spone il decreto in parola, all'art. 7, prevedendo che, tramite decreto del Ministro della giustizia, sono stabiliti i requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante inserimento di captatore informatico su dispositivo elettronico portatile.

Solo apparentemente di banale importanza, la disposizione in esame ha delle inevitabili, quanto importanti, ricadute di natura economica: i *software* di captazione si dovranno adattare ai requisiti tecnici che dovranno essere stabiliti adottando misure idonee di affidabilità, sicurezza ed efficacia al fine di garantire che i programmi informatici utilizzabili si limitano all'esecuzione delle operazioni autorizzate; tutto ciò in una frenetica corsa di evoluzione delle tecnologie digitali nel settore delle comunicazioni commerciali a cui, gioco forza, dovrebbe far fronte una *task force* di esperti e giuristi pronti a rielaborare ed aggiornare i contenuti del D.M. per le esigenze di interesse giudiziario.

5. Captatore informatico e corrispondenza elettronica

In tema di intercettazioni è noto che l'attività di scambio di corrispondenza sia diverso rispetto alla mera attività di consultazione della corrispondenza in giacenza presso un server o presso il computer dell'indagato.

Mentre lo scambio di e-mail tra due o più utenti è facilmente intellegibile come attività intercettiva di un flusso di comunicazioni telematiche, la seconda attività è, evidentemente, molto più simile se non proprio corrispondente a quella della perquisizione, con eventuale conseguente utilizzo dell'ulteriore e spesso conseguenziale strumento del sequestro.

In molti si domandano quindi che tipo di qualifica dare alla posta elettronica in giacenza sul computer o sul *device* dell'indagato.

L'attività di acquisizione deve essere effettuata con i requisiti previsti dall'art. 247, comma 1-*bis*, c.p.p., seguita dalla disciplina del sequestro del documento informatico (art. 260 c.p.p.) così come introdotto nel nostro ordinamento dalla L. n. 48/2008, atteso il valore di prova "documentale" di detti atti?

È evidente che l'utilizzo del captatore informatico riapre questi scenari non completamente risolti dalla prassi e dalla giurisprudenza (né dalla recente riforma normativa) perché l'utilizzo del "*trojan di Stato*", in questo contesto, significherebbe entrare nell'identità digitale dell'indagato, interagendo *obtorto collo* con differenti forme di documentazione (documenti, file audio, video, immagini, corrispondenza, cronologia degli avvenimenti) con la possibilità, almeno in astratto, di poter alterare, modificare o distruggere ogni singolo file violando i principi ed inquinando (in buona fede) la *scena criminis* "a monte".

Ma, soprattutto, violando il presupposto di liceità di quella stessa atti-

vità di perquisizione e sequestro caratterizzata dall'avviso e dal diritto dell'indagato di farsi assistere da un difensore di fiducia durante lo svolgimento delle operazioni suddette.

Sembra quasi di poter aderire alla tesi di chi specifica che l'utilizzo del *trojan di Stato*, in questi termini e con queste modalità, significhi riportare l'Italia indietro di molti anni, addirittura al cosiddetto processo inquisitorio, così tradendo la riforma del giusto processo, con l'ulteriore aggravante che parte dell'attività investigativa potrebbe essere demandata (da un profilo tecnico) neanche più alle mere forze dell'ordine, ma alle società di gestione dei *software* – non si dimentichi produttrici, amministratrici di sistema e, soprattutto, proprietarie delle relative chiavi *hardware*[39] – e quindi a soggetti privati e, non lo si esclude, ad *influence lobbies*.

Non ci si può nascondere dietro al dito e non dire apertamente che il rischio di alterazione della fonte di prova (anche in buona fede) sia altissimo.

Perché è un limite tecnologico oltre che umano. In spregio a tutte le garanzie costituzionali poste a salvaguardia, si faccia attenzione, non dell'indagato, bensì dell'intero sistema giustizia, ove si rammenti che il compito del P.M. è la ricerca della verità, e non l'inseguimento delle ipotesi investigative della polizia giudiziaria che, seppur strutturate in modo genuino, saranno condizionate da un virtuale telecomando che sceglierà, a singhiozzo, quando attivare e disattivare la registrazione.

