Poliziamoderna

Indagini hi-tech

1. Premessa Quella tra “guardie e ladri” è una lotta la cui origine si perde nei meandri del tempo: più da una parte si cerca il modo di ingannare le leggi e di aggirarle, più dall’altra si studiano e si escogitano le contromisure da mettere in atto per contrastare i malfattori. Una volta questa lotta avveniva quasi esclusivamente nel mondo “reale”, con il poliziotto che inseguiva il malvivente a bordo di una volante, piuttosto che di una motocicletta o anche a piedi, ma oggi, complice anche l’avvento e l’evoluzione della tecnologia, questa atavica partita tra il bene e il male si gioca anche, e quasi soprattutto, nell’ambito dell’informatica. E così, anche la Polizia di Stato ha dovuto adeguarsi, innovarsi e aprirsi a nuove frontiere, dando anche impulso allo sviluppo di nuove tecnologie e formando nuove professionalità.

Certe cose, penserete, siamo abituati a vederle nei film di spionaggio, con soluzioni che a volte, anzi molto spesso, rasentano il fantascientifico o quasi l’irreale… ma spesso, nella nostra realtà, non è così, anzi tutt’altro. Pensate sia impossibile rintracciare una chiamata fatta attraverso una app di instant messaging come Whatsapp o Telegram? Ritenete che, come fa ad esempio Neo, il protagonista di Matrix, infilare un hard disk dentro a un forno a microonde cancelli tutti i dati e sia impossibile recuperarli? O ancora, credete che una fotografia o un fermo immagine sfocato preso da una telecamera di sorveglianza, magari mentre avete anche un cappellino in testa per nascondervi meglio, possa rendere i vostri tratti somatici totalmente irriconoscibili? O, infine, siete sicuri che dentro quel soprammobile posto in bella vista nel salone di casa tramandatovi dai vostri bisnonni non ci sia un qualcosa che registri le vostre “malefatte” in audio e video?

Detta così, sembrerebbe aprirsi uno scenario inquietante, quasi di orwelliana memoria, ma vogliamo rassicurarvi: non avete nulla da temere, sempre che non facciate parte di qualche organizzazione criminale o se avete commesso gravi reati.

Tutto quel che avete letto sopra e quanto leggerete nel prosieguo di questo articolo, è il lavoro quotidiano di una parte della Polizia di Stato che, grazie ad un certo tipo di indagini, sempre più sofisticate e tecnologiche, è di prezioso supporto a chi deve svolgere le indagini e deve portare in dibattimento le prove che inchioderanno o scagioneranno i presunti autori di reati.

La specialità della Polizia di Stato deputata a questo tipo di indagini è la polizia scientifica e, più precisamente, la Sezione “indagini elettroniche”, diretta dal direttore tecnico capo Giovanni Tessitore che alle sue dipendenze conta poliziotti super specializzati che della loro passione per la ricerca in campo tecnologico hanno fatto il proprio lavoro quotidiano.

Al secondo piano del Polo tuscolano ci sono dei veri e propri laboratori; sembra quasi di entrare in quella che nei film di 007 si chiama la “Sezione Q”, dove vengono escogitati tutti i gadget e utilizzate tutte le tecnologie più all’avanguardia per il più famoso agente segreto al servizio di sua maestà.

Iniziamo il viaggio nelle varie aree in cui è divisa la Sezione indagini elettroniche della Scientifica, ricordando che nel mese di dicembre 2023 abbiamo già trattato l’area dedicata alle indagini foniche.

2. Analisi telematiche In apertura, si diceva appunto dell’intercettazione di conversazioni, o di messaggi, effettuati via Whatsapp o Telegram; infatti, ad oggi, quasi tutte le conversazioni tra persone che non vogliono farsi intercettare, o meglio, che non vogliono far trapelare ciò di cui stanno parlando, avvengono quasi esclusivamente con le famose “chiamate vocali” che queste applicazioni mettono a disposizione degli utenti. Da un lato, un grande vantaggio, ad esempio, per chi chiama dall’estero sfruttando una rete wifi per evitare eventuali maggiorazioni tariffarie previste per chiamate internazionali o intercontinentali, dall’altro la “sicurezza” di non essere ascoltati dato che si tratta di telefonate che avvengono su una rete telematica, per giunta criptate. Un bel problema, in quest’ultimo caso, per chi dovesse svolgere indagini di polizia giudiziaria e un’apparente vittoria per chi è dall’altra parte. Ma non è proprio così, anzi: «Ogni applicazione di messaggistica per poter funzionare comunica

