MANUALE FORENSE PER LA POLIZIA PENITENZIARIA

NFC edizioni

Ministero della Giustizia

J-S.A.F.E. - Judicial Strategy Against all Forms of Violent Extremism in Prison JUST-AG-2016-03

MANUALE FORENSE PER LA POLIZIA PENITENZIARIA

A cura di: **SERGIO BIANCHI** - Middle East Expert, UAS Pilot, Editor

Contributi: **ENRICO SBRIGLIA** - fino al 28.02.2020 Provveditore Regionale dell'Amministrazione Penitenziaria per il Triveneto, Ministero della Giustizia; **MANUELA DE GIORGI**, Dirigente del Compartimento della Polizia Postale e delle Comunicazioni del Friuli Venezia Giulia; **GIUSEPPE PANARELLO** - Responsabile del Settore Digital Forensics – Compartimento Polizia Postale e delle Comunicazioni Friuli Venezia Giulia **ANTONIO ZAZA** - Commissario Capo di Polizia Penitenziaria Provveditorato Regionale per il Triveneto, pilota UAS **MARINA CANEVA** - Assistente Capo di Polizia Penitenziaria Provveditorato Regionale per il Triveneto, pilota APR; **LUIGI PROTA** - Agente Scelto di Polizia Penitenziaria, pilota APR; **MARIALUCIA FAGGIANO** - Funzionario Giuridico Pedagogico Provveditorato Regionale dell'Amministrazione Penitenziaria per l'Emilia Romagna e le Marche; **SERGIO BIANCHI** - esperto di studi medio-orientali, arabista, Fondazione Agenfor International, pilota APR; **MARIA LADU** - ricercatrice, Fondazione Agenfor International, pilota APR; **SERENA BIANCHI** - ricercatrice, Fondazione Agenfor International, pilota APR; **SOPHIE KENNEALLY**- ricercatrice, Fondazione Agenfor International. **Componenti associazione LAB4INT: SIMONE BONIFAZI** Esperto in Digital e Drone Forensics - Pilota di APR, **PIER LUCA TOSELLI** - Esperto in Digital Evidence – DES, **ANTONIO BROI** - Esperto in Digital Evidence - DES, **DANIELE PRICCHIAZZI** - Data Scientist.

This project was funded by the Justice Programme.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 740543.

NFC edizioni

Edito da Agenzia NFC di Amedeo Bartolini & C. sas - Rimini
via Dante Alighieri, 29, 31 - (Rimini)
tel. +39 0541 673550
www.agenzianfc.com - www.nfcedizioni.com

ISBN 9788867262755

Progetto grafico:
Gianluca Puliatti
agenzia NFC

Sommario

INTRODUZIONE
HANDBOOK FOR PRISON POLICE AND SECURITY

di Manuela DE GIORGI Dirigente del Compartimento della Polizia Postale e delle Comunicazioni del Friuli Venezia Giulia.

"Handbook for Prison Police and Security" è un importante strumento rivolto agli operatori delle Forze di Polizia in particolare della Polizia Penitenziaria nato nell'ambito dell'ambizioso progetto "JSafe" composto da un consorzio di 7 Paesi Europei di cui il Provveditorato Regionale dell'Amministrazione Penitenziaria del Triveneto è il capofila. L' obiettivo del progetto, concernente le strategie giudiziarie contro ogni forma di radicalizzazione, viene declinato nel manuale con un focus particolare sulla strategia e su un nuovo modello di prevenzione digitale della radicalizzazione nelle carceri.
Interessanti "living labs" nei quali sviluppare progetti pilota connessi con i laboratori di ricerca giuridica hanno permesso di creare con le risultanze un nuovo modello, sperimentando i più innovativi approcci tecnologici ed operativi nell'ambito forensic in paesi con legislazioni ovviamente diverse. In altri termini, sono stati analizzati i nuovi strumenti digitali e di comunicazione per innovare la prevenzione alla radicalizzazione evidenziando il ruolo della tecnologia quale mezzo di prevenzione e contrasto ai processi di radicalizzazione.
La Polizia Postale e delle Comunicazioni del Friuli Venezia-Giulia dal proprio angolo prospettico ha messo a disposizione la propria esperienza nel campo della cybersicurezza, al fine di mettere a fattor comune e di fornire il proprio contributo per il progetto di definire le linee guida sperimentali di una nuova digital forensics penitenziaria.
L'incessante evoluzione tecnologica ha infatti notevolmente semplificato le nostre vite, rendendo possibili in pochi "click" o "tap" operazioni complesse per le quali, fino a qualche anno fa, era necessaria la presenza fisica in un luogo o la presenza di altre persone o intermediari. La possibilità di contattare persone in ogni istante e ad ogni angolo del globo terrestre ha creato network tra soggetti che condividono le medesime idee, interconnettendo idee e nuove relazioni.
Accanto agli innumerevoli benefici che nemmeno con uno sforzo di fantasia sarebbe possibile elencare, abbiamo tutti osservato che, purtroppo, l'informatica ha dato la possibilità di commettere crimini prima inesistenti. La stessa rete Internet ha offerto, ad esempio, la possibilità di divulgare online materiale multimediale a contenuto pedopornografico e di effettuare attacchi informatici a scopo estorsivo generando così enormi profitti per organizzazioni criminali transnazionali, reati che in Italia vedono in prima linea proprio la Specialità della Polizia di Stato che si occupa della sicurezza cibernetica in tutte le sue cangianti declinazioni.
La tecnologia quindi è un trend globale e ovviamente non esclude nessun mondo, neanche quello penitenziario che deve essere in grado di affrontare la nuova sfida sfruttandone a 360° le potenzialità. Nel manuale è stata dettagliatamente analizzata la prevenzione nell'era digitale e il grosso impatto che

le tecnologie hanno all'interno delle carceri in particolare sul servizio reso, che non può evidentemente eludere l'aspetto umano, rieducativo, etico e relazionale. Inoltre, partendo proprio dall'analisi dei casi di radicalizzazione si è visto come il mondo virtuale si intreccia con quello reale e come il nuovo terrorismo navighi anche in questo caso ormai in rete. In questo contesto, partendo dal particolare, ossia dalla gestione dei dati digitali all'interno degli istituti penitenziari sono stati approfonditi i princìpi della digital forensics, così come applicabili in quei tratti fondamentali comuni tra gli ordinamenti dopo la sottoscrizione della Convenzione del Consiglio d'Europa sulla Criminalità Informatica (c.d. "Convenzione di Budapest").
Mediante la digital forensics, infatti, è possibile ricostruire gli eventi a partire dalle tracce informatiche, a volte poche, sparse su vari dispostivi e apparentemente indecifrabili. La complessità aumenta vieppiù negli scenari già esistenti e sempre più frequenti ove l'eterogeneicità dei dispositivi, la diffusione del cloud, la crittografia e le tecniche di anonimizzazione rendono complesso il lavoro alle forze dell'ordine. La prova informatica, fragile e volatile, necessita di particolari accorgimenti, da adottare di volta in volta a seconda dello scenario e del device ove è contenuta, tenendo in considerazione la multifattorialità dei vincoli giuridici e operativi nell' operare quelle scelte -ad esempio quella di acquisire sul posto l'evidenza digitale piuttosto che procedere al sequestro del device ove è contenuta - che risulteranno fondamentali per il prosieguo delle indagini.
In tale contesto, l'elaborato definisce la figura specialistica del Digital Evidence First Responder appartenente alle forze dell'ordine, trait-d'union tra le competenze di Polizia giudiziaria, di Polizia di Prevenzione e di "pronto intervento" sui dispositivi informatici, figura che raccoglie la doppia sfida tecnologica/giuridica. Il DEFR di polizia, figura specialistica che opera nella cornice dell'ordinamento giuridico di riferimento, possiede altresì padronanza della norme tecniche di settore e delle best practices internazionali che, prescindendo dal contesto giuridico, si pone come fine quello di salvaguardare la prova informatica durante il suo ciclo di vita -dall'acquisizione alla catena di custodia- per renderla efficace nella fase dibattimentale.
In conclusione, l'uso a fattor comune della tecnologia nelle attività di polizia, multidisciplinari per definizione, rappresenta un'enorme opportunità per gli operatori delle Forze dell'Ordine, che consente e consentirà di affrontare con la giusta determinazione e serenità le sfide che vengono poste quotidianamente, per rendere al meglio il nostro servizio alla collettività.

INTRODUZIONE

La strategia giudiziaria di contrasto alla radicalizzazione violenta in carcere rappresenta il punto focale del progetto J-SAFE e dei laboratori sperimentali del progetto MINDb4ACT, finanziati dalla Commissione Europea e supportati rispettivamente dalla Direzione Generale Giustizia della Commissione Europea e dalla Research Executive Agency (REA), con diverse agenzie e istituzioni raggruppate in consorzi di numerosi Stati Membri in qualità di partner. In particolare, il progetto J-SAFE coinvolge sette Stati Membri (Bulgaria, Repubblica Ceca, Germania, Spagna, Grecia, Italia, Romania) ed è coordinato dal Provveditorato Regionale dell'Amministrazione Penitenziaria per il Triveneto - Ministero della Giustizia. Il progetto ha l'obiettivo di sostenere giudici, pubblici ministeri, magistrati e staff penitenziari nell'assumere decisioni informate, a tutti i livelli, su casi di radicalizzazione che conduce al terrorismo.

MINDb4ACT, guidato dall'Istituto spagnolo Elcano, è un progetto di ricerca all'interno del programma europeo Horizon2020 e ha un carattere multi-agenzia che coinvolge 17 partner di 9 paesi.

Al fine di sperimentare la praticabilità di nuove soluzioni, il progetto J-SAFE è stato coordinato con le iniziative pianificate all'interno di MINDB4ACT, nel quale erano previsti laboratori sperimentali, definiti 'laboratori viventi' (living labs), nei quali sviluppare attività innovative (progetti pilota). Pertanto, sono state connesse le risultanze dei 'laboratori viventi', implementati in MINDb4ACT, con i laboratori di ricerca giuridica in Germania, Italia e Spagna, realizzati nell'ambito di J-SAFE, che hanno visto la partecipazione di giudici, avvocati, investigatori, consulenti penitenziari, criminologi, componenti degli staff dei centri giovanili, psicologi ed educatori penitenziari, che rappresentano le figure professionali più idonee per identificare i punti chiave del fenomeno della radicalizzazione nelle carceri.

Infine, sfruttando i risultati di queste fasi preparatorie di analisi, è stato codificato un progetto pilota sperimentale teso a valutare la creazione di un nuovo modello di prevenzione digitale della radicalizzazione, una nuova frontiera della prevenzione giudiziaria. A tale scopo, è stato costituito un gruppo di lavoro con operatori penitenziari del Prap Triveneto e personale della Fondazione Agenfor International che ha sperimentato soluzioni tecnologiche ed operative all'interno del laboratorio forense recentemente istituito (*ELPeF - Experimental Lab of Penitentiary Forensics*), per validare empiricamente i risultati della ricerca teorica e dare sostanza agli input ricevuti dagli esperti nei diversi gruppi di lavoro.

Queste linee guida sono state quindi supportate da una ricerca approfondita nell'ambito delle prassi giudiziarie, con riferimenti incrociati rispetto ai dati sulle migliori prassi nazionali nei paesi in cui sono stati organizzati i laboratori di ricerca giuridica, come pure l'analisi di norme, prassi e politiche dell'Unione

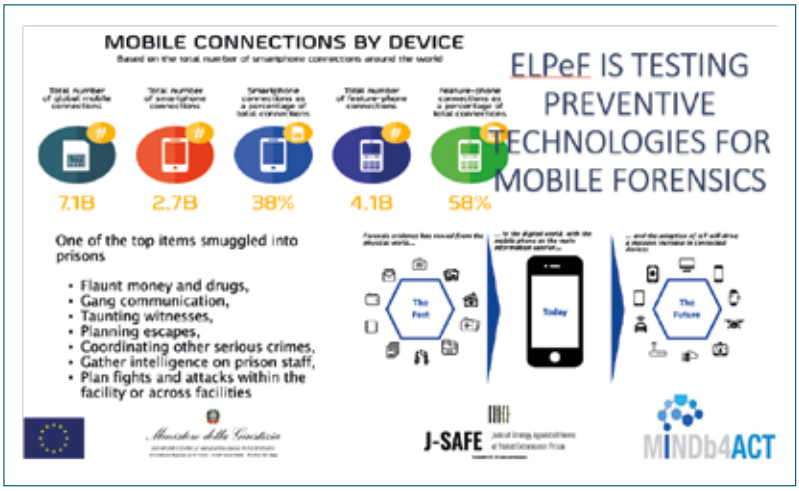
Europea e degli organismi internazionali. I risultati di questo complesso lavoro di analisi comparativa presentano variabili nazionali che differiscono da paese a paese, ma anche una serie di elementi comuni, che possono essere utili per costituire un progetto armonico di contrasto alla radicalizzazione in carcere con una prospettiva europea e un approccio completamente nuovo. Lo sforzo, in questa fase, è stato focalizzato sul tentativo di fornire una base comune alle prassi preventive, investigative e di analisi, nonostante le differenze dei contesti giudiziari nei diversi paesi e le difformità procedurali, in alcuni casi particolarmente marcate. I partecipanti ai diversi laboratori di ricerca giuridica e ai 'living labs' hanno identificato quattro elementi di criticità: (a) la mancanza di modelli legali, concettuali o teorici che spieghino come gli individui attraversano il processo dinamico della radicalizzazione; (b) come questi si relazionano con la violenza e il terrorismo, cioè quale sia il 'nexus' radicalizzazione-terrorismo e, conseguentemente, (c) quale sia la più appropriata strategia legale e giudiziaria per la prevenzione e il contrasto; (d) la tecnologia, ed in particolare i nuovi strumenti digitali e di comunicazione, sono stati individuati come i mezzi attraverso i quali innovare la prevenzione e sperimentare nuovi approcci al 'disengagement'.

Il manuale è diviso in tre parti.

La prima parte analizza i modelli di osservazione penitenziaria in diversi paesi. Attenzione particolare è stata riservata al modello italiano, in cui l'osservazione penitenziaria sul fenomeno della radicalizzazione si coniuga con l'Ordinamento Penitenziario. Il modello danese, che presenta caratteristiche sociali e multidisciplinari completamente diverse da quello italiano, è stato usato come elemento di confronto. In questo modo, si sono descritti i due diversi modelli di prevenzione presenti in differenti forme e gradi in tutti i paesi membri.

La seconda parte si pone l'obiettivo di costruire un modello standard di analisi preventiva, partendo dal presupposto che la prevenzione della radicalizzazione, anche se quest'ultima non costituisce reato, richiede una solida base giuridica e procedurale, in linea con la più recente giurisprudenza della Corte Europea dei Diritti dell'Uomo e con la dottrina emergente in Europa sulla differenziazione dei modelli di prevenzione giuridica, sociale e amministrativa. In questa seconda parte, che fa leva sulle precedenti ricerche di J-SAFE e MINDb4ACT, si evidenzia il ruolo della tecnologia, sia quale facilitatore dei processi di radicalizzazione (esempio droni o cellulari illegittimi), sia quale mezzo di prevenzione e contrasto (esempio tecniche di digital forensics).

Nell'ultima parte il lavoro definisce linee guida sperimentali di una nuova digital forensics penitenziaria, partendo da esperienze acquisite attraverso casi specifici e il lavoro di simulazione tecnologica effettuato all'interno del laboratorio ELPeF.



(Fig. 1 Aumento delle connessioni mobili)

Per quest'ultima parte sono state sviluppate linee guida con il coinvolgimento e il feedback di esperti interforze, sfruttando anche nuovissimi manuali sulle prove forensi digitali a livello internazionale.

II. LA PREVENZIONE DELLA RADICALIZZAZIONE TRA L'OSSERVAZIONE DELLA PERSONALITÀ E LA SICUREZZA

Il presente lavoro ha come background le precedenti ricerche condotte nell'ambito del progetto MINDb4ACT sul tema della radicalizzazione da un lato e, dall'altro, il lavoro di ricerca giuridico-dottrinale sulla prevenzione della radicalizzazione all'interno del progetto J-SAFE. La combinazione di tali ricerche evidenzia alcuni importanti elementi sui quali si basa il presente "Handbook for Prison Police and Security". Ciò che ne emerge sono infatti quattro diverse lezioni sulla base delle quali costruire le metodologie europee e internazionali di lavoro comune, pur nel quadro delle rilevanti differenze procedurali e legislative in materia di prevenzione e contrasto della radicalizzazione a livello di stati membri.

II.1 - STUDIO N. 1 - DUE DIVERSI APPROCCI

L'analisi e la casistica condotte nel 'living lab'1 di MINDb4ACT[1] hanno posto in evidenza due principali tendenze sul contrasto all'estremismo violento in Europa. Queste due tendenze molto diverse fra loro hanno un impatto sulle dimensioni giuridiche e operative delle pratiche di prevenzione e segnano una differenza sostanziale a livello politico. Definiamo le due tendenze come 'approccio welfare', da un lato, e 'approccio preventivo-securitario', dall'altro. Le differenze sono evidenziate da quattro diversi elementi, che descriveremo di seguito in maniera comparativa. Prima di tutto, come esempio di 'approccio welfare' possiamo utilizzare il cosiddetto 'modello Arhus' della Danimarca. Tale modello, che con alcune variabili e modifiche è utilizzato anche nei Paesi Bassi, in Finlandia, Svizzera e nel Regno Unito, ed è stato adottato dall'Unione Europea nei suoi documenti strategici, è costruito su una metodologia dal basso. Questo approccio non è stato imposto dallo Stato, quanto piuttosto sviluppato in collaborazione tra diversi ed egualmente importanti attori pubblici e privati, a livelli centrali e locali. Operatori locali hanno ricevuto alcune linee guida In seconda battuta, l'approccio nella sua interezza poggia su una serie di premesse fondamentali, fondate su di un'idea particolare del ruolo dello Stato sociale quale attore dei cambiamenti desiderati nelle devianze. I programmi di prevenzione in questi paesi si basano fortemente sulla collaborazione e il beneficio che deriva dalla fiducia tra le agenzie, da una parte, e la fiducia della popolazione, dall'altra. Di conseguenza, le iniziative sono fissate in una doppia agenda. Una è la sicurezza, cioè la protezione dello Stato (la personalità giuridica dello Stato e delle sue istituzioni), mentre l'altra è la responsabilità dello stato sociale per il benessere dell'individuo. Uno tra i principali risultati di questa doppia agenda è che il ruolo delle agenzie di intelligence e delle

1 MINDb4ACT, (2019), Living Labs context analysis, WP1 Living Labs: knowledge ecosystems for action, D1.1., p.46 e segg.

forze di Polizia, che sono gli attori tradizionali della sicurezza, è trasformato in direzione di modelli di polizia di comunità, stabilendo una sorta di centro di informazioni in ogni distretto di polizia (vedi di seguito). Le giurisdizioni e l'attribuzione dei poteri tendono a confondersi in questo modello, che vede una sostanziale degiurisdizionalizzazione delle prassi di prevenzione. Il terzo aspetto riguarda il modello multi-agenzia, che necessita di diversi meccanismi per condividere le informazioni tra una vasta gamma di agenzie pubbliche e private. Per questo motivo la Danimarca, così come numerosi altri Stati Membri, ha modificato l'Atto dell'Amministrazione della Giustizia Danese (par.115), stabilendo che le autorità possono condividere le informazioni relative ad un individuo se necessario per la cooperazione nella prevenzione del crimine o per la collaborazione tra polizia, servizi sociali e autorità in psichiatria e salute mentale, nel tentativo di aiutare individui socialmente vulnerabili. Tuttavia non è semplice coniugare queste politiche e prassi con le nuove regole dettate dal Regolamento Generale sulla Protezione dei Dati (GDPR). Come esempio comparativo di approccio securitario di prevenzione è possibile utilizzare il caso italiano, esemplare per la maggioranza degli Stati membri dell'Unione Europea, particolarmente nel Sud dell'Europa e nell'Est europeo, dove sono in vigore approcci strategici più tradizionali. Prima di tutto, il modello italiano si basa su un approccio centralizzato, che definisce una chiara gerarchia tra i diversi attori coinvolti nelle attività di prevenzione. Contrariamente all'approccio dal basso, tipico di altri Paesi, le strategie italiane di prevenzione sono per lo più il risultato di un processo giuridico di adeguamento e integrazione, basate su una cultura dell'antiterrorismo e attivate in maniera verticistica. L'iniziativa di solito prende avvio da agenzie ministeriali, spesso Forze dell'Ordine, basate su input internazionali, come l'UNSCR 21782[2]. La tabella sottostante descrive questo processo in Italia; in Europa lo stesso è articolato nelle tre fasi di riforma del 2001, 2005 e 2015, culminato nel 2017 con la nuova direttiva europea sul contrasto al terrorismo.

In secondo luogo, mentre in Danimarca la prevenzione segue un doppio percorso, protezione dello Stato e autolesionismo degli individui radicalizzati, sicurezza e welfare, in Italia l'approccio alla sicurezza si basa sull'ibridazione giuridica del nesso 'radicalizzazione/terrorismo', come in numerosi Stati membri. Il suo obiettivo è e rimane il terrorismo e ciò spiega perché strategie effettive di transizione (exit strategies) verso la riabilitazione di radicali e terroristi sono scarsamente implementate, mentre sono applicate forti misure di sicu-

2 Simili processi si sono verificati in alcuni Stati membri: France, LOI n° 2014-1353 du 13-11-2014, UK CT Security Act 2015, Spain Ley Orgánica 2/2015, Germany GVVG-Änderungsgesetz GV- VG-ÄndG, 12-6-2015, Belgium Loi visant à renforcer la lutte contre le terrorisme, 20-7-2015, Italy Decreto Legge 18 febbraio 2015, n. 7, Portugal Law 60/2015, Bulgaria 175, Malta ACT No. VIII of 2015, and Luxembourg Loi du 18 décembre 2015 modifiant le Code pénal et le Code d'instruction criminelle aux fins de mettre en oeuvre certaines dispositions de la Résolution 2178 (2014) du Conseil de sécurité des Nations Unies.

rezza, utilizzando gli strumenti giuridici della prevenzione securitaria. Mentre in Danimarca lo Stato ha l'obiettivo di proteggere l'individuo contro comportamenti autolesivi come la radicalizzazione, in Italia il principale obiettivo delle politiche di deradicalizzazione è la protezione della personalità giuridica dello stato e delle sue istituzioni. Questo è il bene giuridico da tutelare, per usare il linguaggio di Birnbaum.

