

Cose utili da sapere (dalle carte dell'operazione "Diana")

Nel fascicolo dell'operazione Diana sono riportate, in tutto o in parte, le carte relative a diversi procedimenti penali. Uno di questi è quello relativo ad un 270 bis nei confronti di diversi compagni e compagne e persone vicine al nostro amico e compagno Stecco.

Quello che lo Stato ha messo in campo per arrestarlo è piuttosto impressionante. Se teniamo presente che Stecco, quando ha levato le tende, aveva un definitivo da scontare di 3 anni e 6 mesi, la sproporzione tra la sua condanna e l'accanimento sbirresco per scovarlo rivela quanto lo Stato consideri insopportabile che ci si possa sottrarre alle sue galere; e quanto il trattamento riservato ad anarchiche e anarchici abbia, sia pure dentro un avvitamento repressivo generale, un carattere indubbiamente selettivo.

Una conoscenza aggiornata delle tecniche impiegate dalla polizia politica contro compagne e compagni passa molto spesso attraverso la lettura dei faldoni delle indagini poliziesco-giudiziarie. Per questo è importante che le indicazioni che ne emergono siano socializzate.

Nel farlo è sempre necessario tener presenti due aspetti: il primo, è che si tratta di materiale fornito dal nemico; il secondo, è che la condivisione (ovviamente selezionata e omettendo nomi e cognomi che appaiono nelle carte) di tale materiale può involontariamente ingenerare il sentimento di una sorta di onnipotenza del nemico, con il relativo corredo di paranoia e di scarsa fiducia nei propri mezzi. È quindi bene ricordare che il dispiegamento di uomini e mezzi per la ricerca di latitanti non è lo stesso che si riserva al monitoraggio/indagine su altre circostanze che si danno nell'ambito dei movimenti e delle lotte; che nonostante l'avanzamento poliziesco-tecnologico, alcuni compagni ricercati hanno assaporato la libertà per mesi e anni; che ci sono compagne e compagni tutt'ora uccel di bosco in Europa e nel mondo.

Sapere come si muove la controparte è necessario per adottare le contromisure più opportune, imparando dagli errori e facendo tesoro delle esperienze.

Partiamo da alcuni dati quantitativi per fornire un'idea dell'estensione dell'intervento poliziesco:

- Telecamere davanti a 6 abitazioni.
- Intercettazioni ambientali nella casa di una persona vicina a Stecco, di altre persone connesse ad una persona particolarmente "attenzionata" e dello spazio anarchico "El Tavan".
- Intercettazioni telefoniche di oltre 40 persone: compagne e compagni, ma anche amici e persone vicine.
- Sono state disposte intercettazioni ambientali "puntuali" in un caso in cui si riteneva che una persona vicina a Stecco potesse incontrare una persona che secondo la Digos avrebbe potuto fornirle delle informazioni su di lui.
- Una persona particolarmente "attenzionata" viene pedinata almeno una volta dai servizi (l'intestazione della relazione di servizio è "Ministero degli interni", mentre tutte le altre sono di varie Questure).
- Analisi dei tabulati telefonici storici di 69 persone e di una cabina telefonica (il tempo massimo per cui si può tornare indietro sono 72 mesi).
- Gps installati in 12 auto. Per alcune persone vicine a Stecco anche l'intercettazione ambientale e video.

- “Attenzionate” le targhe di 311 auto.
- Richiesta di esibizione bancaria di 59 persone per verificare l'esistenza di movimenti “sospetti” riconducibili ad eventuali appoggi economici alla latitanza.
- Installazione di un dispositivo di tracciamento (nello specifico un localizzatore GSM, dunque non satellitare ma cellulare, di tipo “Spora”, ovvero un localizzatore miniaturizzato che comunica in tempo reale ad un telefono in utilizzo alla polizia la cella agganciata via sms) su una bicicletta ritenuta in uso da Stecco, localizzata tramite l'utilizzo di una telecamera in un paese nel quale è stato ripreso durante il periodo di latitanza.
- In questo caso come nel caso della latitanza di un altro compagno, sono stati ritrovati dei documenti falsificati le cui generalità sono risultate appartenenti a persone realmente esistenti. Da questo è stato dato inizio ad una serie di ricerche e interrogatori alle persone interessate, con l'intento di confrontare spostamenti, pernottamenti in alberghi, controllo dei movimenti di alcuni conti correnti (ed anche, per esempio, la “carta Decathlon” almeno in un caso, sulla quale rimane una cronologia degli acquisti effettuati) indietro nel tempo di diversi anni (più di 10).
- Mobilitata la polizia politica di Treviso, Padova, Verona, Brescia, Bergamo, Milano, Trento, Trieste, Genova. A partire dal momento in cui hanno iniziato a “stringere il cerchio”, la Digos di Trento ha ricevuto personale di rinforzo in pianta stabile, di sicuro almeno un agente da Trieste.

