

Il controllo degli accessi

# Il portiere

## INVISIBILE

*La sorveglianza elettronica degli ingressi fra tradizione e innovazione.*

*Il rapporto fra sistemi biometrici e rispetto della privacy*



**Michele Santoro.** Il controllo degli accessi è stato sempre molto diffuso negli ambienti lavorativi, soprattutto per verificare gli orari di ingresso e uscita. Anche se le apparecchiature elettromeccaniche sono ormai in disuso, la frase "timbrare il cartellino" è rimasta nel gergo comune ed evoca spesso stratagemmi poco ortodossi, attuati con la complicità dei colleghi, per eludere la sorveglianza dei capi e uscire durante l'orario di lavoro senza essere scoperti. Anche se le moderne tecnologie lo consentono, sono ancora poche le aziende che associano al sistema di controllo orario un dispositivo per riconoscere in modo univoco la persona. Nella stragrande maggioranza dei casi, infatti, l'assenza nell'ambiente lavorativo viene notata subito; diverso è il caso in cui il sistema di riconoscimento venga utilizzato per l'apertura di un accesso e coinvolga problematiche connesse alla sicurezza dei locali. Riconoscimento e accesso sono attuati in due fasi diverse e con dispositivi ben distinti, che possono essere integrati tra loro, in modo da costituire un apparato autonomo, oppure collegati a un sistema centrale, con

funzioni evolute, in grado di gestire più varchi, anche con autorizzazioni differenti. Mentre il riconoscimento coinvolge dispositivi puramente elettronici, l'apertura dell'accesso viene attuata con sistemi elettromeccanici. Vale la pena di soffermarsi dapprima su questi ultimi, che sono i principali protagonisti della sicurezza del varco.

### *Dalla parte della serratura*

Il sistema più utilizzato per l'apertura a distanza delle porte è lo scrocco elettromagnetico. A muoversi, in questo caso, non è la serratura, ma il riscontro su cui si impegna il chiavistello dello scrocco, che si piega in avanti grazie alla spinta della persona, dopo essere stato sbloccato da un elettromagnete. Utilizzare un elemento indipendente dalla serratura presenta indubbi vantaggi: evitare di rimanere chiusi fuori, in caso di rottura della componente elettromeccanica o per mancanza di corrente, poter chiudere il varco a chiave nei periodi in cui non è abilitata l'apertura au-

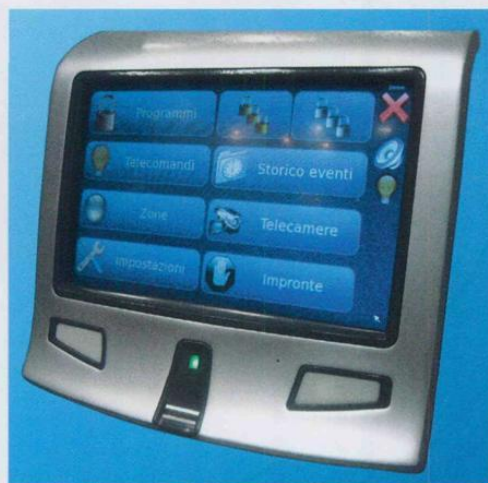
A destra, dall'alto: terminale di gestione dell'impianto di sicurezza con video integrato proposto da Tecnoalarm, con accesso tramite riconoscimento termocapacitivo dell'impronta; esempio di integrazione del controllo accessi nell'impianto di sicurezza: tastiera di controllo di un impianto antintrusione con riconoscimento ottico delle impronte digitali (Master Guardian); cilindro europeo con integrati nel pomolo motorizzazione e sistema di riconoscimento della chiave elettronica. Il tutto alimentato da rete o a batteria (Kaba). Nella pagina a sinistra, sistema di riconoscimento targhe tramite telecamera ad alta risoluzione per il controllo accessi. Utilizzato inizialmente nei parcheggi, oggi è presente in molte città per la regolamentazione delle aree a traffico limitato (Faac).

tomatica, utilizzare un dispositivo unico per tutte le serrature, economizzando i costi di produzione e semplificando la fase di installazione, anche nel caso di porte esistenti.