con i propri server – ci dice Giovanni Tessitore – utilizzando una sorta di linguaggio convenzionale (ossia un “protocollo informatico”, come, ad esempio, lo Stun tipico delle chiamate Whatsapp, ndr.). A seconda del tipo di linguaggio adottato e dei server contattati, è possibile risalire alla specifica applicazione utilizzata dagli interlocutori e al tipo di flusso dati scambiato, nonostante il contenuto della comunicazione sia cifrato».

Ma quel che è particolarmente interessante è che, nel caso delle comunicazioni VoIP, come ad esempio le chiamate vocali o le videochiamate effettuate per mezzo delle suddette app, le connessioni instaurate sono del tipo “peer to peer” (cioè mettono in comunicazione diretta i due interlocutori): in presenza di specifica autorizzazione dell’autorità giudiziaria è possibile analizzare il flusso dati tra gli interlocutori, per risalire all’indirizzo IP del dispositivo contattato e, successivamente, agli estremi anagrafici dell’utente. Ovviamente, come già detto, non è possibile ascoltare la conversazione, ma sapere chi sia stato chiamato, quante volte e per quanto tempo, è già un’informazione rilevante, soprattutto se incrociata poi con altri elementi investigativi.

Tuttavia la problematica maggiore si riscontra proprio nel passaggio dagli IP dei dispositivi allo storico del traffico, in questo caso telematico, analogo al cosiddetto tabulato telefonico “classico”. Allo stato attuale, su richiesta dell’autorità giudiziaria, tutti i gestori delle reti di telefonia forniscono una mole di documenti con tante informazioni da correlare e analizzare che mal si prestano all’immediata individuazione di comunicazioni VoIP: solo con un’attenta analisi manuale condotta da operatori specializzati, è possibile risalire a dati anagrafici quali nome, cognome, codice fiscale, etc. associabili agli IP individuati. «E questa attività va ripetuta per ogni singola chiamata – prosegue Tessitore – si immagini una situazione in cui si hanno molteplici target in contemporanea e ognuno di questi effettui dozzine di chiamate VoIP al giorno. Una marea di dati».

Ed è qui che entra in gioco la tecnologia, con un portale (Linc – Log ip network communications analysis) interamente sviluppato “ in house” dalla Sezione indagini elettroniche e che, nella “marea di dati” messa a disposizione, riesce a estrapolare e individuare automaticamente, grazie ad un sofisticato algoritmo, l’identità informatica dei due interlocutori.

L’area analisi telematiche si occupa anche di altre attività tra cui l’analisi della radiocopertura cellulare, nel caso sia necessario individuare l’area fisica coperta dalla cella telefonica da cui è partita o in cui è arrivata una telefonata: «Il metodo usato dagli operatori telefonici – conclude Tessitore – dà una stima abbastanza ampia della zona, poiché viene utilizzata una simulazione matematica con un modello che tiene conto di parametri che sono quelli riguardanti una specifica antenna e la conformazione del territorio. Noi invece, per avere dati più precisi ai fini delle indagini, o ai fini forensi, operiamo in un altro modo: andiamo sul posto, con un’apparecchiatura specifica misuriamo più volte il campo di irradiazione spostandoci nelle vicinanze della cella telefonica e poi interpoliamo questi dati creando una stima dell’area realmente coperta».

3. Digital forensic Sempre più spesso, le “prove” di un qualche reato sono contenute in un hard disk, in una memoria usb o anche nella memoria di un telefono cellulare e il riuscire a estrapolarle può rafforzare o anche cambiare radicalmente il corso di un’indagine. Ma come riuscire a farlo nel caso in cui i dati contenuti nelle varie memorie siano, come quasi sempre accade, protetti da password o sistemi di cifratura? E, soprattutto, come farlo in modo che poi possano essere utilizzati in dibattimento?