Questo processo si verifica attraverso l'ibridazione della legge facilitata dalle definizioni paralegali di origine internazionale che sono entrate a far parte delle leggi, della giurisprudenza e dei programmi operativi degli Stati membri, seguendo i modelli tipici del 'legalismo globale'.[3]

Nonostante la sua complessità ed estensione, la cornice legislativa italiana, come tutti gli altri approcci legislativi centralizzati, non si riferisce direttamente alla radicalizzazione, che non è considerata un reato, ma solo al reato di terrorismo nelle sue varie sfumature e manifestazioni (reati connessi al terrorismo). Un fenomeno analogo è comune alla maggior parte dei paesi europei: esiste la legislazione sul terrorismo ma non sulla questione della radicalizzazione, che è sempre legata al terrorismo in maniera informale ("*la radicalizzazione che conduce al terrorismo*"). Nel periodo compreso tra gli anni 2001, 2005 e 2015, in previsione della riforma legislativa auspicata a livello internazionale, i diversi strumenti legislativi adottati coprivano pienamente l'area della pena per i reati di terrorismo o ad esso correlati, incluse le circostanze aggravanti, ma non affrontavano mai apertamente il fenomeno della radicalizzazione da un punto di vista giuridico, quanto piuttosto a livello di piani di azione socio-preventiva. Questo è il motivo per cui definiamo il fenomeno della radicalizzazione come una costruzione legale "ibrida".

Basato sui tre elementi precedentemente indicati, il caso della Spagna probabilmente si adatta alla "categoria di sicurezza preventiva", sebbene ci sia un chiaro e progressivo interesse a collaborare con la società civile adottando un approccio multi-agenzia. Prima di tutto, la cornice legislativa spagnola è ancora focalizzata principalmente sul terrorismo più che sulla radicalizzazione e il modello di prevenzione è basato su un approccio centralizzato. Infatti, lo Stato e gli uffici amministrativi sono riconosciuti come gli attori incaricati di implementare la strategia di prevenzione. Comunque, la società civile e i leader/rappresentanti delle popolazioni vulnerabili sono indicati come 'soggetti collaboratori' nell'architettura e implementazione della strategia[4]. Inoltre, benché il sistema penitenziario consideri come ugualmente importanti la sicu-

3 Cassese S., The Global Polity: Global Dimension of Democracy and the Rule of Law, Sevilla, Global Law Press, 2012.

4 CITCO (2015), Aprobado el Plan Estratègico Nacional de Lucha contra la Radicalizaciòn Violenta, p.9.

rezza e la riabilitazione/reintegrazione dei soggetti radicalizzati, fin dal 2014, un programma di trattamento mirato per tali detenuti non è stato ufficialmente implementato. Tuttavia, sono stati registrati dei progressi. Per un anno, un programma di trattamento mirato è stato testato su tre gruppi A, B e C. Tale programma mira ad ottenere lo sganciamento dei singoli dalla radicalizzazione (non de-radicalizzandoli), puntando sulla (ri) connessione dei detenuti con le loro famiglie e con le comunità locali. Nel caso della Catalogna, un programma di intervento destinato ai detenuti jihadisti è stato progettato e sarà implementato come esperienza pilota all'interno della cornice del progetto europeo PREPARE, in zone identificate come problematiche (ad es. Terrassa), adottando un approccio multi-agenzia.

La ***Strategia nazionale bulgara sul contrasto alla radicalizzazione e terrorismo*** (2015-2020) unifica i tre diversi elementi descritti precedentemente. Essa specifica i meccanismi per una migliore collaborazione con la società civile, le organizzazioni private, le comunità locali e i leader religiosi[5]. La Strategia mira inoltre a rafforzare gli sforzi di contrasto al terrorismo posti in essere dal governo coinvolgendo tutte le agenzie competenti e ottimizzando il coordinamento interagenzia.

II.1 - STUDIO N.2 - 'LA CONNESSIONE RADICALIZZAZIONE/TERRORISMO'

La ricerca di J-SAFE ha messo in evidenza un secondo importante elemento delle politiche di prevenzione dell'Unione Europea sulla radicalizzazione[6]. Dal report giuridico di J-SAFE[7] è emerso che mentre esistono diversi modelli preventivi a livello europeo per la prevenzione della radicalizzazione, i decisori politici europei hanno deciso di trattare tale tema in maniera parallela a quello del terrorismo a causa del fatto che il fenomeno della radicalizzazione, nelle sue multiformi dimensioni, è collocato in una zona grigia di estrema di rilevante importanza giuridica, con un grado di indeterminazione che potrebbe sfociare nell'arbitrarietà, se non appropriatamente regolamentato. Per questo motivo, l'attuale legislazione italiana sul terrorismo ha introdotto una complessa struttura di anticipazione della soglia di punibilità penale per le ipotesi di attentato in assenza di materialità degli atti e ha esteso l'azione penale a comportamenti molto vicini a quelli tipici della radicalizzazione, cioè quando il reato, la violenza o l'attacco ancora non sono compiuti, ma sussiste il pericolo connesso ad un'ipotesi anticipatoria di reato specifico. Questa è anche la dire-

5 Cfr. US Department of State, Country Reports on Terrorism 2017 – Bulgaria, 19 September 2018, disponibile all'indirizzo https://www.refworld.org/docid/5bcf1fb3a.html.

6 AGENFOR (2019), Harmonised Guidelines for Judges in Cases of Radicalisation leading to Terrorism, D3.8.

7 AGENFOR et al. (2019), Harmonised Guidelines for Judges.

zione intrapresa dalla nuova Direttiva (EU)2017/541, che è al centro delle politiche di prevenzione italiane e di molti altri paesi. Questa Direttiva aggiunge tre nuovi componenti alla definizione giuridica di terrorismo, che può essere facilmente usata per la prevenzione legale della radicalizzazione:

1 Definisce nuovi reati terroristici integrativi di quelli precedentemente esistenti (viaggi, sia all'estero che verso un paese europeo al fine di commettere una reato terroristico, per unirsi a un gruppo terroristico o per addestramento correlato al terrorismo; reclutamento per il terrorismo; fornire o ricevere addestramento in diverse forme; pubblico incitamento a commettere reati terroristici o sostenere il terrorismo, anche online; approvvigionamento di fondi per commettere reati terroristici o contribuirvi);

2 Criminalizza gli atti preliminari/preparatori;

3 Criminalizza l'intenzione di commettere specifici atti qualificati come terrorismo in assenza di 'tentativi e/o atti'.

Nell'ottica della stretta connessione fenomenologica tra radicalizzazione e terrorismo, la Direttiva (EU) 2017/541 fornisce alcuni chiarimenti a proposito della radicalizzazione ai punti 31, 32 e 33, che sono stati informalmente inseriti nelle legislazioni nazionali sul terrorismo e oggi rappresentano la base per le politiche di prevenzione. Ciò genera un serio problema di tecnica legale poiché non si tratta di un articolo della direttiva, ma solo di una parte del cosiddetto 'recital'. Con questa nuova legislazione si è aperta la strada per una legge soggettivistica verso reati basati sul profilo e le intenzioni dei criminali (*dolo specifica per delitti d'autore*), rispetto ai principi di base del diritto penale. In Italia la giurisprudenza e la prassi giuridica si sono mossi verso questa direzione, che integra la tradizionale giustizia prevista dal Codice Penale con quella parte delle misure di sicurezza finalizzate a prevenire reati gravi, che erano ampiamente utilizzate nelle strategie anti-mafia[8]. Perciò, come evidenziato dall'ampia giurisprudenza italiana prodotta in MINDb4ACT (D2.1), il perseguimento dei reati porta all'assimilazione dei casi di radicalizzazione a quelli di terrorismo, essendo questa una posizione giuridicamente più solida. Per esercitare le prerogative relative all'imposizione di misure afflittive, ma non sanzionatorie, tipiche della prevenzione e della sicurezza, è stata usata una serie di indicatori di pericolosità. Questa seconda strada, che oggi è la

8 Per l'Italia i casi di studio sulle misure preventive sono molto estesi: leading case C. edu, Plenary, sent. 6 November 1980, Guzzardi c. Italy, in particular §§ 90-103; C. edu, Plenary, sent. 22 February 1989, Ciulla c. Italy, in particular §§ 38-39; C. edu, Camera, sent. 22 February 1994, Raimondo c. Italy, in particular §§ 39-40; C. edu, Grand Chamber, sent. 6 April 2000, Labita c. Italy, in particular. §§ 193-197; C. edu, Section I, sent. 17 July 2003, Luordo c. Italy, in particular §§ 94-97; C. edu, Section III, sent. 1 July 2004, Vito Sante Santoro c. Italy, in particular §§ 42-46; C. edu, Section II, dec. 8 October 2013, Monno c. Italy, in particular §§ 21-22 and 26-28.

più comune ed è utilizzata sia dai giudici che dalla polizia, sembra essere rischiosa, poiché non ci sono basi scientifiche ed accademiche che attestino in modo univoco gli elementi di pericolosità sociale e criteri per effettuare la valutazione prognostica della pericolosità dei radicalizzati, che sono invece elementi fondanti del potere di ricognizione del giudice, assieme alla presenza di un quadro legislativo completo ed alla prevedibilità della legge. La cornice legislativa necessaria a garantire soprattutto i due elementi chiave per l'applicazione delle misure di sicurezza, ad es. "la qualità della legge" e la "prevedibilità", come riferito nella sentenza De Tommaso[9] della Corte Europea dei Diritti dell'Uomo, è assente nel caso della radicalizzazione. Tuttavia, sono state adottate, come principale strumento di prevenzione in questo specifico campo, numerose misure amministrative (esempio l'espulsione e rimpatrio forzato), sulla base dei rischi di sicurezza nazionale e ordine pubblico. In Italia, circa trecento individui sospettati di radicalizzazione e terrorismo sono stati rimpatriati attraverso misure amministrative.

II.3 - STUDIO N. 3 – COLLABORAZIONE PUBBLICO-PRIVATA

Il terzo pilastro di questo 'approccio preventivo-securitario' per contrastare la radicalizzazione è rappresentato da un concetto diversissimo di 'collaborazione multi-agenzia'. Mentre in Danimarca questo concetto implica un approccio collaborativo tra istituzioni pubbliche e private, assistenza sociale, sicurezza e agenzie di intelligence, in altri Stati membri, come l'Italia, la "collaborazione multi-agenzia" è intesa come una cooperazione tra le agenzie d'intelligence e diverse agenzie di sicurezza, con un alto livello di specializzazione di alcune forze speciali connesse alla polizia di prevenzione. In effetti, con la riforma del 2005, l'ambiguità normativa sul legame radicalizzazione/terrorismo ha generato in Italia una massiccia introduzione nella legislazione nazionale di misure amministrative di prevenzione, modificando anche alcuni principi istituzionali ed il necessario rapporto di checks and balances nei poteri politici, giudiziari ed esecutivi di alcuni stati membri, potenzialmente compromettendo i principi fondamentali dello stato di diritto. L'Italia può essere utilizzata ancora una volta come esempio comparativo per capire le tendenze europee, nonostante il fatto che sia stato mantenuto un buon livello di controlli ed equilibri, grazie al ruolo dei magistrati, dei giudici dell'antimafia nazionale e dell'antiterrorismo, rispetto ai poteri esecutivi dei Prefetti, dei servizi di polizia e di intelligence.

9 Nel caso "De Tommaso contro Italia" (n.43395/09), 23 febbraio 2017, la Gran Camera della Corte Europea di Strasburgo ha definito una serie di nuovi criteri relativi all'applicabilità delle misure di prevenzione. Questi criteri possono essere estesi con estrema precisione al fenomeno della radicaliz- zazione, intesi come indicatori di rischio sociale. Questo aspetto è l'oggetto del nuovo libro collettivo che sarà pubblicato a breve da Springer. Vi abbiamo contribuito con l'articolo di S. Bianchi (2018) "Radicalisation: no prevention without juridicalisation".

Preventive interception	L. 144/2005
Investigative interviews	
Undercover activity	L. 146/2006 e L. 136/2010
Expulsion of foreigners	L. 144/2005
Personal prevention measures of special surveillance and obligation to stay	D.L. 159/2011 e D.L. 7/2015
Passport Withdrawal	D.L. 7/2015
Internet Black Lists and online content removal	

(Fig. 2 Evoluzione delle misure di polizia in Italia)

Diversamente dalla polizia di comunità (community police), nella maggioranza degli Stati membri con una posizione più tradizionale a base costituzionale, la prevenzione della radicalizzazione, percepita come una minaccia alla sicurezza nazionale, all'ordine pubblico e come un'anticipazione del crimine (pre-crimine e indicatori di pericolosità), ha condotto alla costituzione di corpi di polizia altamente specializzati e ha contribuito a sfumare le tradizionali divisioni tra le attribuzioni delle agenzie di intelligence e i corpi di polizia (intelligence-led policing approach).

II.4 - STUDIO N. 4 – OSSERVAZIONE PENITENZIARIA E SORVEGLIANZA

Il mondo penitenziario ha attraversato alcune importanti trasformazioni a seguito delle nuove strategie di prevenzione, che hanno rafforzato le misure amministrative di sicurezza, come le espulsioni, rispetto a quelle giudiziarie e prodotto nuovi modelli informativi, modificando e integrando i tradizionali approcci di osservazione scientifica della personalità ed il peso delle misure di sorveglianza. Il tema dell'emergenza delle tendenze alla radicalizzazione e del fenomeno del jihadismo terrorista negli istituti penitenziari ha, infatti, imposto una distinzione, nell'ambito della popolazione ristretta, tra detenuti condannati per reati 'comuni' e i detenuti per reati di terrorismo. Per questi ultimi, in Italia, è prevista l'allocazione in sezioni dedicate, denominate Alta Sicurezza 2 (AS2), al fine di evitare influenze su altre categorie di detenuti, e sono previste, a mente della loro assegnazione in sezioni separate, forme particolari di trattamento, simili a quelle riservate ai detenuti ristretti per reati collegati alla criminalità organizzata. Modelli analoghi sono presenti in quasi tutti i paesi europei, con rare eccezioni. I detenuti in questi circuiti di sicurezza sono soggetti a un regime restrittivo, che ne limita l'assegnazione al lavoro all'esterno, ai permessi premio e alle misure alternative alla detenzione, esclusa la liberazione anticipata. Dunque, si tratta di un *regime ostativo altamente desocializzante,* che può avere conseguenze negative sulla società nel suo insieme, se non adeguatamente controllato[10].

10 Bianchi S., (2019), Restorative Justice beyond the emergency caused by terrorism, Justice Trends, n.5, July 2019

Per gli altri detenuti condannati per reati comuni, specifici controlli di tipo amministrativo sono stati istituiti al fine di prevenire e intercettare fenomeni della radicalizzazione e proselitismo o comprendere se tra loro vi siano detenuti che potrebbero essere vicini al terrorismo, anche se ristretti per altri tipi di reati. La vita negli istituti penitenziari, infatti, con la sua inevitabile promiscuità e sovente penalizzata da una condizione di sovraffollamento, comporta il rischio che i detenuti della prima categoria possano subire influenze e pressioni da parte di compagni di detenzione e gruppi estremisti, sia in forma diretta che indiretta.

Un doppio canale di informazione è stato perciò introdotto all'interno degli istituti penitenziari europei: da un lato modelli dell'*osservazione scientifica della personalità,* funzionale ai processi di riabilitazione e basata sul ruolo multidisciplinare dell'équipe di osservazione e trattamento e del GOT (Gruppo di Osservazione e Trattamento), ma dall'altro, forme di *'monitoraggio' di sicurezza o di sorveglianza,* funzionali alla prevenzione di rischi come la radicalizzazione, in cui la prevalenza spetta al ruolo della Polizia Penitenziaria e allo scambio di informazioni con l'Intelligence e altre Forze dell'Ordine.

Sul piano formale, che non sempre coincide con quello sostanziale, l'Italia presenta una buona prassi[11] riconosciuta nella capacità di equilibrare l'osservazione scientifica della personalità con metodi strutturati di sorveglianza, in un'ottica preventiva e investigativa. Di seguito verranno illustrati due pilastri di tale buona prassi attraverso cui ci si addentra in nuove sfide per la prevenzione della radicalizzazione nell'era digitale, che rappresentano il focus di questo Manuale.

II.4.A - OSSERVAZIONE SCIENTIFICA DELLA PERSONALITÀ

IN Italia la procedura dell'osservazione scientifica della personalità[12], posta in essere in progressivo distacco dal modello medico, a favore di un'analisi che valorizzi i profili psicologici e comportamentali, ed effettuata nei confronti dei detenuti condannati, rappresenta la peculiarità del trattamento rieducativo attuato nei confronti della popolazione detenuta condannata negli istituti penitenziari. In particolare, costituisce lo strumento mediante il quale viene sostenuto ed incentivato il processo di reinserimento sociale dei detenuti. L'obiettivo principale è l'accertamento dei bisogni dei singoli a mente delle carenze fisio-psichiche, affettive, educative e sociali eventualmente rilevate e delle altre cause del disadattamento sociale. A tale scopo è necessaria l'acquisizione documentale di dati giudiziari, penitenziari, clinici, psicologici

11 RAN, Collection of Inspiring Practices in https://ec.europa.eu/home-affairs/node/11686_en

12 In Italia è definita dall'art.13 della Legge n.354 del 1975 "Norme sull'ordinamento penitenziario e sulla esecuzione delle misure privative e limitative della libertà"

e sociali e la successiva valutazione integrata degli stessi. Lo svolgimento di colloqui, sulla base dei dati acquisiti, con il soggetto sottoposto ad osservazione da parte dello staff penitenziario competente, innesca un processo di revisione critica, cioè una riflessione sulle condotte antigiuridiche poste in essere, sulle motivazioni, sulle conseguenze negative e sulle percorribili azioni di riparazione delle conseguenze del reato. Dalle descritte attività si ricavano gli elementi indispensabili per la formulazione del programma individualizzato di trattamento, ed in rapporto al livello di adesione del detenuto alle offerte trattamentali ne viene registrata l'evoluzione della personalità; l'osservazione prosegue, dunque, nel corso dell'esecuzione della pena. Per ogni detenuto, in base ai risultati dell'osservazione, sono formulate indicazioni in merito al trattamento da attuare e viene compilato il relativo programma, integrato o modificato secondo le esigenze che si rilevano nel corso della detenzione, in vista del futuro reinserimento sociale. In base a quanto previsto dalle norme europee e del Consiglio d'Europa, le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione della persona condannata. Perciò, a mente del fatto che l'imputato non è considerato colpevole fino alla sentenza finale, nel rispetto del principio della presunzione di innocenza, è necessario tenere conto della posizione giuridica del detenuto. La sentenza penale di condanna deve, infatti, essere passata in giudicato, perché per gli autori di reato definitivi, l'azione di rieducazione e risocializzazione deve favorire un processo di cambiamento dei comportamenti nei confronti della famiglia e delle relazioni ai fini di un corretto reinserimento nella società libera, mentre per gli imputati questo si concretizza nella proposta di interventi volti a rinforzarne gli interessi umani, culturali e professionali. Non essendo praticabile nei confronti dei detenuti in attesa di giudizio l'osservazione scientifica della personalità, i relativi bisogni vengono rilevati dagli operatori penitenziari in occasione dei diversi momenti di vita detentiva grazie a strumenti formali che possono rappresentare elementi di valutazione del comportamento, ad esempio i colloqui e i rapporti con gli altri detenuti, con i familiari e con gli operatori stessi. L'adesione alle attività trattamentali previste dalla normativa penitenziaria deve in ogni caso essere volontaria e costituisce una libera scelta del detenuto di beneficiare degli elementi del trattamento penitenziario. Il programma di trattamento si compone degli interventi e delle offerte rieducative che gli operatori penitenziari suggeriscono di articolare nei confronti del detenuto nel corso dell'esecuzione della pena, ritagliati sulla personalità così come emersa dalle risultanze dell'osservazione scientifica. Il programma è articolato in una serie di offerte trattamentali e concepito per favorire il reinserimento sociale del detenuto una volta dimesso dall'istituto penitenziario. Si tratta di un trattamento "individualizzato", quindi concepito sulla valutazione delle specifiche condizioni del soggetto. L'attività di osservazione è tesa anche all'assegnazione dei detenuti condannati ai diversi istituti penitenziari e, all'interno di questi, alle differenti sezioni, all'individuazione delle priorità e delle modalità di impiego degli elementi del trattamento, costituiti dall'istruzione, dal lavoro, dalla formazione, dalla religione, dalle attività culturali, ricreative, sportive, dai contatti con il mondo esterno e dai rapporti

con la famiglia[13]. L'elemento religioso[14], che rappresenta uno dei principi su cui si basa il trattamento, disciplinato in Italia dall'art. 26 della L. 354/75, è un aspetto assolutamente non trascurabile nella vita detentiva dei ristretti. Devono essere favorite le pratiche religiose inerenti culti diversi da quello cattolico, nel costante tentativo di superare eventuali ostacoli all'esercizio di tale diritto. All'interno degli istituti penitenziari hanno accesso Ministri dei culti evangelista, buddista, ebraico, protestante, islamico e di altre ramificazioni delle religioni presenti anche nella società esterna. Il rispetto delle diversità religiose viene garantito anche mediante l'elaborazione delle tabelle del vitto e nella garanzia di pratica del culto come l'applicazione di regole ad hoc durante il periodo del Ramadan per i praticanti la religione islamica.
Anche i percorsi scolastici e di formazione professionale fungono da volano per un reinserimento bilanciato e sostenibile. La formazione scolastica e professionale è effettuata mediante l'organizzazione di corsi della scuola d'obbligo e di corsi di formazione professionale. All'interno delle strutture penitenziarie vengono favoriti percorsi scolastici a vari livelli, che rappresentano uno strumento di apprendimento indispensabile e propedeutico a gradi di integrazione sociale più complessi. L'offerta scolastica rappresenta infatti un'occasione di rivisitazione delle proprie scelte di vita per acquisire nuove abilità e per scardinare sistemi di valori spesso rigidi e derivanti da esperienze di vita pregresse, trasformando la detenzione da contesto di esclusione a opportunità di acquisizione di competenze e abilità linguistiche, sociali e professionali utili ad un efficace reinserimento.
Le competenze acquisite dalla persona detenuta permettono di concordare piani individualizzati che contemplano l'inserimento lavorativo attraverso la formazione, creando un portfolio delle competenze lavorative, spendibile nell'immediato sia all'interno che all'esterno della struttura penitenziaria. Le norme che disciplinano il lavoro penitenziario lo definiscono come "obbligatorio, non afflittivo, remunerativo", utile per ottenere un'appropriata formazione professionale al fine di un futuro reinserimento sociale prevedendo costante cooperazione con imprese pubbliche e private sia in relazione alla formazione che al lavoro vero e proprio. Le attività lavorative sono strutturate in base a norme analoghe a quelle vigenti nella società libera e prevedono la possibilità di essere integrate da iniziative formative e di tutoring. È infatti l'opportunità di mantenere un impiego fisso a seguito dell'espiazione della pena a rappresentare il principale requisito in un'ottica di riduzione della recidiva, supportando il percorso del detenuto verso il rientro nella società e consentendogli di ampliare le proprie prospettive e di esprimere le proprie potenzialità, anche con riguardo alla percezione che i ristretti hanno del tessuto sociale, interpretato generalmente come espulsivo. Si tratta di un risultato che richiede profonda sinergia tra l'Amministrazione Penitenziaria e le opportunità offerte dal terri-

