TRUSTED PEOPLE

LA SICUREZZA NEL 2025

LE FALLE NORMATIVE E LE NUOVE ARMI DEI LADRI

LO STUDIO CONDOTTO DA BOR

La Sicurezza nel 2025: Lo studio condotto da BOR sulle Minacce, le Falle Normative e le Nuove Armi dei Ladri

Siamo tutti cresciuti con l'incubo di subire il furto di un oggetto di valore, a partire da quando eravamo all'asilo e notavamo che un altro bambino si era appropriato del nostro modellino che non trovavamo più, fino ad arrivare a oggi, quando l'incubo ha assunto contorni assai più ampi e non ci si limita più a un piccolo oggetto di valore, ma va ben oltre ciò che possiamo toccare.

Un tempo, sentir parlare di furto ti faceva subito pensare a persone con il volto coperto che usavano grimaldelli, chiavi bulgare, martelloni o piedi di porco per forzare le serrature, oggi invece il furto ha uno spettro molto più ampio.

L'evoluzione tecnologica ha dotato i ladri di tecnologie e strumenti avanzati per rubare qualcosa di ancora più prezioso: l'identità, la reputazione, il benessere mentale e, non ultimo, il portafoglio elettronico.

È naturale interrogarsi sull'efficacia dei dispositivi in uso, per prevenire e proteggersi contro i furti e dei sistemi normativi in vigore, per punire chi commette furti.

Dal 2018 a oggi abbiamo rilevato e gestito con successo più di mille tentativi di furto e, inevitabilmente, abbiamo analizzato lo scenario criminale sotto diversi aspetti, arrivando alla conclusione che l'informazione, l'aggiornamento, gioca un ruolo fondamentale nella prevenzione.

Conoscere le tecniche in uso, il modus operandi dei ladri, è il primo passo verso la gestione adeguata del rischio. Tenersi informati e aggiornati è necessario per ridurre il rischio di finire vittima di persone prive di scrupoli che, per realizzare un profitto personale, non disdegnano di danneggiare gli altri.

Nel corso degli anni, abbiamo più volte trattato l'argomento per sensibilizzare i consumatori all'uso consapevole dei canali di comunicazione, per evitare di fornire informazioni importanti ai malintenzionati, all'utilizzo di sistemi di prevenzione e protezione efficaci, all'adozione di comportamenti finalizzati a prevenire il rischio di subire furti.

Il nostro obiettivo è indagare lo scenario criminale per tenere informato il consumatore e sensibilizzarlo sulle minacce del crimine e del web.

La natura di questa indagine, che si sviluppa in più articoli, è puramente informativa e approfondisce le tipologie di furto, le nuove frontiere del crimine, le normative a tutela delle persone, le pene, la procedibilità dei reati, le falle e le criticità delle riforme in materia di sicurezza e le misure preventive da adottare per mitigare i rischi.

Per cominciare il nostro percorso di formazione e prevenzione, facciamo luce sulle tipologie di furto e sulle differenze legali che le distinguono.

Dal Furto Semplice al Deep Fake: Le Nuove Frontiere del Crimine e la Legge Italiana

Quando parliamo di "furto" l'immagine che istintivamente si proietta nella mente delle persone, è quella del ladro che, con il piede di porco, tenta di forzare la porta di un'abitazione ma, questa immagine da sola, non è sufficiente perché esistono diverse tipologie di furto, e la legislatura interviene a seconda del caso, con normative specifiche per fare distinzioni cruciali per la procedibilità, per la definizione delle pene e quindi sull'impatto di queste ultime su chi commette il reato.

Conoscere le tipologie di furto contemplate dal Codice Penale ci aiuta ad avere maggiore consapevolezza del rischio e a gestirlo adeguatamente.

Cos'è il furto?

Il furto è un reato contro il patrimonio, che consiste nell'impossessarsi della cosa mobile altrui, sottraendola a chi la detiene, con l'intenzione di trarne profitto per sé o per altri.

Quanti tipi di furto esistono?

Facciamo una prima distinzione tra furto semplice e furto aggravato.

Il **furto semplice** è disciplinato dall'art. 624 del codice penale e si realizza quando una persona sottrae, *senza violenza o minaccia*, un bene che appartiene a un'altra persona, per trarne profitto.

L'assenza di violenza è ciò che distingue il furto semplice dal furto aggravato e si materializza per esempio quando un impiegato sottrae materiale di cancelleria dal cassetto aperto dell'ufficio per portarlo a casa e utilizzarlo per scopi personali; quando una persona sottrae un borsellino lasciato incustodito sul tavolino del bar dal legittimo proprietario, approfittando della sua distrazione ma senza destrezza o violenza, oppure quando in palestra qualcuno sottrae il telefono dal giubbotto custodito nell'armadietto non chiuso a chiave, senza forzare la serratura.

Il **furto aggravato** è disciplinato dall'art. 625 del codice penale e si materializza quando il furto semplice, per la modalità di esecuzione, il luogo o il tipo di oggetto sottratto, è realizzato con destrezza, con scasso o con mezzo fraudolento.

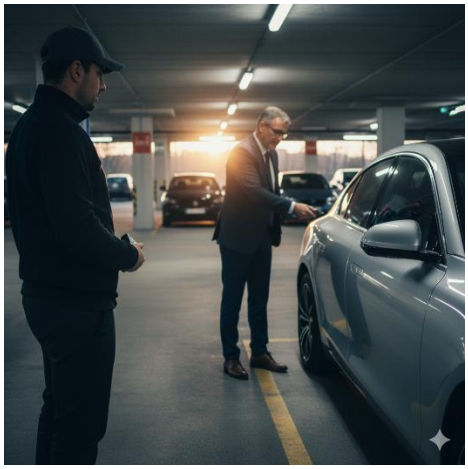
Pensa ai borseggiatori che sottraggono il portafoglio dalla tasca della vittima senza che questa se ne accorga, oppure alle persone sottraggono merce da un negozio nascondendola. Queste due circostanze descrivono esattamente il **furto con destrezza**.

Roberto Benigni, nella mitica scena https://www.youtube.com/shorts/krS1eadqCDA del supermercato nel film "Il Mostro", dà una dimostrazione esemplare del furto con destrezza.

L'utilizzo di martelloni, piedi di porco, smerigliatrici per forzare le barriere di protezione è ciò che classifica il "**furto aggravato dalla circostanza dello scasso**".

La possibilità di disporre di strumenti per il fai-da-te a batterie, ha agevolato l'attività illecita di molti ladri che, dotandosi di smerigliatrici portatili, hanno danneggiato serrande di attività commerciali per farsi largo all'interno dei locali e sottrarre velocemente merce, valori e contanti.

