normattiva.

इतालवी नागरिक संहिता, अनुच्छेद 1136 — सभा का गठन और निर्णयों की वैधता ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1136
Normattiva.

Garante Privacy — वीडियो निगरानी ↗ — https://www.garanteprivacy.it/temi/videosorveglianza
इतालवी डेटा संरक्षण प्राधिकरण का विषय पृष्ठ।

Garante Privacy — वीडियो निगरानी पर FAQ, मार्गदर्शिका और बोर्ड का नमूना ↗ — https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9496574
सरलीकृत सूचना (बोर्ड) और संग्रहण अवधियों पर मार्गदर्शन।

EDPB — वीडियो उपकरणों के माध्यम से व्यक्तिगत डेटा के प्रसंस्करण पर दिशानिर्देश 3/2019 ↗ — https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it
यूरोपीय डेटा संरक्षण बोर्ड।

स्थानीय परिप्रेक्ष्य

परिसर Fino Mornasco नगरपालिका (कोमो प्रांत) में स्थित है। नीचे सूचीबद्ध निकाय समन्वय के संभावित पक्ष हैं: परियोजना में उनके साथ पहले से किया गया कोई समझौता शामिल नहीं है।

किसी भी आपात स्थिति में यूरोपीय आपातकालीन नंबर 112 हमेशा लागू होता है।

Fino Mornasco नगरपालिका ↗ — https://www.comune.finomornasco.co.it/
नगर प्रशासन और स्थानीय पुलिस (Polizia Locale): स्थानीय नियमों और बोर्डों पर समन्वय।

Arma dei Carabinieri ↗ — https://www.carabinieri.it/
स्थानीय रूप से सक्षम स्टेशन: सूचनाओं के लिए संभावित सहमत प्रक्रिया।

✉

आपका प्रस्ताव या टिप्पणी

परियोजना का पहला चरण निवासियों के साथ चर्चा है। हमें बताएँ कि क्या बेहतर किया जा सकता है और किस बात पर प्रश्न या संदेह हैं।

या सीधे हमसे संपर्क करें

CLARYEL Perimetro — यह निवासियों और परिसर प्रशासन के साथ चर्चा हेतु एक परियोजना है। आवश्यक स्वीकृतियों के बाद ही इसका कार्यान्वयन संभव है।

सामग्री केवल जानकारी के लिए है और कानूनी सलाह नहीं है।

CLARYEL SRLS · Fino Mornasco (CO) · VAT 04258140138 · CLARYEL वेबसाइट: claryel.com