13 In Italia regolato dall'art.15 dell'Ordinamento Penitenziario.

14 Regolato in Italia dall'Art.26 della Legge n.354/1975.

torio, poiché il trattamento rieducativo si articola proprio tra l'istituto penitenziario e il luogo in cui questo si colloca.
Per favorire il contatto con l'esterno, l'Ordinamento Penitenziario prevede inoltre benefici come i permessi premio, orari o di alcuni giorni, le uscite del detenuto dal carcere per motivi di studio o lavoro o per assistere i figli minori, e il coinvolgimento della comunità esterna mediante la partecipazione di privati, istituzioni, associazioni pubbliche o private, attivando collaborazioni con risorse esterne utili nel processo di risocializzazione dei detenuti.
L'attività di osservazione esita nella stesura di una relazione di sintesi che contiene in forma sinottica i risultati conclusivi del periodo di osservazione iniziale. Gli operatori che compongono l'équipe di osservazione e trattamento predispongono contestualmente il programma individualizzato di trattamento, soggetto all'approvazione, mediante decreto, del Magistrato di Sorveglianza che, nel caso di violazione di diritti dei detenuti, provvede alla restituzione alla Direzione dell'istituto penitenziario, che vi apporterà le necessarie modifiche eliminando le violazioni identificate. Le risultanze del trattamento individualizzato vanno a coadiuvare le decisioni dei Magistrati di Sorveglianza per quanto concerne la concessione di benefici penitenziari e misure alternative. I contenuti del documento di sintesi definito dall'équipe devono essere condivisi con tutti gli operatori del Gruppo di Osservazione e Trattamento coinvolti nella presa in carico del detenuto. Prima di formalizzare il documento è indispensabile che l'équipe certifichi ed acquisisca la collaborazione e il consenso del detenuto in merito alle proposte trattamentali sviluppate nel corso dell'osservazione, al fine di escludere la strumentalità dei comportamenti. A seguito dell'approvazione del Magistrato la relazione verrà formalizzata nel "Patto trattamentale", siglato dal detenuto alla presenza del Direttore del carcere e contenente gli obiettivi specifici che il Gruppo di Osservazione e Trattamento monitorerà durante l'applicazione del programma, e che verrà integrato o modificato a seconda delle esigenze che si palesano nel corso dell'esecuzione penale. All'interno del documento saranno specificate le finalità (definizione di ipotesi intramuraria oppure esigenza di fornire alla Magistratura le informazioni necessarie alla valutazione della concessione di benefici), le indicazioni dell'équipe in merito al trattamento individualizzato intramurario o alle eventuali ipotesi trattamentali extra murarie. Nella prima parte della relazione sono indicati gli elementi necessari alla comprensione del soggetto in ordine al suo vissuto personale, familiare e sociale, mentre nella seconda parte, conseguente alla precedente, si delineano le linee fondamentali degli interventi da attuare ai fini del reinserimento sociale del detenuto. Il documento di sintesi può essere organizzato come segue: dati anamnestici e socio-familiari, dati relativi al soggetto in osservazione, comprendenti carenze fisio-psichiche, affettive, educative e sociali, dati e notizie necessari alla comprensione del vissuto del detenuto, descrizione del contesto soggettivo, del contesto familiare, e delle problematiche o potenzialità, descrizione del soggetto nel contesto di esecuzione penale, delle relazioni instaurate con gli operatori penitenziari e con i compagni di detenzione, del comportamento del detenuto nelle attività trattamentali già sperimentate, della sfera emozionale del detenuto con rife-

rimento al rapporto con i familiari in occasione dei colloqui, individuazione e descrizione di quali offerte trattamentali contemplate nel progetto d'istituto sono congrue rispetto al soggetto, progettazione dell'ipotesi trattamentale e tempistica, valutazione del livello di condivisione da parte del detenuto dell'ipotesi trattamentale, individuazione e descrizione delle risorse interne ed esterne da coinvolgere, indicazione dei momenti di verifica che l'équipe riterrà opportune e con quali modalità.

La Grecia applica un sistema simile di osservazione dei detenuti, che tuttavia non è creato ad hoc per l'identificazione dei detenuti radicalizzati, o di quelli vulnerabili alla radicalizzazione e alla violenza. Il sistema di osservazione in essere è implementato dai funzionari penitenziari e ha l'obiettivo di relazionare alle autorità penitenziarie e giudiziarie, relativamente al comportamento del ristretto e il progresso rieducativo in generale. Nello specifico disposto di legge, l'osservazione può influenzare lo status penale del detenuto (liberazione anticipate, permessi, ecc.) tuttavia, con l'eccezione del sostegno garantito a tutti I detenuti negli istituti penitenziari (supporto sociale, sostegno e trattamento alla salute psicologica e altri servizi connessi). Tali monitoraggi nel sistema greco non sono solamente effettuati nel caso in cui si manifestino comportamenti estremisti e violenti (de-radicalizzazione), ma sono generali. Dunque in Grecia una strategia mirata è assente.

Tutti i detenuti nuovi giunti in **Bulgaria** sono soggetti ad una valutazione del rischio di recidiva e pericolosità (Art. 55 dell'Atto di esecuzione delle sanzioni penali e detenzione in custodia cautelare). La metodologia della valutazione del rischio usata per entrambi i tipi di valutazione si basa sul Sistema di Valutazione del Reo (OASys), che comprende 14 sezioni. Ogni sezione si riferisce a uno specifico fattore connesso al reato. Al termine di ciascuna sezione sono presenti domande che permettono allo staff penitenziario di collegare diversi aspetti non solo al reato commesso ma anche al rischio di pericolosità per l'individuo, per lo staff penitenziario, e/o la società.

La metodologia è stata sviluppata sulla base di una ricerca che dimostra che il comportamento passato dell'individuo può servire come elemento determinante nella previsione del suo comportamento futuro. Gli elementi che caratterizzano l' OASys dovrebbero soddisfare i seguenti criteri:

- essere collegati al rischio di recidiva e successiva condanna;
- essere collegato al rischio di pericolosità;
- essere un fattore chiave per altri tipi di valutazione.

La metodologia mette insieme i fattori di rischio statici e dinamici per:
- verificare la possibilità di commettere nuovamente un reato;
- definire e classificare i bisogni del colpevole in base al reato commesso;
- agevolare la gestione del rischio di recidiva e il rischio di pericolosità; ▪ collegare la valutazione con il programma di esecuzione penale;

- determinare il bisogno di future valutazioni specifiche;
- quantificare il grado di cambiamento avvenuto lungo la durata della condanna.

L'accertamento del rischio di recidiva e pericolosità costituisce una valutazione del condannato e dei cambiamenti dipendenti dal comportamento. I risultati ottenuti sulla base dell'accertamento possono essere usati per segnalare l'introduzione dei cambiamenti nel sistema per l'espletamento della condanna; la possibilità di un rilascio con la condizionale, e la pianificazione di misure per il lavoro individuale e di gruppo, incluse attività specifiche.

Lo scopo principale dell'accertamento è di identificare se il condannato:

- costituisce un serio pericolo per gli altri;
- costituisce un serio pericolo per lo staff penitenziario;
- costituisce un serio pericolo per sé stesso;
- rischio di evasione, clandestinità, sorveglianza, o abuso della fiducia;
- costituisce un rischio dovuto a fragilità.

II.4.B - MONITORAGGIO DELLA RADICALIZZAZIONE

Il monitoraggio della radicalizzazione è un'osservazione empirica attraverso la quale accertare l'effettiva adesione a idee estremiste da parte di alcune tipologie di detenuti, in particolare musulmani e stranieri, predisponendo, in caso di imminente scarcerazione, segnalazione alle forze dell'ordine locali per attuare le pertinenti misure di prevenzione.
Trattandosi di un processo complesso e delicato, prevede un completo coinvolgimento e una collaborazione sinergica e coordinata degli operatori penitenziari[15]. E' necessario il coinvolgimento dello staff multidisciplinare e degli esperti previsti dall'art.80, Legge 26 luglio 1975 n.354 in quanto l'attività di monitoraggio non deve limitarsi alla (mera) attività di osservazione ex art. 27 D.P.R. 230/2000 , ma deve costituire l'input per la pianificazione di una efficace strategia di prevenzione e de-radicalizzazione[16].
Le risultanze di questo tipo di attività vengono condivise, nell'ottica della cooperazione con le altre istituzioni deputate alla raccolta e all'elaborazione di tali informazioni, mediante il Nucleo Investigativo Centrale (NIC) e le sue articolazioni regionali (NIR), presso cui convergono tutte le informazioni raccolte dagli istituti penitenziari in merito ai soggetti segnalati per presunte attività di proselitismo, reclutamento e radicalizzazione. Tale analisi del fenomeno si ar-

15 Lettera circolare n.GDAP-0388766 del 20/12/2019 "Direttive sull'attività di osservazione del fenomeno della radicalizzazione violenta e del proselitismo in ambito penitenziario"

16 Ibidem

ticola in tre diversi livelli di osservazione[17]: 1° livello - classificato alto: soggetti ristretti per reati connessi al terrorismo internazionale e quelli di particolare interesse per atteggiamenti che rilevano evidenti forme di proselitismo, radicalizzazione o di reclutamento per estremismo islamico/jihadismo; 2° livello - classificato medio: detenuti che all'interno dell'istituto hanno posto in essere atteggiamenti che fanno presupporre la loro vicinanza alla ideologia jihadista e, quindi, ad attività di proselitismo e reclutamento; 3° livello - classificato basso: detenuti nei confronti dei quali le notizie risultano generiche e, pertanto, richiedono un ulteriore approfondimento sulle determinazioni utili. Le informazioni considerate significative, sebbene non definiscano precisamente un percorso generale di radicalizzazione a causa dei numerosi elementi che contribuiscono alla strutturazione del processo ideologico e decisionale di ciascuno, sono state individuate a mente di alcune caratteristiche rilevate in numerosi casi, quali la giovane età, i precedenti penali, l'occupazione lavorativa, la situazione familiare, il rapporto con la religione e la presenza di disturbi mentali. Lo staff penitenziario dispone di una serie di indicatori sulla radicalizzazione che permettono di evidenziare situazioni meritevoli di attenzione, come cambiamenti fisici (modo di vestire, crescita della barba) o nel comportamento (intensificazione della preghiera, ostilità nei confronti del personale), e comunque connessi all'osservazione della routine quotidiana, all'organizzazione delle camere di pernottamento, al comportamento nei confronti di altre persone e a eventuali commenti sugli eventi politici e di attualità.

Inoltre, le informazioni relative alla comunicazione dei detenuti con l'esterno sono analizzate mensilmente per il primo livello, ogni due mesi per il secondo livello e semestrale per il terzo livello. Precipua importanza assumono dunque il cambiamento, l'isolamento dei detenuti o la formazione di sottogruppi e l'allontanamento dal nucleo familiare. Tali indicatori, estrapolati dal manuale "Violent radicalization - recognition and responses to the phenomenon by professional groups concerned", sono stati realizzati dagli Stati Membri dell'Unione Europea. È importante ricordare che non si tratta di prove o indicatori di rischio informatici di effettiva radicalizzazione, bensì di segnali che devono essere esaminati nell'ambito di un contesto di caratteristiche personali e di specifiche circostanze di un dato caso, al fine di non trarne conclusioni arbitrarie, ma di stimolare costantemente, prudentemente e con differenziata osservazione da parte del personale.

Questi soggetti vengono segnalati allo staff multidisciplinare del carcere per la presa in carico e per l'individuazione delle strategie di depotenziamento più idonee, che si concretizzano mediante una serie di specifiche misure di controllo preventivo. È importante sottolineare che i detenuti sotto osservazione e monitorati per fenomeni di radicalizzazione, diversamente dai membri dei

17 Ibidem

gruppi di criminalità organizzata, non sono limitati nei loro diritti fondamentali: hanno accesso alle stesse opportunità (lavoro, comunicazioni, contatti, ecc.) degli altri detenuti e quando sono adottati provvedimenti (ad esempio trasferimenti), questi sono effettuati nella piena applicazione delle leggi, regolamenti e le giurisdizioni che coinvolgono tutte le Autorità competenti.

Il flusso di informazioni sul comportamento, non forensi e non giudiziarie, con rilevanza di sicurezza, è tenuto separato dagli elementi del trattamento: i due elementi sono complementari ma non si influenzano l'un l'altro perché tutti i detenuti sono considerati uguali davanti alla legge e posso accedere agli stessi servizi. Per questa ragione, i dati sul monitoraggio sono solo raccolti, utilizzati e condivisi a scopo preventivo, da una prospettiva di sicurezza. Lo scambio delle informazioni di sicurezza e socio-riabilitative si realizza all'interno di un percorso istituzionale e tra professionisti autorizzati dalla legge, mantenendo chiare le differenze giuridiche, operative e socio-riabilitative tra le competenze e i mandati dei diversi attori pubblici e privati. Il Nucleo Investigativo Centrale contribuisce alla composizione di complessi incastri di informazioni dal punto di vista della sicurezza, unitamente ad altre forze di polizia. I dati relativi alla vita intramuraria del detenuto e al contatto con il mondo esterno sono informazioni qualitative di sicurezza, che non fanno parte del fascicolo del detenuto e non sono accessibili ai detenuti o ai loro avvocati. Questi dati non possono essere scambiati con altri corpi pubblici o privati, a meno che una misura giudiziaria non sia assunta dal Giudice per autorizzarlo. L'analisi condotta dal Nucleo Investigativo Centrale sui soggetti radicalizzati e terroristi è poi incanalata verso il Comitato di Analisi Strategica Antiterrorismo (C.A.S.A.)[18], se appropriato.

La Sicurezza Preventiva è il risultato delle attività professionali delle Forze di Polizia e dell'Intelligence. Il C.A.S.A. è al vertice del flusso di informazioni sulla prevenzione securitaria. Viceversa, le informazioni relative a potenziali crimini, che costituiscono la base per le indagini, sono trasmesse dalla polizia giudiziaria della Polizia Penitenziaria alle competenti Autorità Giudiziarie. Le informazioni di intelligence possono fornire apporti pre-investigativi per le indagini; si tratta di attività ben regolate dalla legge italiana, con numerose garanzie per i sospettati. Una caratteristica chiave del processo di monitoraggio è infatti rappresentata dalla gestione di un flusso di informazioni dalla periferia al di-

18 Il C.A.S.A., istituito nel 2004, è un organismo che svolge analisi generale e ha compiti di valutazione di documenti di particolare rilevanza relativi al terrorismo nazionale e internazionale. È un organismo permanente che si compone di tutte le Forze dell'Ordine sotto l'egida dell'Ufficio Centrale della Polizia Preventiva (Ministero dell'Interno). Il CASA si incontra settimanalmente per valutare le infor- mazioni sulla minaccia terroristica nazionale e internazionale per attivare la necessaria prevenzione e le misure di contrasto. I Magistrati e Procuratori assumono le iniziative quando le informazionidi sicurezza relative ai cittadini dell'Unione Europea passano dal pre-crimine all'area legale; sono responsabili per il coordinamento delle indagini formali e per incaricare la polizia giudiziaria per le indagini operative.

partimento centrale, dove sono raccolti e analizzati i dati. Una sala situazioni attiva 24 ore su 24 e 7 giorni su sette permette di avere un monitoraggio costante e un sistema di alert a tutti i livelli, e condivide le informazioni dal livello territoriale a quello centrale in tempo reale. Gli eventi di radicalizzazione sono integrati in un sistema di allerta per eventi critici che opera in tempo reale.

A seconda dell'obiettivo finale (sicurezza o reintegrazione), ciascun attore coinvolto mantiene il proprio profilo istituzionale all'interno di chiare gerarchie e procedure istituzionali e utilizza i propri metodi e strumenti per raggiungere le diverse priorità nell'interesse comune. Ciò garantisce un pieno sfruttamento dei poteri socio-istituzionali e aiuta ad evitare la loro sovrapposizione.

In **Spagna**, il Sistema Penitenziario (sia a livello nazionale che catalano) prevede protocolli di valutazione del rischio per individui a rischio di radicalizzazione o già radicalizzati, sistemi di classificazione dei criminali così come programmi di formazione per il personale penitenziario. A livello nazionale, in base alla direttiva nazionale 8/2014, il Segretario Generale degli Istituti Penitenziari (SGIP) ha adottato un programma di sorveglianza e monitoraggio per detenuti condannati per reati di terrorismo o per avere instaurato relazioni con gruppi e attività terroristiche (FIES 3). Questo protocollo ha l'obiettivo di prevenire il proselitismo estremista islamico e il reclutamento nelle carceri. A seconda del livello di radicalizzazione, i detenuti collegati in qualche modo al jihadismo sono suddivisi in 3 categorie: A, B e C. Il Gruppo A (rischio alto) include i detenuti condannati per reati di terrorismo jihadista; il Gruppo B (rischio moderato) si riferisce ai detenuti coinvolti nelle attività di proselitismo e reclutamento; il Gruppo C (rischio basso) riguarda i detenuti condannati per altri reati che sono stati individuati come vulnerabili al reclutamento e/o indottrinamento. La rilevazione delle informazioni sui detenuti e l'attività di monitoraggio sono gestite da gruppi specializzati di funzionari penitenziari e membri delle forze di polizia appositamente addestrati per individuare i segnali, monitorare il detenuto e analizzare le informazioni raccolte. Il fatto che la polizia e lo staff penitenziario lavorino insieme in questo gruppo facilita lo scambio di informazioni dall'esterno all'interno del carcere. Inoltre, tutti gli staff penitenziari all'inizio della loro carriera ricevono una formazione che include un modulo sulla radicalizzazione, sull'individuazione e sul monitoraggio di tale fenomeno e sulla conoscenza degli indicatori utilizzati per identificare il rischio di radicalizzazione.

Nelle carceri e nei sistemi di correzione greci, il monitoraggio della radicalizzazione e dei fenomeni estremisti è stato implementato in base a procedure di osservazione e relazionando come sopra descritto. Attraverso le osservazioni e i colloqui dei funzionari penitenziari e giudiziari competenti, vengono raccolte significative informazioni, che frequentemente si rivelano di cruciale importanza. Questa intelligence interna è raccolta ed elaborate in un database centrale, che tiene informate le autorità penitenziarie e giudiziarie sul grado di rischio di ciascun detenuto e sul progresso rieducativo. Nonostante non ci sia una categorizzazione ufficiale di rischio alto, medio o basso dei detenuti, i singoli istituti

penitenziari mantengono un meccanismo sistematico di monitoraggio, specialmente focalizzandosi sul terrorismo e sui detenuti estremisti violenti. Tuttavia, questa intelligence funziona come un gruppo di conoscenza all'interno del carcere ed è utilizzata solo per finalità correttive e riabilitazione. C'è una lacuna nel flusso di informazioni e attualmente ciò non è stato formalizzato tra le autorità penitenziarie, la polizia e le forze di polizia, e l'intelligence comunitaria. La condivisione delle informazioni si realizza eccezionalmente, sotto la supervisione dell'autorità giudiziaria, principalmente per motivi di prevenzione da forte minaccia terroristica e altre minacce criminali.

In **Bulgaria** i programmi esistenti per lo sviluppo del personale permettono al personale penitenziario di potenziare la comprensione del contrasto alla radicalizzazione e di imparare come identificare e indicare i segnali di radicalizzazione. Questo tipo di formazione permette al personale penitenziario di essere adeguatamente preparato e svolgere le proprie funzioni professionali nel caso si riscontrino casi di radicalizzazione. Il programma di formazione per la lotta alla radicalizzazione prevede lezioni e seminari che coprono una vasta gamma di argomenti, incluso il processo di radicalizzazione e le credenze e ideologie che possono alimentarlo, i fenomeni del terrorismo e dell'estremismo violento, la deradicalizzazione e lo sganciamento. Il materiale del corso è adattato ai bisogni del personale penitenziario e fornisce dettagli sui diversi strumenti normativi e di polizia (ad es. documenti europei, normativa nazionale e strumenti strategici, linee guida del Consiglio d'Europa) Al fine di favorire la tolleranza etnica e religiosa tra i detenuti nelle carceri, sono stati realizzati i seguenti programmi:

- promozione della tolleranza;
- tolleranza in carcere, tolleranza nella vita;
- riduzione della violenza etnica e promozione della tolleranza.