Per un'analisi più qualitativa, invece, bisogna entrare nel merito delle tecniche impiegate. Diciamo che le indagini si muovono su due binari: l'analisi di un'enorme mole di dati telefonici e il controllo quasi costante di alcune persone, con particolare attenzione alle loro assenze dai rispettivi luoghi di residenza. Quando tali persone vengono di nuovo localizzate, si procede a ricostruire il più possibile a ritroso i loro spostamenti. La raccolta dei dati viene fatta con calma e in modo sistematico. Ecco alcuni esempi.

- Due compagni in viaggio in treno vengono pedinati da quattro agenti della Digos, che si posizionano due in testa e due in coda al treno. In ognuna delle stazioni intermedie sono poi presenti due poliziotti in borghese nel caso in cui i compagni scendano dal treno; a tal fine è stata mobilitata polizia politica di sette Province. Dalle carte sembra che questo pedinamento sia stato disposto all'ultimo momento quando, la sera precedente, la polizia ha appreso in diretta dai microfoni installati in casa delle persone vicina ad una delle due persone, che questa sarebbe partita in treno il giorno dopo.
- Dalle carte emerge che gli sbirri, oltre a chiedere a RFI di visionare le telecamere delle stazioni, hanno chiesto al gip di installare delle telecamere apposta in stazione a Rovereto per poterle visionare direttamente in Questura. Hanno anche potuto vedere quali biglietti sono stati emessi con ognuna delle biglietterie automatiche, quali ricerche siano state effettuate anche senza acquistare i biglietti e accedere alla telecamera che in alcuni casi sono installate direttamente sulle macchinette. Queste ultime telecamere conservano i video per massimo 10 giorni (nonostante la durata massima generale per *infrastrutture meritevoli di maggior tutela* sia di 7 giorni secondo il provvedimento del 2010 a firma del GDP, salvo specifiche richieste).
- Avendo osservato che una persona particolarmente “attenzionata” aveva cercato gli orari dei treni per una determinata città con una biglietteria automatica, nel momento in cui questa persona si è assentata da casa sono state visionate le telecamere della stazione di quella città e di almeno altre quattro stazioni. È probabile che siano stati analizzati i dati relativi a più stazioni,

che si trovano lungo tratte che portano alla città per la quale era stata effettuata la ricerca. Infatti, dato che dopo 7 giorni i dati vengono cancellati, la Digos di Trento si è recata in fretta e furia negli uffici di RFI Lombardia a Milano perché ritenevano di aver individuato la persona in una stazione (che non era né quella ricercata sulla macchinetta, né quelle vicine alla sua abitazione) in cui era passata 7 giorni prima e c'era il rischio che le immagini venissero sovrascritte prima che il download dei dati terminasse.

- Nel tentativo di ricostruire il percorso della persona, visionano i dati di un esercizio commerciale esterno alla stazione in cui ritengono di averla localizzata, oltre che le telecamere del treno su cui ritengono sia salita in quella stazione. Dato che, tramite queste ultime, durante il viaggio la vedono leggere l'ultimo numero di una rivista di compagni, uscito da poco, chiedono l'esibizione bancaria anche per questa rivista.

- Per ricostruire a ritroso il percorso che l'ha portata a quella stazione, si concentrano inizialmente sugli Intercity, dato che c'è l'obbligo di biglietto nominativo. Avendo individuato dall'elenco fornito da FSI un acronimo che ritengono sia riconducibile a quella persona, verificano dove sia stato emesso il biglietto relativo. Non avendo più a disposizione i video della stazione di acquisto a causa del decorso della durata di conservazione delle immagini, cercano di ricostruire in che modo la persona sia arrivata nella stazione di acquisto del biglietto.