Una possibile soluzione potrebbe essere quella di far accompagnare l'attività di captazione da svolgersi in presenza di un difensore d'ufficio all'uopo nominato, che sottoscriva il verbale relativo alle modalità di svolgimento delle operazioni. Resterebbe il problema dell'avviso da dare (telematicamente?) all'indagato (il quale potrebbe interrompere il collegamento?) Ipotesi evidentemente non praticabili che non ci consentono però di risolvere il problema.

Non possiamo infatti ritenere che in una società digitalizzata il controllo sulla propria identità, sfugga, neanche per pochi momenti alla sfera dell'individuo, e possa essere posta nelle mani di chiunque, sebbene autorizzato.

---

[39] Sul tema della "proprietà" del software in senso più ampio va aggiunto che molti degli *spyware* in commercio, seppur commercializzati ed amministrati da aziende italiane o comunitarie, sono in realtà realizzati in altre parti del mondo ed i *partners* commerciali che li distribuiscono non hanno i privilegi di accesso all'architettura degli stessi, non avendo la disponibilità delle relative chiavi *hardware*, cosicché potrebbe accadere, oggi, che il *software* spia commercializzato in Italia dall'azienda "tal dei tali" ed in noleggio per esigenze di giustizia sia, di fatto, occultamente controllato da soggetti terzi, sconosciuti, che potrebbero avere interessi di spionaggio – si voglia per esigenze di sicurezza, di *balance* geopolitico, militare, giudiziario, commerciale o industriale – in contrasto con i principi ed interessi interni.

La digitalizzazione delle informazioni correlate allo stato patrimoniale della persona nonché a quello relativo alla sfera della salute (DNA, dati biometrici e patologie varie, necessariamente custoditi su supporto informatico) fanno comprendere come la sfera della riservatezza dell'individuo, quando si accede al suo computer, sia così intima che una violazione della stessa debba avvenire con il massimo delle cautele che il sistema ha l'obbligo costituzionale di garantire.

Il modello disegnato del *trojan di Stato*, tanto moderno nell'uso dei mezzi ipertecnologici quanto anacronistico con riferimento al tipo di modello di diritto che delinea, si rivelerà in un futuro prossimo ancor più pericoloso, visti come prossimi gli sviluppi della biomedicina, la quale vede l'inserimento di apparati informatici all'interno del corpo umano.

Provocatoriamente concludendo sul punto, c'è da domandarsi chi di noi, tra qualche anno, consentirebbe l'accesso da parte di terzi al database di un microchip sottocutaneo inserito nel proprio corpo, ove, accanto alla preziosa informazione ricercata, relativa all'ultima conversazione ricevuta tramite orecchio "bionico" (oggi già presente sul mercato), si possa custodire anche l'algoritmo di funzionamento di quello stesso apparato uditivo.

Fino a che punto l'indagine ed i poteri ispettivi si vorranno spingere, in spregio ai limiti della dignità umana? La risposta non è così scontata.

6. Acquisizione delle trascrizioni di conversazioni intervenute tramite *whatsapp* e sms

Prima del D.Lgs. n. 216/2017 che stiamo esaminando in questo capitolo, è utile riprendere la pronuncia della Suprema Corte di Cassazione che, con sentenza del 19/06/2017 ha statuito che la registrazione delle conversazioni avvenute tra due utenti, effettuata da uno degli stessi, costituisca una forma di memorizzazione di un fatto storico, della quale si può certamente disporre legittimamente ai fini probatori, trattandosi di una prova cosiddetta documentale.

L'art. 234 c.p.p., comma 1, infatti prevede espressamente la possibilità di acquisire documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo,[40] l'utilizzabilità della stessa è, tuttavia, condizionata dall'acquisizione del supporto – telematico o figurativo contenente la menzionata registrazione, svolgendo la relativa trascrizione una funzione meramente riproduttiva del contenuto della principale prova documentale[41].

[40] Cass. pen., sez. I, sent n. 6339 del 22/01/2013; e sez. VI, sent. n. 16986 del 24/02/2009.

[41] Cass. pen., sez. II, sent. n. 50986 del 06/10/2016, Cass. pen., sez. V, sent. n. 4287 del 29/09/2015.

Perché occorre controllare l'affidabilità della prova medesima mediante l'esame diretto del supporto, per verificare, con certezza, sia la paternità delle registrazioni, sia l'attendibilità di quanto da esse documentato.