In conclusione, non fa parte dell'obietto di questo deliverable definire quali potrebbero essere le migliori o più promettenti prassi tra i due modelli comparati. Comunque, è chiaro dagli esempi comparativi derivanti dalle ricerche parallele svolte in MINDb4ACT e J-SAFE che l'Unione Europea, in linea con gli stati nazionali, ha sinora deciso di non regolamentare giuridicamente questo specifico tema della prevenzione della radicalizzazione e dell'estremismo. In gran parte, ciò è dovuto alla difficoltà di produrre un'immagine congruente nello stretto percorso tra le nuove norme anti-terrorismo, che anticipano la soglia di punibilità penale e svincolano il crimine dall'atto e dalla giurisdizione territoriale, e le disposizioni della convenzione della Corte Europea dei Diritti dell'Uomo, che fissano invece rigidi confini a tutela delle libertà fondamentali difficilmente derogabili. Inoltre, i decisori politici hanno lasciato ampio spazio per tutte le possibili soluzioni preventive, dalle misure socio-preventive e di collaborazione pubblico-privata, a rigide misure preventive di sicurezza basate sulle espulsioni, come parte dell'area della cooperazione giudiziaria che ha l'obiettivo di prevenire la radicalizzazione.

II.4.C - DALLE MISURE ALTERNATIVE ALLE PROCEDURE GIUDIZIARIE E AMMINISTRATIVE

La natura giuridicamente ibrida del fenomeno della 'radicalizzazione', che sorge a metà strada tra le procedure giudiziarie, le misure di prevenzione legale e le attività di riabilitazione sociale, richiede la valutazione di percorsi alternativi all'esercizio dell'azione criminale e all'applicazione di rigide misure preventive e di sicurezza, quando le sentenze giudiziarie non riconoscono un chiaro collegamento tra la radicalizzazione e i reati legati al terrorismo.

Uno dei settori più sensibili a questo aspetto è il sistema penitenziario. Infatti, questo ambito è considerato prioritario dai documenti strategici dell'Unione Europea poiché fenomeni di radicalizzazione possono essere rafforzati dalle condizioni di detenzione. Lo sviluppo di strategie innovative e soluzioni il cui obiettivo è ridurre il potenziale violento dei comportamenti radicali è al centro di numerose Raccomandazioni, Decisioni e Direttive Europee che hanno focalizzato l'attenzione sugli effetti positivi delle misure alternative alla semplice condanna ed esecuzione penale in carcere. L'obiettivo delle diverse norme europee è certamente quello di proteggere le vittime, ma questo concetto può essere facilmente esteso a tutti gli attori vulnerabili' del processo di radicalizzazione esposti al rischio di essere trascinati nel terrorismo. Come riferito nella Direttiva Antiterrorismo, la soluzione è delineata dalla prospettiva della giustizia riparativa, che ha l'obietto di risolvere e ridurre il conflitto e creare una società più sicura.

Alcune delle indicazioni con impatto europeo e transnazionale sono: la Raccomandazione relativa alla posizione delle vittime nell'ambito del diritto penale e del processo penale (Commissione dei Ministri del Consiglio d'Europa - Raccolta N. R (85) 11 di 28 del 28.6.1985), la Risoluzione sullo Sviluppo e sull'Esecuzione degli Interventi di Giustizia Riparativa e di Mediazione nell'ambito della Giustizia Penale (United Nations Economica and Social Council N. 1999/26 del 28.7.1999), la Raccomandazione sulla Mediazione in Questioni Penali (Committee of Ministers of the Council of Europe No. R (99) 19 adottata il 9.15.1999), la Dichiarazione di Vienna sul Crimine e la Giustizia (X Congresso delle Nazioni Unite sulla Prevenzione del Crimine e il Trattamento dei detenuti – Vienna 10-17 Aprile 2000), la Risoluzione sulla Dichiarazione di Vienna sul Crimine e la Giustizia: Nuove Sfide nel ventunesimo secolo (Assemblea Generale delle Nazioni Unite – N. 55/59 del 4.12.2000), la Decisione Quadro del Consiglio dell'Unione Europea sulla posizione della vittima nei procedimenti penali (2001/200/JHA del 15.3.2001) sostituita dalla Direttiva EU 2012/29 del 25.10.2012. [19]
La possibilità di ricorrere alla giustizia riparativa, o a forme alternative di mediazione sociale come parte delle misure socio-riabilitative, varia in relazione

19 Cfr. Negri A., "La radicalizzazione jihadista negli istituti di pena", 14 dicembre 2018 su www.ispionline.it – sito dell'Istituto per gli Studi di Politica Internazionale

ai reati e alle condizioni in cui un caso può aver avuto inizio in base alla legislazione di ogni Stato Membro. Nonostante la differenza delle forme esistenti di giustizia riparativa, tutte condividono due caratteristiche principali:

1. l'adesione volontaria all'attività riparativa;

2. la necessità che il percorso e l'attività siano guidate da soggetti terzi, imparziali e specificatamente formati per questo tipo di intervento.

Le principali forme di giustizia riparativa includono:

1. invio di una lettera di scuse;

2. incontri di mediazione estesi che tendono a creare un dialogo con i gruppi parentali e/o tutti i gruppi coinvolti nella commissione di un crimine (consulto familiare/di comunità di gruppo);

3. svolgimento di attività lavorative a favore della vittima (Servizio personale alla vittima) o a favore della comunità (Servizio alla comunità);

4. mediazione tra l'autore del reato e la vittima (mediazione vittima-reo) e

5. incontri tra le vittime e i trasgressori per atti simili a quelli di cui sono stati vittime (Victim/Community Impact Panel).

Negli ultimi anni, le Agende europee hanno richiesto la profusione di importanti risorse, in linea con le priorità individuate a livello nazionale e transnazionale per la lotta contro il radicalismo violento nelle istituzioni penitenziarie. Le emergenze identificate dall'UE e la specificità del mandato istituzionale degli organi giudiziari hanno motivato il concepimento e lo sviluppo di soluzioni e strategie innovative per combattere il fenomeno del radicalismo violento. Alcuni paesi membri hanno dovuto affrontare attacchi terroristici fondati sul credo religioso. Non sembra superfluo sottolineare che il terrorismo per motivi religiosi non sembra essere l'unica forma di radicalismo violento presente oggi nella nostra società, sia in termini di prevenzione del fenomeno su scala europea che in termini di complessità e vastità dello stesso. Paesi come l'Italia, l'Austria, la Bulgaria, la Croazia e Cipro non hanno subito attacchi nei loro territori, ma va sottolineato che nessun paese è esente dalla responsabilità di contrastare i processi di radicalizzazione, segnatamente nel contesto della detenzione. Come dimostrato dai dati finora raccolti, la possibilità per i detenuti di essere esposti a ideologie estreme e violente, in modo più o meno cosciente, è più alta che in altri contesti[20].

20 "Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power" adottata dall'Assemblea Generale delle Nazioni Unite nel 1985.

Le autorità giudiziarie sono attori cruciali in tutti gli Stati in quanto rendono possibili diverse forme di giustizia e insieme agli operatori dei servizi sociali sono in grado di ricostruire le fratture causate dal conflitto/crimine, offrendo sia alla società/comunità colpita che al trasgressore la possibilità di una reciproca espressione del loro dolore. Lo scopo di diffondere forme di giustizia riparativa si basa sull'intenzione di passare da un discorso sulla violenza a un discorso sulla sofferenza. Le suddette pratiche di giustizia condividono l'intento di promuovere un metodo di riparazione del danno causato e una riconciliazione (simbolica o specifica) tra le parti, rafforzando così il senso di sicurezza collettiva. Non è necessario che un cittadino europeo sia direttamente colpito da un reato penale connesso a crimini terroristici perché avverta che la propria sicurezza è sempre più a rischio a causa di queste nuove forme di criminalità. Infatti, coloro che "individualmente o collettivamente hanno subito pregiudizi, in particolare un'offesa alla loro integrità fisica o mentale, sofferenza morale, la perdita materiale o un grave attacco ai loro diritti fondamentali a causa di azioni o omissioni che violano le leggi penali in vigore in uno Stato membro, compresi gli abusi di potere criminosi" si sentono colpiti nel loro insieme[21].

II.4.D. LA PREVENZIONE NELL'ERA DIGITALE

Nonostante le differenze legali e procedurali, vi è un elemento di grande importanza che emerge dalle ricerche condotte nel progetto MINDb4ACT, in particolare dalla relazione delle visite di studio (Deliverable 3.1), dal "Database on various court-decisions on human rights, radicalisation and security" (Deliverable 4.1) e, infine, l'Elenco dei Casi studio (Deliverable 1.2), così come dai laboratori legali del progetto J-SAFE in Germania, Italia e Spagna (D 3.4, 3.5, 3.6 e 3.7). Questo elemento comune è dato dal profondo cambiamento che le tecnologie digitali e di comunicazione hanno impresso al mondo della sicurezza e prevenzione, da una parte e, dall'altra, come esse abbiano sviluppato modelli di prevenzione e d'indagine che modificano profondamente le prassi operative delle forze di polizia e degli operatori.

L'analisi dei casi di radicalizzazione mostra con estrema chiarezza che le tecnologie digitali, che ormai sono parte della vita di ognuno, possono trasformarsi in grandi facilitatori sia di processi di integrazione sociale, poiché tendono a conservare anche nella distanza reti sociali ed opportunità di lavoro, ma anche di fenomeni di radicalizzazione e terrorismo, poiché espongono fasce vulnerabili ad attività di propaganda, indottrinamento, reclutamento e auto-reclutamento. Inoltre, l'evoluzione delle tecnologie, dalla crittografia alla miniaturizzazione dei sistemi, produce nuovi modus operandi del mondo del

21 Geosatis (2019), GPS Technology – A tool for the reintegration of radicalized offenders into soci- ety, Justice Trends, n.5, July 2019

crimine, così come delle forze di polizia impegnate nelle azioni di prevenzione e contrasto. Questo trend globale non esclude il mondo penitenziario, in cui le tecnologie sono penetrate in diversi modi: innanzitutto, quale componente legale dei processi di rieducazione (dalla formazione alla comunicazione con le famiglie, fino agli strumenti di monitoraggio delle misure alternative) o del management penitenziario (ad esempio applicazioni per gli eventi critici in caso di radicalizzazione ormai diffuse a livello europeo, ai software di offender management, ai sistemi biometrici di supporto agli uffici matricola, alle telecamere nella gestione della cosiddetta 'sorveglianza dinamica' ecc.). In secondo luogo, anche quale importantissima componente illegale, come documentato dai massicci sequestri di telefoni cellulari rinvenuti in possesso dei detenuti, spesso miniaturizzati di produzione cinese, o dalla cattura di droni illegali, usati come nuovi strumenti per trasportare droghe, SIM card e altri oggetti non consentiti all'interno delle carceri.

In termini di mantenimento dei rapporti sociali, vale la pena menzionare le forme alternative alla telefonia, quali Skype e videochiamate via internet, che stanno progressivamente penetrando negli istituti penitenziari al fine di mantenere le relazioni sociali a distanza, e ciò pone nuovi problemi in merito a come adeguare la sorveglianza penitenziaria, ma anche parallele questioni di sicurezza e trasparenza per l'introduzione di dati video nella comunicazione. Queste problematiche sono tanto più importanti per i detenuti che hanno accesso a misure alternative alla detenzione o a percorsi di messa alla prova, dove l'accesso agli strumenti sociali di comunicazione online (dai cellulari, a internet, sino ai social media) è quasi sempre totale, fatte salve restrizioni da parte degli organi competenti. In diversi Stati membri dell'Unione Europea, come anche negli Stati Uniti, si registra con sempre maggior frequenza l'uso di strumenti geolocalizzati applicati ai detenuti come misura di accompagnamento nei programmi alternativi alla detenzione[22].

Nel prossimo futuro, con lo sviluppo dei processi di digitalizzazione e di cablaggio negli istituti penitenziari europei, è facilmente immaginabile che i sistemi di monitoraggio e di relazione sociale tra detenuti e con l'istituzione penitenziaria passino sempre più attraverso sistemi di rete controllati.
La ricerca scientifica dimostra che, mentre i comuni studi sull'innovazione hanno orientato il loro focus sul miglioramento dei prodotti, teorie più recenti mostrano che oggi l'attenzione è maggiormente orientata sull'impatto che le tecnologie hanno sul servizio reso all'interno delle carceri, che non può evidentemente eludere l'aspetto umano, rieducativo, etico e relazionale. Se, da una parte, la tecnologia può garantire l'evoluzione e il miglioramento di alcuni servizi, dall'altra la sostituzione del personale operativo causa la riduzione dei

22 Van de Steene S., Knight V., "The capacity and capability of digital innovation in prisons: towards smart prisons", www.smartcorrections.org, 2017

contatti umani e, conseguentemente, riduce la qualità e il valore del servizio in una prospettiva più ampiamente riabilitativa[23].

È evidente che se da un lato la tecnologia può rispondere alle esigenze di sicurezza per proteggere gli operatori dai conflitti violenti con i detenuti, dall'altro l'assenza di una relazione umana tra i lavoratori e i detenuti può in realtà provocare un livello di violenza più alto perché non c'è coinvolgimento relazionale. L'idea alla base dell'uso della tecnologie è di non impiegare il personale per compiti di controllo che possono essere svolti facilmente dalle macchine ma, invece, di utilizzare le risorse umane appartenenti alle Forze di Polizia che operano in carcere per attività di investigazione, acquisizione e analisi dei dati, analisi delle dinamiche dei gruppi e, ultimo ma non meno importante, per collaborare con gli operatori il cui ruolo è direttamente connesso all'aspetto della rieducazione del reato e al reinserimento dei detenuti nella società.

Oggi, questo già succede con i cosiddetti metodi 'pagamento sicuro'. In molti stati membri, infatti, già oggi l'accredito di denaro ai detenuti da parte delle loro famiglie e reti sociali avviene attraverso strumenti digitali che possono essere tracciati, non più mediante la consegna del denaro contante durante i colloqui, come avviene in Italia. Le stesse spese personali dei detenuti e la gestione della contabilità individuale all'interno degli istituti avvengono attraverso strumenti digitali tracciabili.

Tutte queste attività generano un cospicuo volume di dati, l'analisi dei quali può fare parte della valutazione delle reti sociali, degli aspetti comportamentali dei detenuti e del loro ambiente di riferimento, sempre nel contesto del rispetto dei diritti fondamentali e dei principi di privacy.

Comunque, verosimilmente l'incremento esponenziale di dati disponibili come pure la diversità nella tipologia di tali dati (informazioni, immagini, suoni e

23 Knight, V. (2015) Some Observations on the Digital Landscape of Prisons Today Prison Service Journal July 2015 No. 220 pp. 3-9; Knight, V. (2016) The Technology of Confinement and Quasi-Therapeutic Control: Managing Souls with Incell Television in Mcguire, M. (2016) The Handbook of Technolo- gy and Crime, London Routledge; Graham, H., & White, R. (2014) Innovative justice. Routledge; Hildebrandt, M. (2015). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar Publishing; Jewkes, Y., & Johnston, H. (2009) Cavemen in an Era of Speed-of-Light Technology: Historical and Contemporary Perspectives on Communication within Prisons. The Howard Journal of Criminal Justice, 48 (2), pp.132-143; Jewkes, Y & Reisdorf, (2016) A brave new world: Problems and opportunities presented by new media technologies in prisons Criminology & Criminal Justice, 2016, Vol. 16 (5) 534 Knight, V. (2016) Remote Control: Television in Prison London, Palgrave Macmillian; Knight, V. & Van De Steene, S. (2017) Digitizing the Prison- The Light and Dark Future Prison Service Journal May 2017 pp.22-30; Van De Steene, S., & Knight, V. (2017). Digital transformation for prisons: Developing a needs-based strategy. Probation Journal; Van de Steene, S. (2017), Technologies in correction: Challenges and Strategies, Justice Trends, June 2017.

voci, metadati, codici hash, collegamenti alle mappe, ecc.) richiede l'uso di nuovi strumenti di analisi con metodologie tipiche dell'intelligenza artificiale. Secondo numerose previsioni, nei prossimi anni il mondo penitenziario sarà caratterizzato da una massiccia trasformazione tecnologica, adesso tanto inevitabile quanto necessaria[24].

In questo contesto, le politiche di prevenzione della radicalizzazione devono fare un salto di qualità, lavorando in più direzioni e innovando i tradizionali metodi di osservazione, prevenzione e contrasto.

Non è realistico oggi immaginare che in un'era di avanzate comunicazioni digitali la tradizionale osservazione penitenziaria, sulla quale è basata, allo stato, la maggior parte della raccolta dei dati all'interno degli istituti penitenziari, possa restare immutata. Sarebbe come cogliere solo una parte della vita di una persona. Sebbene il carcere tenda a rimanere un universo digitalmente chiuso, troppe sono le occasioni in cui l'osservazione penitenziaria tradizionale richiede di essere integrata con un'osservazione digitale che la completi, così come troppo alta è la mole di dati generati dalla vita intramuraria per un'analisi che sia limitata al lavoro mnemonico e manuale degli operatori o alla gestione cartacea di 'rapporti' e 'domandine'.
Nel progetto pilota "Sperimentazione di nuove tecnologie avanzate e loro implicazioni per contrastare e prevenire i reati nell'ambiente penitenziario", implementato come parte del progetto MINDb4ACT, tra le soluzioni tecnologiche analizzate, è stato esaminato l'effetto dell'utilizzo di totem digitali/chioschi e sistemi correlati di informazioni automatizzate nell'ottica di un processo di automazione amministrativa. Ad oggi gli operatori penitenziari raccolgono, nella maggior parte dei casi, le informazioni manualmente in registri cartacei (telefonate, colloqui, ingressi di operatori e visitatori esterni, somme di denaro disponibili alla popolazione detenuta e loro utilizzo...). In Italia, ad esempio, è disponibile il database SIAP/AFIS, ma deve essere alimentato manualmente. Un software sul modello di CRM, capace di attivare procedure coordinate, di aggregare dati e contestualizzarli, renderebbe possibile eseguire statistiche e comparazioni su scala nazionale di ingressi, colloqui e altri dati significativi in maniera automatica, intensificando la sorveglianza e la capacità di analisi, come pure fornendo simultaneamente servizi ai detenuti che possono ottenere informazioni in un assetto di sicurezza. Perciò, anche a livello di definizione dei programmi di reinserimento sociale, da una parte, o di analisi delle minacce dall'altra, la "dimensione digitale del detenuto", sempre in crescita, merita particolare attenzione. Tale dimensione digitale deve essere considerata come parte della rieducazione così come anche una nuova componente della prevenzione.

24 Bianchi S. (2019), Restorative Justice beyond the emergency caused by terrorism, Justice Trends, n.5, July 2019

In particolare, i detenuti condannati per reati connessi al terrorismo dal 2015[25] in poi presentano un'altissima percentuale di casi in cui il reato è commesso attraverso o in rete, la cosiddetta 'associazione liquida', cioè forme associative che non hanno registrato un contatto fisico diretto, bensì unicamente relazioni virtuali. Se si intende innescare un processo di revisione critica per questi detenuti, che hanno comunque condanne mediamente brevi, tra i sei e gli otto anni, ciò non può escludere una riflessione sulle condotte antigiuridiche poste in essere in rete, sulle motivazioni, sulle conseguenze negative e sulle percorribili azioni di riparazione delle conseguenze del reato collegato, da cui ricavare gli elementi indispensabili per la formulazione del programma individualizzato di trattamento che, per questa tipologia di soggetti particolarmente vulnerabile ai messaggi in rete e alla propaganda online, integri anche nuove forme di literacy digitale che ne rinforzino i fattori protettivi rispetto alle fake-news e alla propaganda estremista in rete.

25 In Italia, per esempio, l'osservazione è condotta in base alle disposizioni dell'art. 28 del Decreto del Presidente della Repubblica n. 230 del 2000 (Regolamento Esecutivo). Il ruolo centrale è svolto dall'èquipe, composta da operatori dell'Amministrazione Penitenziaria e anche da professionisti in- dicati nell'art. 80 della Legge Penitenziaria (esperti in psicologia, pedagogia, psichiatria, criminologia clinica e assistenti sociali), con il coordinamento e la responsabilità del Direttore d'istituto. L'équipe poi è distinta dal Gruppo di Osservazione e Trattamento (GOT), che costituisce un gruppo esteso composto, in aggiunta ai componenti coordinati dal Funzionario giuridico-pedagogico, da tutte le figure che interagiscono con il detenuto o collaborano nel suo trattamento (personale della Polizia Penitenziaria, insegnanti, volontari, assistenti sociali indispensabili per la valutazione dell'ambiente dove la personalità del detenuto si è sviluppata e per l'individuazione di supporti esterni, attraverso le inchieste sociali il cui obiettivo è raccogliere e coordinare le informazioni sociali, famigliari, storiche e mediche, opportunità di reinserimento esterno, I rapporti famigliari e personali). Questa compo- sizione non è fissa, ma i protagonisti sono intercambiabili, in base a chi ha in carico il detenuto, lo accompagna e supporta durante la fase detentiva, perciò dando vita allo scambio di informazioni tra operatori per coordinare gli interventi.