La sicurezza dello scrocco elettromeccanico è andata sempre crescendo nel tempo. Rimane però il limite fisico della dimensione e della tenuta del nottolino, che non può essere paragonato ai chiavistelli multipli delle serrature per porte blindate o ai catenacci a baionetta dei serramenti in acciaio. Se l'accesso da controllare è la porta di ingresso principale dei locali, è più sicuro ricorrere alla serratura motorizzata. Una volta era un accessorio molto costoso; oggi, con la diffusione delle porte blindate elettroniche, si trovano sul mercato modelli a meno di mille euro, mentre ancora più economici sono i sistemi per serramenti, con catenaccio a baionetta, adatti per le porte in acciaio condominiali o per la motorizzazione delle porte-finestre al piano terreno. L'affidabilità di questi prodotti è elevata: tutti sono dotati di batteria tampone in caso dovesse venire a mancare la corrente e comunque, se dovesse bloccarsi il motore, è sempre presente la serratura a chiave tradizionale, del tipo a fungo nella stragrande maggioranza dei modelli, con cilindro europeo di sicurezza.

Se all'interno della componente elettromeccanica c'è sempre una serratura con chiave, perché ricorrere al controllo automatico e non usare invece quest'ultima come sistema di accesso? Valutiamo, ad esempio, un caso limite: il condominio con diverse abitazioni in cui, salvo rare eccezioni, ad altri sistemi di accesso elettronico viene preferita la chiave. Se si guarda il sistema dalla parte della serratura, l'installazione di un modello elettromeccanico o di uno scrocco è indispensabile, altrimenti non si potrebbe aprire la porta a distanza dal citofono. D'altronde, ormai quasi tutti i condomini montano sulla serratura cilindri ad alta sicurezza, con chiave a riproduzione controllata tramite scheda utente, dal costo elevato, generalmente superiore ai 12 euro. Una scelta del genere presenta notevoli inconvenienti: usura del cilindro, che richiede di essere sostituito dopo una decina d'anni; abbassamento del livello di sicurezza nel caso vada persa o venga rubata una delle chiavi; elevato costo del duplicato della chiave.

Questo è il tipico caso in cui un sistema di controllo accessi è sicuramente più conveniente. Si evita infatti l'uso della chiave, si possono utilizzare strumenti di riconoscimento diversificati, con autorizzazione permanente per i condomini e ingresso a fasce orarie per il personale di servizio, la serratura si usura di meno e, in caso di furto di una scheda di accesso, basta riprogrammare il lettore per escluderla senza dover sostituire le altre. Il grande vantaggio di questa scelta è che non è sostitutiva della chiave, ma si affianca a essa. E quindi, se uno dei condomini preferisce il sistema tradizionale, potrà ancora utilizzarlo, a condizione però che, in caso di smarrimento della chiave o furto, si accoli l'onere di sostituire la serratura e una quota delle chiavi di ricambio.



## Il controllo degli accessi

Qui sotto, a sinistra, lettore a induzione elettromagnetica, con integrato sistema di apertura varchi (Kaba) e, a destra, lettore di impronte Toca a strisciamento, basato sulla mappatura termica del dito. Nella versione più economica memorizza fino a cento impronte (Interel). In basso, controllo accessi studiato per i condomini, con molteplici lettori di attivazione: radiofrequenza, chiave e trasponder, tastiera (Fiam-Iseo).

### Il riconoscimento elettronico

I dispositivi di riconoscimento, come detto, si affiancano alla chiave, ma diversamente da essa sono personali e programmabili singolarmente. La personalizzazione è il grande punto di forza del controllo accessi e anche la ragione per cui viene coinvolta la privacy dell'individuo, perché nella stragrande maggioranza dei casi i dispositivi di riconoscimento registrano in una memoria interna per ogni singolo accesso l'ora e il codice identificativo dell'utente autorizzato. In alcuni contesti, come nei parcheggi a pagamento, non è affatto necessario far corrispondere al tagliando magnetico un individuo, perché lo scopo è conteggiare il tempo tra l'entrata e l'uscita del veicolo; in altri casi è estremamente importante ai fini della sicurezza che possa essere identificato univo-