Scartati gli Intercity, non avendo trovato nessun nominativo riconducibile, si concentrano sui treni regionali e chiedono a FSI di comunicare per ognuno il numero di biglietti emessi dalle biglietterie automatiche delle stazioni di partenza, di quelle intermedie e di altre nelle vicinanze, in località “abitualmente frequentate” da anarchici: 150 pagine di liste trasmesse dalle Ferrovie. Controllano anche i traghetti e gli autobus. Dato che non trovano nulla, chiedono gli stessi dati di prima sulle biglietterie di 69 ulteriori stazioni e di eventuali multe emesse a bordo treno di 5 regionali. Parallelamente, chiedono alle Ferrovie l'elenco di tutti i biglietti acquistati con quell'acronimo nei mesi precedenti e di attivare un “alert di segnalazione automatica” nel caso in cui dovesse essere utilizzato nuovamente per acquistare dei biglietti.

- Per ricostruire gli spostamenti di certe auto, vengono visionate le telecamere di vari caselli autostradali; una volta localizzata una macchina in un casello ritenuto sospetto, controllano anche le telecamere stradali del Comune.

- Una volta individuata la zona in cui ritengono possa trovarsi Stecco, la Digos chiede di installare 5 telecamere “video lunga distanza” con riconoscimento facciale e 10 per “ripresa video interno/esterno” intorno a una data stazione, comprese fermate urbane e extraurbane degli autobus. Non vi è traccia della richiesta del PM al giudice, quindi non sappiamo se poi siano state installate o meno. Analizzano anche le immagini delle telecamere presenti sugli autobus. Chiedono di intercettare una persona e sua madre, nonché di avere accesso ai loro tabulati, perché in passato avrebbero affittato in zona delle abitazioni a dei compagni.

- Una volta arrestato Stecco, mostrano la sua foto e interrogano varia gente del posto fino a quando non individuano la casa in cui avrebbe soggiornato. Prelevano impronte digitali e DNA da tutto quello che sequestrano nella casa.

- Per quel che riguarda la ricerca tramite i telefoni, è da segnalare che non vengono intercettati solo i numeri di telefono, ma anche i dispositivi in cui alcune SIM sono state inserite, tramite numero IMEI. Questo non avviene per tutti i numeri, ma solo per quelli ritenuti più “interessanti” e sembra che sia sufficiente che la SIM venga inserita una sola volta (ed

utilizzata). Inoltre, come già sappiamo, l'intercettazione comporta anche la geolocalizzazione del telefono, anche non smartphone (sebbene in questo caso si possa risalire solo alle celle via via agganciate e non alla posizione esatta).

- Sotto il profilo dell'analisi del traffico telefonico, una volta stretto il cerchio su una determinata zona, cercano nei tabulati già acquisiti eventuali numeri di telefono di anarchici lì residenti (cioè se una delle 69 persone di cui hanno i tabulati abbia chiamato qualcuno che stava lì nei 6 anni precedenti), quindi tutte le chiamate fatte da Stecco nei 5 anni precedenti (prima che levasse le tende) a numeri che si trovavano in quella zona.

- Cercano nei tabulati storici se ci sono delle chiamate ricevute da delle cabine telefoniche. Quindi cercano se dalla cabina di cui hanno i tabulati storici siano state fatte chiamate a numeri stranieri; una volta individuati, vedono se questi numeri abbiano mai chiamato i numeri emersi dai tabulati storici. Verificano inoltre se dalla cabina siano stati chiamati fissi o cellulari in quattro regioni italiane.