III. - LA PREVENZIONE DIGITALE COME NUOVA TECNICA DI PROVE FORENSI PENITENZIARIE

Questo nuovo orizzonte dell'osservazione scientifica della personalità e della prevenzione della radicalizzazione attraverso forme integrate di sorveglianza digitale, quale ausilio all'osservazione e al monitoraggio tradizionali, pone molte questioni aperte. Si tratta di nodi legali ma anche tecnici, di carattere sia procedurale che operativo. Sul piano tecnico-operativo dei programmi di riabilitazione, si pone per esempio il nodo di come ampliare i nuclei multidisciplinari per permettere la formazione di una visione globale del soggetto detenuto, che ne consideri il vissuto detentivo, il background e la situazione famigliare, ma anche le relazioni virtuali o le attività svolte alla luce di processi di comunicazione digitale, dal lavoro nei call-center alla formazione su piattaforme a distanza. In diversi paesi europei, l'attività multidisciplinare è disposta per via legislativa, tuttavia i vari modelli permettono una certa flessibilità importante al fine di introdurre nuovi esperti nei nuclei di valutazione[26]. È evidente che occorrono nuove competenze e professionalità digitali e forensi per affrontare sfide di tale portata, così come nuovi sistemi tecnologici per monitorare i detenuti durante le attività intramurarie ma, soprattutto, extramurarie, laddove beneficino di misure alternative alla detenzione.

III.1 - INFORMAZIONI DIGITALI TRA L'OSSERVAZIONE, LA SORVEGLIANZA E LE PROCEDURE

Anche sul piano della sorveglianza, come per quello dell'osservazione, si pongono questioni legali e procedurali, come ad esempio la questione di quali siano i nuovi indicatori di pericolo connessi alle tecnologie digitali e come li si possa monitorare in un modo che non contrasti con i principi di privacy ed etica alla base del GDPR e dei diritti fondamentali, oltre che delle buone prassi europee in materia di tutela del detenuto.

> Ad esempio, il possesso illegittimo all'interno di un carcere di un telefono cellulare o di una SIM utilizzabile su più dispositivi, può integrare l'analisi e il monitoraggio della radicalizzazione, essere cioè un elemento degli indicatori di rischio? I dati contenuti in quel telefono possono entrare a far parte di un processo preventivo di sorveglianza e analisi digitale, volto a verificare la rete di contatti, i contenuti e le attività del detenuto in funzione preventiva? Con quale procedura, legale o amministrativa, è possibile accedere alle estrazioni forensi di quel telefono mobile?

26 Agenfor, (2019), Harmonised Guidelines for Judges in Cases of Radicalisation leading to terrorism, J-SAFE, D3.9.

Il possesso di un cellulare in un istituto penitenziario, soprattutto quando si trova in possesso di detenuti sottoposti ai profili di analisi a causa del rischio di radicalizzazione, assume indubbia rilevanza nel processo di osservazione messo in atto dagli operatori penitenziari, ben essendo in grado di rappresentare un nuovo, significativo indicatore di rischio.
Il tentativo di questi soggetti di stabilire comunicazioni con il mondo esterno assume contorni ancora più sintomatici rispetto ai casi in cui altri detenuti ne sono protagonisti, poiché i rischi generati dalla radicalizzazione all'interno degli istituti penitenziari sono integrati da attività dirette all'esterno, con un evidente pericolo di contatti con organizzazioni terroristiche e di pianificazione di attacchi da parte di militanti che stanno per essere scarcerati. In effetti, il processo investigativo può anche trarre vantaggio dall'analisi delle apparecchiature telefoniche utilizzate dai detenuti monitorati per il rischio di radicalizzazione, fornendo informazioni sui contatti effettuati e aprendo nuovi scenari investigativi. I dati contenuti nei telefoni possono certamente far parte di un processo di analisi preventiva, soprattutto se si sospetta che il telefono sia stato utilizzato per commettere reati. Anche in questo caso, soprattutto se la paternità del dispositivo è nota, per l'analisi dei contatti, del contenuto e dei tabulati è necessaria l'autorizzazione dell'Autorità Giudiziaria. Per quanto riguarda la procedura nelle estrazioni forensi, come verrà spiegato di seguito, la Procura è l'organismo delegato a rilasciare una disposizione di autorizzazione che consente alle Forze di Polizia competenti di effettuare analisi forensi dei dispositivi telefonici.

Un altro problema centrale è la qualificazione giuridica delle informazioni digitali ottenibili in relazione alla procedura di acquisizione. Attualmente, i dati relativi al monitoraggio sulla radicalizzazione sono dati amministrativi, cioè informazioni di sicurezza, consistenti in report prodotti dal personale penitenziario e trasmessi a organi gerarchici o ad altre forze di polizia e di intelligence. Tali dati relativi alla sicurezza preventiva oggi non vengono inseriti nei fascicoli dei detenuti e non sono accessibili ai loro difensori. Si tratta di dati di intelligence o pre-investigativi. Sono contenuti in sezioni speciali dei sistemi SIAP/AFIS 2.0 e SIDET WEB 2, disponibili per i Ministeri della Giustizia e dell'Interno e canalizzabili verso le agenzie di intelligence sulla base della loro rilevanza. La domanda che sorge con le nuove acquisizioni digitali è se i dati acquisibili attraverso perquisizioni informatiche, amministrative o giudiziarie possano considerarsi ed essere gestiti anch'essi come dati puramente amministrativi, considerando le normative nazionali ed europee in materia e le questioni connesse alla conservazione dei dati. In molti paesi, l'acquisizione di dati e dispositivi è soggetta a procedure giurisdizionali, regolate dal potere di autorità della magistratura. Pertanto, tali dati verrebbero rimossi dalla sfera amministrativa e diverrebbero indizi o prove nei procedimenti penali, quindi accessibili ai difensori dei detenuti con tutte le garanzie che questo implica. Un'altra questione non irrilevante riguarda la possibilità o meno di trasmettere tali dati ad agenzie terze, sia in Europa (ad esempio Europol) che in paesi extraeuropei (direttamente o tramite Interpol, ad esempio) e quando, in

quale fase del procedimento amministrativo o giudiziale. I progetti DERAD e TRAINING AID, finanziati rispettivamente dalla DG Justice e DG Home, hanno evidenziato gravi difficoltà nella trasmissione di dati sensibili connessi alla radicalizzazione ad agenzie di paesi membri dell'UE in funzione preventiva, sia che si trovino nello stato di informazioni amministrative o, ancora di più, quali dati investigativi nel quadro di procedimenti non conclusi in forma definitiva. Come emerge dal report conclusivo del progetto DERAD, *"come conseguenza del processo di de-giurisdizionalizzazione, i detenuti sospettati di atteggiamenti, idee, convinzioni o comportamenti radicali, di solito sottoposti a monitoraggio per radicalizzazione, in molti casi non possono beneficiare delle disposizioni delle decisioni quadro 909/829/947. Inoltre, non esistono procedure per comunicare alla Magistratura di Sorveglianza informazioni riguardanti osservazioni sulla radicalizzazione nelle carceri dello Stato in cui si esegue la condanna. Per questi motivi, nessun detenuto sospettato di comportamenti radicali è stato trasferito nel suo paese di origine o di residenza, contrariamente a quanto previsto dalle tre decisioni quadro. Tali procedure sono in netto contrasto con le disposizioni europee e rischiano di essere sottoposte al controllo della Corte di Giustizia dell'UE o della CEDU".*

Ognuna di queste domande rimanda ad una questione più generale, che sorge da una contraddizione tra le procedure di prevenzione e il principio di legalità, ripetutamente riaffermato dalla giurisprudenza e dalla dottrina comunitarie di rango superiore. Come ha evidenziato il Deliverable 3.9[27] del progetto J-SAFE, la prevenzione della radicalizzazione si pone oggi in un'area grigia tra le attività social-preventive e le indagini ibride sui reati connessi al terrorismo, considerando che le nuove normative antiterrorismo anticipano la soglia della punibilità a comportamenti che sono quelli tipici della radicalizzazione. Non è raro leggere sentenze in cui i giudici di merito identificano la radicalizzazione come un fenomeno di anticipazione criminale[28].

La difficoltà che ogni operatore giuridico incontra nello studio o nella valutazione di un fenomeno radicale è quella di dover inquadrare se tale fenomeno si tradurrà in attività violenta a causa di fenomeni esogeni che scatenano l'idea radicale già presente nel soggetto. L'estrema cautela con cui la componente radicale deve essere valutata sotto il duplice aspetto della prevenzione e della punizione è quindi evidente. È altresì evidente che, di fronte a situazioni di emergenza, la protezione sociale troverà più spazio della protezione indivi-

27 Esempio: CORTE DI CASSAZIONE, SEZ. VI PENALE - SENTENZA 11 settembre 2018, n.40348 - Pres. Fidelbo – est. Silvestri "Si assume che tutti i soggetti coinvolti nel procedimento si sarebbero 'radicalizzati', assumendo posizioni religiose estreme di matrice islamista, condividendo tra loro, attraverso facebook, immagini, filmati, preghiere inneggianti al califfato ed al jihad armato contro i miscredenti (così testualmente l'imputazione)."

28 Vittorio Platì, "Nesso tra radicalizzazione e terrorismo", 28 agosto 2019 (comunicazione privata).

duale. Anche se le garanzie contro il soggetto interessato non devono mai essere ridotte, esse rappresentano la differenza tra i sistemi di diritto evoluti rispetto ai sistemi in cui si applica la logica del nemico da eliminare. È altrettanto vero che non tutte le ipotesi possono essere regolate perché esiste in natura un margine di imprevedibilità che è una diretta conseguenza di tutto ciò che improvvisamente si manifesta. Di conseguenza è chiaro che non tutti coloro che sono definiti in vari modi come radicalizzati possono essere sottoposti a misure di prevenzione o di controllo perché non tutti hanno un margine di pericolo. Secondo le sentenze della suprema Corte di Cassazione italiana, il terrorismo è un metodo violento di cui la violenza è un elemento costitutivo. Rebus sic stantibus, la radicalizzazione diverge dal terrorismo per scopi, obiettivi e metodi. Infatti, nella radicalizzazione la violenza è un dato potenziale, eventualmente presente in forma ideologica, ma che non necessariamente si esprime in atti materiali, dati i quali essa si trasformerebbe in un reato.

L'obiettivo, dunque, sarebbe quello di chiarire i fenomeni di radicalizzazione distinguendo differenti misure preventive, sociali, legali o securitarie, volte a contrastarli, combinando programmi di de-radicalizzazione e misure preventive, per incorporarli in una logica di reato con ovvia risposta criminale laddove sia prevalente l'aspetto securitario. La regola, inoltre, nel ricordare la strategia dell'UE, fa una chiara distinzione allorquando cita la radicalizzazione che porta al terrorismo e all'estremismo violento, così da ipotizzare l'esistenza di una radicalizzazione che diversamente dalla prima non conduce al terrorismo e all'estremismo violento[29].

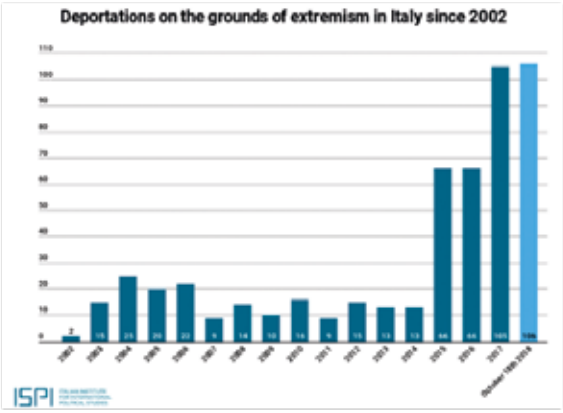
Le conseguenze dei sospetti di radicalizzazione 'verso il terrorismo' possono essere molto significative in termini di restrizioni alle libertà fondamentali come definite dalla CEDU. Esse comprendono restrizioni ai movimenti, nonché la revoca della cittadinanza, la confisca di passaporto e altri documenti analoghi, l'applicazione di misure di sorveglianza speciale di prevenzione personale e dell'obbligo di restare fino all'espulsione, ove vi siano indicatori di minacce all'ordine pubblico o alla sicurezza nazionale[30].

In Italia le espulsioni amministrative per motivi di sicurezza nazionale hanno svolto un ruolo crescente nella strategia antiterrorismo italiana. Alla data del 18 ottobre 2018, ci sono già state 106 espulsioni per estremismo nel 2018, superando le 105 espulsioni dell'anno precedente. Il numero è cresciuto dal 2015, e il loro utilizzo diventa più comune. La disposizione può essere utilizzata solo nei confronti di persone straniere presenti sul territorio italiano in

29 In Italia la materia è regolata dal Decreto Legislativo n.286/1998 e dal Decreto Legge n.144/2005.

30 Vittorio Platì, "Nesso tra radicalizzazione e terrorismo", 28 agosto 2019 (comunicazione privata).

quanto ogni espulsione è riportata al Sistema d'informazione Schengen (SIS) dell'Unione europea.[31]



(Fig. 3 Figura di espulsione in Italia utilizzata come misura preventiva)

Inoltre, il sospetto di legami con il terrorismo può dar luogo al ricorso a tecniche investigative speciali di natura emergenziale. Tra queste, l'intercettazione preventiva, l'uso di agenzie di intelligence all'interno delle istituzioni penitenziarie, colloqui investigativi, attività sotto copertura, rilascio di permessi speciali per i collaboratori, ecc. In generale, si tratta di provvedimenti giudiziari, ma alcuni hanno anche un valore amministrativo, come nel caso delle espulsioni. Considerando che le conseguenze dei sospetti sulla radicalizzazione possono essere anche molto significative in termini di restrizioni sulle libertà fondamentali come definite dalla Corte Europea dei Diritti dell'Uomo, la Corte ha equiparato le misure preventive che limitano la libertà di movimento a quelle relative alle misure restrittive dei diritti civili in carcere, collocandole nella stessa categoria di limitazione preventiva dei diritti civili, esplicitamente tutelati dall'art. 6, c.1 della Convenzione. La conclusione menzionata nel giudizio "De Tommaso v. Italy" (Application n.43395/09) era categorica:

> *149. La Corte ha inoltre concluso che qualsiasi restrizione che leda i diritti civili di una persona deve poter essere contestata nel corso di un procedimento giudiziario, data la natura delle restrizioni (ad esempio,*

31 Per l'Italia la casistica sulle misure di prevenzione è molto estesa: leading case C. edu, Plenaria, sent. 6 novembre 1980, Guzzardi c. Italia, in particolare §§ 90-103; C. edu, Plenaria, sent. 22 febbraio 1989, Ciulla c. Italia, in particolare §§ 38-39; C. edu, Camera, sent. 22 febbraio 1994, Raimondo c. Italia, in particolare §§ 39-40; C. edu, Grande Camera, sent. 6 aprile 2000, Labita c. Italia, in parti- colare §§ 193-197; C. edu, Sez. I, sent. 17 luglio 2003, Luordo c. Italia,in particolare §§ 94-97; C. edu, Sez. III, sent. 1 luglio 2004, Vito Sante Santoro c. Italia,in particolare §§ 42-46; C. edu, Sez. II, dec. 8 ottobre 2013, Monno c. Italia, in particolare §§ 21-22 e 26-28.

il divieto di ricevere più di un certo numero di visite mensili da parte di familiari o il monitoraggio continuo della corrispondenza e delle conversazioni telefoniche) e delle loro *possibili ripercussioni (ad esempio, difficoltà nel mantenere legami familiari o relazioni con persone diverse dai familiari, o esclusione dall'attività fisica all'aperto)" (ibid., § 106).*

Per analogia, pertanto, si pone la questione della legittimità (e della legalità) del ricorso a misure preventive che limitano i 'diritti civili dei detenuti e delle persone soggette a restrizioni' sulla base di indicatori di radicalizzazione e della loro profilazione, di una sorveglianza rafforzata o di limitazioni della loro parità di diritti rispetto a tutti gli altri detenuti ristretti per reati simili, ma che non sono 'classificati' come radicalizzati.
Misure preventive nei confronti dei detenuti considerati radicalizzati sulla base dei diversi livelli di rischio, applicate in molti paesi membri e, in alcuni di essi, su base amministrativa, sono configurabili come quelle identificate dalla Corte nei casi Gülmez v. Turchia, n. 16330/02, §§ 27 31, 20 maggio 2008 (limitazione delle visite), Ganci v. Italia (n. 41576/98, §§§ 20-26, CEDU 2003 XI), Musumeci v. Italia (Nr. 33695/96, § 36,11 gennaio 2005) e Enea v. Italia ([GC], Nr. 74912/01, § 107, CEDU 2009), tutte relative a visite, monitoraggio della corrispondenza e conversazioni telefoniche e limiti all'attività fisica all'aperto, o Stegarescu e Bahrin v. Portogallo (No. 46194/06, §§ 37- 38, 6 aprile 2010), che stabilisce visite limitate ad un'ora alla settimana e solo previa separazione mediante una parete di vetro, attività fisica esterna limitata ad un'ora al giorno, e l'impossibilità per il primo richiedente di continuare gli studi e sostenere esami. Nonostante ciò, e nonostante le significative restrizioni alla libertà dei detenuti sospettati di radicalismo presenti in molti paesi membri, la nuova direttiva europea sul terrorismo (Direttiva UE 2017/541), ha scelto di non regolamentare per via legislativa il fenomeno della radicalizzazione, trattato solo negli articoli 31, 32, 33, ma non nell'articolato di legge. La Direttiva inquadra la radicalizzazione nell'ambito della prevenzione del terrorismo in senso lato. I magistrati, i procuratori e gli investigatori devono pertanto considerare la radicalizzazione come un possibile "movente" di reati connessi al terrorismo o come un indicatore di pericolo sociale, non come un reato tipicizzato e neppure come l'anticipazione di un crimine punibile secondo le norme antiterrorismo o i codici penali più in generale. Pertanto, la radicalizzazione ha un proprio ambito legale specifico nelle misure di prevenzione e nei provvedimenti di sicurezza preventiva, mentre altre condotte radicali, come l'apologia di reato, entrano nelle procedure penali tradizionali, ivi incluse quelle inerenti i crimini di pericolo anticipato. L'analisi dei casi evidenzia che si tratta di indicatori di pericolo o ipotesi di reato consumate nella maggior parte dei casi online, al fine di acquisire contatti, promuovere idee estremiste di movimenti terroristici, per formare o auto-formarsi in percorsi di training a supporto del terrorismo, o per effettuare viaggi in zone di guerra, di propria iniziativa o per conto di terzi. In altri casi, si tratta di reati volti a finanziare individui o gruppi considerati terroristi. Quando le condotte in questione sono tipicizzate in forma di reato, dunque perseguibili, la procedura è molto chiara e, solitamente,

definita nei codici di procedura penale. Quando invece la procedura è di tipo preventivo, sia amministrativo che giurisdizionalizzata, la questione si complica, poiché lo spazio d'azione individuale delle autorità di polizia è molto più ampio. A ragione, dunque, la CEDU ha stabilito chiari limiti all'adozione di misure preventive, che non si configurano come una riproduzione o duplicazione del procedimento penale, ma richiedono comunque precise garanzie procedurali per le persone sospette, di conseguenza precise regole di raccolta delle 'indizi di pericolosità'.

Tra queste garanzie, la previsione per legge delle misure di prevenzione adottabili in un procedimento comunque giurisdizionalizzato; standard di qualità della legge che ne assicurino l'accessibilità, vale a dire la conoscibilità da parte delle persone interessate, e la prevedibilità, cioè la possibilità di prevedere a chi e a quali comportamenti si riferiscono le norme; funzionalità alla prevenzione della criminalità; necessità in una società democratica; proporzionalità[32]. Come ha sostenuto Bianchi S. (2018) in un suo recente lavoro di ricerca[33] per J-SAFE, "ai sensi della direttiva 2017/541/UE, l'Unione e i suoi Stati membri hanno ampliato in modo significativo l'ambito dei reati connessi al terrorismo a tutti i cosiddetti atti preparatori. Inoltre, l'articolo 13 della direttiva ha stabilito un nuovo principio di indagine penale e di giudizio del giudice:

"Affinché un reato di cui all'articolo 4 o al titolo III sia punibile, non è necessario che un reato di terrorismo sia effettivamente commesso, né è necessario, per quanto riguarda i reati di cui agli articoli da 5 a 10 e 12, stabilire un collegamento con un altro reato specifico previsto dalla presente direttiva."

L'estensione di tali misure penali in una forma così flessibile consente probabilmente l'introduzione di elementi di fatto tipici dei processi criminali nelle procedure di prevenzione, analogamente a quanto avvenuto in Italia con la Legge Reale sull'applicazione di misure preventive verso "soggetti politicamente pericolosi". Con la sentenza "De Tommaso v. Italy" (Application n. 43395/09) del 23 febbraio 2017, la Gran Camera della Corte Europea di Strasburgo ha ulteriormente rafforzato i principi di legalità alla base delle misure di prevenzione. A questo proposito, vale la pena richiamare i principi ispiratori della "Rule of the Law", che raccomanderebbero una regolamentazione specifica in sede europea del merito e delle procedure di prevenzione personali e patrimoniali: "Esso richiede in particolare che i principi di legalità[34], tra cui un proces-

32 Bianchi S., (2018) "Radicalisation: no prevention without radicalisation".

33 Judgment of the Court of Justice of 29 April 2004, CAS Succhi di Frutta, C-496/99 PE-CLI:EU:C:2004:236, paragraph 63.

34 Judgment of the Court of Justice of 12 November 1981, Amministrazione delle finanze dello Stato v Srl Meridionale Industria Salumi and others Ditta Italo Orlandi & Figlio and Ditta Vincenzo Divella v Amministrazione delle finanze dello Stato. Joined cases 212 to 217/80, ECLI:EU:C:1981:270, paragraph 10.

so trasparente, responsabile e democratico per la promulgazione delle leggi, la certezza del diritto[35], il divieto di arbitrarietà dei poteri esecutivi[36], la separazione dei poteri[37], l'accesso alla giustizia e un'efficace protezione giudiziaria di fronte a tribunali indipendenti ed imparziali[38] siano rispettati[39]. Tali principi si conformano, fra l'altro, ai principi della Commissione Venezia del Consiglio d'Europa e anche alla pertinente giurisprudenza della Corte Europea dei Diritti dell'Uomo[40]. Questo quadro emergente, composto di giurisprudenza, procedura e dottrina, impone oggi di trattare i dati digitali finalizzati alle misure di prevenzione secondo modelli procedurali coerenti con le norme più generali sulle indagini, a partire dall'Ordine di Indagine europeo (EIO), dall'azione di vigilanza preventiva europea e dalla Roadmap di Stoccolma, con un ulteriore sguardo al dibattito tecnico-politico inerente le e-evidences.

