Atti della Lawful Interception Academy edizione 2017

La Lawful Interception Academy ha raggiunto lo straordinario risultato delle oltre **1.000 persone formate**, durante le prime tre edizioni, sui temi multidisciplinari afferenti alle intercettazioni delle comunicazioni. L'edizione 2017 della LIA si è svolta dall' 8 al 10 novembre ed è stata ospitata dalla Direzione Centrale Anticrimine (DAC) della Polizia di Stato a Roma.

di Giuseppe Corasaniti

LE INTERCETTAZIONI ED IL FUTURO DELLE INVESTIGAZIONI DIGITALI

Dott. Giuseppe CORASANITI è Sostituto Procuratore Generale della Procura generale della Repubblica presso la Corte Suprema di Cassazione.

Per interrogarci sulla dimensione, più o meno invasiva, dello strumento investigativo delle intercettazioni occorre forse una riflessione preliminare di carattere molto generale, ma che è rafforzata da alcune perplessità circa l'attualità stessa, forse, oggi dello strumento intercettativo tradizionale, il senso di una captazione di contenuti (sonori) comunicativi nell'ambito di una indagine penale, tenendo conto dei mille modi di celare o di codificare un contenuto e delle mille sfumature di evoluzione che la tecnologia informatica ci offre, ogni giorno di più, per nascondere o svelare nuovi contenuti e diffonderli ovunque.

Sappiamo bene che si contesta al nostro paese di farne un uso estremamente rilevante. Io credo invece che sia un uso estremamente proporzionato al carattere che ha nel nostro paese il crimine organizzato, e che corrisponde anche a dato statistico, che nessuno poi cita in concreto poi quando si interviene in questa polemica, e cioè che nel nostro paese vi è un fortissimo uso di apparati telefonici mobili[1].

Vi è sempre stato un consumo di tecnologie di comunicazione individuale, paradossalmente mentre c'è una certa arretratezza in materia di uso di tecnologie informatiche almeno a livello collettivo e sociale. Le scelte sociali di tipo criminale sono anche un riflesso, se si vuole, proprio di tale anomalia.

C'è una certa arretratezza nell'uso di Internet, mentre vi è una grande diffusione, certamente anomala rispetto alle statistiche che riguardano gli altri paesi europei, degli strumenti (personali) di telefonia cellulare, che in questi anni poi sappiamo bene sono diventati dei computer: lo *smartphone* ha, a tutti gli effetti, la stessa memoria, le stesse funzioni operative e applicative del *computer*. Sicché una intercettazione di uno smartphone confina, anche tecnicamente, con una procedura di intervento su un computer. Il *trojan* non è un altro che un programma informatico, è un virus che, inserito all'insaputa del destinatario, esattamente come un cavallo di troia, si installa e trasmette dati significativi in termini di informazione agli inquirenti.

1 In Italia gli abbonamenti alle compagnie di telefonia mobile sono più numerosi dei cittadini: ce ne sono 108,4 per ogni 100 abitanti. È quanto emerge dai rapporti di Eurostat sulle telecomunicazioni nell'Unione europea, dal quale viene fuori inoltre che le connessioni a internet nella penisola, sia normali che a banda larga, in percentuale restano di molto inferiori alla media europea.

Qui vi è il primo profilo di attenzione perché è uno strumento oggi alla portata di qualunque tasca, di qualunque intenzione criminale. Quindi si può percepire perché sul piano della intercettazione legale ormai anche il trojan deve considerarsi uno strumento investigativo essenziale e ormai tipizzato[2].

Eppure non abbiamo mai abbastanza considerato il *trojan* all'inverso. Cioè non abbiamo mai considerato appieno forse il fattore di rischio di essere intercettati in ambito istituzionale, tanto più in un contesto nel quale la sicurezza informatica è un problema quotidiano. Chi si occupa dei reati informatici sa bene che vi è sempre il rischio che le posizioni di acquisizione informativa si invertano da un momento all'altro. Il trojan è regolamentato e sarà regolamentato così in dettaglio da un lato, ma chi ce lo dice che non sia oggi già utilizzato in modo assai discreto proficuo dall'altro?

Perciò va considerata prioritaria a livello istituzionale, in tutte le sedi istituzionali, compresa la magistratura, anzi primo luogo la magistratura, una seria ed avanzata politica di sicurezza tecnologica, che passa anche e soprattutto dall'uso "personale" del computer, dall'utilizzazione dalla registrazione sul computer di dati processuali e che richiederebbe una consapevolezza, a partire dalla magistratura, di questa serie di cautele che io francamente vedo però ancora, purtroppo, scarsamente diffusa.

E credo che l'aspetto fondamentale su cui mi vorrei oggi soffermare è che il momento della comunicazione è un momento sempre più essenziale nella sua ricostruzione, in dettaglio, e nella sua conseguente proiezione dibattimentale.