L'eventuale utilizzo di uniformi ufficiali, consente al ladro di compiere un **furto aggravato dalla simulazione della qualità di pubblico ufficiale**, ai danni di vittime che, impressionate dalla fiducia o dall'autorità dell'uniforme, diventano facili prede da raggirare e a cui sottrarre valori.



Anche l'utilizzo di **Jammer** per neutralizzare i sistemi di controllo, rappresenta una circostanza che favorisce il **furto con l'aggravante del mezzo fraudolento**. Pensa a quanti furti d'auto vengono realizzati così… il proprietario del veicolo crede di aver chiuso la macchina con il telecomando, ma ignora che qualcuno nei paraggi, dotato di jammer, ha neutralizzato il segnale e riesce così ad appropriarsi della vettura agevolmente.

Il furto aggravato, lo abbiamo detto prima, è un furto semplice *aggravato* da specifiche circostanze che riguardano la modalità con cui viene eseguito, il luogo o il bene sottratto. Le caratteristiche che emergono sono la destrezza, lo scasso e i mezzi fraudolenti.

Lo scasso si realizza quando il ladro agisce con violenza sulle cose per rubare merce, valori o contanti. Quando la violenza viene esercitata non più sulle cose, ma sulle persone, si parla di Furto con Strappo e Rapina.

Qual è la differenza tra furto con strappo e rapina?

È necessario fare questa distinzione perché l'impatto delle pene previste per tali reati sulla persona che commette il reato è maggiore, così come è maggiore l'impatto del trauma su chi subisce un'azione del genere.

Il furto con strappo è disciplinato dall'art. 624-bis del codice penale e di realizza quando il ladro strappa con violenza la cosa dal corpo della vittima. La violenza in questo caso è maggiormente esercitata sulla cosa e di riflesso sulla vittima che oppone resistenza fisica allo strappo. Non c'è una vera e propria violenza sulla persona.

Il furto con strappo è punito con la **reclusione da quattro a sette anni** e con la **multa da euro 927 a euro 1.500**.

La rapina è il reato contro il patrimonio più grave e, in quanto tale, è punito con pene molto più severe perché danneggia la liberta e l'integrità fisica della vittima. È disciplinato dall'art. 628 del codice penale e si materializza quando l'autore usa violenza o minacce sulla persona per sottrarre o per assicurarsi il possesso della cosa rubata.

Quando avviene una rapina?

La rapina avviene per esempio, quando un ladro minaccia un cassiere con un'arma per farsi consegnare i soldi oppure quando aggredisce fisicamente una persona per immobilizzarla e sottrarle il portafoglio.

La rapina che si realizza con violenza o minaccia alla persona, è punita con la **reclusione da quattro a dieci anni** e con la **multa da euro 927 a euro 2.500**. Tali pene aumentano drasticamente (*fino a vent'anni di reclusione*) se ricorrono circostanze aggravanti, come l'uso di armi o se il fatto è commesso da più persone riunite.

Come è punito il furto semplice?

Secondo quanto disposto dalla Riforma Cartabia, il furto semplice è procedibile a querela della persona offesa, cioè l'azione penale può essere innescata solo se la vittima del furto presenta formale richiesta all'Autorità Giudiziaria.

Come è punito il furto aggravato?

Fino al 2019, quando era in vigore la legge sulla Legittima Difesa, il furto aggravato era procedibile d'ufficio, e lo Stato poteva perseguire il reato non appena ne veniva a conoscenza, anche senza la querela della vittima. Secondo quanto disposto oggi dalla Riforma Cartabia invece, il furto aggravato è procedibile a querela della persona offesa, cioè l'azione penale può essere innescata solo se la vittima del furto presenta formale richiesta all'Autorità Giudiziaria, eccetto in quei casi in cui l'offeso sia incapace o nei casi in cui il furto avviene in abitazione. Approfondiremo tali eccezioni nei prossimi articoli.

Il furto d'identità digitale è un furto semplice o aggravato?

Con la diffusione dei mezzi informatici, abbiamo già detto che il furto assume uno spettro più ampio e ci tocca indagare anche questo aspetto, infatti sebbene le circostanze con cui si realizza lo identifichi più come frode, parliamo del furto di identità digitale, conosciuto anche con il termine **Cybercrime,** come *primo passo* per

commettere *altri* atti illeciti contro il patrimonio o contro l'immagine personale della vittima. Il furto di identità digitale produce dati sempre più allarmanti se consideriamo che riguarda diverse ipotesi illecite, quali l'apertura di conti correnti bancari, il rilascio di carte di credito, l'acquisto di beni e servizi.

L'art. 640 ter del Codice Penale contempla il delitto di frode informatica, stabilendo che chiunque alteri in qualsiasi modo il funzionamento di un sistema informatico o telematico o interviene senza averne diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico, procurando a sé stesso o ad altri un ingiusto profitto a danni di altri, è punito con reclusione e multa.

Come è punito il furto di identità digitale?
La misura con cui viene applicata la pena dipende dalla gravità e dalle modalità con cui il reato viene commesso.
Il delitto di frode informatica aggravata dal furto di identità digitale è procedibile d'ufficio, con reclusione da due a sei anni e multa da euro 600 a euro 3mila se è aggravata dal furto o indebito utilizzo dell'identità digitale di uno o più soggetti.

Ecco alcuni suggerimenti che dovresti seguire per limitare l'esposizione dei dati sensibili al rischio di furto.

L'evoluzione esponenziale dell'Intelligenza Artificiale (AI) ha aperto una nuova e inquietante frontiera: la manipolazione della percezione e della realtà attraverso la creazione di contenuti iper-realistici.

Nel prossimo paragrafo ci concentreremo proprio sui **DeepFake**: la creazione di video, audio e immagini falsificate che sfruttano il volto e la voce di persone reali per scopi illeciti.

Questa tecnologia non minaccia solamente il patrimonio, ma colpisce direttamente l'onore, la reputazione e la credibilità.

Deepfake Finanziario: Il Furto d'Identità che Svuota il Conto. L'Art. 612-quater c.p. e le Misure Anti-AI

Dopo la pubblicazione nella Gazzetta Ufficiale, la **legge n. 132/2025** per la disciplina nazionale sull'Intelligenza artificiale è entrata in vigore il 10 ottobre.

La legge regola l'impiego di sistemi di intelligenza artificiale nei diversi settori dell'attività economica, amministrativa e sociale, introducendo nuove aggravanti e nuovi reati, a cui precedentemente venivano applicate norme pensate per fattispecie diverse, evitando così il ricorso a costruzioni interpretative forzate.

