e-privacy XXXIV @ Firenze

DISPOSITIVI DI SORVEGLIANZA E PROFILAZIONE: ASPETTI TECNICI

Dott. Davide Bassani

DIFFERENZA TRA SORVEGLIANZA E INTERCETTAZIONE

Sorveglianza:

- Comprende un'ampia gamma di attività volte a monitorare persone, luoghi o attività.
- Può avvenire attraverso metodi diretti (come l'osservazione fisica o l'utilizzo di telecamere) o indiretti (come la raccolta di dati da dispositivi digitali).
- Non implica necessariamente l'intercettazione di comunicazioni private.
- Può essere attuata per diversi scopi, come la prevenzione di reati, la tutela della sicurezza pubblica o la ricerca di informazioni.

DIFFERENZA TRA SORVEGLIANZA E INTERCETTAZIONE

Intercettazione:

- Consiste nella captazione e registrazione di comunicazioni private, come conversazioni telefoniche, messaggi di posta elettronica o chat online.
- Viene generalmente utilizzata per scopi investigativi, al fine di raccogliere prove in materia di reati gravi.
- Richiede un'autorizzazione specifica da parte dell'autorità giudiziaria, che la concede solo in casi eccezionali e motivati.
- Costituisce una grave intrusione nella sfera privata e il suo utilizzo è soggetto a rigorose garanzie per tutelare i diritti dei cittadini.

DIFFERENZA TRA SORVEGLIANZA E INTERCETTAZIONE

In sintesi, la sorveglianza è un concetto più ampio che comprende l'intercettazione come una delle sue possibili modalità. L'intercettazione, invece, rappresenta un'azione specifica e invasiva che richiede una specifica autorizzazione.

Esempi:

- Sorveglianza: la videosorveglianza di un luogo pubblico, la geolocalizzazione di un sospettato, l'utilizzo di software per il riconoscimento facciale.
- Intercettazione: la captazione di una conversazione telefonica tra due persone indagate per traffico di droga, la lettura di messaggi di posta elettronica contenenti informazioni su un attentato terroristico.

I DISPOSITIVI UTILIZZATI PER LA SORVEGLIANZA

La tipologia di dispositivi utilizzati per la sorveglianza è molto ampia e varia in base alle specifiche esigenze e al contesto di utilizzo.

- Telecamere di sorveglianza
- Telecamere con riconoscimento facciale
- Microfoni ambientali
- Dispositivi di geolocalizzazione (GPS)
- Software di sorveglianza informatica
- Droni

I DISPOSITIVI UTILIZZATI PER LA SORVEGLIANZA

I DISPOSITIVI UTILIZZATI PER LA SORVEGLIANZA

Oltre a questi dispositivi, esistono molte altre tecnologie che possono essere utilizzate per la sorveglianza, come la scansione biometrica, la raccolta di dati dai social media e l'analisi del traffico web.

È importante sottolineare che l'utilizzo di dispositivi di sorveglianza solleva importanti questioni relative alla privacy e alla protezione dei dati personali. È fondamentale che l'utilizzo di tali dispositivi sia conforme alle leggi vigenti e che sia garantito il rispetto dei diritti fondamentali delle persone.

METODOLOGIE DI INSTALLAZIONE DEI DISPOSITIVI PER LA SORVEGLIANZA

Le metodologie di installazione dei dispositivi per la sorveglianza variano notevolmente a seconda del tipo di dispositivo, dell'ambiente in cui verrà installato e degli scopi previsti.

- Valutazione delle esigenze
- Scelta dei dispositivi
- Posizionamento dei dispositivi
- Configurazione dei dispositivi

METODOLOGIE DI INSTALLAZIONE DEI DISPOSITIVI PER LA SORVEGLIANZA

Sicurezza dei dati:
è importante adottare adeguate misure di sicurezza per proteggere i dati raccolti dai dispositivi di sorveglianza, come l'utilizzo di password complesse, la crittografia dei dati e l'accesso limitato ai dati stessi.

Privacy:
l'installazione e l'utilizzo di dispositivi di sorveglianza devono rispettare le normative sulla privacy e la protezione dei dati personali. È necessario informare le persone che si trovano nell'area sorvegliata della presenza dei dispositivi e delle modalità di utilizzo dei dati raccolti.

RILEVAMENTO DEI DISPOSITIVI PER LA SORVEGLIANZA

Esistono diversi metodi per rilevare la presenza di dispositivi di sorveglianza nel proprio ambiente, sia che si tratti di abitazioni private, uffici o spazi pubblici.