Proprio di questo si occupa un’altra area della Sezione indagini elettroniche, quella del *digital forensic*. Qui, tramite macchinari di ultima generazione e software particolarmente sofisticati, è possibile estrarre i dati da un qualsiasi device, anche se gravemente danneggiato.

«Noi lavoriamo su delega dell’autorità giudiziaria – precisa Alessandro Allegrini, vice ispettore responsabile dell’area *digital forensic* – quando con la commissione di un reato sul posto vengono effettuati sequestri di dispositivi cellulari oppure memorie di massa. In tali circostanze, l’AG delega a questa sezione il compito di effettuare la “copia forense” dei dispositivi, sulla quale poi l’ufficio investigativo compirà le proprie analisi, che viene realizzata tramite software che consentono di non alterare le informazioni contenute nel reperto, quindi senza modificarlo, ottenendo una copia “bit a bit”, o il più fedele possibile, che poi viene messa a disposizione dell’ufficio investigativo e dell’autorità giudiziaria».

Può accadere che si debbano estrarre i dati da device danneggiati, ma: «Con una particolare strumentazione che con precisione riesce a fondere lo stagno con cui vengono saldate le memorie

sulle schede – prosegue il vice ispettore della Scientifica – riusciamo a effettuare il “chip off”, ovvero una rimozione del componente di memoria dal dispositivo, il tutto accuratamente documentato da sensoristica di precisione per evitare il danneggiamento della memoria stessa e preservare l’utilizzo dei risultati per finalità forensi. Una volta separato il componente, questo viene collegato a un’altra apparecchiatura per la lettura del contenuto,andando quindi a bypassare l’hardware originario in cui il chip era collocato».

E se ad esempio un hard disk fosse danneggiato fisicamente? Qui interviene la “maestria” degli operatori che, attraverso una serie quasi infinita di “ricambi”, contenuti in decine di cassetti del laboratorio, riescono a riassemblare il tutto operando in una cosiddetta “camera bianca”, ossia una cappa a flusso laminare in grado di eliminare qualsiasi impurità e di consentire agli operatori di lavorare in un’area completamente sterile. Ma non solo vengono estratti dati dai “classici” device che tutti conosciamo, come tablet, pc o cellulari con qualsiasi sistema operativo, bensì anche da strumenti particolari, come ci racconta ancora Alessandro Allegrini: «Ultimamente abbiamo lavorato anche su un sistema di infotainment, un navigatore installato su un veicolo. È stato impossibile riuscire ad accedere ai dati attraverso i sistemi convenzionali, tipo la presa USB della macchina; ci abbiamo provato anche con software specifici, ma senza successo perché la casa costruttrice nel caso in particolare aveva fatto un aggiornamento per cui aveva installato una specie di protezione, un gateway, che impediva l’accesso ai dati dall’esterno anche attraverso i punti di diagnostica che ogni produttore di veicoli rende disponibili sulle schede madri. Alla fine, tramite il procedimento del “chip off” siamo riusciti a estrarre il chip di memoria e a leggerlo. È stata anche un’esperienza interessante a livello formativo, perché in quel caso addirittura abbiamo dovuto installare su un nostro computer un sistema operativo *real time* chiamato QNX come quello che viene usato nella maggior parte dei sistemi di *infotainment* e che ci ha consentito di accedere ai dati del navigatore».

4. Analisi video e riconoscimento facciale Oggi, nelle nostre città, ci sono milioni di “occhi” che scrutano h24 quasi ogni angolo delle strade, rendendo estremamente difficile nascondersi perché siamo quasi sempre sotto l’obiettivo di una videocamera di sorveglianza, che sia quella di una banca, di un museo o anche semplicemente del controllo del traffico stradale o addirittura del portone di un condominio. Centinaia di migliaia di ore di registrazioni e altrettante immagini, di differente qualità e risoluzione, da poter estrapolare nel caso in cui venga commesso un reato e sia necessario individuarne l’autore.