Molto più recentemente, la Suprema Corte di Cassazione ha in qualche modo sviluppato un simile ragionamento con la pronuncia n. 1822/2018, in cui ha infatti ribadito il principio che, le conversazioni avvenute tramite *whatsapp* e gli sms (*short message system*) si possono acquisire come prova, in quanto la loro acquisizione non soggiacerebbe alle regole stabilite dal codice di rito per la corrispondenza, o per le intercettazioni telefoniche.

Più nel dettaglio, la Suprema Corte arriva a stabilire che, ai messaggi rinvenuti in un telefono sottoposto a sequestro, non si applica la disciplina prevista dall'art. 254 c.p.p. relativo al sequestro della corrispondenza, in quanto la nozione di corrispondenza, secondo la Corte "implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito"[42].

Anche in questo caso, come in quello precedente, il Supremo Collegio, conformemente tra l'altro a quanto fatto nel 2015, si è espresso specificando che i dati informatici acquisiti dalla memoria del telefono in uso all'indagata (sms, messaggi whatsApp, messaggi di posta elettronica "scaricati" e/o conservati nella memoria dell'apparecchio cellulare) hanno natura di documenti ai sensi dell'art. 234 c.p.p.

Né si possono applicare in tali contesti le norme sulle intercettazioni, in quanto non vi è il presupposto normativo relativo alla captazione di un flusso di comunicazioni in corso tra mittente e destinatario.

Recuperare i messaggi da un *mobile phone* posto sotto sequestro è mera attività che documenta i flussi della comunicazione, ma *ex post.* Si agisce quindi sul database del telefono estrapolando dati che sono stati oggetto di un flusso di comunicazione e che adesso sono meramente custoditi nella memoria dello stesso.

Una opportuna precisazione cenno sull'argomento riguarda le modalità di estrapolazione dei dati di interesse probatorio dal *device*, attività tecnica che sarebbe – sempre – meritevole di rilievo scientifico forense, attraverso il travaso con *software* di analisi forense[43] in grado di documentare chiaramente ed inequivocabilmente quanto contenuto in quell'apparato (di converso, sarebbe impensabile l'esibizione della prova attraverso la "visualizzazione a display", o attraverso la "copia" di *screenshot*).

Ma un ultimo, doveroso, cenno va fatto alle tante modalità di alterazione informatica che, oggi, sono in grado di camuffare la veicolazione di

[42] Cass. pen., sez. III, sent. n. 928 del 25/11/2015, depositata nel 2016.

[43] Come, ad esempio, i sistemi *UFED Cellebrite* ed *Oxygen forensic*, già in uso ai reparti della polizia giudiziaria che effettuano attività scientifica.

stringhe di comunicazione digitale (sia essa un sms, una foto, un file audio o un messaggio multimediale), così da alterare fittiziamente le generalità (attraverso un numero telefonico o un *account* alfanumerico) del mittente.

Un esempio di scuola è quello delle comunicazioni *ioci causa* che è possibile effettuare attraverso molteplici piattaforme presenti sul *web*, in modalità gratuita, e che lasceranno su quel *device*, traccia di un numero telefonico inesistente o attribuito fittiziamente dal *software* di appoggio[44]; o, addirittura, di modificare il codice IMEI che contraddistingue il *device* utilizzato[45], senza effettuare alcuna operazione di *root*[46] sull'apparato[47].

Ben più sofisticata è la possibilità che detta procedura di alterazione del mittente venga effettuata da aziende specializzate in tecnologie di *intelligence* e di *hackeraggio*; si rimanda sul punto al paragrafo concernente la "geolocalizzazione di una macroarea" ed alla possibilità di invio di SMS *clone* di adescamento.

7. Le intercettazioni nelle *chat pin-to-pin*

Prima della recente riforma, la Corte di Cassazione è stata investita più volte in merito al delicato problema inerente le intercettazioni da svolgersi nell'ambito delle *chat pin-to-pin*.

Nella pronuncia n. 21911/2017, il Supremo Collegio ha affrontato la problematica specifica correlata alle *chat pin-to-pin* effettuate tramite l'uso dei telefonini di marca *BlackBerry* localizzati in Italia.