camente chi varca il punto controllato, utilizzando sistemi di riconoscimento avanzati, come quelli biometrici. Alla stregua della chiave che si impegna nella serratura, anche i sistemi di controllo hanno un lettore e una chiave. Gli apparati più datati sono i lettori di badge, come quelli del bancomat e delle carte di credito. In questo caso il riconoscimento utente è demandato, oltre che al lettore, a una tastiera in cui digitare un codice univoco, che solo la persona conosce. Lo svantaggio di questo metodo di lettura è la grande facilità con cui può essere riprodotta la carta. Meno riproducibile è la scheda con microchip incorporato, come la sim dei cellulari o alcune carte di credito avanzate, in cui i dati dell'utente sono criptati in funzione del codice di accesso e non possono essere letti senza digitare quest'ultimo. Il limite dei dispositivi a scheda è che possono essere facil-



## Il portiere invisibile

mente sabotati. Una tecnologia più sicura è quella della lettura a induzione elettromagnetica: la chiave di accesso è dotata di una spira e un microchip; quando entra nel raggio di azione del lettore viene investita da un campo elettromagnetico, che induce una corrente nella spira, che a sua volta alimenta il microchip interno, permettendo la comunicazione tra chiave e lettore, sempre tramite onde elettromagnetiche. Il vantaggio di questo sistema, denominato trasponder, è l'inaccessibilità del lettore, che addirittura può essere annegato nella muratura, e l'assenza di contatto con la chiave nella fase di riconoscimento. I lettori a trasponder sono ormai diffusissimi, alcuni esempi sotto gli occhi di tutti: gli skipass, oppure i sistemi antitaccheggio presenti nei centri commerciali. L'unità mobile può avere qualsiasi forma, essere nascosta in un'etichetta, nell'impugnatura della chiave tradizionale, fusa all'interno di un badge o in una moneta di plastica e perfino posizionata sottopelle, come accade negli ospedali dove, per motivi igienici, l'accesso ad alcuni locali deve essere effettuato senza contatto e senza l'utilizzo di corpi estranei. L'ultima frontiera del controllo accessi è il riconoscimento biometrico. Relegata in passato nei sistemi di alta sicurezza e basata sulle caratteristiche fisiche dell'individuo, questa metodologia si sta diffondendo anche nei sistemi di riconoscimento legati ai varchi

grazie all'introduzione sul mercato di lettori di impronte digitali a basso costo. Inizialmente l'impronta era archiviata in formato ottico, utilizzando miniscanner; attualmente la tecnologia più sicura è quella a strisciamento, che si basa sulla misurazione del gradiente termico tra le singole dorsali dell'impronta digitale. Il dito scorre su una banda di rilevazione fissa, le variazioni di temperatura vengono trasformate in un codice numerico tramite un efficace programma di compressione e il codice viene confrontato con un database presente nella memoria del dispositivo, per verificarne la compatibilità con quelli autorizzati. Presentato per la prima volta nel 2004 dall'azienda altoatesina Interel, questo lettore, prodotto in Austria e distribuito oggi anche da altre società specializzate in controllo accessi, come la francese Eff Eff, ha rivoluzionato in poco tempo il mercato grazie al suo costo contenuto, inferiore ai 100 euro, e alla sua affidabilità. Altri sistemi più sofisticati si basano sul controllo dell'iride, sul riconoscimento della voce, sull'analisi della conformazione della mano: altrettanto efficaci ma più costose, queste tecnologie richiedono una speciale liberatoria per essere utilizzate, poiché impattano sulla privacy dell'individuo, mentre la lettura termocapacitiva dell'impronta non memorizza immagini, ma una mappa termica. E da questa è impossibile risalire ai tratti somatici della persona. ☑

*Sotto, da sinistra: lettore di impronte a tecnologia capacitiva, associato a un trasponder che legge la mappatura del dito da una tessera personale prima di eseguire la verifica biometrica; in tal modo è possibile gestire migliaia di utenti senza allungare i tempi di riconoscimento e rispettare la privacy (Apice); blocco maniglia con controllo accessi integrato: la sicurezza di questo dispositivo è curata nei particolari, in caso di emergenza è possibile anche alimentarlo dall'esterno e al posto della tastiera è possibile installare un lettore di impronte digitali (Eff Eff); riscontro elettromagnetico di sicurezza, con sistema di apertura in folle negli orari di accesso libero (Eff Eff).*