Che l’immagine sia nitida o sfocata, poco importa perché, grazie a particolari software implementati anche con algoritmi di intelligenza artificiale, è possibile ricostruire il volto di una persona anche da un’immagine di bassa qualità. Un esempio di come sia possibile è accessibile a tutti, grazie alle decine di software messi a disposizione online, ma nell’area analisi video della Sezione indagini elettroniche è possibile spingersi oltre, grazie a tecnologie e programmi particolarmente performanti, costruiti per l’uso investigativo, così che da un frame di un filmato si possa arrivare a identificare, in poco tempo, l’autore di un reato, come avviene grazie al portale Sari (Sistema automatico di riconoscimento immagini), sviuppato dalla polizia scientifica ed in uso alle forze di polizia, che è in grado di ricercare la foto di un soggetto ignoto all’interno della banca dati dei soggetti fotosegnalati Afis (la stessa in cui vengono salvate le impronte digitali). Il risultato del Sari non è mai un “match” come siamo abituati a vedere nei film stile CSI ma una lista di candidati che deve essere revisionata a mano da un operatore specializzato alla ricerca di un possibile candidato su cui concentrare ulteriori investigazioni. Un’applicazione pratica? La risoluzione del caso legato al furto dei gioielli del Maraja in mostra al Palazzo Ducale di Venezia nel 2018: «Tra le varie immagini raccolte dalle telecamere – racconta il commissario capo tecnico, Fabrizio Corrado Adamo, funzionario addetto alla Sezione indagini elettroniche – vi era anche quella non particolarmente nitida del volto di uno dei rapinatori. Il Sari riuscì a trovare il match con un’altra immagine precedentemente inserita nel sistema e così fu possibile catturare i rapinatori che appartenevano a un’organizzazione criminale internazionale chiamata “Pink Panthers” (chiaramente ispirati dai film con Peter Sellers protagonista, ndr.). Quando è necessario un confronto “forense” (ad esempio tra il volto estrapolato da una videocamera sul luogo del reato e quello relativo a un cartellino fotosegnaletico) è necessario condurre un’ analisi 1 a 1. La polizia scientifica in questo ambito utilizza una metodologia chiamata “analisi morfologica” che, dal punto di vista scientifico, offre maggiore affidabilità, seguendo best practice riconosciute a livello internazionale. Ma l’area video non si occupa solo di analisi del volto! Quando il volto non è visibile perché il soggetto è ad esempio ripreso di spalle o indossa un casco, gli operatori di quest’area sono in grado di stimarne l’altezza a partire dalle immagini, un dato che non è certo identificativo ma che può essere determinante per le indagini o per escludere un sospettato. Sempre nell’area video ci si occupa di stabilire l’autenticità di un’immagine alla ricerca di segni di manomissione inseriti per esempio per creare un alibi. Si tratta di un’attività che sarà sempre più importante anche alla luce della crescente diffusione dei c.d. *deep fake* ovvero immagini create da algoritmi di intelligenza artificiale del tutto simili a quelle reali.

5. Intercettazioni audio/video Un classico dell’investigazione “sul campo”, così come

nell'immaginario collettivo stimolato dai tanti telefilm a stelle e strisce sulle indagini scientifiche, è rappresentato dalle intercettazioni audio, con microspie, e video, con microcamere inserite negli oggetti più disparati. Anche di questo si occupa la Sezione indagini elettroniche, come ci spiega Giovanni Tessitore: «Sono attività che vengono utilizzate sia per esigenze di polizia giudiziaria, come ad esempio monitorare un'area quale potrebbe essere una piazza di spaccio, sia per la tutela dell'ordine pubblico, ad esempio con operatori che effettuano riprese durante una manifestazione. E poi ci sono le classiche intercettazioni ambientali che, essendo attività che si svolgono il più delle volte in luoghi privati, necessitano di un decreto di autorizzazione da parte dell'autorità giudiziaria».

Ma anche il "pedinamento" qui acquisisce un'altra accezione perché, invece di seguire una persona o anche un mezzo a vista, è possibile farlo tramite il tracciamento GPS, in modo tale da azzerare letteralmente la possibilità di essere scoperti a vista da parte della persona seguita: «È svolta con una strumentazione dedicata – prosegue Tessitore – che viene installata ad esempio sull'autovettura da seguire; è un monitoraggio elettronico che in parte si sostituisce a quella che è la classica osservazione visiva, ma che è svolta completamente da remoto e che dal punto di vista giuridico è assimilabile al classico pedinamento, quindi un'attività d'iniziativa, e sfrutta la tecnologia dei satelliti GPS commerciali, cercando di fare in modo di avere sempre più satelliti disponibili contemporaneamente, così da avere una precisione maggiore».