Orbene, procedendo con la descrizione del fatto dal punto di vista tecnologico, occorre ricordare che la *chat* in questione è uno strumento che consente di comunicare a due utenti attraverso una preliminare operazione di cifratura che avviene già nella fase preliminare della cosiddetta emissione del messaggio dal proprio *smartphone*.

Il messaggio criptato viene spedito ad un server, in questo caso allocato presso la sede principale della società, in Canada, che a sua volta rispedisce il messaggio sullo *smartphone* del destinatario, che lo decripta per renderlo intellegibile al proprio fruitore.

In buona sostanza, se si effettuasse una intercettazione "classica" del messaggio durante la sua transazione dal mittente al destinatario, la stessa sarebbe sostanzialmente inutile, perché il messaggio intercettato sarebbe criptato in maniera indecifrabile[48].

---

[44] Tra le tante, ad esempio, le app *Fake my phone* e *Spoofbox.*

[45] Ad esempio, il tutorial: *https://desktopsolution.org/guida-come-cambiare-codice-imei-su-android/*

[46] Cioè di sblocco dei privilegi di sistema.

[47] *https://drfone.wondershare.com/it/sim-unlock/change-imei-android.html*

[48] Per quanto concerne questo paragrafo, si veda anche l'approfondimento da cui è anche parzialmente tratto: Mauro Trogu, *Blackberry ed intercettazioni di comunicazioni*

È quindi accaduto che tramite accordi, le Procure hanno ottenuto la possibilità da parte della società filiale che gestisce questo traffico di dati in Italia, di ottenere i testi decifrati relativi alle comunicazioni effettuate tramite apparecchi di comunicazione oggetto d'intercettazione, attraverso l'utilizzo dello strumento procedurale fornito dall'art. 266-*bis* c.p.p.

Ciò non ha completamente risolto il problema perché, in realtà, quella italiana è soltanto una filiale di riferimento e la società madre che custodisce realmente i dati sui propri server si trova in Canada e la richiesta di accesso ed estrazione di quelle informazioni, nonché la conseguente decriptazione, richiederebbe una procedura di rogatoria internazionale.

Ma, soprattutto, la domanda da porsi è: viene inoltrata una richiesta di cosa, di un flusso di comunicazioni tra due utenti? Evidentemente no, viene inoltrata una richiesta di un pacchetto di dati custoditi (criptati) su un server. Ed è questa forse un'attività inquadrabile nell'alveo della mera intercettazione di flusso di comunicazioni?

È chiaro che questo aspetto apre la problematicità delle operazioni svolte, perché occorre comprendere se, così facendo, si stia procedendo attraverso un'operazione di vera e propria intercettazione (poco probabile), oppure attraverso un'operazione di sequestro probatorio.

In tali contesti, perché si possa parlare di intercettazione e non di sequestro, occorre che il flusso di comunicazioni venga acquisito prima che giunga al destinatario (intercettazione), altrimenti ricadremmo più facilmente nell'ambito di un'attività di sequestro probatorio.

Secondo aspetto critico relativo alle intercettazioni in oggetto: dalla lettura dell'art. 268 c.p.p., comma 3 sappiamo che le operazioni di intercettazione vengono affidate agli impianti dislocati presso i server degli Uffici della Procura della Repubblica.

Quando oggetto dell'intercettazione sono le comunicazioni telematiche, l'ufficio del P.M. può disporre l'uso di impianti appartenenti ai privati.

Se analizziamo bene la vicenda in esame ci accorgiamo che ciò significa non rivolgersi ad una società italiana che gestisce il traffico, ma a quella canadese, la quale effettua, senza la presenza di alcuna Forza dell'Ordine od appartenente alla polizia giudiziaria (italiana o delegata all'estero) questa attività di estrazione ed eventuale decriptazione del dato. Stiamo affidando cioè il lavoro ad un soggetto privato e dobbiamo fidarci.

La stessa problematica, già in passato trattata, e relativa all'estrazione dei *file di log* di sistema presso le società terze private. Orbene, è noto

---

trasmesse tramite tecnologia pin to pin Corte di Cassazione, Sezione III, sentenza 10 novembre 2015, n. 50452 – Pres. Franco; Rel. Rosi Come si intercettano le chat pin to pin tra dispositivi Blackberry, in *Processo Penale e Giustizia*, n. 3 del 2016, Torino.

che il processo penale (e le regole poste a fondamento dello stesso) non si basa sulla fiducia degli operatori, ma sul rispetto di regole procedurali "certe", che dovrebbero essere tutte orientate verso il giusto processo.