Perché poi tutto quello che noi facciamo livello di accertamento di criminalità informatica, rischia di non servire a nulla se non sappiamo ben prospettare, innanzitutto al magistrato e anche soprattutto al magistrato inquirente. Perché il primo rapporto quello fra polizia giudiziaria e magistrato che riceve la notizia di reato grezza e che ha il compito di costruirci su una imputazione, ecco proprio questo mi conferma l'importanza di questa relazione istituzionale strettissima e propulsiva tra polizia giudiziaria e magistrato inquirente; nella fissazione di priorità, nella determinazione degli indirizzi di indagine, nella determinazione di quelle che sono le fondamentali scelte investigative iniziali che sono enucleabili dallo stato delle tracce sullo scenario digitale.

Credo di poter affermare come che sin dall'inizio un'indagine qualifica la sua finalità e il suo destino. Se l'indagine viene svolta bene soprattutto quella in ambienti informatici addirittura nei primissimi minuti, questa indagine avrà ottima possibilità di riuscita. Se invece nel momento iniziale il Pubblico Ministero non attribuisce particolare rilevanza al materiale raccolto dalla polizia giudiziaria o addirittura adombra problematiche che non sono poi strettamente giuridiche e magari astratte ma sono organizzative, evidentemente l'indagine comincia su un terreno accidentato e rischia di chiudersi su un terreno ancor più accidentato.

Perché la nostra capacità di ricostruzione di un contesto relazionale, perché questo è in sostanza poi l'intercettazione. L'intercettazione telefonica serve, nel nostro sistema giudiziario, per ricostruire e rendere trasparente una relazione organizzativa. Sarà tanto più efficace quanto saremo in grado di prevedere tutte le ramificazioni organizzative, che sono oggetto del nostro investigare, e tutti i ruoli svolti nell'articolazione delle comunicazioni che andiamo ad acquisire.

Il nostro sistema è ben diverso da quello statunitense, laddove vi è un larghissimo uso di intercettazioni telefoniche, molto più vasto di quanto non appaia, ma caratterizzato dal fatto che l'intercettazione telefonica nel sistema americano non ha alcuna rilevanza probatoria processuale; e dove uno dei principi fondamentali della Costituzione degli Stati Uniti è appunto quel quarto emendamento che prevede che "*Non potrà essere violato il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, di fronte a perquisizioni e sequestri ingiustificati; e non si rilasceranno mandati di perquisizione se non su fondati motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare*" . Si tratta di una logica garantista che richiede attenzione e soprattutto uno sforzo sistematico di prospettazione positiva, per esporre quello che è un percorso argomentativo in itinere, essenziale, che sottende alla ricerca di una prova in un ambito privato.

Il nostro legislatore, senza avere un gran senso della comparazione tra ordinamenti diversi, sembra avere sempre la tentazione di riportare pari pari nella disciplina (italiana) delle intercettazioni telefoniche un presupposto (quello della garanzia funzionale) che negli Stati Uniti è nato per impedire abusi della polizia. Per cui addirittura prima di procedere a perquisizione personale o locale, la polizia giudiziaria deve avere il fondato sospetto che in quel luogo per determinati motivi articolati, si stia commettendo un crimine. Questo è più difficoltoso in un contesto relazionale complesso.

Laddove l'intercettazione o meglio la sua trascrizione, è diventata in questi anni nel nostro paese, soprattutto nei procedimenti di criminalità organizzata, un elemento probatorio direttamente rilevante in quanto tale, che determina la ricostruzione logica di una relazione personale, della articolazione dell' organizzazione criminale sul territorio, e quindi le ripartizioni dei ruoli, ma che ci vede ogni giorno di più in un ambito problematico per quanto riguarda l'interpretazione di questi contenuti.

Pensiamo solamente a un aspetto organizzativo da molti sottovalutato che è quello però di primo livello; cioè del soggetto che ascolta le conversazioni e le trascrive. Ambito che preoccupa molto perché lo stesso schema di decreto sulle intercettazioni in itinere, che si occupa anche delle intercettazioni ordinarie e soprattutto delle intercettazioni ordinarie, prevedrebbe un ruolo nuovo della polizia giudiziaria, addirittura "interpretativo" in ordine alla essenzialità dei contenuti. Francamente ritengo ultroneo e addirittura irreale se non surreale questo nuovo ruolo perché fra qualche anno probabilmente non avremo più un agente "umano" che ascolterà le conversazioni, ma avremo invece un sistema informatico che, opportunamente centrato sulla voce (sui toni di voce sonori) da intercettare, sarà in grado di trascriverle fedelmente da solo e, in caso di dubbio persino di segnalarlo all'operatore. Qualcosa del genere esiste già nei programmi informatici di dettatura, che nei prossimi anni saranno resi ancora più sofisticati in base alle strategie di intelligenza artificiale, peraltro personalizzabili a livello utente.