6. Laboratorio di stampa 3D Per trovare l'ultima area nata della Sezione indagini elettroniche, bisogna scendere qualche piano più in basso, al -1. Spesso è proprio nei sotterranei che vengono celate le meraviglie e anche stavolta questa diceria non viene smentita. Si apre una porta a vetri automatica e ad accoglierci troviamo Massimo Ruggeri e Vincenzo Contasti, rispettivamente sovrintendente e assistente capo coordinatore, che ci fanno entrare in un mondo unico, particolare: due stanze in cui, come in tutte le altre aree della Sezione, la tecnologia la fa da padrona, ma che allo stesso tempo assume un fascino decisamente particolare.

Alcune delle cose che abbiamo visto qui dentro non possiamo raccontarvele, per non svelare segreti che un domani potrebbero dare un vantaggio a qualche malintenzionato o "bruciare" qualche importante indagine, ma possiamo assicurarvi che qui, con un po' di filamento plastico o di resina, può essere ricreata ogni cosa inanimata.

Come è possibile? Grazie a varie stampanti 3D (delle quali una grande quanto una cabina doccia) che utilizzano tecnologie e software di ultima generazione, ma che solo grazie alla passione e alla professionalità di Massimo e Vincenzo riescono a dare anima e forma ai bit inseriti nei programmi di disegno 3D.

Tra le cose che possiamo citare, oltre alla ricostruzione del volto del pittore del '500 Vincenzo Lotto (del quale abbiamo già parlato sul numero di giugno 2023 di Poliziamoderna), anche quella del cranio di una delle Tre Marie di Veroli: «Abbiamo scansionato i resti del cranio originale – raccontano i due operatori – e grazie all'aiuto di un medico legale, siamo riusciti a ricostruire e "stampare" il resto, compresa la mandibola con la dentizione intera».

Un aiuto molto prezioso per le indagini, ma anche e soprattutto per l'analisi forense, può essere dato dalla stampa 3D che, grazie a un'accurata scansione dell'originale, può riprodurre fedelmente qualsiasi cosa e riuscire a portare in dibattimento elementi che non potrebbero essere fisicamente rimossi dalla propria sede perché troppo grandi, così come accaduto nelle indagini legate al disastro ferroviario di Pioltello del 2018, quando un treno deragliò a causa di un danno alle rotaie:

«Ovviamente in aula non poteva essere portato il binario della stazione, così come la ruota del treno – ricordano Massimo e Vincenzo – quindi dovevamo trovare il modo di farlo. Dopo aver scansionato sul posto, con uno scanner 3D, il tratto di rotaia incriminato e la ruota del treno deragliato, venimmo in laboratorio per rielaborare tutti i dati al computer, fare una simulazione a video dell'incidente dopo aver visionato le immagini delle telecamere, e stampare una sezione della rotaia in scala 1:1 (circa tre metri) con il giunto saltato che aveva causato l'incidente e la ruota del treno. Il tutto fu portato in dibattimento».

Qui non ci sono solo le classiche stampanti "a filamento", ma anche apparecchiature che sfruttano tecnologie particolari come la stampa da resina liquida (praticamente si vede la forma progettata al computer "sorgere" piano piano da questo liquido bianco) con cui è stata realizzata la testa di Vincenzo Lotto, o ancora la classica fresa, ma a controllo numerico, con cui intagliare o rifinire qualsiasi manufatto.

La tecnologia della stampa 3D è in continua evoluzione e qui, ovviamente, si pensa già al futuro, ossia a una stampante con tecnologia “a polvere” in grado di riprodurre meccanismi funzionanti e già assemblati, praticamente come il “replicatore” di Star Trek…

«La prossima sfida? – concludono i due titolari di quello che è il vero e proprio “Settore Q” della Scientifica – Quello in cui le macchine ancora non sono riuscite: stampare una sfera perfetta».

E c’è da giurarci che ci riusciranno… sempre che, mentre andiamo in stampa, non ci siano già riusciti!

09/01/2024