In considerazione di tutti i casi che si sono verificati di recente, è nata l'esigenza di una disciplina chiara e specifica per la tutela delle persone e dei diritti fondamentali, minacciati dalla rapida diffusione degli strumenti informatici e dell'uso improprio dell'intelligenza artificiale, e di adeguare il diritto penale e commerciale ai nuovi reati, resi possibili dalla tecnologia.

L'art. **612-quater** del codice penale disciplina il "**reato di illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale**", stabilendo che chiunque, *senza il consenso dell'interessato*, ceda, pubblichi o diffonda immagini, video o voci falsificati o alterati mediante AI, idonei a indurre in inganno sulla loro genuinità, sia punito con la reclusione da uno a cinque anni.

Come è punito il reato di deepfake?

Il reato è punibile a querela dell'offeso, ed è procedibile d'ufficio se il fatto è commesso nei confronti di una persona incapace per età o per infermità, se è connesso con un delitto perseguibile d'ufficio oppure se è rivolto contro una pubblica autorità.

Il reato di illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale o ***deepfake*** si colloca tra i *delitti contro la libertà morale* e tutela la dignità, la reputazione e l'identità personale delle vittime di manipolazioni digitali.

Il termine *Deepfake* nasce dalla combinazione di due specifiche componenti che spiegano come sia possibile che l'intelligenza artificiale e l'apprendimento profondo possano essere impiegati per creare o alterare contenuti audio e video iper-realistici e falsi.

Quali sono le minacce del deepfake?

Abbiamo già avuto dimostrazioni reali di quali sono gli ambiti di applicazione del *deepfake* dalle notizie diffuse dai media su truffe realizzate utilizzando il volto o la voce di una persona per eludere i sistemi di sicurezza biometrici, per estorcere denaro dalle vittime o ancora sulla diffusione di video/audio compromettenti per ricattare o diffamare la vittima.

Il deepfake arreca sicuramente danni all'identità, alla reputazione e alle finanze della vittima.

Come vengono usati i deepfake?

Truffe vocali. Ricevi una telefonata da un numero sconosciuto. Sebbene tu risponda, dall'altro capo del telefono nessuno parla! Presta attenzione a questa circostanza, potrebbero registrare la tua voce per clonarla ed eludere sistemi di sicurezza o estorcere denaro ai tuoi conoscenti. Oppure ricevi una telefonata con la voce clonata di tuo figlio o del tuo datore di lavoro che ti chiede di eseguire un bonifico istantaneo, agisci con prudenza ed esegui il protocollo del canale secondario, più avanti illustrato.

Deepfake Video. Ricevi una video-chiamata o un messaggio video che ti induce a divulgare dati sensibili o ad accedere a link malevoli.

Estorsione. Vengono diffuse in rete immagini video iper-realistiche alterate e sei indotto a pagare per farle rimuovere.

Deepfake finanziario. Non danneggia solo la tua reputazione, ma svuota il tuo conto corrente. Un finto video che sembri provenire dalla tua banca, può spingerti a cliccare su un link per "verificare la sicurezza del conto", rubando le credenziali e azzerando in pochi minuti il tuo conto.

La voce clonata o un video deepfake che riproduce l'aspetto e il labiale del tuo CEO che ordina un trasferimento di capitale a un fornitore pinco pallino… è già successo, svariate volte!

Come si previene il Deepfake?

La prevenzione è importante almeno quanto le misure di protezione, perché è una misura a tutela dell'identità, della reputazione e delle finanze dell'interessato.

Combinando la formazione a contromisure specifiche alle singole minacce, è possibile contrastare gli attacchi deepfake.

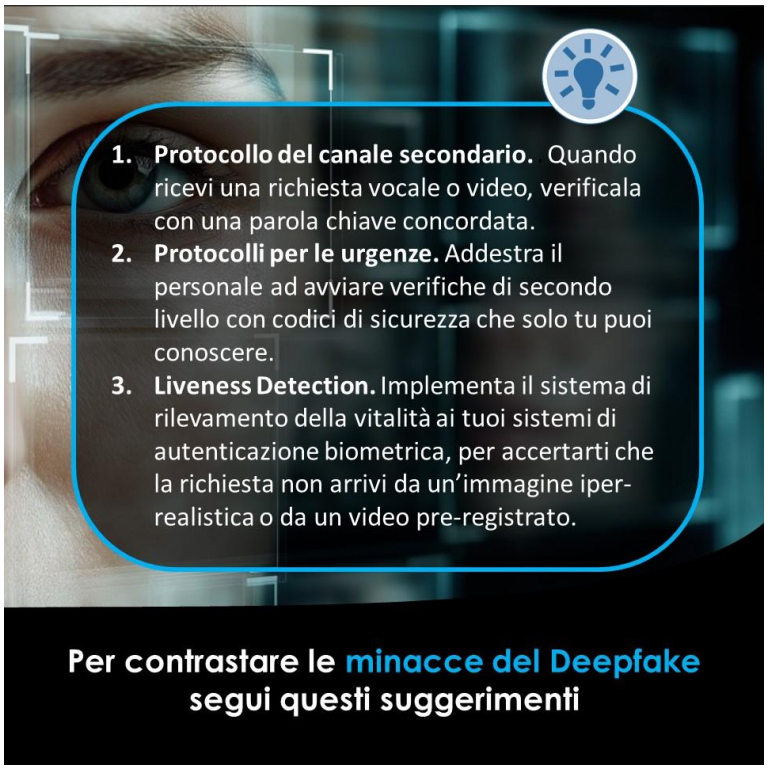
Cosa fare per contrastare il Deepfake?

Vediamo insieme alcune misure da adottare per contrastare il fenomeno.

Protocollo del canale secondario. Quando ricevi una richiesta vocale o video, non agire d'impulso. Verificala con un messaggio di testo o con una parola chiave concordata. Se ricevi una telefonata da un numero sconosciuto con la voce di tuo figlio che ti chiede di eseguire un bonifico istantaneo per gestire un'emergenza, prendi fiato e, prima di agire, ponigli una domanda a cui solo lui può rispondere.

Protocolli per le urgenze. Addestra i tuoi dipendenti a diffidare dalle richieste di pagamento che invocano segretezza o urgenza. Definisci bene le circostanze in cui potresti chiedere loro di eseguire pagamenti urgenti e addestrali ad avviare verifiche di secondo livello nel caso in cui dovessero ricevere richieste urgenti, con codici di sicurezza che solo tu puoi conoscere.

Liveness detection. Implementa il sistema di rilevamento della vitalità ai tuoi sistemi di autenticazione biometrica, per accertarti che la richiesta non arrivi da un'immagine iper-realistica o da un video pre-registrato.