A tale importante dimensione deve essere aggiunto il fatto che le operazioni di polizia penitenziaria da lungo tempo tendono ad espandere la loro giurisdizione ben oltre le mura del carcere. Infatti, la cattura di un drone all'interno di un istituto penitenziario o il sequestro di un telefono cellulare, ad esempio, aprono scenari molto più ampi per le relazioni esterne che questi dati offrono, la possibilità di aprire indagini su persone non detenute, o l'opportunità di analizzare reti a rischio in ambito di terrorismo o criminalità organizzata. Tale espansione della giurisdizione penitenziaria acquista particolare rilevanza allorquando l'attenzione è concentrata su soggetti sospetti che abbiano avuto accesso ai benefici di legge e alle misure alternative, i quali dunque conducono una vita all'esterno del carcere, operano all'interno di aziende o cooperative, e hanno reti relazionali sul territorio. Peravere un'ideadella portatadel fenomeno,si rileva che durante i primi nove mesi dell'anno 2020 sono stati 1.761 gli apparecchi rinvenuti nelle carceri italiane, requisiti all'interno o bloccati prima del loro ingresso. Nello stesso periodo

35 Judgment of the Court of Justice of 21 September 1989, Hoechst, Joined cases 46/87 and 227/88, ECLI:EU:C:1989:337, paragraph 19.

36 Judgment of the Court of Justice of 10 November 2016, Kovalkovas, C-477/16, ECLI:EU-:C:2016:861, paragraph 36; Judgment of the Court of Justice of 10 November 2016, PPU Poltorak, C-452/16, ECLI:EU:C:2016:858, paragraph 35; and Judgment of the Court of Justice of 22 December 2010, DEB,C-279/09, ECLI:EU:C:2010:811, paragraph 58.

37 Judgment of the Court of Justice of 27 February 2018, Associação Sindical dos Juízes Portugueses v Tribunal de Contas C-64/16, ECLI:EU:C:2018:117, paragraphs 31, 40-41; judgment of the Court of Justice of 25 July 2018, LM, C-216/18 PPU, ECLI:EU:C:2018:586, paragraphs 63-67.

38 Communication from the Commission "A new EU Framework to strengthen the Rule of Law", COM(2014) 158 final, Annex I.

39 Report of the Venice Commission of 4 April 2011Study No. 512/2009 (CDL-AD(2011)003rev).

40 Interpol, Fine Nr. 2019/15826-1, Modus Operandi, Illegal delivery of contraband to prison systems using unmanned aerial systems (UAS).

del 2019 erano stati 1.206, mentre nel 2018 se ne erano registrati 394.

Un altro settore di grande interesse è quello dei droni. Attraverso tali mezzi avvengono consegne illegali in carcere. Nel gennaio 2019, Interpol ha segnalato a tutti i Ministeri della Giustizia[41] l'insorgenza di tale rischio. Infatti, il Centro di innovazione Interpol ha individuato come sistemi aerei privi di pilota (UAS), comunemente denominati droni, siano utilizzati con crescente frequenza per trasportare illegalmente merci di contrabbando nelle carceri dei paesi membri di INTERPOL. I dispositivi UAS sono utilizzati da individui o gruppi organizzati esterni ai penitenziari collusi con detenuti. Ciò si ottiene installando un carico sul dispositivo che utilizza un sistema di aggancio o un sistema di sganciamento remoto. Questi sono progettati per consegnare il carico presso un luogo concordato in precedenza, dove verrà raccolto da un destinatario all'interno dell'istituto. Spesso i dispositivi UAS utilizzati sono piccoli e difficili da individuare attraverso mezzi convenzionali di sorveglianza, in quanto non seguono traiettorie tradizionalmente esaminate per spedire i loro carichi. In alcuni casi, i carichi trasportati dai dispositivi UAS nel sistema penitenziario sono stati creati per assomigliare ad altri oggetti come palle da tennis, contenitori di succo e uccelli morti nel tentativo di mascherarne il contenuto. I mezzi che consentono di consegnare con successo oggetti di contrabbando in un sistema penitenziario richiedono minime conoscenze o formazione sulle attrezzature UAS. Il trasgressore utilizza spesso dispositivi UAS multicottero disponibili in commercio per spedire carichi di contrabbando ai propri obiettivi. Queste unità ampiamente disponibili possono essere acquistate facilmente dal pubblico. Interpol ha osservato che le descritte attività degli UAS sono state segnalate in diversi paesi membri. Ogni anno che passa, il numero di casi segnalati continua ad aumentare. Si raccomanda che il sistema penitenziario adotti le seguenti misure precauzionali:

1. sviluppare protocolli di risposta per le incursioni da drone;
2. fornire i mezzi per la messa a terra e/o la cattura di droni UAS in superficie in aria e in aria;
3. creare un perimetro geofencing intorno allo spazio aereo del carcere con i produttori di droni UAS;
4. garantire un adeguato controllo perimetrale delle carceri;
5. installare apparecchiature di rilevamento droni UAS;
6. utilizzare apparecchiature di disturbo del segnale nello spazio aereo progettate per contrastare i droni UAS;
7. costruire barriere fisiche per evitare che i carichi dei droni UAS raggiungano i detenuti;
8. condividere le migliori prassi e i casi esemplari con Interpol.

41 https://www.lastampa.it/cronaca/2018/10/25/news/a-taranto-cade-un-drone-in-carcere-dentro-c- erano-telefonini-e-droga-1.34055436?refresh_ce

Nel 2018 un drone è caduto nel carcere di Taranto mentre tentava di consegnare droga e due micro telefonini al terzo piano dell'edificio. Tutti questi apparecchi, una volta acquisiti dalle forze dell'ordine, sono preziose fonti d'informazioni. Purtroppo, oggi il loro potenziale rimane inesplorato. Ad esempio, dei circa 250 apparecchi telefonici in possesso dei 16 istituti penitenziari del Triveneto, solo su pochissimi sono state condotte analisi appropriate. Per lo più vengono o distrutti, dopo essere stati conservati per un certo tempo nelle casseforti degli istituti penitenziari in attesa di decisioni dell'autorità giudiziaria, o riconsegnati ai proprietari all'atto della scarcerazione.

Pertanto, in questa terza parte del manuale verranno illustrate le procedure che la polizia penitenziaria o le forze dell'ordine devono applicare quando si tratta di dati digitali provenienti da diversi tipi di dispositivi, con funzione di prevenzione o anche pre-investigativa, con particolare attenzione all'ambito della radicalizzazione e del terrorismo. E' comunque chiaro che le medesime regole si applicano anche al settore della criminalità organizzata, sia nelle attività di prevenzione che in quelle d'indagine.

Tutti questi oggetti e dati digitali contribuiscono a rafforzare la doppia dimensione dell'analisi sulla radicalizzazione: essi possono condurre ad un quadro rafforzato di politiche di prevenzione o, nei casi più gravi, all'avvio di indagini per reati connessi al terrorismo o altri reati. Lo scenario può essere quello dell'acquisizione per via amministrativa di un telefono mobile illegittimamente detenuto da un ristretto all'interno dell'istituto, operabile con più SIM, o di particolari USB che possano operare su dispositivi di reti legali in forma illegale; oppure di un'operazione di polizia giudiziaria condotta da un nucleo investigativo di Polizia Penitenziaria all'esterno del carcere, su delega o sub-delega della magistratura. Infine, le medesime procedure si applicano nel caso di eventi critici o eventi maggiori, ivi compresi casi di rivolta penitenziaria, all'interno delle cui dinamiche vengano rinvenuti strumenti digitali (telefoni, computer, tablets, USB o altro).

(Fig. 5: Immagini di dispositivi mobili sequestrati nelle carceri di diversi paesi)

III.2 - CASI PENITENZIARI RELATIVI ALLA GESTIONE DEI DATI DIGITALI.

Di seguito verranno illustrati due casi di attività rilevanti d'indagine e prevenzione concernenti la gestione di dati digitali all'interno degli istituti penitenziari.

III.2.1 - RICERCA

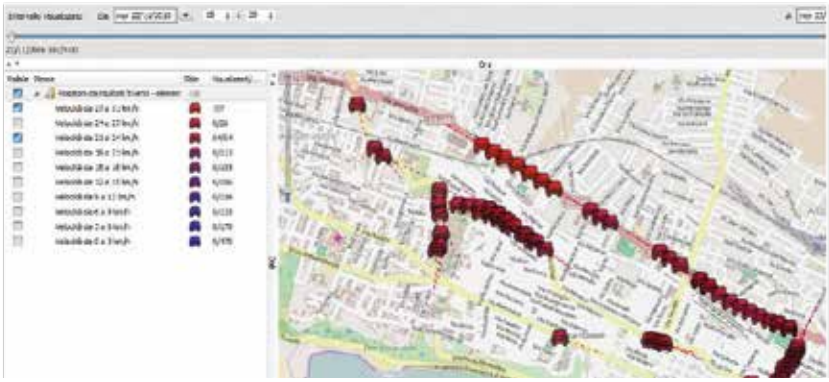
Alle ore 08:00 il Comandante di Reparto nella consueta conferenza di servizio, disponeva, avvalendosi dei sott'ufficiali presenti, un servizio di perquisizione di un padiglione detentivo. All'atto della perquisizione della stanza detentiva n. 7 si rinveniva un telefono cellulare di piccolissime dimensioni modello I8star; provvedevo ad informare tempestivamente il coordinatore della perquisizione, il quale, verificava preventivamente se il cellulare fosse spento o acceso, dopodiché procedeva ad identificare il detenuto utilizzatore e lo invita a fornire il codice di sblocco se presente. Dopodiché procedevamo al sequestro del dispositivo, inoltrando gli atti presso la locale Procura della Repubblica, richiedendo delega di indagine finalizzata ad estrarre copia forense del dispositivo ed analizzarne il contenuto, altresì richiedevamo l'emissione di un decreto di acquisizione del traffico telefonico e telematico relativamente al numero telefonico e all'IMEI del dispositivo cellulare. Ricevuta la delega d'indagine, la Procura della Repubblica disponeva l'acquisizione del contenuto del telefono cellulare ai sensi dell'art. 359 c.p.p., pertanto si provvedeva ad ottemperare a quanto disposto dall'Autorità Giudiziaria adoperando le cautele del caso. Prima di tutto si collegava il dispositivo al pc ove vi è installato il software Xry, al fine di identificare il modello ed il profilo più idoneo per estrarre copia forense. Una volta individuato il modello corrispondente, si avviava la procedura guidata, che terminava positivamente e restituiva diversi elementi utili per l'indagine.

(Fig. 6 Esempio di estrazioni forensi)

Una volta identificato il modello corrispondente, è stata avviata la procedura guidata, che ha avuto suc-

cesso e ha rivelato diversi elementi utili per l'inchiesta. Allo stesso modo, sono stati elaborati i tabulati telefonici precedentemente acquisiti dagli operatori di telefonia mobile, analizzandone ogni aspetto relativo alla posizione di aggancio delle celle telefoniche, nonché ai contatti intercorsi tra il bersaglio ed i diversi interlocutori.

(Fig. 7: contatti risultanti da un'estrazione forense)



(Fig. 8: geolocalizzazione dei contatti da un'estrazione forense)

Dalle analisi effettuate si evince che l'interlocutore del nostro target nel giorno del colloquio con il suo familiare si è recato dal suo indirizzo di residenza verso la struttura detentiva e ivi permaneva sino al termine del colloquio per poi ritornare presso la propria residenza. Al termine di tale attività si provvedeva a redigere apposita informativa da inoltrare all'Autorità Giudiziaria per le eventuali successive direttive d'indagine. Il caso in esame offre una breve panoramica di alcuni dei luoghi in cui la popolazione detenuta tende a nascondere oggetti non consentiti, noti al personale della Polizia Penitenziaria grazie dell'esperienza acquisita.
Questi includono:

- sulla persona, in particolare negli orifizi;
- sugli indumenti indossati , specie sotto la suola delle scarpe;
- in anfratti ricavati nel mobilio o nei materassi o cuscini;
- in cavità strutturali dell'edificio, prese elettriche, cavedi, cassette di derivazione elettrica, anfratti presenti tra il muro e oggetti a questo fissati (lavandini, lavabi, water, specchi);
- all'interno di elettrodomestici (televisori, ventilatori, plafoniere elettriche);
- in generi alimentari liquidi o solidi;
- in anfratti ricavati in muri perimetrali e abilmente occultati;
- in locali comuni (passeggi, sale socialità, bagni comuni, finestre, corridoi, palestre, carrelli per il trasporto del vitto).

III.2.2 - COMUNICAZIONE DELLE INFORMAZIONI

Successivamente ad una segnalazione anonima, il Comandante di Reparto, avvalendosi delle unità cinofile predisponeva un servizio teso a reprimere l'ingresso di stupefacenti all'interno del carcere. All'ingresso dei familiari a colloquio il cane dell'unità cinofile puntava un familiare il quale dopo una iniziale modesta resistenza, consegnava spontaneamente della sostanza stupefacente del tipo hashish. Veniva immediatamente notiziato il Comandante del Reparto che provvedeva a sua volta ad interessare il PM di turno chiedendo l'autorizzazione a procedere all'analisi del telefono cellulare al fine di verificare se vi fossero stati contatti con soggetti interni al carcere. Pertanto si provvedeva ad analizzare sul posto il dispositivo del famigliare del detenuto, estrapolandone il contenuto della messaggistica e del registro delle chiamate, nonché della rubrica.

(Fig. 9 Extraction of a chat)

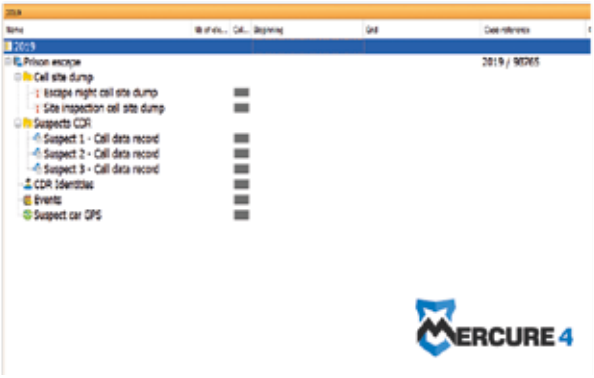
Da una rapida analisi emergevano diversi contatti con il detenuto familiare presente in istituto, il quale in diverse occasioni ordinava sostanza stupefacente tramite sms. Preliminarmente si aggiornava il PM in merito alle novità emerse, chiedendo di poter procedere alla perquisizione domiciliare e di ogni altra pertinenza del familiare del detenuto, e contestualmente si provvedeva a perquisire

la stanza detentiva del detenuto in questione. La perquisizione domiciliare dava esito positivo, in quanto venivano rinvenute diverse dosi di stupefacente presso l'abitazione del familiare. Successivamente al fine di approfondire la rete di collegamenti dello spacciatore, si provvedeva a richiedere all'Autorità Giudiziaria un decreto di acquisizione del traffico telefonico, teso a carpire la rete di soggetti coinvolti nello spaccio.

(Fig. 10 Link Chart)

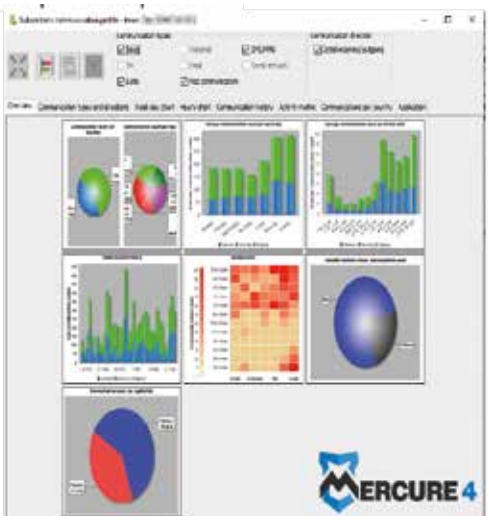
III.2.3 - SOFTWARE APPS

In entrambi i casi abbiamo utilizzato un'applicazione commerciale, che si è rivelata molto utile per l'analisi nelle carceri. È una soluzione software per l'analisi dei flussi di dati telefonici, che può anche integrare dati prodotti da altre fonti, come ad esempio estrazioni forensi da telefoni cellulari, dati GPS, informazioni prodotte da database esterni (ad esempio: dati amministrativi quali IVA, località, ecc.). I dati importati sono classificati in file separati, a seconda dei contesti, in modo da visualizzare chiaramente l'intera operazione.



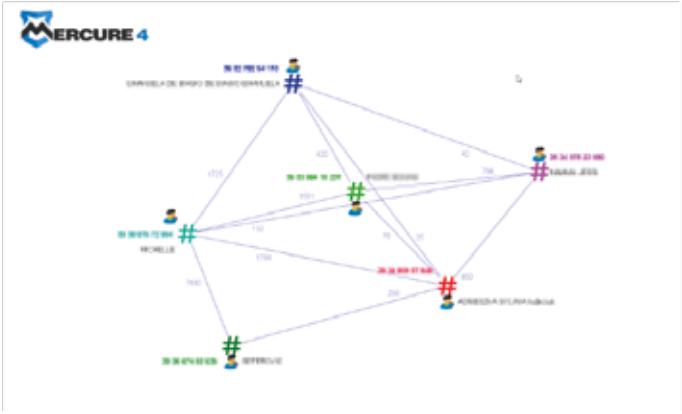
(Fig. 11: File Classification in Mercure)

Il software può generare differenti grafici definiti come “profili di comunicazione”. Tali profili facilitano l’analisi degli utilizzatori. I profili di comunicazione possono essere prodotti usando diversi dati sorgente: flussi telefonici, analisi degli hotspot e altri parametri.

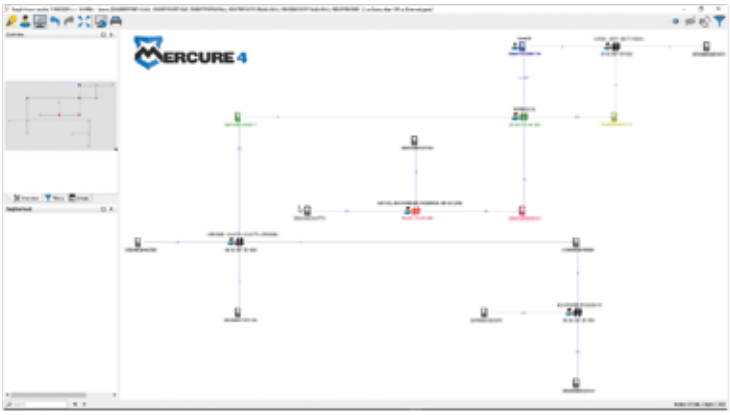


(Fig. 12: Visual Graphic in Mercure)

La figura seguente mostra i collegamenti tra le diverse connessioni telefoniche selezionate per l’analisi:



Questa figura è il risultato della ricerca ‘MSISDN associata a più IMEI’, ma mostra anche (all’interno del set di dati selezionato dall’operatore) tutti gli utenti che utilizzano più di un EMEI. Questa funzione è molto utile per evidenziare i collegamenti tra diversi utenti dello stesso dispositivo (i cosiddetti ‘telefoni dell’ala’, utilizzati da più di un detenuto).

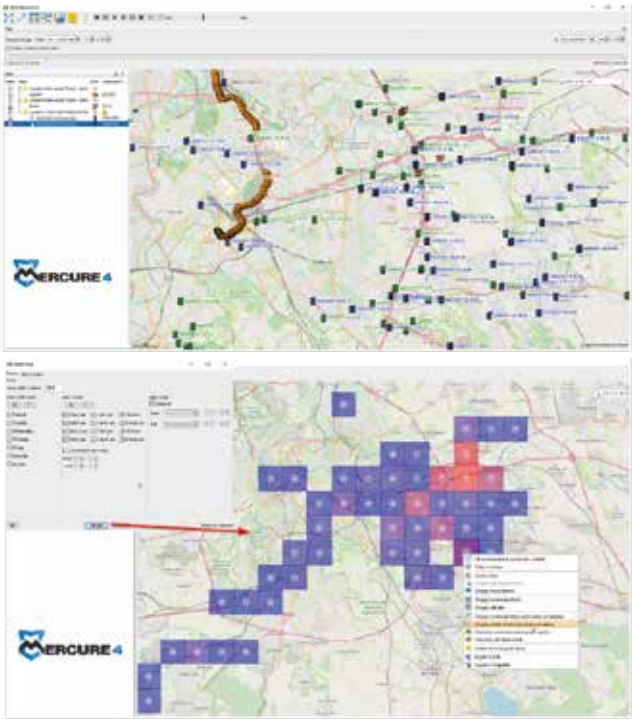


La presentazione visiva della timeline fornisce un'istantanea dell'evoluzione temporale dei diversi eventi connessi al traffico telefonico in uno o più dispositivi. È interattiva e può essere personalizzato nella definizione di molteplici cornici temporali.

