Le indagini digitali sotto copertura per la repressione dei reati di pedopornografia

Le indagini sotto copertura sono quelle poste in essere da corpi specializzati della polizia giudiziaria e finalizzate alla repressione di particolari reati di organizzazione criminale e terroristica.

Tale particolare modalità investigativa, denominata "undercover", rientra tra le "special investigative techiniques", ossia quelle tecniche non convenzionali compiute dagli organi investigativi per il contrasto della criminalità organizzata e di reati per i quali ogni altra attività investigativa risulti inefficace. Nello specifico la locuzione "sotto copertura" indica l'attività di un ufficiale di polizia giudiziaria che, "mascherando" la propria reale identità, si infiltra all'interno di organizzazioni criminali allo scopo di ottenere prove ed informazioni in grado di "incastrarne" i partecipanti .

Tra le operazioni di contrasto annoverate all'art.14 l. 3 agosto 1998, n. 269, gli organi di polizia sono autorizzati a svolgere, limitatamente agli illeciti indicati dalla norma, un vero e proprio ruolo di agente provocatore[1]. Si possono, infatti, annoverare tutti quegli espedienti volti a dissimulare specifiche operazioni di polizia, mascherate con indicazioni di copertura, anche attraverso la creazione di siti "civetta" cioè siti Internet creati *ad hoc* dagli organismi investigativi per cogliere in flagranza eventuali pedofili. Il contenuto di tale sito può, ad esempio, assumere le sembianze di un social network nel quale opera un software perfettamente in grado di simulare l'identità di un bambino, con le caratteristiche linguistiche e comportamentali dei minori ricompresi tra gli otto e i tredici anni[2].

La costruzione del sito, sotto l'aspetto tecnico, deve essere quindi curata con molta attenzione, dal momento che l'attività sottocopertura deve risultare credibile e impostata all'acquisizione di dati e operazioni poste in essere dagli utenti. Anche il nome del sito deve essere studiato magistralmente in modo da inserirsi adeguatamente in un ambiente ostile senza destare sospetti. In pratica, i siti civetta servono soprattutto a localizzare soggetti interessanti sul piano investigativo, sui quali poi orientare attività di indagine più mirate: in questo modo, coloro che frequentano abitualmente predetti siti vengono controllati e cercati in altri siti web (nelle chat e nei newsgroup, in particolare)[3].

L'intercettazione così disposta consentirà di avere copia di tutte le informazioni transitate da e per il sito durante ogni "sessione" di collegamento dell'utente, con l'esatta riproduzione delle operazioni da lui compiute e delle specifiche immagini visualizzate e scaricate sul suo computer.

Viene quindi acquisito presso il provider l'indirizzo IP di coloro che si collegano al sito, identificati i quali si procederà alla perquisizione e al sequestro per rinvenire il materiale illecito scaricato dal sito e far esaminare lo stesso ad un consulente informatico[4]. In questo senso, si ricorda che le indagini attinenti crimini compiuti nel mondo virtuale, a prescindere dalla specifica tipologia di reato indagato, sono previste metodologie investigative, volte soprattutto, a verificare la reale identità dell'utente online interessato dall'indagine[5]. Nelle prime fasi investigative, infatti, gli operatori di polizia generalmente non si relazionano con persone di cui conoscono l'identità ma interagiscono con utenti virtuali *prima facie* "sconosciuti" per poi individuarne i dati relativi alla connessione incriminata e risalire così all'utenza telefonica attraverso la quale tali soggetti si sono connessi in rete (indirizzo IP, file log ecc).

La predisposizione di siti web civetta non è sempre agevole dal punto di vista del rispetto delle garanzie costituzionali: infatti, è facile oltrepassare i limiti consentiti da parte del legislatore. In questi anni, difatti, ci sono stati casi giudiziari molto discutibili come ad esempio all'utilizzo da parte della Procura di Salerno di un sito civetta dotato di assoluta genericità ed essendo in grado di allettare e confondere la pressoché totalità degli utenti internet italiani non interessati a materiale pedopornografico[6].

L'attività d'indagine *undercover* online può poi estrinsecarsi nella partecipazione, nonché realizzazione e gestione di aree di comunicazione o di scambio di materiale pedopornografico su reti o sistemi telematici.