Fino a poco tempo fa i Deepfake venivano perseguiti attraverso l'estensione di reati esistenti (come Diffamazione o Frode Informatica); con l'art. 612-quater c.p. il legislatore ha senz'altro riconosciuto un'identità giuridica distinta al reato e una tutela specifica alle vittime, ma non basta.

Come per la gestione delle altre minacce, anche **per contrastare il Deepfake, è necessario adottare misure preventive per *agire prima che si compia il fatto ed evitare* di finire vittima.**

Perché è importante usare misure preventive per contrastare il deepfake?

Prevenire è meglio che curare! Intervenire con azioni preventive è meglio che correre ai ripari quando il fatto è già avvenuto.

L'introduzione dell'art. 612-quater c.p. è un punto di svolta nel panorama legislativo italiano, che definisce una linea giuridica distinta per il deepfake e può essere inteso come strumento di dissuasione per i malintenzionati e di tutela per le vittime, ma agire prima, con un'opportuna formazione e protocolli specifici, rappresenta per le persone e per l'intera comunità la vera difesa contro i deepfake.

Come il furto, anche il deepfake, oltre all'identità e alla reputazione, colpisce il patrimonio e la libertà morale, ed è punibile a querela dell'offeso. Nel prossimo articolo analizzeremo come la Riforma Cartabia abbia influenzato la procedibilità dei reati di furto, frode e delle nuove minacce digitali.

Le Falle della Riforma Cartabia: Come la legge è diventata una Nuova Arma dei Ladri nel 2025

A inizio settembre è esploso il caso dei borseggiatori che hanno denunciato per stalking i cittadini che li hanno fotografati mentre rubavano.

È successo in stazione a Venezia. Alcuni cittadini stanchi di subire le nefandezze dei pickpocket, hanno deciso di agire fotografando i ladri e pubblicando poi in rete le immagini e i video per allertare gli altri cittadini.

È lecito pubblicare sui social le immagini del ladro mentre compie il furto?

Solo le forze dell'ordine possono diffondere volti e immagini per agevolare le indagini o per motivi di sicurezza pubblica.

Quindi la risposta è: no!

In un altro articolo, che ti invito a leggere per approfondire bene l'argomento, è specificato che la diffusione di immagini foto e/o video che rendono le persone riconoscibili, deve avere una base giuridica: il consenso dell'interessato, un obbligo di legge o un legittimo interesse.

Le normative sulla privacy in Italia e in altri Paesi non permettono la diffusione di immagini di persone riconoscibili, anche se riprese durante l'esecuzione di un reato.

Come gestire correttamente le immagini private e intime senza violare la privacy degli interessati?

Il dibattito sulla sicurezza digitale e la protezione dei dati personali è riesploso recentemente, dopo che gli scandali dei siti e dei gruppi social sessisti e delle telecamere-spia, hanno monopolizzato la cronaca, accendendo i riflettori su una problematica che richiede interventi urgenti per sensibilizzare le persone sui rischi legati alla *non corretta gestione delle immagini private* e sulle misure di protezione da adottare, per non finire vittima di persone senza scrupoli e al contempo per salvaguardare la privacy degli interessati.

Analizzando gli eventi, emergono due aspetti su cui riflettere: la *facilità* con cui la privacy di vittime inconsapevoli è stata violata, e la *vulnerabilità* di sistemi che, da dispositivi destinati a proteggere le persone, si trasformano in una minaccia per la loro intimità.
Aspetti che, se si materializzano, diventano pericoli e, in quanto tali, devono essere spiegati adeguatamente a chiunque tratti, anche involontariamente, immagini di persone, affinché conosca le regole base per agire nel rispetto della legge e dell'etica.

Le Regole d'Oro per la Corretta Gestione delle Immagini e della Privacy

Per gestire foto e video senza incorrere in violazioni è necessario rispettare le seguenti indicazioni:

1. **Il Consenso è la Parola Chiave**: prima di procedere alle operazioni di raccolta, archiviazione o, soprattutto, pubblicazione e diffusione di un'immagine che ritrae una persona riconoscibile, devi ottenere il suo consenso.

Questo consenso deve essere:

- **Libero:** Dato senza alcuna coercizione o pressione.
- **Specifico:** Riferito chiaramente all'utilizzo (es. pubblicazione su un sito web, uso in una campagna promozionale, ecc.). Non basta un generico "sì".
- **Informato:** L'interessato deve sapere *chi* tratterà la sua immagine, *perché* (finalità), *come* (modalità) e *per quanto tempo*.
- **Inequivocabile:** Deve essere espresso tramite un'azione chiara (es. la firma di un modulo, una spunta).

Attenzione ai minori: Per le immagini di minori è sempre obbligatorio acquisire il **consenso scritto di entrambi i genitori** o di chi esercita la responsabilità genitoriale.

2. Il Principio di Riconoscibilità

Se il soggetto ripreso non è **identificabile**, la necessità del consenso alla pubblicazione può venir meno.
Se la finalità non è quella di identificare la persona ma di mostrare un contesto, il consenso non è strettamente richiesto, ma il focus *non* deve essere sul singolo individuo.

3. Garantire il Diritto di Opposizione e Cancellazione

Ogni persona ha il **diritto di opporsi** al trattamento della propria immagine e di chiederne la **cancellazione** (*Diritto all'Oblio*). Chi pubblica o detiene l'immagine (il Titolare del Trattamento) deve garantire che tale richiesta possa essere avanzata facilmente e deve agire tempestivamente per rimuovere o anonimizzare il contenuto. Questo vale anche se il consenso era stato inizialmente prestato.

4. Massima Cautela con i Contenuti Intimi e le Chat

- **Non condividere senza consenso esplicito:** La diffusione di immagini o video intimi ricevuti privatamente è reato, anche se la persona li aveva inviati spontaneamente. L'invio a una persona non è mai un consenso alla diffusione a terzi.
- **Sicurezza dei Dispositivi:** Proteggi sempre i tuoi dispositivi (smartphone, computer) con password forti e autenticazione a due fattori, specialmente se contengono foto private. Un dispositivo non protetto è la prima porta d'accesso per il furto di dati.

5. Protezione dei Sistemi di Videosorveglianza

Se si utilizzano telecamere (domestiche o aziendali):

- **Cambia le password predefinite:** Utilizza password complesse e uniche per l'accesso ai *feed* e alle impostazioni delle telecamere.
- **Aggiorna il firmware:** Mantieni aggiornato il software del dispositivo per correggere le vulnerabilità di sicurezza.
- **Limita l'accesso:** Accedi ai filmati solo attraverso reti sicure e limita la visione alle persone strettamente autorizzate.