L'art. 268 c.p.p. non sembra consentire, che le attività di captazione possano essere svolte con impianti dislocati presso società terze, rispetto agli Uffici della procura. Se si riflette sul fatto che l'operazione delicata riguarda la captazione e la decifratura, si comprende bene come questa attività che non avviene in Italia ma presso i server della società estera, è al difuori del controllo esercitabile dall'autorità giudiziaria.

E, ragionando per ipotesi, se il processo riguardasse attività di criminalità organizzata correlata a società dello stesso stato ove risiedono i server, magari società correlate a quelle che detengono i server per quote societarie o partecipazioni azionarie o legate da importanti contratti di appalto di fornitura di beni e servizi, possiamo continuare a fare un "atto di fede" senza violare i principi della certezza del diritto?

È chiaro che dalla violazione delle norme di cui all'art. 268, commi 3 e 3-*bis*, c.p.p., discende l'inutilizzabilità delle intercettazioni eseguite usando impianti installati presso soggetti privati.

Un *escamotage* relativo ai casi in questione, per aggirare giuridicamente il problema della rogatoria, è stato utilizzato attraverso la cosiddetta procedura di instradamento. L'instradamento consente di aggirare il problema della rogatoria internazionale in quanto l'attività di captazione non necessiterebbe di rivolgersi all'autorità giudiziaria di uno Stato estero perché la registrazione avrebbe ad oggetto una conversazione avvenuta in Italia.

Tuttavia, nel caso delle *chat pin-to-pin*, l'Autorità Giudiziaria necessita di rivolgersi all'estero perché è in quella sede che viene custodito il *file* della conversazione da decriptare. Il tutto sempre fatta salva l'ulteriore osservazione che non si tratterebbe neanche di vera e propria intercettazione in questi casi.

Nei casi in oggetto il flusso telematico viene captato e decifrato all'estero, ed "è qui che la fonte di prova può dirsi assicurata pronta per essere custodita in vista delle successive fasi del procedimento probatorio"[49].

Il problema rimane aperto e le recenti riforme normative apportate dal D.Lgs. n. 216/2017 non sembrano aver dato una soluzione sul punto. Lo studio specifico della pronuncia della Cassazione n. 21911/2017 lascia grandi dubbi agli interpreti, ed in dottrina.

[49] *Ivi*.

8. La Polizia Giudiziaria ed i protocolli investigativi di *intelligence*

Per ragioni di sintesi non è possibile spiegare in dettaglio, nel presente approfondimento, quali e quante siano le procedure investigative che la polizia giudiziaria è tenuta a seguire nel corso di un'attività tecnica di intercettazione. A partire dai primi protocolli di *human intelligence*[50] attraverso cui la polizia giudiziaria individua e localizza il bersaglio, passando all'analisi massiva dei tabulati telefonici indispensabile per un primo *screening* e profilazione del bersaglio da controllare; "preliminarmente un primo monitoraggio investigativo trova applicazione con la costituzione di un fascicolo documentale elaborato "a tavolino", cioè effettuato in modo informatico o cartaceo senza l'ausilio di attività tecnica di supporto.

Detto lavoro di "scrematura", spesso può trovare riscontro senza la necessità di articolati provvedimenti autorizzativi delle Autorità demandate. L'attività di analisi in campo investigativo trova molteplici applicazioni in svariati ambiti, così da offrire un quadro d'insieme il più esaustivo possibile, di immediata consultazione.

Il principio che vale nell'attività dell'analista è quello, della elevata specializzazione nel settore di interesse, così da poter offrire a chi di dovere (magistrato e/o avvocato) un flusso di informazioni concreto ed attendibile, che sarà indispensabile nelle scelte d'indagine successive[51].