L'attività d'indagine, in questo caso, consiste nell'ingresso da parte degli agenti, in vere e proprie *chat online*, tramite *nickname* di fantasia, al fine di prendere parte a conversazioni già in corso tra altri utenti aventi a oggetto lo scambio di materiale pedopornografico. È fondamentale precisare che le tali condotte devono opporsi a *iter* criminosi già in corso di svolgimento, "presupponendo nel soggetto provocato un possesso di beni o una seria di accordi finalizzati che di per sé, secondo la normativa di riferimento, già costituiscono reato"[7]. Non sono in alcun modo ammissibili operazioni sottocopertura che si concretizzino in un incitamento a compiere delitti.

Le chat-line rappresentano il settore dove si manifestano rischi maggiori per i minori: infatti, questi strumenti di comunicazione implicano la mediazione di un computer per far sì che s'instauri un rapporto di fiducia tra i due interlocutori "neutralizzando anche alcuni gap di età e culturali che normalmente limitano o selezionano le comunicazioni dirette tra minori e adulti"[8]. La tecnologia della chat, inoltre, facilita l'adescamento da parte di pedofili nella fase di contatto iniziale con la possibile vittima e consente loro forme di molestia di tipo verbale e tentativi di incontro al di fuori della rete.

La pedopornografia è offerta – e richiesta – online su praticamente tutti i canali disponibili: siti web, s*ocial network, chat, e-mail, file sharing*[9] ecc. sulla base di ciò, le investigazioni della polizia giudiziaria hanno l'obbiettivo di coprire integralmente la rete attraverso attività di intercettazione sottocopertura, monitoraggio di siti web e chat, partecipazione a forum community e iscrizione a mailing list[10]. Una delle tecniche a disposizione della polizia giudiziaria è il monitoraggio delle reti peer-to-peer cioè "un'infrastruttura di scambio informazioni tra nodi alla pari in cui due entità oggetto dello scambio possono indifferentemente scambiarsi i ruoli di fornitore e cliente di un determinato servizio"[11]. Il successo di questo servizio è dovuto principalmente alla sua semplicità di utilizzo e alla riservatezza che garantisce, non essendo, infatti, richieste particolari competenze informatiche per utilizzarlo. È sufficiente connettersi al software di

condivisione e ricercare il materiale d'interesse dietro lo schermo del proprio computer. Il modo più efficace per monitorare queste reti consiste nella raccolta di prove direttamente dal nodo, ricevendo o trasmettendo il materiale illecito.

Normalmente l'attività di monitoraggio ha luogo su iniziativa degli investigatori, o nell'ambito di una più ampia attività di monitoraggio coordinata a livello nazionale dal Servizio Polizia Postale e delle Comunicazioni che spesso coinvolge tutti gli Uffici periferici per determinati periodi con turni continui[12].

Quest'attività è quella che fornisce riscontri maggiori ma è anche quella più costosa in termini di larghezza di banda, risorse computazionali e costo di personale[13] in quanto nella maggioranza dei casi, tali siti risultano ubicati in computer non presenti sul territorio italiano e pertanto, tali attività necessitano di rogatorie internazionali o comunque di procedure più complesse al fine di identificare gli autori coinvolti.

La pedopornografia è offerta – e richiesta – online su praticamente tutti i canali disponibili: siti web, s*ocial network, chat, e-mail, file sharing* ecc. sulla base di ciò, le investigazioni della polizia giudiziaria hanno l'obbiettivo di coprire integralmente la rete attraverso attività di intercettazione sottocopertura, monitoraggio di siti web e chat, partecipazione a forum community e iscrizione a mailing list. Una delle tecniche a disposizione della polizia giudiziaria è il monitoraggio delle reti peer-to-peer cioè "un'infrastruttura di scambio informazioni tra nodi alla pari in cui due entità oggetto dello scambio possono indifferentemente scambiarsi i ruoli di fornitore e cliente di un determinato servizio"[14]. Il successo di questo servizio è dovuto principalmente alla sua semplicità di utilizzo e alla riservatezza che garantisce, non essendo, infatti, richieste particolari competenze informatiche per utilizzarlo. È sufficiente connettersi al software di condivisione e ricercare il materiale d'interesse dietro lo schermo del proprio computer[15]. Il modo più efficace per monitorare queste reti consiste nella raccolta di prove direttamente dal nodo, ricevendo o trasmettendo il materiale illecito.