- Analizzano i dati del traffico telefonico transitato per le celle di Tim, Wind, Vodafone e Iliad di nove località in alcuni momenti in cui reputano che vi possano essere stati contatti con un ipotetico telefono utilizzato da Stecco. Dato che la mole è enorme, provano a incrociarli con i numeri intercettati e poi con tutti numeri risultanti dalle utenze di cui hanno le tabulazioni. Questo tipo di ricerca (incrocio dati estrapolati da determinate celle telefoniche con numeri di telefono individuati tramite l'analisi di tabulati storici) viene ripetuto altre volte. In generale, in più punti troviamo l'analisi di tabulati storici, anche molto indietro nel tempo, e i tentativi di incrociare i numeri così estratti con i dati che man mano vengono raccolti nel corso dell'indagine.

- Sebbene non ve ne sia poi traccia nelle intercettazioni, in più punti la Digos chiede l'autorizzazione per scaricare le chat di Whatsapp e in un caso anche di Telegram.

- Per quel che riguarda le ricerche telematiche, è da segnalare il tentativo di installare uno spyware (un virus informatico che permette di ottenere completo accesso al dispositivo “infettato”) “mediante la procedura 1 click” che permette di rendere lo smartphone di una persona vicina a Stecco un microfono per intercettazione ambientale (definizione tecnica: “autorizzare l'intercettazione telematica attiva con eventuale intercettazione tra presenti attraverso l'attivazione di un microfono sul terminale mobile di tipo Android senza root”). Nella pratica, a questa persona viene mandato un sms che contiene un link, che se cliccato avrebbe portato all'installazione del virus. Dato che la persona non clicca sul link, avendo individuato il codice pin del suo telefono mediante una telecamera ad alta risoluzione installata all'interno dell'auto (la quale ha permesso di risalire alla lettura del codice mentre questo veniva digitato sul telefono), la Digos viene autorizzata ad installare direttamente il virus una volta ottenuto il temporaneo possesso del telefono. Questo non sembra sia avvenuto perché nel frattempo le indagini si sono orientate in un'altra direzione.

- Per quel che riguarda le email, sembra che solo libero.it abbia fornito i dati relativi agli indirizzi email (file di Log compresi), mentre altri provider sembra non abbiano nemmeno risposto alle richieste (o quantomeno non c'è nessuna menzione al riguardo).

- Oltre alle email, cercano di ottenere anche tutti i dati relativi a servizi di Microsoft Account e Google, compresi gli acquisti effettuati tramite queste piattaforme.

A quest'ultimo proposito è interessante segnalare l'analisi che viene fatta dell'ID GAIA (*Google Account and Id Administration*) per il quale un numero ritenuto in possesso di Stecco riceve un sms. Praticamente, quando si cerca di entrare in una casella di posta elettronica Gmail da un dispositivo diverso da quello utilizzato normalmente, Google chiede una verifica ulteriore alla password, inviando un sms con un codice numerico ad un numero collegato all'indirizzo email. Dato che un numero collegato a Stecco riceve questo codice, cercano di recuperare i dati relativi al relativo account Google. Per farlo hanno inserito il numero di telefono nella pagina di accesso a Gmail e nella pagina in cui si chiede la password hanno cliccato col tasto destro e selezionato "Visualizza sorgente pagina". Si è quindi aperta una finestra che contiene il codice HTML, hanno digitato CTRL+F (cerca) e nella casella di ricerca dato il comando per ottenere le 21 cifre che costituiscono l'ID GAIA, cioè ,[\"] . Per sapere a chi fosse associato questo ID, hanno usato uno dei servizi di Google, nello specifico Google maps (dalla descrizione sembra che possano usare qualsiasi servizio offerto da Google, ma probabilmente Google Maps è quello in cui è più comune che vengano lasciate delle recensioni o comunque dei contributi).

In pratica, nella barra degli indirizzi hanno digitato [https://google.com/maps/contrib/ID GAIA](https://google.com/maps/contrib/ID%20GAIA), per visualizzare tutte le recensioni lasciate tramite quell'account Google e individuare quindi gli indirizzi email collegati. Hanno quindi chiesto a Google tutti i dati di registrazione relativi alle email, i numeri di telefono, la data in cui sono stati associati agli indirizzi email e le anagrafiche relativi all'ID GAIA e tutti i file di Log di ogni connessione a tale account. Non sembra abbiano ricevuto risposta.

Per provare a fare una sintesi comprensibile, ad ogni ID GAIA possono essere associati più indirizzi email e più numeri di telefono di riferimento, una volta che la polizia conosce uno di questi dati può provare a risalire agli altri.