Le immagini che ritraggono persone identificabili sono a tutti gli effetti **dati personali** e, come tali, sono soggette alla rigorosa normativa del **GDPR (Regolamento Generale sulla Protezione dei Dati)** e alle leggi nazionali. La tutela della persona ripresa è sempre prioritaria.

Cosa fa BOR per proteggere i dati personali dei clienti?
Abbiamo a cuore la privacy dei nostri clienti!
Nell'erogazione del servizio di Tele-portierato, eseguiamo un controllo esterno alla proprietà dei clienti, con tecnologie avanzate che aiutano Gruppi di Guardiani e Supervisori a sorvegliare le aree, seguendo rigidi protocolli di qualità e nel pieno rispetto della normativa sulla Privacy.

I punti di ripresa dell'impianto di monitoraggio, che usiamo per gestire gli accessi, sono disposti all'esterno della proprietà, e sono visionabili, oltre che dalla Centrale di Monitoraggio, dal cliente, che può gestirli mediante l'App My BOR.

La sorveglianza BOR è progettata per funzionare come un sistema di allarme attivo. Per evitare false segnalazioni, preservare la privacy delle persone e mantenere elevata la qualità del servizio, consigliamo di *attivare la Privacy* in caso di: festeggiamenti o eventi privati, lavori di manutenzione o presenza di operai, utilizzo prolungato degli spazi esterni o della piscina.

Quando la funzione Privacy è attiva, la visione live delle telecamere è disabilitata, la registrazione video viene sospesa ed eventuali eventi rilevati non vengono gestiti, né registrati.

La funzione Privacy consente al cliente di oscurare temporaneamente le telecamere del sistema, garantendo la sospensione della visione live e delle registrazioni da parte della Centrale Operativa BOR.
Questa funzione è pensata per tutelare la riservatezza del cliente durante momenti privati o attività particolari.
Il cliente viene formato all'utilizzo della Funzione Privacy e ha la possibilità di impostare una Privacy Totale o Parziale.

La modalità Privacy può essere attivata anche *solo su alcune aree specifiche*, senza disattivare l'intero impianto.
Questo consente una gestione flessibile e intelligente della riservatezza.

Quando viene attivata una ZONA PRIVACY, il cliente riceve un messaggio via chat, con il quale viene informato su quale
ZONA PRIVACY è stata attivata la Funzione Privacy e che la visione live e la registrazione video sono sospese per garantire la sua riservatezza.

Una volta terminata la necessità, è responsabilità del cliente disattivare la Privacy, per ripristinare il normale funzionamento del sistema.

Da questo che leggi, puoi ben comprendere che tra BOR e il cliente s'instaura un profondo rapporto di fiducia e collaborazione, che trova solide fondamenta su principi etici condivisi da tutto il team BOR, a tutela del cliente e a garanzia dell'efficacia del servizio.
Premesso che in Italia non ci si può far giustizia da soli, entriamo nel dettaglio e cerchiamo di capire come si procede in caso in cui si assista a un furto o nel caso in cui si finisca vittima di un furto.

Abbiamo già distinto i casi in cui si concretizza il furto semplice dai casi in cui il furto semplice, per la modalità di esecuzione, il luogo o il tipo di oggetto sottratto, è aggravato dalla circostanza della destrezza, dello scasso o del mezzo fraudolento.

I borseggiatori che sottraggono il portafoglio dalla tasca della vittima senza che questa se ne accorga, commettono un furto con destrezza.

Cosa succede se la vittima se ne accorge e trattiene il borseggiatore?

Salvo i casi in cui cogli in flagranza una persona che sta compiendo un reato grave, se trattieni una persona contro la sua volontà, rischi il sequestro di persona e, di conseguenza, puoi essere punito con la reclusione da sei mesi a otto anni!

Nel caso in cui il borseggiatore è un minore di età, puoi beccarti la pena dai tre ai dodici anni di reclusione.

È evidente quindi che non puoi diffondere le foto o le immagini video di un borseggiatore, né puoi trattenerlo per consegnarlo alle forze dell'ordine perché rischi una querela da parte dei criminali.

Puoi utilizzare le immagini per documentare il reato o il suo autore, ma non divulgare i contenuti in modo che l'interessato possa essere riconosciuto.

Nessuno può trattenere una persona che ha commesso un reato non procedibile d'ufficio. Il furto con destrezza non è procedibile d'ufficio.

Quali sono le leggi a tutela del cittadino che subisce un furto?

Fino al 2019, era in vigore la legge sulla Legittima Difesa e il furto aggravato era procedibile d'ufficio, pertanto lo Stato poteva perseguire il reato non appena ne veniva a conoscenza, anche senza la querela della vittima.

Il furto semplice è disciplinato dall'art. 624 del codice penale, mentre il furto aggravato dall'art. 625 del codice penale. Dal 2022, secondo quanto disposto dalla Riforma Cartabia, furto semplice e furto aggravato sono procedibili a querela della persona offesa, cioè l'azione penale può essere innescata solo se la vittima del furto presenta formale richiesta all'Autorità Giudiziaria, con la sola eccezione per il furto aggravato per i casi in cui l'offeso sia incapace o nei casi in cui il furto avviene in abitazione.

A differenza di altre forme di furto aggravato, il furto in abitazione mantiene un regime di procedibilità più severo, a tutela della dimensione domestica: è rimasto procedibile d'ufficio. **L'azione penale viene avviata dallo Stato automaticamente non appena le Forze dell'Ordine o l'Autorità Giudiziaria ne vengono a conoscenza, senza che sia necessaria la querela della vittima.**

La Riforma Cartabia è entrata in vigore nel 2022 ed è stata promossa dall'allora Ministro della Giustizia Marta Cartabia per: ridurre i tempi dei processi penali, decongestionare il sistema giudiziario e promuovere la giustizia riparativa, agendo su procedibilità, archiviazione retroattiva dei procedimenti, criteri più stringenti per l'iscrizione della notizia di reato e sulle pene alternative e giustizia riparativa.

Quali effetti ha prodotto la Riforma Cartabia?

Otto reati che in passato erano perseguibili d'ufficio sono stati riclassificati come "procedibili a querela della vittima".

Furto aggravato, lesioni personali dolose, sequestro di persona non aggravato, violenza privata, truffa e frode informatica rientrano tra i reati procedibili a querela.

I procedimenti che erano già in corso, per effetto della Riforma Cartabia, sono decaduti per mancanza di querela da parte della vittima.