Normalmente l'attività di monitoraggio ha luogo su iniziativa degli investigatori, o nell'ambito di una più ampia attività di monitoraggio coordinata a livello nazionale dal Servizio Polizia Postale e delle Comunicazioni che spesso coinvolge tutti gli Uffici periferici per determinati periodi con turni continui[16].

Quest'attività è quella che fornisce riscontri maggiori ma è anche quella più costosa in termini di larghezza di banda, risorse computazionali e costo di personale[17] in quanto nella maggioranza dei casi, tali siti risultano ubicati in computer non presenti sul territorio italiano e pertanto, tali attività necessitano di rogatorie internazionali o comunque di procedure più complesse al fine di identificare gli autori coinvolti[18].

Di fronte al moltiplicarsi dei siti pedopornografici, il legislatore italiano ha emanato, la legge 6 febbraio 2006, n.38 che, oltre a un significativo inasprimento delle pene a carico di chi si macchia dei reati di abuso sessuale e sfruttamento di minori o che detengano o si procurino materiale pedopornografico, presso il Ministero dell'Interno viene istituito, all'art.19, il Centro Nazionale per il monitoraggio della pornografia minorile su Internet, con il compito di raccogliere segnalazioni, anche provenienti dall'estero, sull'andamento del fenomeno in rete[19]. Le aree di competenza riguardano, per tanto, il coordinamento delle indagini, l'analisi dei crimini informatici, il monitoraggio della rete e la gestione delle *black list*[20]. Il database del CNCPO utilizza programmi sofisticati che svolgono una rapida comparativa delle immagini acquisite, cercando collegamenti o analogie con altre 600.000 immagini già presenti all'interno dell'archivio in modo da individuare eventuali relazioni e nessi tra le vittime raffigurate[21].

Nel 2003, grazie all'eccellente lavoro d'indagine disposto dalle procure di trentaquattro Paesi, tra cui l'Italia, il gigante statunitense del software Microsoft ha deciso di chiudere definitivamente le "*chat room"* (stanze di comunicazione virtuali) gestite dal suo provider MSN (Microsoft Network)[22]. Il servizio era, purtroppo, utilizzato non solo da *spammers* (coloro che inoltrano email indesiderate c.d. "spazzatura) ma anche da pedofili che utilizzavano le chat per scambiare messaggi e materiale a sfondo pedopornografico. In Italia gli effetti dell'indagine sono stati notevoli: 11 siti illeciti oscurati, un arresto in flagranza di reato e due in esecuzione di misure cautelari; le accuse: detenzione e scambio di immagini pedopornografiche mediante sfruttamento sessuale di minori; sequestrati oltre 200 personal computer e migliaia di floppy disk, cd rom e nastri audiovisivi che sono ancora in via di analisi da parte degli esperti[23].

Un'altra indagine dai riscontri positivi è stata disposta dalla Procura di Venezia denominata "Canal Grande". «In questa è stato utilizzato un sistema di monitoraggio di reti "*fast track"* rete che notoriamente viene utilizzata dalle reti di *file sharing* più famose (ad esempio Emule). Durante questa indagine era stato cerato un sistema automatico di server all'interno del quale si trovava un *database* contenente *hash* di centinaia di file pedopornografici messi a disposizione da precedenti sequestri avvenuti in tutta italia. Questo sistema scandagliava la rete *fast track* con lo scopo di individuare gli indirizzi IP degli utenti e di confrontare gli hash dei file condivisi dagli utenti. Il server, quindi, era in grado di ricercare, attraverso la comparazione degli hash del materiale scaricato con quello messo a disposizione del server, il materiale pedopornografico. A quel punto dell'indagine, entrava in gioco l'agente sotto copertura che, fingendosi anch'egli un pedofilo, scaricava i file messi a disposizione dagli altri pedofili, non solo per rintracciare l'indirizzo IP e quindi individuare il criminale ma anche per aggiornare il database contenente gli hash del materiale[24]».

Nel corso del 2018, grazie all'operazione sotto copertura "*Good Fellas*" sono state effettuate 14 perquisizioni, portando all'arresto di 4 persone nonché la denuncia di altri 12 indagati[25]. Allo stesso modo, l'operazione "*Showcase*" ha contribuito alla realizzazione di 12 perquisizioni, la denuncia di 11 persone e un arresto[26].