Come sempre si guarda al passato anziché al futuro, e di questo strabismo istituzionale ne approfitterà solo la criminalità, che ha invece tutto il tempo e le risorse per evolvere rispetto alle forze istituzionali, frenate anche da un ambiente normativo miope quanto ossessivamente mirato al settore pubblico (e significativamente inerte rispetto alle molteplici violazioni alla riservatezza congegnate ed operate nel settore privato) .

2 Sia consentito il rinvio a Corasaniti G. *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, Nota a ord. Cass. sez. VI pen. 6 aprile 2016, n. 13884 in Il Diritto dell'informazione e dell'informatica, 2016, fasc. 1, pp. 88-103.

Quindi il futuro sarà questo probabilmente. Ma dobbiamo occuparci del presente. Il personale della polizia giudiziaria, quello specificamente destinato a l'operazione di ascolto, dovrà essere all'altezza professionale e capace di leggere le sfumature dei contenuti vocali. Soprattutto per quanto riguarda la capacità di ricostruire le sfumature, i toni, le espressioni sintomatiche ; non dico il tema dei linguaggi, dei dialetti e delle lingue straniere. Oggi le Procure della Repubblica hanno particolari difficoltà in un ambiente di crimine globalizzato qual è il nostro, ma sarebbe opportuno porsi forse il problema in largo anticipo.
Perché chi ascolta la conversazione, è il primo soggetto che apprende l'anomalia o la ricorrenza. Le indagini tecnologiche sono basate appunto su questi due termini scientifici: *anomalia* o *ricorrenza*.

Il tema di prova scientifica e il rapporto fra diritto e scienza non è mai stato felicissimo. Perché il diritto ritiene la scienza un sapere diverso e ritiene, a suo modo, ma da sempre, di dovere interpretare le linee scientifiche a seconda delle opzioni giuridiche e quindi delle norme esistenti, e non può fare altrimenti. Questo tema nasce proprio negli Stati Uniti dove, con due decisioni fondamentali in materia di prova scientifica, la prima il caso "Frye" del 1923, in cui un imputato chiese alla corte di sottoporsi alla macchina della verità. Per la prima volta, si poneva in dubbio tutto il sistema degli interrogatori verbali e dei contenuti raccolti in testo, che avevano anche negli Stati Uniti, e si poneva il problema processuale di acquisire un metodo scientifico assolutamente nuovo che sin da allora era utilizzato. Nel caso Frye, la Corte Suprema americana stabilì che l'uso di una verità scientifica non dovesse accedere nel processo penale se non nel caso in cui, quella verità scientifica, fosse pienamente consolidata e quindi a un tale livello di assestamento da rappresentare in sé stessa una verità "oggettivamente" rilevante, quindi acquisibile quale contenuto attraverso la testimonianza, perché poi da qui tutto passa, processuale di un esperto.
Quindi si utilizza una tecnica di estrema cautela: tecnica che fu mantenuta a quasi 70 anni di distanza in un secondo caso (caso Daubert) del 1993 laddove veniva in gioco invece un problema di malattia professionale. Veniva in gioco l'acquisizione di una base statistica quale elemento per poter fondare un giudizio di responsabilità. Anche in questo caso, era sensibilmente diverso, si immaginò che una mera enunciazione statistica non fosse comunque sufficiente per potere, nella ricorrenza evidentemente di alcuni aspetti sintomatici, in sé indicare una responsabilità.
"*Gli esperti dovranno essere chiamati non solo ad esprimere il loro personale, seppur qualificato, giudizio, ma anche a delineare lo scenario degli studi e a fornire gli elementi che consentano al giudice di comprendere se, ponderate le diverse rappresentazioni scientifiche del problema, possa pervenirsi ad una "metateoria" in grado di fondare affidabilmente la ricostruzione. Di tale complessa indagine il giudice è infine chiamato a dar conto in motivazione, esplicitando le informazioni scientifiche disponibile e fornendo razionale spiegazione, in modo completo e comprensibile a tutti, dell'apprezzamento compiuto*", così poi si esprime la Corte di cassazione con la sentenza 43789/2010 che affronta, per la prima volta in modo organico, il problema dei criteri di validazione della prova scientifica.