La richiesta di elementi probatori più solidi per avviare indagini si traduce spesso nella maggiore difficoltà da parte delle forze dell'ordine nel reperire prove iniziali, pertanto si è avuta una riduzione delle registrazioni di reati per mancanza di prove solide.

In alcune città si è registrato un calo dei reati, ma si presume che ciò non sia dovuto a un'effettiva riduzione della criminalità, bensì a una minore propensione delle vittime (perlopiù anziani, stranieri, turisti o vittime di violenza domestica) a esporre querela perché sottoposte a pressione intimidatoria, per ignoranza della legge o a causa delle barriere linguistiche o logistiche.

Come è punito il furto con destrezza?

Il **furto con destrezza** rientra nella categoria del furto aggravato, è pertanto procedibile a querela della persona offesa, cioè l'azione penale può essere innescata solo se la vittima del furto presenta formale richiesta all'Autorità Giudiziaria.

Come è punito il furto con scasso?

Prima dell'entrata in vigore della Riforma Cartabia, il furto con scasso era procedibile d'ufficio. Oggi l'onere di avviare la procedura è a carico della vittima che deve presentare querela entro tre mesi dall'accaduto. Se la vittima non presenta querela, il caso non viene avviato.

La sensazione che si è diffusa è che la riforma, nel tentativo di snellire la giustizia penale, abbia ridotto le possibilità di difesa dei cittadini e favorito la percezione che la criminalità abbia dalla sua parte la legge.

Il cittadino, se non adeguatamente informato, è più esposto ai rischi legati alla criminalità che, per effetto delle normative a tutela della privacy, delle norme sul sequestro di persona e della Riforma Cartabia, pare che non sia più gestita efficacemente.

I ladri hanno a disposizione nuove armi. Dalla loro parte hanno il progresso tecnologico (smerigliatrici portatili), l'intelligenza artificiale (Deepfake) e persino le leggi che, nel tentativo di tutelare la privacy e la libertà morale e fisica delle persone e per snellire la giustizia penale, nelle loro mani diventano strumenti intimidatori per controllare i cittadini che si coalizzano per agire a tutela della propria sicurezza.

I criminali sfruttano la privacy come scudo legale per denunciare la vittima che diffonde in rete le immagini in cui compiono il furto, così da agire indisturbati.

Sfruttano la *procedibilità a querela* e l'*estinzione del reato* confidando che la vittima non denunci il fatto nei tre mesi successivi.

Usano lo scudo del rischio penale per chi commette il sequestro di persona, per il cittadino che trattiene il borseggiatore così da poter fare i propri comodi.

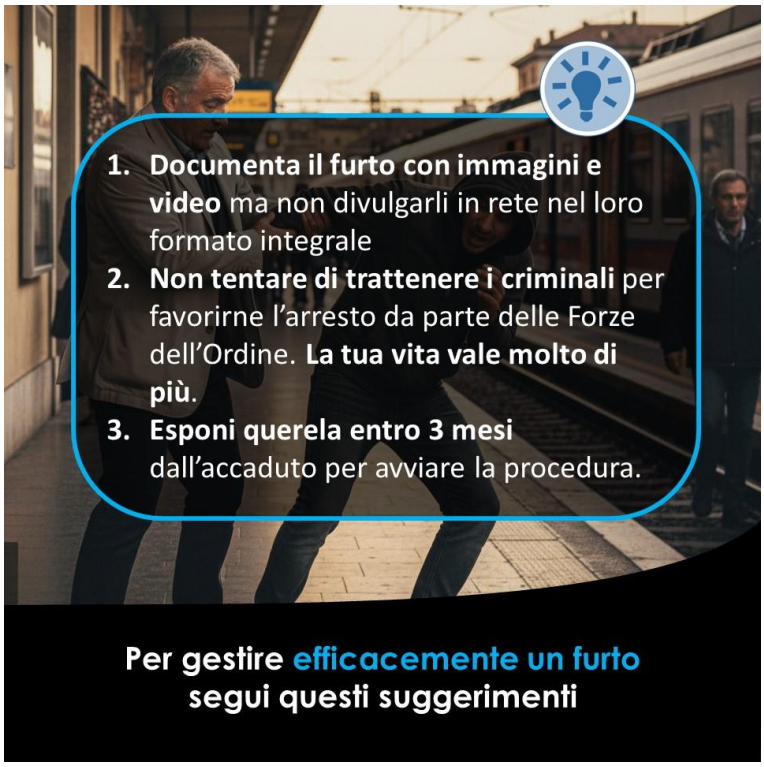
La percezione della sicurezza nel 2025 è quindi calata, a dispetto invece dell'impunità dei criminali, che sanno di avere meno probabilità di essere perseguiti se la vittima non denuncia o se lo fa in ritardo.

Cosa fare per evitare, oltre al danno economico del furto, anche la beffa della querela?

Nell'attesa che le istituzioni correggano le falle normative della Riforma Cartabia per ripristinare l'equilibrio tra efficienza e giustizia, ricorda che puoi produrre immagini foto e video per documentare il furto ma non puoi divulgarle in rete nel loro formato integrale: prima di divulgarle devi oscurare tutti i segni (volto, tatuaggi) che rendono la persona riconoscibile.

Non tentare di trattenere i criminali per favorirne l'arresto da parte delle Forze dell'Ordine. Documenta tutto quello che sta accadendo con video e foto, da esibire all'autorità giudiziaria.

Esponi querela entro 3 mesi dall'accaduto per avviare la procedura.



La percezione di una maggiore impunità stimola i criminali ad agire con maggiore audacia, trasformando quelle che sono leggi a tutela delle persone in strumenti intimidatori per controllare i cittadini.

Il Sistema BOR si pone come misura di prevenzione e protezione definitiva, capace di intercettare e sventare in tempo reale il rischio del furto con scasso, fornendo al contempo la documentazione legale necessaria per blindare ogni azione giudiziaria.

La Criminalità è in Aumento: BOR è la Soluzione che Ti Dà Protezione Totale e ti porta un passo avanti alla criminalità

Milano si conferma la città con il più alto numero di denunce per furti e rapine, lo dice l'indagine pubblicata da "Il sole 24 Ore", per far luce sui principali reati commessi e denunciati nell'anno 2024 in relazione alla popolazione residente.

L'indagine è stata condotta sui dati del Viminale e riflette una tendenza in crescita della criminalità concentrata soprattutto nelle città metropolitane.

Firenze e Roma seguono Milano, registrando un incremento del +7,40% e del + 5,29% rispettivamente. Bologna segue con un preoccupante +9,59% di aumento delle denunce per furti, rapine e criminalità di strada.