Il Centro si identifica come referente italiano nell'ambito delle inchieste internazionali, nonché come organo di coordinamento delle indagini svolte in Italia dalle unità presenti sul territorio[27]. Il CNCPO funziona anche grazie a degli strumenti di filtraggio e delle tecniche in materia di oscuramento dei siti internet che i *provider* devono utilizzare per impedire l'accesso ai siti segnalati. Anche i privati cittadini possono contribuire all'accuratezza del monitoraggio,

segnalando su un'apposita piattaforma online i contenuti pedopornografici individuati nei siti web durante la navigazione. Va chiarito, in merito, che molto spesso le segnalazioni effettuate dagli internauti siano, in realtà, e per fortuna, dei falsi allarmi. Frequenti sono infatti i casi in cui vi sia un errore nell'attribuzione della minore età ai soggetti rappresentati. Inoltre, un altro problema riguardante la segnalazione "privata" riguarda l'impossibilità di analizzarla in quanto questa è sovente presentata solamente tramite "*screen-shot*" o "stampate" dei siti web, senza alcuna indicazione dell'indirizzo internet. Un altro possibile esito negativo per questo tipo di spazio online è legato al dinamismo che caratterizza la gestione dei siti pornografici. In questo senso, una delle modalità adottate dagli amministratori di questi siti internet, per evitare le indagini delle forze di polizia, consista nel mutare frequentemente l'indirizzo web del sito (URL)[28].

I siti web individuati diventano oggetto di indagini mirate in modo da scoprire dove gli stessi siano fisicamente ubicati e per individuare la società o la persona fisica che li gestisca.[29] Nella maggior parte dei casi questi siti sono ubicati all'estero, in particolare in nazioni extra comunitarie dove l'allarme sociale è nettamente inferiore rispetto a quanto non sia in Europa, ma soprattutto dove la legislazione su questi temi risulta estremamente carente[30].

La norma ha inoltre, previsto il diretto coinvolgimento dei fornitori dei servizi resi attraverso reti di comunicazione elettronica, delle autorità bancarie, degli istituti di credito e degli intermediari finanziari che prestano servizi a pagamento[31]. Le informazioni e le segnalazioni d'interesse, previa un'accurata verifica, sono riunite in un elenco aggiornato dei gestori e dei beneficiari dei pagamenti legati alla commercializzazione del medesimo materiale e i dati in esso contenuti sono messi a disposizione sia delle forza di polizia impegnate nelle attività di contrasto, sia dei *provider* per porre in essere le attività di oscuramento dei siti interessati, sia infine, delle autorità bancarie e dei soggetti finanziari per l'applicazione delle misure interdittive e sanzionatorie previste dalla legge, tra cui quelle necessarie a interrompere il circuito dei pagamenti attraverso l'uso di carte di credito[32].

Dette operazioni si avvalgono della collaborazione con il database del materiale pedopornografico gestito dall'Interpol, cioè l'*International Child Sexual Exploitation image database* (I.C.S.Edb). Grazie a questo archivio e all'utilizzo di particolari software per l'esame dei file digitali, viene consentita la comparazione fra il materiale illecito già identificato e presente in questa banca dati con quello rilevato durante le indagini italiane[33].

Tali attività sono di estrema importanza e utilità sia in un'ottica repressiva, sia in un'ottica di prevenzione di questi odiosi crimini. Tuttavia, queste speciali tecniche possono dare i loro frutti se possiedono ingenti finanziamenti: elencare siti web da inserire in una lista nera è un adempimento tutt'altro che agevole. Infatti, tale intervento deve essere svolto anche nel *deepweb*[34], nella *darknet*[35] oltre che nel *public web*[36].

Nell'analizzare il complesso *genus* delle indagini informatiche, è emerso un tratto di tipicità di queste ultime, ovvero il loro continuo mutamento a seconda delle modalità di offesa del bene tutelato dalla fattispecie criminosa. Proprio per questo motivo, unitamente alla fragilità dei dati informatici trattati, è necessario che gli organi inquirenti incaricati dell'acquisizione di tali elementi, debbano possedere un'elevata preparazione tecnico-specialistica al fine di scegliere correttamente la tecnica investigativa più idonea al caso concreto, affinché le indagini risultino maggiormente efficaci.

Dott.ssa Federica Bondavalli

---

[1] Cfr. LUPARIA L., ZICCARDI G., *investigazione penale e tecnologia informatica*, op. cit.