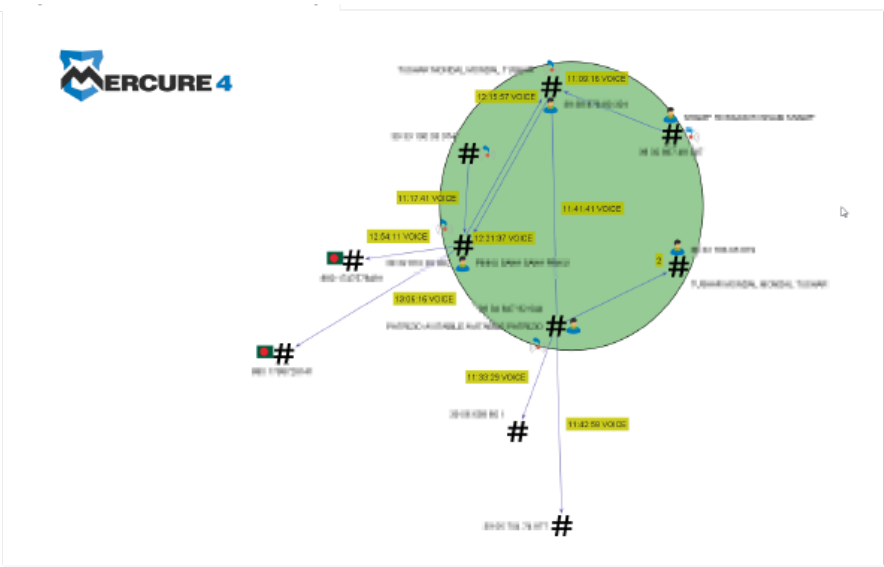
Le mappe geolocalizzate consentono la visualizzazione di eventi multipli in parallelo, combinando le chiamate telefoniche (posizione delle celle, azimuth), le posizioni GPS, le correlazioni con gli eventi, ecc.

La "mappa del calore" visualizza le aree in cui si verificano eventi importanti. Questa mappa è interattiva e può produrre analisi settoriali su misura cliccando sul punto desiderato. Gli utenti possono selezionare l'area geografica o gli intervalli temporali, o entrambi.

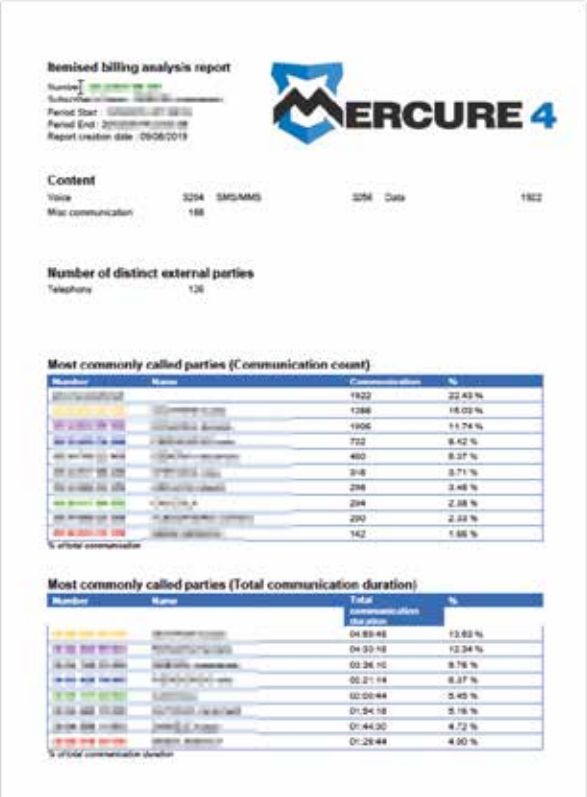
È possibile isolare il traffico telefonico interno (le telefonate tra i diversi utenti all'interno delle cellule interessate) all'interno del flusso di dati di una cella specifica (cioè tutti i numeri di telefono gestiti da n CGI in un periodo di tempo specifico).



Possiamo visualizzare graficamente il flusso di dati del telefono all'interno delle cellule bersaglio (cerchio verde).



Il sistema può quindi generare report PDF o Word che possono essere personalizzati



Itemised billing analysis report

Content

Number of distinct external parties

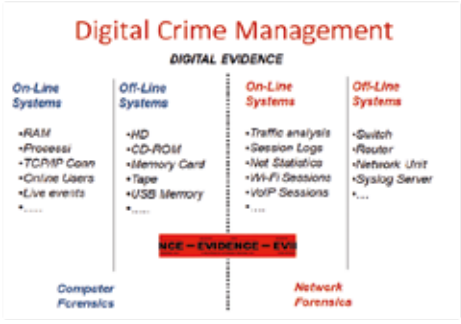
Most commonly called parties (Communication count)

Most commonly called parties (Total communication duration)

Infine, possiamo anche importare dati prodotti da altre estrazioni forensi, incluso il contenuto sotto forma di 'chat'.

III.3 - PRINCIPI DELLA 'DIGITAL EVIDENCE'

Non esiste procedimento preventivo o giudiziario di qualsiasi natura (civile, amministrativo, disciplinare, penale) che oggi non veda l'introduzione nel procedimento di qualche prova o dato "digitale". Anche quando l'elemento digitale non assurge a "prova" le ricostruzioni indiziarie o gli elementi logico-indiziari che possono essere forniti dalle "digital evidence" risultano sempre più determinanti e strategici per stabilire la colpevolezza o meno dell'accusato. Le Digital Evidence, che potremo definire come tutti quei dati, generati, trasmessi, conservati in forma digitale che possono essere utilizzati per affermare o confutare un fatto oggetto di un di un procedimento funzionale all'assunzione di misure di prevenzione o di un procedimento giudiziario; sono fragili per natura, come vedremo in seguito, tanto da richiedere particolari modalità nella loro gestione, che quando non rispettate, implicano talvolta, a seconda degli ordinamenti giudiziari, anche pesanti ripercussioni sulla "validità" di quella prova o indizio di rischio.



Se si intendono approfondire le caratteristiche delle digital evidence per un corretto approccio da parte dell'investigatore penitenziario, si potrebbe soffermarsi sulle seguenti:

- la prima, come già accennato, attiene alla loro natura che le rende altamente volatili. I dati possono essere facilmente sovrascritti, persi perché non memorizzati o persi per danneggiamenti fisico-meccanici del supporto di memoria stesso;

- la seconda è che sono soggette a continue modifiche talvolta indipendenti dalla volontà dell'utilizzatore, ad esempio non tutti gli operatori penitenziari che sequestrino un cellulare riflettono sulla necessità di un dump della memoria RAM prima dello spegnimento del PC, non considerando che con lo spegnimento il contenuto spesso strategico di tale supporto va perduto. La prova digitale è inoltre soggetta a modifiche spesso non note all'utente,

ma che modificano fortemente lo "stato" della prova digitale (metadati che registrano eventuali modifiche apportate al file); la terza attiene alla loro non facile ed immediata "individuazione". Spesso non solo è complicato individuare il "contenitore", ma anche il contenuto è spesso individuabile solo da esperti (i dati di registro del sistema, lo spazio non allocato del disco, l'esistenza di file particolari spesso sconosciuti ma che contengono informazioni utili all'investigatore);

- la quarta è che una volta acquisite, se correttamente trattate possono essere "riprodotte" in una identica copia pressoché all'infinito, permettendo così di conservare sempre inalterata una copia, indipendentemente dalle operazioni di natura tecnica svolte sulla stessa, che potrebbero in alcuni accertamenti modificarne, anche solo minimamente, lo stato;

- la quinta, ogni "contenitore" di digital evidence, ovvero ogni dispositivo digitale presenta, atteso il rapido sviluppo delle tecnologie, caratteristiche spesso nuove e sconosciute ai più, che potrebbero anche provocare pesanti modifiche ai dati in esso contenuti. É quindi necessario un approccio competente e qualificato in grado, ove possibile, di evitare le potenziali modifiche accidentali ai dati contenuti. Parimenti, questa continua "innovazione" tecnologica richiede anche il ricorso a nuove "regole di ingaggio" con il target finalizzate ad impedirne eventuali modifiche/alterazioni. In definitiva la digital evidence dovrà essere quindi ammissibile, ovvero ottenuta attraverso il rispetto della procedure legali e delle cosiddette "best-practices" previste per poter essere ammesse in un procedimento di prevenzione o giudiziario. Il mancato rispetto delle procedure legislative sconterà una censura quale "prova ammissibile" in quanto non ottenuta "legalmente", mentre il mancato rispetto delle best-practices sconterà censure sul piano dell'idoneità delle procedure adottate per la sua acquisizione in ordine alla: Autenticità completezza Affidabilità Credibilità Proporzionalità. Le Best Practices si basano quindi su alcuni principi che devono essere rispettati. La scelta di non definire procedure standardizzate ed obbligatorie è indotta essenzialmente dall'elevato e rapido sviluppo delle tecnologie (tecniche oggi idonee potrebbero non esserlo domani! Ed altrettanto, software oggi "mirabolanti" potrebbero segnare il passo di qui a breve e, non ultimo... vecchi software ormai considerati obsoleti potrebbero ancora dire la loro in termini di efficacia ed efficienza per taluni accertamenti).

III.4 - THE ISO/IEC 27037: 2012 STANDARD: DESCRIZIONE E CONSIDERAZIONI[42] 1

L'Organizzazione Internazionale per la Standardizzazione, definita ISO, e la Commissione Elettrotecnica Internazionale, IEC, costituiscono il sistema specializzato per la standardizzazione a livello mondiale.

Tra le norme elaborate dall'organizzazione ne esiste una dedicata alla digital forensic, denominata "Guidelines for the identification, collection, acquisition and storage of digital evidence".
Tali norme sono applicabili anche alle procedure di prevenzione, che richiedono solide prove o indicatori di rischio informatici per essere sostenute in un contenzioso legale.

In linea generale, tanto più le prassi operative di polizia si avvicinano alle modalità standardizzate descritte nella norma, tanto più affidabile sarà considerato il risultato nel procedimento di prevenzione o nel processo penale.

E' importante sottolineare che la norma ISO non include gli aspetti legali connessi alle varie fasi della digital forensic, mantenendo così un carattere di trasversalità tra gli ordinamenti necessario ad una norma che si concentra esclusivamente sugli aspetti tecnici. La norma, inoltre, non indica le modalità di analisi e reportistica delle evidenze digitali, limitandosi invece a definirne il ciclo di vita dall'identificazione alla conservazione, né indirizza a particolari software o hardware.

III.4.A LA NORMA DEFINISCE DUE FIGURE FONDAMENTALI: IL DEFR E IL DES.

Il DEFR, digital evidence first responder, è l'operatore di Polizia Penitenziaria che effettua il primo intervento sui sistemi, come ad esempio i supporti di memorizzazione d'interesse per l'indagine e l'azione di sorveglianza preventiva, la sorveglianza penitenziaria. Nel caso tipico di un atto di polizia quale ad esempio una perquisizione all'interno di una cella o una perquisizione domiciliare per una persona ammessa alle misure alternative, il DEFR coinciderà con il poliziotto (o con l'ausiliario di polizia giudiziaria) che espleterà le attività di digital forensic nell'abitazione dell'indagato, con l'ausilio di eventuali collaboratori. Il DEFR deve ovviamente possedere una preparazione ed una

42 Il presente capitolo contiene una descrizione sommaria e non esaustiva delle prescrizioni contenuta nella norma ISO/IEC 27037:2012, a cui sono accostate a volte considerazioni e opinioni dell'autore. Per tale motivo, quanto riportato non sostituisce la norma, né la integra. Solo la norma è lo standard interna- zionale di riferimento, alla quale si rimanda per tutti gli approfondimenti ed i contenuti scevri da considerazioni dell'autore, inevitabilmente influenzati dall'esperienza e personale.

qualificazione professionale idonea all'espletamento dell'incarico, tecnica e giuridica allo stesso tempo. L'agenzia o il datore di lavoro deve assicurare che la preparazione tecnica sia, ovviamente, aggiornata costantemente. Il DEFR dovrà utilizzare la diligenza ragionevole nell'espletamento dell'incarico, senza mai andare oltre ciò che è legalmente permesso, e valutando l'opportunità anche di non procedere all'acquisizione o alla raccolta di prove o indicatori di rischio informatici digitali qualora vi siano dei limiti imposti dalle circostanze.

Il DES, oltre a saper espletare il lavoro del DEFR, effettua anche attività specialistiche di un particolare settore (come, ad esempio, la network forensic).

La norma individua anzitutto i requisiti del reperto digitale: la rilevanza, l'affidabilità e la sufficienza.

La traccia digitale, quindi, deve essere rilevante ai fini dell'indagine ed all'azione di sorveglianza preventiva in corso, deve essere affidabile in quanto ai processi utilizzati per gestirla, e sufficiente per condurre un'indagine ed all'azione di sorveglianza preventiva in modo corretto.

La norma si occupa poi del trattamento della prova digitale, definendo i seguenti princìpi:

- verificabilità, intesa come valutazione dell'operato da parte di terzi
- ripetibilità o riproducibilità, ossia la possibilità di ottenere gli stessi risultati a parità di condizioni. Tale principio non è inteso in senso assoluto (nel campo digital forensic non potrebbe essere altrimenti). Il principio viene infatti soddisfatto quando è provata l'affidabilità dei processi utilizzati, anche mediante il controllo di qualità e la produzione di apposita documentazione.

- giustificabilità, che si intende soddisfatta quando si è in grado di giustificare ciò che si è fatto e le metodologie utilizzate per il trattamento delle potenziali prove o indicatori di rischio informatici digitali. In sostanza, bisogna poter dimostrare che è stata sempre effettuata la scelta migliore disponibile in quel momento.

III.4.B - TRATTAMENTO DELLE PROVE DIGITALI

Innanzitutto, è necessario che DEFR o DES siano in grado di utilizzare, almeno nelle operazioni fondamentali, il device su cui è contenuta l'evidenza digitale. Si ritiene che ciò ponga un problema di non poco conto: il personale che effettua tali operazioni deve essere mantenuto in costante aggiornamento, non essendo concepibile che DEFR o DES siano esperti di ogni singolo device immesso sul mercato. Ci si aspetta invece che ciascuno di loro possieda il tempo e le risorse necessarie per poter essere 'al passo con i tempi': in tal senso, sarà necessario conoscere le nuove versioni dei sistemi operativi degli smartpho-

ne, conoscere l'architettura dei software dei dispositivi IOT e smart-home più diffusi, conoscere le modalità di accesso e di gestione degli spazi cloud.
La conoscenza dei device consentirà di minimizzare il numero di manipolazioni che vengono effettuate su di essi, nell'ottica della preservazione del dato. Qualora un device non sia conosciuto, è meglio non spingersi oltre le proprie competenze. Il trattamento consta di quattro fasi: identificazione, raccolta, acquisizione e presentazione.
Prima di affrontare la questione del trattamento, è opportuno menzionare le precauzioni da prendere nel luogo dell'incidente, o nella scena del crimine. Innanzitutto, l'area va messa in sicurezza, in modo che estranei non possano avvicinarsi all'area delle operazioni né ai device.
La norma raccomanda poi di non accendere il device se è spento, e viceversa di non spegnerlo se è acceso. Si ritiene che l'applicazione di tale raccomandazione debba essere vagliata caso per caso; laddove, ad esempio, si ha notizia che il soggetto indagato sia particolarmente abile con l'informatica, è verosimile ritenere che egli abbia crittografato i dati. Nel rispetto delle leggi locali, a mente dell'obiettivo di ottenere il prima possibile la chiave di decrittazione, si ritiene dunque, benché non previsto espressamente dalla norma, che andrebbe valutata l'opportunità di accendere i device e chiedere lo sblocco durante l'intervento di polizia di prevenzione, considerando che al termine delle operazioni sarà più difficile che il soggetto sia disposto a fornirla.
Con particolare riferimento alle password, la norma raccomanda di fare attenzione a post-it, biglietti e manuali dei device, ove la password stessa potrebbe essere stata appuntata.
La scena va poi documentata, con disegni, fotografie e video. La norma prosegue con la raccomandazione di effettuare una dichiarazione del rischio, ove riportare una valutazione dei pericoli e dell'impatto che gli stessi rischi possono avere sulle prove o indicatori di rischio informatici digitali. Solo per citare alcuni rischi citati dalla norma, si ricorda la presenza di dati volatili essenziali all'indagine ed all'azione di sorveglianza preventiva, ma anche l'accesso remoto a qualunque device con capacità di alterarne il contenuto, oppure che il dispositivo potrebbe essere stato configurato per distruggere il proprio contenuto in alcune circostanze.
Le quattro fasi previste dalla norma sono: identificazione, raccolta, acquisizione, conservazione.
L'identificazione dell'evidenza digitale è la prima fase, che consiste nell'individuazione sia del device ove l'evidenza può essere contenuta, sia degli strumenti di archiviazione digitale. Per strumenti di archiviazione non è possibile ormai limitarsi ai consueti hard disk, CD/DVD/Blue Ray, usb-drive e tutto ciò che di tangibile "contiene" dati, che è già di difficile individuazione a causa delle dimensioni sempre più ridotte. La costellazione di dispositivi che memorizzano dati è ormai arricchita di NAS, cloud, e di tutte le memorie flash contenute nei dispositivi wearables ed in tutti gli smart-objects, finanche nei frigoriferi o nelle auto. Per tutti gli strumenti di archiviazione digitale, in ogni caso, è necessario documentarne la posizione e decidere se effettuare acquisizione sul posto o se portar via lo strumento.

Se lo schermo di un computer è acceso, è opportuno annotare cosa si vede sullo schermo.
Va poi effettuata una rilevazione dei segnali wireless con un apposito detector, in modo da identificare device eventualmente nascosti. La norma raccomanda che, una volta identificati tutti i dispositivi digitali, sia fatta una considerazione relativa alla volatilità del dato. Il dato volatile potrebbe infatti non essere più recuperabile: basti pensare al contenuto della memoria RAM di un PC. La considerazione relativa alla volatilità dei dati porterà il DEFR ad una scelta: i dati volatili sono importanti per l'indagine e l'azione di sorveglianza preventiva in corso? Se sì, ad essi va attribuita una priorità elevata.
Si ritiene sia logico pensare che, con il trascorrere del tempo e la diffusione dei dispositivi smart e della connettività 5G, la risposta sarà sempre più affermativa. L'acquisizione dei dati volatili è, tuttavia, onerosa e delicatissima, perché implica manomissioni anche minime - sui sistemi in esecuzione. Tale acquisizione è poi sempre necessaria nel caso di crittografia o rilevamento di malware. Nei residui casi in cui i dati volatili non siano importanti per l'indagine e l'azione di sorveglianza preventiva, può esser loro attribuita loro una priorità più bassa. La seconda fase è chiamata raccolta, e prevede lo spostamento del device presso un laboratorio forense per la successiva acquisizione ed analisi. Tale operazione può avvenire sotto forma di sequestro, qualora il telefono mobile sia trafugato illegalmente all'interno dell'istituto penitenziario, per esempio, ma anche sotto forma di accesso amministrativo al device nel caso di detenuti in misure alternative con indicatori di pericolo, a seconda del contesto e delle condizioni generali. La raccolta può comprendere non soltanto i device, ma tutto ciò che è potenzialmente in grado di fornire informazioni ulteriori (come ad esempio, i post-it per le password).
Tutto il processo va documentato, ivi compreso l'imballaggio. Bisogna fornire motivazioni in merito alla scelta di includere o escludere i device dalla raccolta, così come descrivere le motivazioni alla base del metodo utilizzato in relazione alla procedura legale o amministrativa, situazione, costi, tempi e finanche sull'imballaggio eseguito. La raccolta può riguardare anche prove o indicatori di rischio informatici non digitali, come quelle fornite a voce da parte dell'amministratore di sistema o dei soggetti responsabili dei device.
L'acquisizione, invece, è la creazione di una copia forense sul posto. La scelta di procedere all'acquisizione, rispetto alla raccolta, deve essere adeguatamente motivata in termini di metodo, strumenti utilizzati e attività compiute. Tale attività, eseguita su sistemi in esecuzione (si pensi a sistemi mission critical, bancari o di società che forniscono servizi di connettività per detenuti in misure alternative impiegati presso società o cooperative esterne o per detenuti che svolgono lavoro intramurario con l'ausilio di sistemi di rete) è intrinsecamente invasiva dei sistemi, e comporta inevitabilmente l'alterazione, anche minima, del sistema ove si effettua. Il DEFR, pertanto, dovrà applicare le metodologie meno invasive possibili, documentando pedissequamente le motivazioni dell'adozione del metodo utilizzato e degli eventuali cambiamenti apportati al sistema. Anche gli strumenti utilizzati dovranno essere il più possibile affidabili e riconosciuti.