Dall'indagine emerge un trend in aumento rispetto al periodo pre-covid che mostra una curva in crescita di tutte le tipologie di reato. Il prof. Marco Dugato ha dichiarato che l'incremento può essere considerato fisiologico a fronte delle criticità sociali ed economiche che il Paese sta attraversando, non meno influenza hanno le tensioni internazionali, anch'esse sul banco degli imputati nell'aumento del fenomeno criminale.

Nel 2024 il 44% delle denunce si è concentrato su: furti in abitazione, furti di autovetture, furti con strappo, furti con destrezza e sui delitti di strada, tra cui emergono le rapine, le lesioni dolose e i danneggiamenti.

Ogni 100mila abitanti: a Milano vengono denunciati 6.952 reati contro i 4.479 di Napoli e i 3.936 di Palermo.

Stime che ci suggeriscono che nelle grandi città del Nord Italia ci sia una maggiore cultura e propensione alla denuncia o semplicemente una maggiore informazione sugli strumenti a tutela dei propri diritti.

La cosa certa è che i delinquenti sono ben informati delle tecnologie e delle leggi che, nelle loro mani, spesso diventano scudi normativi da invocare ai danni delle vittime che eccedono nella legittima difesa.

Il confine tra tutela e violazione dei diritti diventa sempre più sottile ed è più che mai doveroso e opportuno *agire preventivamente* per **evitare** di trovarsi nella spiacevole condizione di doversi difendere dall'azione dei ladri.

Nel nostro studio sulla sicurezza nel 2025 abbiamo analizzato le diverse tipologie di reato per inquadrarne la procedibilità, le falle normative e l'evoluzione delle tecniche criminali. La domanda che ora nasce è inevitabile: **come può il cittadino difendersi efficacemente in uno scenario così ostile, dove anche la difesa può trasformarsi in rischio legale?**

I dati più recenti, come quelli riportati dall'ultimo **Indice di Criminalità de Il Sole 24 Ore**, confermano che il rischio è in aumento, specialmente per quanto riguarda la micro-criminalità e i furti. L'escalation della violenza e l'audacia dei ladri non sono più un'eccezione, ma la regola.

In questo contesto, il malintenzionato non si affida più solo alla forza bruta o all'abilità tecnica; ha sviluppato un arsenale sofisticato che sfrutta le zone grigie normative e le paure sociali del derubato.

I malintenzionati sfruttano con cinismo non solo la debolezza dei sistemi di sicurezza, ma anche la paura del cittadino di difendersi e di subire conseguenze legali sproporzionate.

Il cittadino onesto, anche di fronte a un'intrusione violenta nella propria proprietà (sia essa residenziale o aziendale), teme non solo per la propria incolumità, ma anche per le gravi conseguenze legali nel caso in cui la sua reazione sia ritenuta sproporzionata, culminando in **eccesso colposo di legittima difesa**. L'onere di dimostrare la necessità della difesa ricade su chi è stato aggredito, paralizzando di fatto la reazione.

Il ladro conta sulla tua esitazione e sulla tua paura di finire sotto inchiesta.

Pubblicare le prove è un rischio. In un tentativo disperato di identificare i ladri o di mettere in guardia la comunità, molte vittime sono tentate di pubblicare online le riprese integrali del furto, mostrando i volti dei responsabili. Tuttavia, le normative sulla Privacy (GDPR) possono ritorcersi contro la vittima, che rischia di vedersi recapitare una querela per aver diffuso dati personali senza consenso.

Lo studio che abbiamo condotto sulla percezione della Sicurezza nel 2025 ha tracciato un quadro inquietante: la criminalità non solo si è evoluta tecnologicamente (Deepfake, Jammer, smerigliatrici portatili), ma ha imparato a sfruttare le falle e le ambiguità normative per controllare le persone.

L'indagine pubblicata da "Il Sole 24 Ore" conferma l'aumento della criminalità per il 2024 e nonostante rilevi che nel primo semestre 2025 ci sia stata una diminuzione delle denunce per le frodi informatiche, afferma che la tendenza della curva della criminalità è in crescita.

In che modo il ladro usa le leggi a suo favore?

Il ladro utilizza la Privacy (GDPR) per intimidire e denunciare la vittima che ne diffonde il volto. Sfrutta le regole sulla procedibilità della Riforma Cartabia, sapendo che molti reati (come il furto con destrezza o con scasso) decadono se la vittima non sporge querela entro 3 mesi. Confida nella paura della denuncia per sequestro di persona per garantirsi la fuga anche in caso di flagranza.

Come posso tutelare il diritto a esercitare la difesa personale?

Qual è la Soluzione che Ti Dà Protezione Totale e ti porta un passo avanti alla criminalità?

La difesa personale è un terreno minato, dove l'atto di proteggersi qualora fosse considerato sproporzionato può portare a sanzioni e processi. In attesa che le istituzioni correggano le falle normative, la tua sicurezza deve essere affidata a un *sistema che sia un passo avanti alla criminalità*.

Scegliere BOR significa implementare una misura di prevenzione per proteggere i tuoi cari e i tuoi beni senza rischiare la violenza fisica. Siamo costantemente connessi per sorvegliare l'esterno della tua proprietà e per rilevare precocemente situazioni di pericolo.

Qual è l'obiettivo di BOR?

Il nostro obiettivo è tenere te e chi ami al sicuro, attuando protocolli operativi specifici per ogni singola circostanza. Gruppi di Guardiani e Supervisori, *coadiuvati dall'intelligenza artificiale*, monitorano costantemente la tua proprietà e appena rilevano un'anomalia eseguono *in tempo reale* protocolli di sicurezza dedicati per salvaguardare te, le persone che ami, i tuoi valori e la tua libertà.

Appena rilevano l'anomalia ti informano con documentazione fotografica per tenerti sempre informato su quello che accade alla tua proprietà, sia mentre sei all'interno che quando sei distante. Mantieni costantemente il controllo su ciò che accade e disponi di valida documentazione da esibire alle forze dell'ordine per procedere alla querela.

Quali sono i risultati del Sistema BOR?

Dal 2018 a oggi abbiamo gestito con successo oltre 1000 tentativi di furto, con una percentuale di successo del 98,7%. I nostri clienti sono finalmente liberi di disporre del proprio tempo senza doversi preoccupare della sicurezza, della privacy e della loro libertà.

Tra BOR e il cliente s'instaura un profondo rapporto di fiducia e collaborazione, che trova solide fondamenta su principi etici condivisi da tutto il team BOR, a tutela del cliente e a garanzia dell'efficacia del servizio.

Nell'erogazione del servizio di Tele-portierato, eseguiamo un controllo esterno alla proprietà dei clienti, con tecnologie avanzate che aiutano Gruppi di Guardiani e Supervisori a sorvegliare le aree, seguendo rigidi protocolli di qualità e nel pieno rispetto della normativa sulla Privacy.