[2] Cfr. DELLE DONNE M., *Tecniche d'indagine della Polizia Postale nell'ambito dei reati informatici e nella pornografia online,* in *Diritto e Diritti,* 2017

[3] Cfr. BUFFA F., *Profili penali del commercio elettronico,* Giuffrè, 2006, pag. 104

[4] *Ibidem.*

[5] Cfr. MACILOTTI G., *Il contrasto alla pedopornografia online,* op.cit., pag.291.

[6] Cfr. RESTA F., *Nota a Cass. Pen., sez III, 8 maggio 2003.*, in *Dir. Inf.* 2004, pag. 267

[7] Cfr. CAJANI, F., *Le operazioni digitali sotto copertura: l'agente provocatore e l'attività di contrasto nelle indagini informatiche*, in S. ATERNO - F. CAJANI- G. COSTABILE - M. MATTIUCCI - G. MAZZARACO (a cura di), *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Forlì, 2011, pag. 411

[8] Cfr. PASELLI A., *Pedopornografia online, metodologie di contrasto e analisi forense,* in MAIOLI C., *Questioni di informatica forense,* Aracne, 2015, pag.80

[9] Per "file sharing" s'intende la condivisione di file all'interno di una rete di computer collegati tra loro, che comporta una messa in comune di risorse attraverso una rete *client-server* oppure *peer-to-peer* tramite software dedicati. Cfr. PASELLI A., *Pedopornografia online, metodologie di contrasto e analisi forense.* Op.cit.

[10] Cfr. FERRAZZANO M., *Aspetti metodologici, giuridici e tecnici nel trattamento di reperti informatici nei casi di pedopornografia,* Aracne, 2018.

[11] *Ibidem,* pag.102

[12] Cfr. PASELLI A., *Pedopornografia online, metodologie di contrasto e analisi forense,* op.cit. pag.74

[13] Cfr. BAUER K., GRUNWALD D., MCCOY D., SICKER D. (2009) *Bitstalker: Accurately and efficiently monitoring bittorrent traffic. Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS*), London, UK, 2009.

[14] *Ibidem,* pag.102

[15] Cfr. MACILOTTI G., *Il contrasto alla pedopornografia online,* op.cit. pag.78

[16] Cfr. PASELLI A., *Pedopornografia online, metodologie di contrasto e analisi forense,* op.cit. pag.74

[17] Cfr. BAUER K., GRUNWALD D., MCCOY D., SICKER D. (2009) *Bitstalker: Accurately and efficiently monitoring bittorrent traffic. Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS*), London, UK, 2009.

[18] Cfr. MACILOTTI G., *Il contrasto alla pedopornografia online,* op.cit. pag.297.

[19] Cfr. PAVONE M., *una legge necessaria contro la pedopornografia*, in altalex .it

[20] Cfr. BUSO D., *La normativa contro la pedofilia. Le leggi contro lo sfruttamento dei minori online,* in Polizia Moderna, Raccolta inserti, aprile 2009, pp. 57 ss.

[21] Cfr. PASELLI A., *Pedopornografia online, metodologie di contrasto e analisi forense,* op.cit. pag.83

[22] Cfr. CRIVELLI G., *Spammers e pedofili: Microsoft chiude le chat*, ilsole24ore.it, settembre 2003

[23] larepubblica.it

[24] Intervista al dott. Ulrico Bardari, collaboratore della cattedra di Informatica forense presso l'Università Alma Mater Studiorum di Bologna.

[25] Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia

[26] *Ibidem.*

[27] Cfr. MACILOTTI G., *Il contrasto alla pedopornografia online,* op.cit. pag.226.

[28] *Ibidem.*

[29] Cfr. PASELLI A., *Pedopornografia online, metodologie di contrasto e analisi forense,* op.cit. pag.76

[30] *Ibidem.*

[31] Cfr. BUSO D., *La normativa contro la pedofilia*, op.cit. pag.2

[32] *Ibidem.*

[33] Cfr. MACILOTTI G., *Il contrasto alla pedopornografia online,* op.cit. pag.230

[34] Il deep web (web sommerso) è l'insieme delle risorse informative del World Wilde Web, non segnalate dai normai motori di ricerca.

[35] Una darkent (rete oscura) è una rete virtuale privata nella quale gli utenti si connettono solamente con persone delle quali si fidano.

[36] Cfr. TORRE M., *Indagini Informatiche e processo penale.* Op.cit.