Segue, poi, la strategia di attacco delle comunicazioni con la scelta dello strumento più idoneo per agganciare ed "ascoltare" il bersaglio (il telefono di casa, un cellulare, la microfonazione di un autoveicolo o di un

[50] M. Di Stefano, *Intelligence & privacy nelle macroaree: un approccio COMINT/OSINT*, Altalex quotidiano di informazione giuridica, 12/12/2014.: "la HUMINT (*HUMan INTelligence*) concerne l'acquisizione dei dati strategici è svolta da risorse umane che hanno il compito di raccogliere notizie attraverso relazioni interpersonali (agenti e informatori) o l'osservazione diretta (osservatori); IMINT (*IMagery INTelligence*) è la disciplina che cura la raccolta e analisi di immagini aeree o satellitari; MASINT (*MeAsurement and Signature INTelligence*) attiene all'acquisizione di immagini non visibili con sensori elettrici o radar; COMINT (*COMmunication INTelligence*) raggruppa l'intercettazione, selezione e interpretazione dei contenuti inerenti al traffico delle telecomunicazioni (perlopiù flussi di traffico che transitano per i satelliti e i cavi internazionali); ELINT (*ELectronic INTelligence*) studia la ricezione e analisi di segnali elettronici, come ad esempio l'emissione dei sistemi radar; SIGINT (*SIGnal INTelligence*) si interessa della raccolta di dati mediante l'intercettazione di mezzi di comunicazione (ad esempio radio, mail, telefono, ecc); TECHINT (S*cientific and TECHnical INTelligence*) riguarda l'attività d'intelligence nel settore delle armi ed equipaggiamenti, nonché di acquisizione informazioni a livello strategico; OSINT (*Open Source INTelligence*) riguarda l'acquisizione e l'analisi dei contenuti messi a disposizione dalle fonti aperte (stampa, *internet*, *social networks*, *database* pubblici, ecc.)".

[51] M. Di Stefano, B. Fiammella, *Profiling: tecniche e colloqui investigativi. Appunti d'indagine,* Altalex editore, Montecatini Terme, 2013, p. 8.

ambiente, etc.), fino all'avvio delle intercettazioni sulle piattaforme di remotizzazione. In questi contesti l'operatore entrerà nella quotidianità dell'utente sorvegliato, iniziando a conoscerne abitudini, interessi, legami affettivi, amicali, professionali, immergendosi nella "consonanza intenzionale (Gallese 2006), vale a dire la dimensione esperienziale dell'intersoggettività che consente di cogliere direttamente il senso delle azioni eseguite dagli altri, le emozioni e le sensazioni in un ambiente"[52].

Avvierà nuove ricerche per acquisire un bagaglio conoscitivo complesso sul soggetto monitorato, a partire da un approccio OSINT: l'analisi delle *open sources* "comprende diversi ambiti disciplinari combinati tra loro: gli strumenti di hacking della rete per ottenere informazioni sulle identità digitali, l'uso avanzato dei motori di ricerca, l'utilizzo dei portali di investigazioni digitali (dove ottenere le informazioni istituzionali su persone fisiche o giuridiche, proprietà immobiliari, partecipazioni azionarie o societarie, etc.) e infine le tecniche di analisi investigative per valutare il materiale informativo acquisito ed elaborato attraverso strumenti di visualizzazione grafica dei dati"[53]. E traccerà profilazioni attraverso protocolli avanzati di analisi dei *social networks* con le tante tecniche di *SOCial Media INTelligence.*

Da qui l'investigatore/operatore/analista/*profiler* sarà in grado di tracciare un *profile*[54] analitico del bersaglio monitorato che verrà, man mano, implementato dai tanti tasselli che il *profiler* rileverà nel corso dell'attività, spesso insinuandosi proprio in quegli aspetti che rientrano nella sfera della *privacy*, come il gusto sessuale (si pensi ad esempio di un'ipotesi delittuosa a sfondo sessuale, di pedopornofilia, di sfruttamento della prostituzione, di *stalking*, di *cyber crime* a sfondo erotico), l'estrazione razziale ed etnica (si considerino i tanti casi riguardanti proprio ipotesi di discriminazione razziale, di tratta di esseri umani, di fanatismo e terrorismo religioso) le opinioni politiche e l'adesione a partiti, sindacati, associazioni od organizzazioni (si rimandi ai tanti casi di sovversione e di terrorismo interno, ai tanti fenomeni secessionisti e di destabilizzazione).