- Ispezione visiva
- Rilevamento luci LED
- Termocamere
- Rilevatori segnali RF
- Analisi forense dispositivi digitali
- Rilevatori di giunzioni non lineari
- Analizzatori di spettro

È importante ricordare che non esiste un metodo infallibile per rilevare tutti i dispositivi di sorveglianza.

I DISPOSITIVI UTILIZZATI PER LE INTERCETTAZIONI

I dispositivi utilizzati per l'intercettazione possono essere suddivisi in due grandi categorie: quelli per le intercettazioni ambientali e quelli per le intercettazioni telematiche.

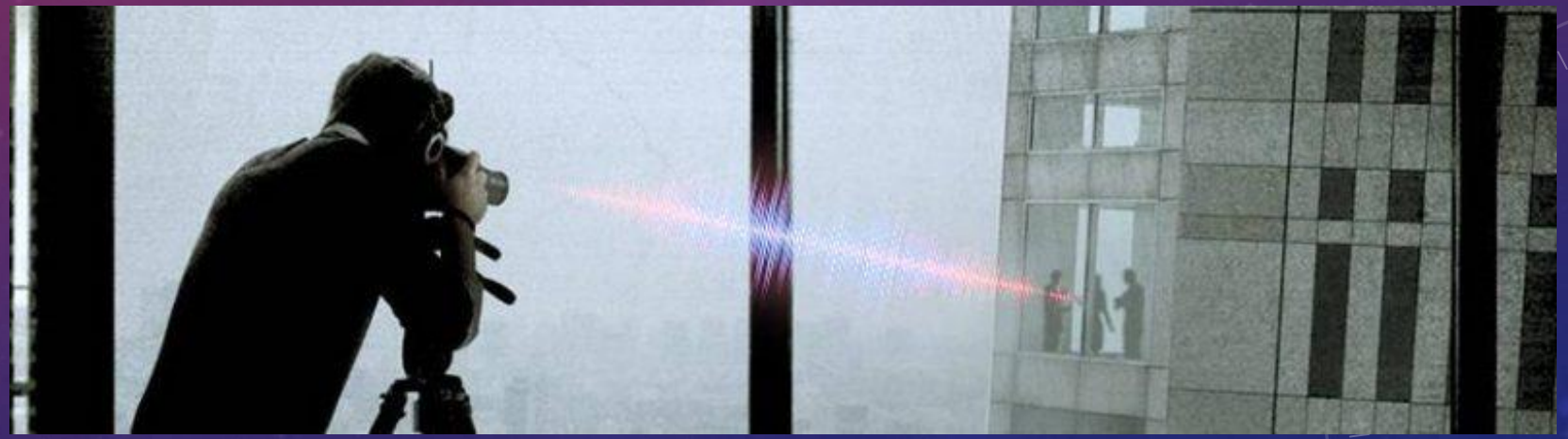
Intercettazioni ambientali:

- Microspie
- Cimici RF
- Registratori audio/video
- Microfoni laser

Intercettazioni telematiche:

- Captatori informatici
- Intercettatori di rete (sniffer)

I DISPOSITIVI UTILIZZATI PER LE INTERCETTAZIONI



METODOLOGIE DI INSTALLAZIONE DEI DISPOSITIVI PER LE INTERCETTAZIONI

Le metodologie di installazione dei dispositivi di intercettazione variano a seconda del tipo di dispositivo utilizzato e dell'ambiente in cui deve essere installato.

Microspie e cimici RF:

- Installazione fisica: Le microspie e le cimici RF possono essere installate fisicamente nell'ambiente in cui si desidera effettuare l'intercettazione. Questo può essere fatto nascondendo il dispositivo in oggetti comuni, come mobili, quadri o soprammobili. In alcuni casi, le microspie possono essere anche installate all'interno di prese elettriche o telefoni.
- Invio a distanza: Alcune microspie e cimici RF possono essere inviate a distanza all'obiettivo. Questo può essere fatto tramite posta, corriere o anche utilizzando droni.

METODOLOGIE DI INSTALLAZIONE DEI DISPOSITIVI PER LE INTERCETTAZIONI

Captatori informatici:

- Installazione fisica: I captatori informatici possono essere installati fisicamente nel computer dell'obiettivo.
- Invio tramite email o allegati: I captatori informatici possono essere inviati all'obiettivo tramite email o allegati. Una volta che l'obiettivo apre l'allegato o clicca sul link, il captatore viene installato sul suo computer.
- Sfruttamento di vulnerabilità: I captatori informatici possono essere installati sul computer dell'obiettivo sfruttando vulnerabilità nel software o nel sistema operativo.