Nel nostro paese, uno strumento che non è nato per essere in sè uno strumento di prova si è trasformato in prova principale, spesso unica di una relazione criminosa. Perché la prova viene raccolta, in un sistema processuale dialettico e ispirato al metodo americano, in dibattimento. Sicché viene ad essere oggetto di un esame come dire, concentrico, della pubblica accusa ma anche della difesa che deve avere accesso al materiale nella sua integrità e deve poter prospettare, non una critica soggettivamente generica all'attività degli inquirenti, ma una critica fondata oggettivamente su degli elementi che danno dello stesso fatto una lettura alternativa.
Nelle indagini più complesse, a maggior ragione quelle di criminalità organizzata e quelle legate al crimine informatico, l'elemento più difficile, più delicato è sempre quello di riuscire a documentare efficacemente la contestualizzazione. A volte per poterlo dimostrare efficacemente è necessario avere un ambiente, io uso un termine informatico ma vorrei tradurlo a livello processuale, *multitasking* ovverosia dovrei sempre essere in grado, attraverso più rappresentazioni di contenuti, di documentare la contestualità e una coerenza indiziaria che, dal punto di vista della logica investigativa, appare compiuta. Un primo problema è, quindi, in un certo senso il futuro stesso delle intercettazioni vocali "tradizionali", perché di questo che si tratta. **Un rinnovamento completo del sistema di realizzazione delle intercettazioni che oggi è basato sulla tecnologia di mera trascrizione del testo intercettato, ma deve essere sempre più basato sistematicamente su un sistema di *marcatori logici* e di *indicizzatori*.** Espressioni testuali e più in generale contenuti captati dovrebbero cioè essere letti e riletti da una pluralità di punti di vista possibile, analizzandone la fonte,il contesto i riferimenti espliciti o impliciti, descrivendone sempre in dettaglio l'ambito di qualificazione così come la presumibile attendibilità sul piano della coerenza logica riferibile ad una azione collettiva in corso e puntualizzandone sempre i riferimenti oggettivi ad altri contenuti disponibili. Si tratta di uno scenario sempre più di tipo ipertestuale e sempre meno di carattere descrittivo o formale[3].
Sto utilizzando termini informatici, ma certo ogni termine utilizzato in un contenuto può avere un significato e può avere soprattutto un significato "comprensibile" o futuro in relazione allo sviluppo imprevedibile delle indagini, può avere un significato futuro in relazione alle improvvise dichiarazione di un pentito che a distanza di tempo offre di quel fatto una lettura completamente diversa. Ed allora il problema è quello della ricostruzione del fatto a distanza di tempo, della puntualità dei riscontri informativi disponibili e conseguentemente della disponibilità di riferimenti esterni che vengono direttamente o indirettamente ad essere indicati, e che necessitano di una conferma o di una smentita.

Ed ecco perché mi vedono assolutamente perplesso gli interventi improvvisati sul tema della conservazione temporale limitata dei dati personali, quando si riferiscono a elementi investigativi utilizzati nelle indagini penali, specie con riferimento a crimini di oggettiva gravità. Non si può pretendere di adottare una tematica strettamente civilistica, e giustamente pensata in ambito civilistico come quella della conservazione e della garanzia dei dati individuali, quale elemento dirimente per incidere sul senso stesso delle indagini penali, che si proiettano nel tempo e che hanno tempi di svolgimento imprevedibili, tanto più in un paese come il nostro caratterizzato dalla forte presenza di organizzazioni criminali sul territorio.

3 Mital Vijay, Elliman Anthony D., Document Assembly and Evidence Analysis: Two Approaches to Hypertext (Composizione del documento e analisi delle prove: due approcci all'ipertesto) in Informatica e diritto, 1994, fasc. 2, pp. 149-175] 1994 ; Nanard Marc, Nanard Jocelyne, Hypertext as a tool for information gardening for legal applications (Ipertesto come strumento per l'informazione relativa alle applicazioni giuridiche) in Informatica e diritto, 1994, fasc. 2, pp. 47-77.

Sul piano giuridico, peraltro, in Europa non si sovrappone il tema dei dati giudiziari in ambito processuale penale (che entra in gioco solo con riferimento alla non emarginazione o discriminazione, che è il contenuto" essenziale" della *privacy* quando dei dati ne viene fatto abuso e diffusione esterna) e quello della riservatezza in rapporto ad un accertamento penale basato sulla raccolta (indispensabile) di dati anche personali e anche inevitabilmente sensibilissimi[4].

La regolamentazione comunitaria sulla conservazione sul trattamento dei dati giudiziari attua uno schema di conservazione e di garanzia che può apparire omologo, ma che deve porsi il problema della conservazione dei dati "esterni" delle conversazioni in rapporto ad una disciplina generale che prevede termini temporali fin troppo ristretti. E' facile prevedere che nei prossimi anni la dialettica fra forze dell'ordine, anche a livello europeo, autorità (giudiziarie) inquirenti e garante della *privacy*, si baserà esattamente su questo. Quando distruggere il dato, quando utilizzare quel dato perché funzionale a un'indagine non ad un'altra. Ma un approccio burocratico al tema, soprattutto un approccio insensibile alle tematiche della sicurezza collettiva, specie in tempi come questi e di fronte al terrorismo internazionale più imprevedibile, è non solo illogico sul piano giuridico ma in concreto devastante sul piano investigativo.
Esso si basa sulla accettazione passiva di un presupposto di primazia della *privacy* (che attiene all'individuo che va rispettato in quanto tale e in quanto capace di relazionarsi socialmente e di organizzarsi in modo altrettanto libero) rispetto alle essenziali metodologie di accertamento comportamentale e relazionale specie in occasione di delitti associativi e gravi.