Si tratta, quindi, dell'acquisizione di molteplici dati che, sicuramente probabilmente, sono da intendersi, *latu sensu*, "sensibili", ma indispensa-

[52] D. Coppola, *Parlare, comprendersi, interagire. Glottodidattica e formazione interculturale*, Felici editore, San Giuliano Terme, 2009: *"*risulta evidente che l'intersoggettività e la cognizione sociale sono direttamente coinvolti nello sviluppo cognitivo così come nell'acquisizione del linguaggio. Da qui emerge, inevitabile, la dimensione interculturale dell'abitare l'alterità, propria e altrui, in cui entrano prepotentemente in gioco le emozioni (relazione di Luciana Brandi, Tra lingue, culture e formazione della soggettività".

[53] L. Reitano, *Esplorare Internet. Manuale di investigazione digitale e Open Source Intelligence*, Minerva edizioni, Bologna, 2014, p. 9.

[54] M. Di Stefano-B. Fiammella, *Profiling: tecniche e colloqui investigativi. Appunti d'indagine,* cit., p. 14.

bili per la costruzione dell'attività, per la sua prosecuzione e per una valutazione *ex post* dei contenuti che non può, di certo, essere programmata e filtrata *a priori* in una fase iniziale dell'attività investigativa.

9. Le misure di sicurezza nelle attività d'intercettazione

Già nel 2013 il Garante per la protezione dei dati personali[55] aveva impartito direttive in materia di "misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica"[56]. Il provvedimento aveva abbracciato, nello specifico, le criticità riguardanti la necessità di costituire presso le Procure della Repubblica dei Centri Intercettazioni Telecomunicazioni C.I.T.), soggetti a misure di sicurezza fisiche ed informatiche[57]. La struttura in questione è costituita dai locali ove sono situate le postazioni di ascolto, unitamente agli apparati elettronici e informatici utilizzati per lo svolgimento dei servizi di intercettazione, tra cui: gli apparati su cui vengono indirizzate le telefonate e le altre forme di comunicazione intercettate per la loro registrazione e il loro successivo trattamento; i server tramite i quali vengono erogati i servizi per la gestione informatica e documentale delle intercettazioni (compilazione dei c.d. "brogliacci", trascrizione delle conversazioni, dati accessori); gli apparati per la generazione e conservazione di copie di sicurezza dei dati (*backup*). I locali in cui viene effettuata la registrazione delle conversazioni telefoniche o ambientali, o di dati digitali anche a carattere audiovisivo, nonché i locali in cui sono installati gli apparati terminali connessi

[55] Provvedimento del 18/07/2013 n. 356, G.U. n. 189 del 13/08/2013.

[56] I cui termini prescrittivi sono stati differiti con provvedimento del 26/06/2014, G.U. n. 149 del 30/06/2014, per poi essere ulteriormente dilazionati fino al luglio 2016 con deliberazione del 25/06/2015, fino ad un ulteriore provvedimento di proroga del 28/07/2016 andato a scadere il 31 gennaio scorso.

[57] – comunicazioni elettroniche tra l'Autorità giudiziaria e i gestori effettuate esclusivamente in modo cifrato con strumenti, anche di tipo on line o web, che assicurino comunque l'identificazione delle parti comunicanti, l'integrità e la protezione dei dati, nonché la completezza e la correttezza delle informazioni temporali relative alle informazioni trasmesse (date ed orari di formazione dei documenti o della loro trasmissione e consegna);

– protezione dei documenti informatici trasferiti su supporti rimovibili con idonee tecniche crittografiche, ricorrendo preferibilmente ad algoritmi a chiave pubblica (come nel caso dell'uso di strumenti di firma digitale in funzione di cifratura), evitando comunque la trasmissione di chiavi simmetriche di cifratura in modo informale su canali insicuri;

– utilizzo nelle comunicazioni tra Autorità giudiziaria e gestori della posta elettronica Internet esclusivamente nella forma di posta elettronica certificata (Pec) di cui all'art. 48 del d. lg. 07/03/2005, n. 82, e del telefax esclusivamente nella forma di fax digitale "gruppo 4" (ISDN) oppure di Fax over IP;

– trasmissione cifrata delle comunicazioni telematiche intercettate (flussi IP, posta elettronica) dal punto di loro estrazione dalla rete del gestore fino agli apparati riceventi presso i C.I.T.