METODOLOGIE DI INSTALLAZIONE DEI DISPOSITIVI PER LE INTERCETTAZIONI

Intercettatori di rete:

- Installazione fisica: Gli intercettatori di rete possono essere installati fisicamente sulla rete a cui è connesso l'obiettivo. Questo può essere fatto dall'amministratore di rete o da una persona che ha accesso fisico alla rete.
- Intercettazione Wireless: Gli intercettatori Wireless possono essere posizionati nel raggio di copertura di un router Wi-Fi e monitorare il traffico di rete. E’ necessario avere le credenziali di accesso.
- Intercettazione remota: Gli intercettatori di rete possono essere utilizzati per intercettare il traffico di una rete da remoto. Questo può essere fatto utilizzando software speciali o dispositivi dedicati.

RILEVAMENTO DEI DISPOSITIVI PER LE INTERCETTAZIONI

Ispezioni fisiche:

- Un'attenta ispezione dell'ambiente, alla ricerca di oggetti sospetti che potrebbero nascondere dispositivi di intercettazione. Questo può includere l'ispezione di mobili, quadri, prese elettriche, telefoni e altri oggetti che potrebbero essere utilizzati per nascondere microspie o cimici RF.

Software per la scansione dei computer:

- Esistono software specifici in grado di rilevare la presenza di captatori informatici installati su dispositivi digitali; questi software funzionano analizzando i processi in esecuzione, i file di sistema, lo scambio dati e altre aree del dispositivo alla ricerca di segni di attività sospetta.

Analisi forense dispositivi digitali

- Viene eseguita la copia forense del dispositivo e viene effettuata un’analisi delle applicazioni installate, dei file di log, dei registri di sistema, ecc.

RILEVAMENTO DEI DISPOSITIVI PER LE INTERCETTAZIONI

Considerazioni importanti:

- La scelta del metodo di rilevamento più adatto dipende da una serie di fattori, tra cui il tipo di dispositivo che si sospetta sia presente, l'ambiente in cui si presume sia installato e il budget a disposizione.
- È importante sottolineare che il rilevamento dei dispositivi di intercettazione è un'operazione complessa che richiede competenze specifiche e una conoscenza approfondita delle tecnologie utilizzate in questo campo.

PROFILAZIONE DEI DISPOSITIVI DIGITALI

La profilazione dei dispositivi digitali è la tecnica di raccolta e analisi di dati da vari dispositivi digitali per creare un profilo unico per un individuo. Questi dati possono includere:

- Indirizzo IP: L'indirizzo IP è un numero univoco assegnato a ciascun dispositivo che si connette a una rete. Può essere utilizzato per identificare la posizione approssimativa di un dispositivo e per tracciare la sua attività online.
- Browser web: Il browser web è il software utilizzato per accedere a Internet. Può essere utilizzato per identificare il tipo di browser e le sue impostazioni.
- Applicazioni installate: Le applicazioni installate su un dispositivo possono essere utilizzate per identificare gli interessi e le attività dell'utente.

PROFILAZIONE DEI DISPOSITIVI DIGITALI

- Cronologia di navigazione: La cronologia di navigazione è un registro di tutti i siti web visitati da un utente. Può essere utilizzata per creare un profilo dettagliato degli interessi e delle attività online dell'utente.
- Cookie: I cookie sono piccoli file di testo che vengono memorizzati su un dispositivo quando un utente visita un sito web. Possono essere utilizzati per tracciare l'attività dell'utente sul sito web e per creare un profilo dei suoi interessi.
- Dati di geolocalizzazione: I dati di geolocalizzazione possono essere utilizzati per determinare la posizione fisica di un dispositivo. Questi dati possono essere raccolti da GPS, Wi-Fi o celle telefoniche.

PROFILAZIONE DEI DISPOSITIVI DIGITALI

LINEE GUIDA PER LA TUTELA DELLA PRIVACY IN AMBITO DIGITALE

1. Adotta pratiche sicure per la gestione delle password
2. Prestare attenzione ai siti web e alle app che si utilizzano
3. Utilizzare software di protezione (antivirus e firewall)
4. Non lasciare incustoditi i propri dispositivi digitali
5. Non utilizzare reti Wi-Fi pubbliche
6. Limitare la quantità di dati personali condivisi online
7. Utilizza strumenti per la tutela della privacy
   - Estensioni per browser che bloccano i tracker e la pubblicità mirata.
   - VPN (Virtual Private Network) che criptano il traffico internet e mascherano l'indirizzo IP.
   - Motori di ricerca che rispettano la privacy e non tracciano le ricerche.