La privacy è fenomeno che riguarda prima di tutto le imprese, i soggetti privati, ed è disciplinata nel settore pubblico non per uniformare ed appiattire burocraticamente, ma per prevenire abusi basati sulla diffusione incontrollata di informazioni personali estratte e conseguentemente trattate da soggetti pubblici.
Senza una piena attenzione a questa differenza funzionale la regolamentazione della *privacy* diviene una disciplina uniformante e omologativa che non tiene conto di quello che è la dimensione essenziale di una attività istituzionale, quella di polizia che si basa proprio sulla prevenzione, e che proprio nella Convenzione europea dei diritti umani e nella dichiarazione dei diritti umani vede la sua dimensione istituzionale rilevare proprio per proteggere i diritti fondamentali di tutti, in primo luogo quello alla vita ed alla sicurezza civica.[5]
Bisogna considerare sempre primarie, quindi, le esigenze investigative, specie in un paese come il nostro che è caratterizzato fortemente da incisioni sempre più marcate della criminalità organizzata e da un terrorismo che da noi ha assunto un carattere internazionale (peraltro credo che l'Italia detenga anche il primato mondiale sulle organizzazioni criminose nazionali presenti ed addirittura operanti quasi tutte anche in sede transnazionale).

Occorre allora un metodo investigativo ed operativo del tutto nuovo, logico ed insieme molto qualificato dal punto di vista tecnologico. Perché è la logica applicata alla tecnologia il vero strumento vincente. E la capacità di adattare più schemi di pensiero e la capacità di intervenire in un contesto evolutivo e anche molto complesso di indagine, valutando tutti gli elementi presenti, tutti i contenuti investigativi e, soprattutto, sapendoli decodificare. E allora lo strumentario investigativo essenziale è uno strumentario aiuta in questa decodificazione; che può essere territoriale o convenzionale, può essere un codice inventato o addirittura strutturato, a livello informatico attraverso l'uso di programmi che consentono di mascherare un oggetto all'interno dei contenuti.
Bisogna allora considerare gli strumenti nuovi d'investigazione. Che sono, a volte prodotto di fonti e tecnologie aperte, a volte legati ai *"big-data"*, a volte quindi sulla base di elementi apparentemente esterni, il movimento di una autovettura, o i dati del GPS[6].

Ogni navigazione è tracciata. Ogni accesso ai contenuti e condivisione di contenuti è ricostruibile e registrabile. Ma bisogna essere capaci di leggere e di acquisire, tempestivamente e logicamente. Perché per ottenere questi dati essenziali bisogna saperli chiedere soprattutto con una motivazione adeguata e saperli individuare e successivamente elaborare. Bisogna essere in grado di capire che questi dati sono disponibili e questi dati ci possono dare un elemento di enorme rilevanza sul piano processuale.
Ma vanno chiesti subito, vanno chiesti prima che il sistema li cancelli. Sono i dati di navigazione, i dati di interlocuzione sui *social network*, che possono essere decisivi, tanto più in un contesto di terrorismo internazionale che fa uso degli stessi strumenti, prima di fare uso di altri strumenti. Forse le indagini tecnologiche si sposteranno sempre di più sul terreno del dinamismo funzionale, con una *"real time tracking"* in presenza di anomalie rilevanti o predefinibili, ma ciò comporterà problemi acquisitivi documentali molto delicati, e l'esigenza di verificare in modo sinottico il quadro degli elementi informativi così disponibili . Le indagini digitali si svilupperanno come mai prima sul terreno della immediatezza, e saranno fondamentali per la prevenzione di attività criminali non solamente digitali.

4 Realfonzo Umberto, *Privacy e dati giudiziari in sede di giudizio ordinario ed amministrativo,* in Nuova rassegna di legislazione, dottrina e giurisprudenza, 2005, fasc. 21, pp. 2261-22 ; D'Ambrosio Marcello, Il c.d. principio dell'"openness" nelle procedure giudiziarie tra oblio e anonimato ([The so called principle of "openness" in the judicial proceedings between oblivion and anonymity]) Intervento al Convegno "E-Government e diritti fondamentali nello Stato costituzionale", Università Europea di Roma, 20 novembre 2015 in Rassegna di diritto civile, 2017, fasc. 1, pp. 37-56

5 Borlini Leonardo, Tutela della "privacy" e protezione dei dati personali a fronte della sicurezza pubblica e dell'integrità del sistema finanziario europeo (Rights to privacy and data protection v. public security and the integrity of the European financial system) in Diritti umani e diritto internazionale, 2017, fasc. 1, pp. 23-49; La Piscopia Sebastiano, Rilevanza penale del c.d. "Habeas Data" in materia di terrorismo internazionale (Criminal recognition of the so-called "Habeas Data" on international terrorism) in Periodico di Diritto e Procedura Penale Militare, 2017, fasc. 3, pp. 14 ; Bonini Monica, Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea ([Security and technology, between negative freedom and liberal principles. Apple, Schrems and Microsoft: or "violable" rights in the name of fight against terrorism and other dangers, the US and European experience]) in Rivista AIC, 2016, fasc. 3, pp. 33.