I punti di ripresa dell'impianto di monitoraggio, che usiamo per gestire gli accessi, sono disposti all'esterno della proprietà, e sono visionabili, oltre che dalla Centrale di Monitoraggio, dal cliente, che può gestirli mediante l'App My BOR.

Il dibattito sulla **sicurezza digitale e la protezione dei dati personali** che è riesploso recentemente, dopo che lo scandalo delle telecamere-spia ha monopolizzato la cronaca, ha acceso i riflettori su una problematica che richiede interventi urgenti per sensibilizzare le persone sui rischi legati alla *non corretta gestione delle immagini private* e sull'importanza di scegliere con cura le misure di protezione da adottare, per non finire vittima di persone senza scrupoli e al contempo per salvaguardare la privacy degli interessati.

Come fa BOR a gestire i rischi legati alla gestione della sicurezza dei dati?
BOR esegue procedure combinate per tutelare la sicurezza dei dati dei propri clienti, gestendo i rischi a vari livelli. Applica tecniche di crittografia, monitoraggio e controllo per limitare gli accessi con firewall e sistemi IDS per rilevare, segnalare e bloccare tempestivamente le attività sospette, tentativi di intrusione nella rete informatica o anomalie. Esegue regolarmente test sui piani di backup e ripristino per assicurare l'eventuale rapido recupero dei dati, minimizzando i disagi per i clienti.

Ma ancora prima di tutto questo, BOR adotta un approccio sistematico che inizia con un'analisi del rischio approfondita per garantire che ogni soluzione sia "ritagliata sulle specifiche esigenze del consumatore", un aspetto fondamentale che le telecamere di largo consumo non possono offrire.

Qual è il vantaggio di affidarsi a BOR?
Quando ti affidi a esperti della sicurezza la strada si allunga un po' perché, prima di suggerirti una misura contro i rischi di furto e intrusione, analizziamo le criticità a cui è esposta la tua proprietà e tanti altri fattori che impattano sulla progettazione di un ambiente sicuro, conforme ai criteri di sicurezza e alla normativa europea in tema di protezione dei dati.

Cosa fa BOR per condurre un'analisi del rischio personalizzata?
BOR valuta attentamente l'ambiente da sorvegliare, identificando i punti critici, le aree a rischio e le condizioni ambientali che potrebbero influire sulla qualità delle riprese, i rischi tecnici, i rischi operativi e normativi:

- **sceglie le tecnologie più appropriate**, valutando la vulnerabilità hardware e software per prevenire il rischio di attacchi informatici,
- **analizza i rischi legati alla riservatezza**, integrità e disponibilità delle immagini e dei dati registrati per prevenire accessi non autorizzati, definendo protocolli operativi per autorizzare e monitorare i log e prevenire abusi,
- **esamina la capacità del sistema** di continuare a funzionare con piani di backup, sistemi di alimentazione di emergenza e procedure di ripristino dei dati,
- **identifica la probabilità di falsi allarmi o guasti** del sistema che potrebbero compromettere l'efficacia della sorveglianza.

Che cos'è il Sistema BOR?

Il Sistema BOR è una **misura innovativa di prevenzione e protezione** che combina tecnologie evolute e intelligenza artificiale presidiate in tempo reale da Gruppi di Guardiani e Supervisori che analizzano i comportamenti sospetti e gestiscono l'anomalia *da remoto e in tempo reale*, interagendo con i malintenzionati in live e costringendoli alla fuga, **prima che facciano danni**.

Quando il Gruppo di Guardiani e Supervisori rileva la presenza di sospetti lungo il perimetro di un'area sorvegliata da BOR: i ladri scappano a mani vuote mentre tu sei libero di dedicarti alle tue passioni, senza alcuna preoccupazione.

BOR non è un sistema di allarme, è un processo innovativo in continua evoluzione che implementa tecnologie moderne e forza umana per analizzare gli eventi e produrre procedure operative adeguate alle singole circostanze.

BOR è protezione attiva che non richiede alcun intervento fisico da parte tua. Garantisce l'allontanamento immediato dei malintenzionati, salvaguardando la tua incolumità e quella di chi ami.

Perché dovrei scegliere BOR per la sicurezza?

BOR è un'azienda tecnologica che fa della sperimentazione il suo credo. Osserva e Analizza attentamente gli eventi per individuare eventuali falle nei propri processi, per sviluppare miglioramenti continui e restare al passo con l'evoluzione tecnologica.

Non ha la pretesa di essere l'unica soluzione per la tua sicurezza. È una misura da implementare nel tuo sistema di sicurezza insieme al nebbiogeno e alla tradizionale blindatura per evitare che i malintenzionati oltrepassino un certo limite e mettano in pericolo la tua incolumità fisica e psicologica, e per stare un passo avanti ai criminali.

Abbiamo strutturato un sistema di controllo qualità per la gestione delle problematiche comportamentali, a garanzia e tutela del benessere dei nostri clienti. Abbiamo un'organizzazione sistemica per accompagnarti in tutte le fasi del processo di vendita e post vendita, perché siamo "*gente fidata*" con l'obiettivo di rendere la tua vita serena.

Potrai percepire la nostra presenza costante attraverso messaggi di benvenuto o i nostri saluti, riceverai avvisi in tempo reale sull'efficienza tecnologica del tuo impianto, e assistenza dedicata e interventi specialistici.

Siamo un team multidisciplinare al tuo servizio che pensa costantemente a come migliorare la tua vita.

Imparerai a interagire con il tuo Gruppo di Guardiani e Supervisori e a ricevere assistenza in tempo reale come fossero proprio accanto a te.

Cosa succede quando non ci si affida a professionisti specializzati nella sicurezza?

La strada più facile e veloce può sembrare la migliore, ma spesso è la più pericolosa. Se acquisti telecamere di largo consumo, ignorando la progettazione professionale e l'analisi del rischio, è come scegliere un sentiero comodo che, però, non ti porterà mai in cima. **Se le strade impervie ci spaventano, non potremo ammirare tutto il paesaggio che sta al di là della cima.**

Affidarsi a esperti non significa complicarsi la vita, ma garantirsi una vista sicura e senza rischi, sapendo che ogni aspetto: a partire dall'analisi del rischio per garantire un'installazione impeccabile fino all'erogazione del servizio di Telepresenza, nonché alla gestione delle problematiche, delle immagini e delle password, viene curato con etica e competenza.
La sicurezza non è un'opzione, ma un investimento nella tua serenità.


BOR
TRUSTED PEOPLE