- In seguito ad un'intercettazione ambientale in cui viene nominato un indirizzo email, chiedono a Microsoft l'anagrafica, i dati fatturazione dell'account nel caso in cui siano stati effettuati acquisti su Microsoft Online Store, i Log delle connessioni IP, tutti gli indirizzi email e i numeri di telefono associati a tale indirizzo e tutti i soggetti che si sono registrati con un nome collegato a quell'email. Inoltre chiedono al provider subito.it il tabulato dei file di Log e degli indirizzi IP utilizzati da questa email.

- In un altro fascicolo, legato alla ricerca di un altro compagno latitante, abbiamo trovato questo passaggio relativo all'intercettazione telematica attiva e passiva di un computer: "Come noto, alla luce delle attuali tecnologie risulta assai difficoltoso effettuare un'infezione di un pc, in quanto sono numerose le variabili che determinano la riuscita o meno del servizio (sistema operativo, antivirus, scheda di rete, etc.). Pertanto, come da prassi, è indispensabile effettuare in un primo momento uno studio di fattibilità per stabilire il tipo di sistema operativo usato e gli eventuali antivirus attivi attraverso un'intercettazione passiva, per poi procedere all'intercettazione telematica attiva. Le modalità per procedere all'inoculamento dello spyware verranno successivamente concordate con i tecnici della ditta incaricata dell'inoculazione del virus. Da attività di osservazione, si è notato che [...] lascia talvolta il computer nel bagagliaio della propria autovettura [...] quando si reca al lavoro in [...]. Previa autorizzazione di codesta A.g., il tecnico provvederebbe ad installare un file a computer spento (ciò è fattibile solo lasciando inserita una chiavetta USB o qualunque altro supporto fisico di memoria nel pc), file che all'avvio verrà eseguito dal computer in automatico e provvederà ad installare altri piccoli

programmi malevoli, necessari per svolgere lo studio dell'ambiente software presente sul dispositivo, per poi ottimizzare lo spyware che permetterà l'intercettazione telematica richiesta”.

- Dopo aver sequestrato una chiavetta Tails, cercano la password con il programma “bruteforce-luks”. Nella comunicazione puntualizzano che non è possibile stimare i tempi di questa operazione.

Significativamente, la sola delle 11 cartelle che formano l'indagine “Diana” a risultare vuota è quella con la dicitura: “Spese”. Ci sono comunque alcuni preventivi per il noleggio dei dispositivi per le intercettazioni, da cui tra l'altro emerge che quelli di localizzazione spesso offrono anche “l'opzione intercettazione”, quindi si tratta di un unico oggetto polivalente. Inoltre sembra che dal Covid siano possibili anche delle postazioni di ascolto da casa per il telelavoro.

L'apertura di un fascicolo presso il Ministero degli Interni e alcune annotazioni che ne riportano l'intestazione suggeriscono il coinvolgimento dei servizi segreti.

Ultimo ma non meno importante: contemporaneamente alle indagini per la ricerca di Stecco era attiva almeno un'altra indagine per 270 bis in cui parte degli indagati sono gli stessi del 270 bis relativo a Stecco. Giusto per dare un'idea della pervasività e della quotidianità del controllo a cui alcuni compagni sono sottoposti.

Utile sapere che gli sbirri possono impiegare anche settimane a visionare le telecamere di stazioni, treni, caselli autostradali, autobus, alla ricerca di immagini che suggeriscano percorsi e destinazioni. Provando a farlo anche andando a ritroso rispetto a un viaggio che viene ritenuto sospetto, ricostruendo buona parte di un percorso a partire da quando questo termina, cercando le coincidenze tra momenti di “sparizione”, giorni, orari, mezzi utilizzati.

Ognuno/a farà le sue valutazioni.

Che si dia ancora più incisività alla critica pratica nei confronti del mondo della video sorveglianza e del controllo digitale, come campo di intervento irrinunciabile perché siano ancora possibili sogni e progetti di sovversione e di libertà.

Che la fortuna arrida a chi è uccel di bosco e a chi, nella lotta per la libertà, sfida ogni identificazione.