6 Giannaccari Andrea, La storia dei Big Data, tra riflessioni teoriche e primi casi applicativi, in Mercato concorrenza regole, 2017, fasc. 2, pag. 307; Di Porto Fabiana, La rivoluzione "big data". Un'introduzione in Concorrenza e mercato, 2016, pt. 1, pp. 5-14.

E tanto più in un contesto in cui anche uno strumento di trasporto innocente, come un camion, può essere trasformato in uno strumento di morte. Perché noi siamo stati abituati a un terrorismo tradizionale che si approvvigiona di armi. Tutto questo non sarà e non è più necessario ed è la prima lezione secca che abbiamo appreso l'undici settembre 2001 con il "*dual use*" che è diventato la regola propria di ogni azione terroristica. Perché nessuno si aspettava che con un simulatore di volo e con un taglierino da cartolaio fosse sviluppato il più grosso atto terroristico mai concepito ai danni dell'occidente. Il cigno nero, secondo Popper l'evento improvvisato, quello che però crea uno scompenso nel nostro modo di intendere i contenuti[7]. Ciò dovrebbe indurre a rileggere tutti i contenuti in modo assolutamente diverso. Ecco il primo sforzo per l'*intelligence* : non solo la ricostruzione ma la previsione degli scenari possibili del crimine. In sostanza il ruolo delle intercettazioni si appresta a diventare sempre più complesso dal punto di vista tecnologico ed anche sempre più delicato dal punto di vista delle implicazioni giuridiche ogni qual volta si affronti uno scenario di tipo informatico.

Noi inquirenti dovremmo essere abituati a un ragionamento di tipo induttivo, perché quello è il nostro schema. Quello ce l'ha insegnato un grande filosofo come Francis Bacone. Ma nessuno cita anche il fatto che era Pubblico Ministero, Procuratore generale del Regno in Gran Bretagna. Quindi queste sue tecniche, che sono poi le tecniche tabellari, che sono tecniche alla base del sapere scientifico, lo strumento di confronto sperimentale, devono e possono essere alla base del nostro stesso modo di investigare. Dobbiamo sapere prospettare sinteticamente e efficacemente, dobbiamo "saper" crescere prospettando e raffrontando elementi fattuali riportati con oggettività, ma dobbiamo anche e soprattutto sapere indurre, attraverso la registrazione di elementi di contenuto ricorrenti e significativi, a ritenere confermata (o al contrario smentita) una relazione.
L'essenza del rapporto tra scienze e tecnologie applicate al diritto processuale penale, dal punto di vista degli organismi inquirenti sta in una visione corretta e sinergica, che sia insieme coerente ed evolutiva.
Dovremmo cioè avere degli strumenti investigativi di buon livello che ci aiutino sempre a caratterizzare e a qualificare, sin dall'inizio questi contenuti, indicizzando le conversazioni e tutti i documenti comunque disponibili per l'indagine, anche e soprattutto se di carattere multimediale.

Questo forse è il tentativo della norma, ma per fare questo occorre anche una un enorme impegno organizzativo, che c'è stato da parte delle procure più importanti in Italia, ma che sarà ancora più forte, io ritengo, sulla base della prospettiva che ci da la nuova norma. **Vorrei sottolineare anche il ruolo che in questi anni ha svolto proprio la Procura Nazionale Antimafia ed antiterrorismo, che è stato un ruolo prima di tutto strategico, fondamentale, a livello tecnologico che è stato quello di intervenire qualificandosi come interlocutore istituzionale qualificato dal punto di vista dell'autorità giudiziaria inquirente, in relazione allo sviluppo tecnologico**. Si tratta di una esperienza preziosissima che andrebbe qualificata proprio in rapporto alle tecnologie emergenti, cui non dovrebbe mancare anche l'apporto della Procura generale della Corte di cassazione anche a livello interlocutorio interno ed internazionale in tema di indagini informatiche. Immagino cioè una cooperazione costante e sempre più intensa nell'ambito delle rispettive competenze per il più efficace coordinamento delle indagini relative a reati commessi ai danni di dati o sistemi informatici o commessi mediante sistemi informatici con l'individuazione di protocolli di indagine e di buone prassi organizzative nei rapporti con la polizia giudiziaria delegata e sul più efficace uso delle risorse tecnologiche per le relative indagini .Perché quello che è il nostro sapere oggi, rischia di essere inadeguato ed obsoleto addirittura nel giro di pochi mesi. Quindi, partire con una fissazione normativa, con una prescrizione che non dia quel carattere di elasticità e di adattamento alla possibile mutazione tecnologica, è già un elemento che ci dovrebbe indurre qualche riflessione.

E' stata in questi anni solo la Procura Nazionale Antimafia a svolgere un intelligente contraltare rispetto alle osservazioni, a mio parere eccessive, che il mondo dei garanti ha svolto ossessivamente rispetto agli atti giudiziari, finendo per chiedere un controllo improprio e sperequato. Perché una cancellazione, peraltro a volte persino intempestiva a seconda del tipo di sistema, rischia di produrre un freno, se non un annullamento di tutte le indagini e quindi di annullare proprio quelle esigenze di giustizia e, soprattutto, di verità processuale che sono basilari in ogni autentica democrazia, specie quelle più delicate che riguardano, invece, non solo il terreno dell'eversione organizzat, tipicamente italiano, ma il mondo nuovo delle attività organizzate criminali, che viene a svolgersi nel modo in cui ormai tutte le altre attività si organizzano, cioè nel *web*.

Allora tutto questo ci dovrebbe indurre a qualche possibile riflessione finale: quale sarà il futuro delle intercettazioni foniche? Perché di questo si tratta. Quale sarà, invece, il futuro di strumenti di intercettazione più ad ampio raggio?
È vero che il *Trojan* ci consente un'incisione che può apparire anche inquietante sulla personalità altrui e che ciò rischia di porsi quale elemento problematico sotto il profilo dell'articolo 15 della nostra Costituzione. Ma è anche vero che se si legge la convenzione Europea dei diritti umani, a volte molto citata, questo non impedisce affatto lo svolgersi delle intercettazioni, persino di quelle più invasive. Sia l'articolo 8 che l'articolo 10 della Convenzione, pone un importante principio per le intercettazioni istituzionali, secondo il quale queste devono essere concertate e, soprattutto, controllate in modo "legale" [8]. Quindi devono essere disciplinate dalla legge in senso stretto ma anche e soprattutto *coordinate e controllate sotto il preciso controllo giudiziario* [9].

7 Nassim N.T. *Il cigno nero. Come l'improbabile governa la nostra vita*, Milano 2015.

8 Cuomo Luigi, Giordano Luigi, *Informatica e processo penale (Computer science and criminal trial)* in Processo penale e Giustizia, 2017, fasc. 4, pp. 15.

9 Ed è questa, infatti l'unica indicazione rilevante che promana dalla CEDU, cfr. 04/12/2015 (Grande Camera) n. 47143/06ROMAN ZAKHAROV contro RUSSIA. In particolare, il diritto russo non specificava chiaramente le categorie di persone che avrebbero potuto essere sottoposte a misure di intercettazione e le misure di sorveglianza non erano limitate alle persone sospettate o accusate di reati. Poteva essere intercettata l'utenza telefonica di chiunque disponesse di informazioni relative a un reato. La CEDU ha ribadito che un'ingerenza può essere giustificata solo ai sensi dell'articolo 8 comma 2 della Convenzione e cioè soltanto se è prevista (espressamente) dalla legge, persegue uno o più fini legittimi indicati ed è necessaria in una società democratica per conseguire uno di tali fini. La Corte conclude che le disposizioni del diritto russo che disciplinano le intercettazioni di comunicazioni non forniscono garanzie adeguate ed effettive contro l'arbitrarietà e il rischio di abuso inerente a qualunque regime di sorveglianza segreta, e che è particolarmente forte in un sistema in cui grazie ai mezzi tecnici i servizi segreti e

Spesso in ambito internazionale si incontrano difficoltà a mettere insieme un comune principio di diritto sostanziale o processuale comune in ambienti giudiziari differenti.
Però il principio di fondo è il controllo giudiziario che, nel nostro paese, è addirittura moltiplicato perché viene svolto dal Pubblico Ministero che, a sua volta controlla, in un'ottica costituzionale, la polizia giudiziaria in termini di legittimità: è il primo filtro, ma successivamente da un giudice terzo che controlla entrambi. E successivamente sia nel primo grado di merito che nei successivi gradi di giudizio tutti gli atti di intercettazione possono essere oggetto di riesame giudiziario. Una tutela, quella italiana, che è ben superiore rispetto a quella degli altri Paesi. Una tutela che sovrappone e non dimentica le garanzie e che fa della supervisione giudiziaria (sui requisiti oggettivi e soggettivi di ogni operazione captativa) il suo punto più qualificante.

La Corte europea dei diritti umani più volte, quando è stata chiamata ad esprimersi proprio in relazione alle intercettazioni (telefoniche ed ambientali), ha riconosciuto all'Italia un'adeguatezza e specificità di garanzie nel nostro sistema processuale penale e un elevato grado di controllo giudiziario [10].
Ora, con la prossima riforma, attendiamoci anche un controllo di tipo logico. Bisognerà che la polizia giudiziaria sia capace di prospettare efficacemente al Pubblico Ministero, e poi il Pubblico Ministero dovrà conseguentemente essere altrettanto capace di prospettare al giudice il perché debbano essere acquisiti quegli elementi cognitivi di tipo "ubiquitario", cioè contenuti su un device portatile. Non potremo più fare uso di formule generali, ma bisognerà essere anche in grado di ordinare logicamente i dati. Bisognerà essere capaci di offrire un quadro, sia pur sintetico ma univocamente significativo, di un'attività criminale tuttora in svolgimento.
Si può intervenire bene, grazie al contributo delle forze di polizia giudiziaria di eccellenza, ovviamente la prima è quella che ci ospita, quella postale e delle comunicazioni, formando adeguatamente sul piano tecnico il personale della polizia giudiziaria. Si tratta di un punto di svolta per realizzare anche una preziosa interfaccia fra le forze di polizia sul territorio e le decisioni della degli organismi (giudiziari) inquirenti.

Ci sono state anche delle esperienze quanto mai preziose come ad esempio quelle svolte dalla Procura della Repubblica di Milano che hanno consentito di formare, in breve tempo, del personale specializzato distrettuale ad altissimo livello, in questi anni si è andati molto avanti. La polizia delle comunicazioni costituisce un esempio di eccellenza a livello mondiale. Ma non basta. Speriamo allora di potere a breve definire un progetto organizzativo più ampio. Speriamo di potere vedere saldate queste visioni istituzionali in un consapevole ambito regolatorio di reciprocità e sensibilità così come di leale cooperazione istituzionale.
Perché, a mio parere anche le più complesse attività criminali hanno un punto debole, basta saperlo cercare, e per saperlo cercare sarà sempre più necessaria una tecnologia avanzata e tutte le attività illecite possono essere riconosciute e conseguentemente contrastate solo con la efficace comunicazione e la organizzazione, e soprattutto con la condivisione delle esperienze positive di indagine.
E' uno schema che dura da millenni, in fondo lo stesso sistema che i guerrieri Achei inventarono, per di più certamente con mezzi tecnici limitati e improvvisati, per abbattere quello che sembrava il muro allora più resistente.

E la logica applicata ha finito per abbattere inesorabilmente la tecnica, persino la più forte. Questo è importante in definitiva sottolineare, **se la tecnologia ha un ruolo che consideriamo determinante non dobbiamo mai tirarci indietro nel confronto "logico" con la tecnologia, e soprattutto dobbiamo sempre e comunque dialogare quotidianamente con la tecnologia**, comprendendola appieno nei suoi aspetti positivi e negativi e soprattutto analizzandone opportunità e rischi, tanto più rispetto a possibili utilizzazioni criminali, garantendo sempre la disponibilità di controlli appropriati e di ricostruzione delle comunicazioni per fini investigativi penali, cercando di capire quello che possiamo avere in relazione all'indagine che stiamo conducendo; e conformando ordinando e riordinando i nostri dati attraverso quello che gli informatici chiamano *dataset*, in modo intelligente, perché possa essere prospettato in modo convincente e soprattutto vincente in ogni dibattimento penale, specie di fronte a reati organizzati sul piano tecnologico. Sarà questa, e solo questa, la sfida che ci aspetta nei prossimi anni. Ed è il senso stesso della legalità e della sua effettiva difesa nella società futura. ©

la polizia hanno *accesso diretto a tutte le comunicazioni di telefonia mobile*. In particolare, *non sono definite con sufficiente chiarezza le circostanze in cui le pubbliche autorità hanno la facoltà di ricorrere a misure di sorveglianza segreta*. Le disposizioni sull'interruzione della sorveglianza segreta non offrono sufficienti garanzie contro le ingerenze arbitrarie. *Il diritto interno consente la conservazione automatica di dati manifestamente irrilevanti e non definisce con sufficiente chiarezza le circostanze in cui il materiale intercettato deve essere conservato o distrutto alla conclusione del processo.* Le procedure di autorizzazione non sono così in grado di assicurare che le misure di sorveglianza segreta siano disposte soltanto quando è "necessario in una società democratica". La vigilanza sulle intercettazioni è attualmente organizzata mediante procedure che non soddisfano i requisiti di indipendenza, di poteri e competenze sufficienti a esercitare un controllo effettivo e continuo, di un esame pubblico e di concreta efficacia. L'effettività dei ricorsi è compromessa dall'assenza in qualsiasi fase della notificazione delle intercettazioni, o di un accesso adeguato ai documenti relativi alle intercettazioni.

10 Decisioni 26/09/2017 MAZZARELLA contro ITALIA,24059/13; 23/02/2016 ; CAPRIOTTI ALESSANDRO contro ITALIA. N. 28819/12 del 23/02/2016 ; 01/09/2015 Quarta Sezione Caso: Gaetano Davide GRECO contro ITALIA. n. 70462/13; 19/05/2015 Quarta Sezione Caso: SAMPECH Giorgio contro ITALIA, n. 55546/09Seconda Sezione, Caso: GIUTTARI Michele contro ITALIA n. 42733/07 del ; 02/12/2014.