Tale processo è comunemente denominato 'live forensic', a cui è dedicato un apposito capitolo nel presente elaborato.
Le copie dei dati, anche parziali (es. singola directory) devono essere sottoposte ad una procedura di verifica rispetto all'originale, comprovata ed attuale (ci si riferisce, ovviamente, alle funzioni di hash); deve essere documentata l'eventuale circostanza nei casi in cui ciò non sia possibile. Il sistema in esecuzione, infatti, potrebbe variare continuamente i dati acquisiti e dunque la funzione di hash potrebbe sembrare inutile; tuttavia si ritiene comunque utile effettuare la funzione di hash anche quando non serve ad attestare la conformità all'originale del sistema, ed inserirla nell'apposita documentazione; ciò consentirà di verificare le copie di lavoro o quelle successive necessarie per il giudizio o per l'analisi dei dati da parte della difesa, qualora si arrivi alla formalizzazione di un procedimento di prevenzione o ad un dibattimento.
Come si è potuto intuire, la seconda e la terza fase, raccolta e acquisizione, sono alternative tra loro, ed è necessario dunque un processo che porti alla scelta se effettuare l'una o l'altra. La norma si occupa anche del processo decisionale alla base della scelta alternativa tra raccolta ed acquisizione, elencando una serie di criteri da tenere in considerazione. Volatilità (RAM, processi in corso, connessioni network), crittografia del device e dei dati, e vincoli di tipo legale sono tra i parametri principali da prendere in considerazione.
Si ritiene pertanto che la domanda che il DEFR dovrebbe porsi è la seguente: "Se opto per la raccolta, e non per l'acquisizione, ho ragionevole certezza che il dato sia disponile nel momento successivo, quando in laboratorio dovrà essere acquisito ed analizzato?" Se, con ragionevole certezza, il dato può raccolto per un'analisi successiva, si ritiene che il DEFR possa attribuire priorità maggiore alla raccolta rispetto all'acquisizione. Vi sono tuttavia delle eccezioni, che l'investigatore penitenziario investito di poteri di Polizia Giudiziaria dovrebbe tenere presenti. Nell'ordinamento italiano, ad esempio, è possibile procedere all'arresto facoltativo per detenzione di ingente quantità di materiale pedopornografico (art. 600-quater c.p.), se cioè tale materiale viene rinvenuto durante la perquisizione informatica.
In tale occasione, il DEFR potrebbe preferire l'acquisizione alla raccolta, allo scopo di rilevare la presenza di video o foto con contenuti pedopornografici, quantificarla e procedere dunque all'arresto dell'indagato. La norma poi definisce i criteri da adottare in presenza di device accesi e di quelli spenti, ma anche delle situazioni critiche che possono presentarsi.
L'acquisizione di un digital device spento dovrebbe essere effettuata con una procedura di imaging convalidata, dopo aver rimosso il supporto di archiviazione dal device qualora possibile e se opportuno, con riferimento alla probabilità di rottura del supporto. Dovrà essere prodotta idonea documentazione del supporto e calcolata l'impronta di hash. Per l'acquisizione dai digital device accesi, si rimanda al contenuto della norma, ed alla trattazione specifica negli appositi capitoli. L'acquisizione può essere parziale, ad esempio quando ci si trovi di fronte a sistemi mission critical, data center o con un mandato di perquisizione circoscritto all'estrazione di una certa tipologia di dati. In tal caso, occorrerà individuare i file e le directory che contengano quanto d'interesse e

procedere all'acquisizione logica. In ogni caso, si ritiene che il DEFR dovrebbe sempre tenere a mente quanto riportato nella Convenzione di Budapest, il cui filo conduttore è sempre quello di evitare l'alterazione dei dati.
La fase successiva è chiamata conservazione dei dati. Essa consiste nella preservazione dell'integrità dei dati e dei device da eventuali alterazioni naturali, dolose o colpose. La conservazione riguarda tutto il processo di trattamento della prova digitale. Va sottolineato anche l'aspetto confidenziale del dato: la conservazione dovrà quindi garantire che la lettura dei dati sia possibile solo al personale autorizzato. In tal senso, la conservazione dovrà avvenire in una struttura dotata di sicurezza fisica con eventuale limitazione degli accessi. Tutto il processo di conservazione dovrà assicurare, oltre alla confidenzialità, l'integrità e la disponibilità delle potenziali prove o indicatori di rischio informatici digitali. I device dovranno essere imballati con strumenti adeguati alle caratteristiche fisiche del device stesso.
E' noto, ad esempio, che gli hard disk meccanici possono essere alterati a seguito di esposizione a campi elettromagnetici, ma anche danneggiati in caso di urto; in tal caso, la soluzione ottimale sarebbe quella dell'utilizzo delle anti static bags. Per gli smartphone e i PDA, invece, potranno essere utilizzati i sacchetti con gabbia di Faraday, che sono i grado di togliere la connettività, a patto di utilizzare un alimentatore aggiuntivo per evitare lo scaricamento rapido della batteria. Si ritiene che, in questi casi, la modalità migliore in cui conservare il device sia la "Airplane mode". L'imballo dovrà poi contenere l'etichettatura identificativa, che andrà firmata almeno dal DEFR. Si ritiene comunque utile, quando non prescritto dall'ordinamento, la controfirma dell'indagato. Fondamentale è mantenere la cosiddetta catena di custodia. Si tratta di un documento ove, in ordine temporale e sin dal processo di raccolta o acquisizione, sono registrate le operazioni di movimentazione e di trattamento delle evidenze digitali. Mediante tale documento, il DEFR potrà render conto della storia dell'evidenza digitale fino al momento attuale, rispondendo così alle eventuali domande: "quando, dove e chi ha avuto accesso alla prova?" e "c'è stata un'alterazione? Se sì, in che momento?". Alla catena di custodia è poi associato il momento del trasporto del device o della digital evidence, sempre nell'ottica di evitare l'alterazione dei dati. La norma raccomanda di utilizzare la crittografia in tutti i casi in cui il "reperto" non sia trasportato dal DEFR.

Si riporta un esempio di documento di catena di custodia.

DESCRIPTION OF EVIDENCE

ID	SERIAL NUMBER	DESCRIPTION

CHAIN OF CUSTODY

ID	DATE and TIME	RELEASER	RECEIVER	COMMENTS

La norma prosegue poi indicando un apposito capitolo al briefing, o riunione informativa con l'autorità competente, sia essa la magistratura inquirente o un superiore in ambito di misure amministrative. In tale riunione, bisognerà anzitutto definire le circostanze dell'incidente, in modo da circoscrivere cosa cercare, quali prove o indicatori di rischio informatici ci si aspetta di trovare o meno. I partecipanti, al termine della riunione, dovrebbero avere ben chiari i propri ruoli. Nel briefing dovrebbero essere fornite le informazioni necessarie per la raccolta o l'acquisizione delle prove o indicatori di rischio informatici digitali, che possono derivare da una precedente azione di monitoraggio sulla radicalizzazione o dalla sorveglianza preventiva effettuata, unitamente a raccomandazioni varie quali ad esempio quella di spegnere il Wi-Fi dei dispositivi personali per evitare alterazioni involontarie dei dati. Il briefing dovrebbe anche affrontare il tema del personale coinvolto nell'indagine e nell'azione di sorveglianza preventiva o nell'incidente critico: non è infrequente, infatti, che alle operazioni partecipi anche personale extra-informatico, con competenze mediche, biologiche ecc. La norma poi pone particolare attenzione ai networked devices, ossia tutti quei dispositivi connessi ad una rete, fornendo delle linee guida per la corretta raccolta ed altre linee guida per l'acquisizione. Le linee guida per la raccolta indicano di tracciare le connessioni attive del device e poi, se necessario, isolare il device dalla rete (ad esempio staccando il cavo di rete) solo se si ha la certezza che tale azione non comprometterà dati rilevanti e non produrrà malfunzionamenti su sistemi critici. In generale le best practices tengono conto dei principi di seguito elencati senza pretesa di esaustività, consigliando agli operatori di prenderne visione in dettaglio a seconda dei rispettivi ordinamenti giuridici, essendo alcune di queste, per taluni ordinamenti, "elementi essenziali" del processo di gestione delle digital evidence. Le attività svolte non dovrebbero mai modificare i dati, i dispositivi o i supporti elettronici. Tutte le attività vanno attentamente documentate sia per consentire la "ripetizione" delle operazioni effettuate, ove tecnicamente possibile, sia quale verbalizzazione delle operazioni svolte, peraltro utile a costituire il cd. "primo anello" della catena di custodia (Chain of Custody) che verrà analizzata in seguito. Le attività, ove possibile, andranno eseguite da personale esperto e, ove non disponibile, limitarsi a quelle operazioni che arrecano minor pregiudizio in termini di "ammissibilità" della prova o dell'indicatore di rischio. Allo stesso modo, il personale anche non esperto che effettua il cosiddetto 'primo intervento' dovrà essere adeguatamente formato sulle modalità di ricerca, individuazione ed assicurazione delle digital evidence in attesa dell'intervento successivo sul posto, o postumo a distanza di alcuni giorni da parte del personale più esperto.

III.5 - ASPETTI OPERATIVI

Tutti sono concordi nel ritenere che il primo "passo" che l'investigatore digitale deve compiere sia quello dell'individuazione del "target" o bersaglio, o in gergo tecnico, dei dispositivi che dovranno essere attenzionati perché ritenuti di particolare interesse in funzione dell'azione di prevenzione, pre-investigativa o investigativa. L'operazione è oggi complicata:

1 dalla “proliferazione” di dispositivi e conseguentemente di potenziali “bersagli” da controllare nel corso di perquisizioni, ispezioni e sequestri, non solo PC-Desktop, NAS, Notebook, Netbook, Tablet, Smartphone, Hard-Disk, Pen Drive, etc. ma anche il cosiddetto IoT Internet of Things, il cloud, e tutto ciò che nel linguaggio comune definiamo “intelligente” (auto, elettrodomestici, dispositivi indossabili etc.)

2 dalle difficoltà di accedere agli stessi, nel rispetto delle “best practices” di seguito descritte; per esempio tutti i dispositivi che non presentano i classici “connettori” USB, o che hanno supporti di memorizzazione di non facile accesso, ma anche constatando che tali dispositivi sono ormai sempre più frequentemente accompagnati da affinati sistemi di sicurezza che, se da un lato assicurano un’efficace tutela dei dati, dall’altro rendono sempre più difficoltoso il lavoro della polizia di prevenzione e degli investigatori;

3 Inoltre, va considerato che in un’epoca di inarrestabile digitalizzazione decine di dispositivi digitali sono presenti nelle nostre abitazioni, uffici e spesso anche indossati. La mole di dispositivi che oggi si pone dinanzi all’operatore di polizia di prevenzione ha raggiunto livelli tali che uno dei problemi che affliggono l’investigatore digitale è quello di ‘quale dispositivo sottoporre ad esame’ a scapito di molti altri.

Si crede, erroneamente, che l’informatica abbia velocizzato le operazioni di ricerca ed individuazione delle digital evidence di interesse. In realtà, a cagione di quanto sopra evidenziato, sottoporre sul posto ad analisi, quand’anche speditive, tutti i potenziali contenitori di dati oggi è una chimera, se non in rarissime occasioni che ormai costituiscono più casi di scuola che non realtà operativa. Le soluzioni finora consigliate ‘segnano il passo’ di fronte alla realtà sopra tratteggiata. Si pensi alla possibilità di sequestro dei dispositivi riservando ad una fase successiva l’esame del loro contenuto; tale soluzione, tutt’ora adottata, sta incontrando tuttavia diverse difficoltà sia sul piano della problematica del “superamento del sequestro”, di natura più squisitamente “processuale”, sia sul piano pratico, in quanto tale procedura non sempre è adottabile (mainframe, server strategici, Cloud, IOT). Pertanto, a soluzione del problema occorrono l’esperienza ed il patrimonio investigativo dell’operatore di polizia di prevenzione, che attraverso una “analisi di contesto” potrà restringere il campo dei “possibili target” solo a quei dispositivi che per il particolare “contesto” potranno con più probabilità contenere i dati digitali che si stanno ricercando. In pratica è quindi necessario, nell’evidenza che l’investigatore digitale non è dotato di poteri magici, procedere ad un adeguato “briefing” che lo renda consapevole dei dettagli: dello scopo, dell’oggetto e del metodo di esecuzione delle operazioni; delle abitudini informatiche (ove ottenibili) del soggetto, utili per definire anche brevemente le reali capacità informatiche. Sul luogo delle operazioni sarà necessario imparare, anche attraverso l’adozione di tecniche di indagine e l’azione della sorveglianza preventiva tradizionale, i luoghi in cui i dispositivi possono essere nascosti, considerato che,

in particolare coloro che non hanno familiarità con i dispositivi informatici, tendono a nasconderli, piuttosto che ricorrere a "tecniche" come crittografia, steganografia, ecc., più utilizzati da persone più esperte e che in virtù della sicurezza "intrinseca" in questi sistemi non si occupano di nasconderli. Occorre prestare particolare attenzione:

- a tutti quei supporti che possono essere facilmente nascosti e camuffati in oggetti di uso quotidiano (mattoni Lego USB, gadget, ecc.);

- alla capacità del soggetto di interagire con le piattaforme "cloud" e "social";

- al monitoraggio della "rete" attiva sul sito al fine di identificare eventuali dispositivi "remoti" spesso nascosti in cavità, soffitte e altri luoghi che non sono facilmente ispezionabili;

- a tutti quei dispositivi che hanno una particolare "vicinanza" al soggetto, "smartphone", dispositivi "indossabili", notebook, ecc. Infatti, non esiste alcuna "regola" o manuale che possa garantire le azioni dell'investigatore con procedure prescritte, volte all'identificazione. Ogni contesto rappresenta un caso particolare e richiederà approcci propri. Molto spesso il buon senso e l'intuizione dell'investigatore sono in grado di raggiungere una sufficiente identificazione del bersaglio. Una volta identificato il nostro obiettivo, il passo successivo e necessario è cercare di ricondurlo ad una delle categorie di dispositivi noti. Tale operazione è non è semplice o immediata perché richiede una comprensione di ciò che accadrà. Oggi, ciò implica elevate competenze tecniche e informatiche, al fine di giungere ad una precisa "qualificazione" del target. Al giorno d'oggi troviamo nuovi dispositivi, spesso sconosciuti o addirittura "ibridi", che non solo non facilitano la loro identificazione, ma ne rendono anche la gestione successiva più complessa in termini di identificazione, acquisizione e recupero.

Dispositivi accesi o spenti – In merito all'acquisizione del dispositivo, il primo elemento da dirimere è l'accertamento circa lo stato di "acceso" o "spento" del dispositivo, poiché dallo stato del dispositivo dipendono le azioni successive da intraprendere a cagione delle profonde e spesso irreversibili modifiche che il dispositivo subisce allorquando è acceso e viene spento o, viceversa, da spento viene acceso. Le implicazioni derivanti dallo stato del dispositivo si riverberano anche sugli aspetti concernenti gli accertamenti urgenti, quelli ripetibili ed irripetibili, approfonditi a parte. Ad ogni buon conto, stabilire se un dispositivo è acceso o spento può essere operazione tutt'altro che facile ed agevole. Si pensi a quei dispositivi di nuova generazione comandati da remoto nei quali non sempre sono presenti spie luminose o altro (tasti on/off) utili a comprenderne/dedurne lo stato di acceso/spento. Stabilire se il dispositivo è acceso o spento diventa pertanto strategico onde intraprendere il corrispondente percorso che condurrà alle successive fasi di acquisizione sul posto o di sequestro del dispositivo. É noto che le canoniche fasi di acquisizione e

preservazione, che consistono in una serie di best practices da applicarsi per assicurare i migliori risultati in termini di integrità e disponibilità dei dati digitali, sono strettamente correlate e dipendenti dallo stato di acceso o spento del dispositivo, tant'è che a seconda dello stato del target si è soliti distinguere tra l'esecuzione di tali fasi in:

- **post mortem forensics;**
- **live forensics.**

Tale distinzione viene tutt'ora utilizzata come riferimento, tant'è che potremo affermare che non esiste manuale di digital forensics che non origini da tale fondamentale assunto (strettamente collegato allo "stato" di acceso/spento del dispositivo), prima di specificare le "best pratices" da applicarsi per una corretta acquisizione e gestione del dispositivo attenzionato.
Il personale penitenziario non esperto, che si trova di fronte a mobile devices illegali all'interno di un istituto penitenziario, molto spesso non è in grado di effettuare operazioni che vadano oltre il mero spegnimento e repertamento del dispositivo acceso o spento, non disponendo di alcuna cognizione circa l'ordine di volatilità del dato e, purtroppo, non disponendo il più delle volte dell'hardware e del software utili all'effettuazione delle operazioni necessarie a preservare lo stato in cui è stato trovato il reperto acceso. Neppure, detto personale "ordinario" si sente adeguatamente responsabilizzato o non è adeguatamente formato ed informato sulle proprie responsabilità, prediligendo nell'incertezza delegare operazioni a personale "esperto" che tuttavia, ad oggi, è ancora in numero inadeguato rispetto alle concrete necessità operative degli istituti ed al rilevante numero di sequestri effettuati.
Nel tempo si è creato un mantra, che recita: *"se il PC è spento, va lasciato spento; se il PC è acceso, va spento"*, che può sembrare una soluzione adeguata nella maggior parte dei contesti operativi e che anticipa la presenza di personale non specializzato responsabile delle operazioni di sorveglianza e di ricerca. Le cose, tuttavia, appaiono diametralmente opposte allorquando nel medesimo contesto venga invece a trovarsi personale adeguatamente formato per attività di sorveglianza in materia di radicalizzazione e terrorismo.
In tal caso le operazioni potranno, a seconda dello scenario, distinguersi nelle canoniche "live" o "post mortem" forensics. Invero tale differenziazione prenderà spunto proprio dalla condizione di acceso/spento in cui verrà rinvenuto il target all'interno dell'istituto o nell'ambiente in cui opera la persona in misure alternative alla detenzione o in libertà vigilata. Differente sarà quindi l'approccio che il personale esperto dovrà avere a seconda che il target sia rinvenuto in modalità acceso o spento.
A titolo esemplificativo e pratico si descrive di seguito una situazione operativa nella quale vengono rinvenuti due telefonini o due PC, uno acceso e uno spento. Riguardo a quello spento verrà rimessa al personale esperto, eventualmente, l'opportunità di procedere, attraverso l'utilizzo delle cd. "Live_Linux_Forensics" (es. DEFT, CAINE, PALLADIN, etc.), all'effettuazione di una "preview" volta ad apprenderne il contenuto. Tale operazione, svolta in moda-

lità RO (read-only), non andrà ad alterare in alcun modo i dati e permetterà al personale di perquisirne il contenuto già sul posto.
Tale operazione è rimessa al solo personale esperto che saprà adottare le tecniche idonee e descriverle, assicurando ove possibile che le operazioni di perquisizione siano avvenute nel rispetto della legge nazionale o dell'EIO e delle best practices. Occorre infine evidenziare come in tale ipotesi il rischio di alterabilità dei dati presenti è più basso, a condizione che vengano adottate le cautele previste dalle best practices (ad esempio accesso alle memorie in modalità RO (read only). Di tutt'altra complessità è invece la gestione del telefonino o PC rinvenuto acceso nell'appartamento di una persona in misura alternativa alla detenzione, al di là delle già complesse modalità di spegnimento che dovranno adottarsi.
Nel caso di un dispositivo acceso e collegato alla rete, l'operazione di acquisizione dei dati diventa anche per l''esperto" un'attività molto rischiosa in termini di genuinità, inalterabilità ed immodificabilità dei dati rinvenuti al momento dell'atto, nonché in termini di garanzie difensive da riconoscersi alla controparte, sulla base delle norme previste dalla Stockholm's Roadmap e dalle leggi nazionali. In alcuni casi, nell'esecuzione di una perizia informatica, lo spegnimento del PC comporta la perdita di tutta una serie di dati ed informazioni contenute nella RAM, purtroppo spesso sottovalutate, ma che successivamente si rivelano di importanza fondamentale in sede di assunzione di misure di prevenzione, di sicurezza o di dibattimento giudiziario. Ad esempio: processi in esecuzione, volumi crittografati "aperti" (Truecrypt, Veracrypt, BitLocker etc.), connessioni attive, chat aperte, moduli caricati ed in utilizzo, nonché una serie di informazioni, anche datate, che potrebbero comunque rivelarsi di interesse per il caso.
Peraltro non si esclude che il PC rinvenuto acceso costituisca in quel preciso momento uno stato di "flagranza di reato" che richiede un tempestivo ed immediato congelamento di determinati dati, costituenti prova del reato, i quali a seguito dello spegnimento dello stesso potrebbero andare persi (volumi criptati, connessioni on banking, chat room aperte etc). In tali contesti si rende necessario procedere ad un "congelamento" dello stato della RAM del PC in esecuzione. Tale operazione si renderà necessaria ogni qualvolta uno degli elementi volatili sopra citati costituisse elemento necessario e strategico per l'indagine e l'azione di sorveglianza preventiva. L'operazione tecnica di "dump" della RAM non è certo scevra di controindicazioni, atteso che per procedervi sarà necessario avviare specifici tool che in modo più o meno incisivo e diretto andranno comunque ad alterare lo stato preesistente anche della RAM. Si comprende come l'analisi di contesto divenga allora imprescindibile poiché costituisce l'ago della bilancia che andrà ad indicare all'esperto se procedere ad un mero spegnimento, in tutti quei casi in cui il contenuto della RAM e le altre connessioni attive non assumono alcuna rilevanza, ovvero procedere consapevolmente ad un "dump" della stessa, prima di procedere allo spegnimento del sistema, in base al principio secondo cui in assenza di altre soluzioni praticabili, l'operatore di Polizia Penitenziaria apporterà modifiche al sistema ma disporrà comunque di un risultato. Analoga considerazione andrà

effettuata in ordine agli eventuali volumi "decriptati" e a quelli di rete collegati in quel momento, nella considerazione che lo spegnimento del PC comporterà la perdita di detti collegamenti e della possibilità di accedere ai volumi criptati in assenza delle password/credenziali. In assenza di personale penitenziario esperto e dei necessari strumenti, si potrà comunque procedere con metodi "alternativi" a cristallizzare in qualche modo "lo stato delle cose"; video e foto saranno ormai strumenti nelle mani di tutti, pertanto si potrà procedere anche con tali devices, come un semplice smartphone, a documentare (il termine qui è giuridico) lo stato delle cose. O si potrà procedere all'ibernazione di un sistema Windows anziché al suo spegnimento. Si tratta della procedura che l'operatore di Polizia Penitenziaria deve applicare in caso di attività di sorveglianza, indicatori di rischio o nel quadro di un'indagine con funzioni di polizia giudiziaria:

- verifica dello stato di acceso/spento:
- molti dispositivi prevedono una spia di stato: riferirsi a questa, comunque con attenzione in quanto non è complicato invertire i led ed ingannare gli operatori. Fare riferimento in tal caso ai rumori della ventola o al calore emesso dal dispositivo;
- attenzione agli stati di stand-by dei portatili spesso azionati dall'apertura e chiusura del coperchio; nei portatili considerare ove possibile la rimozione della batteria;
- verificare attraverso la tastiera o il mouse che il dispositivo non si trovi in stato di risparmio energetico;
- documentare ogni azione intrapresa sia per iscritto sia, ove possibile, con documentazione foto-video;
- nel dubbio, contattare personale esperto. Dopo aver accertato lo stato del dispositivo, ci sono due ipotesi di lavoro:

IPOTESI DI DEVICE ACCESO: richiedere l'intervento di personale esperto con competenze di live-forensics oltre che di prevenzione della radicalizzazione. Tuttavia, in attesa di personale più esperto, è possibile: "congelare la scena" attraverso rilievi fotografici e video che documentino lo stato di attività del dispositivo; valutare attentamente, prima dello spegnimento del dispositivo, ove possibile e realizzabile, l'opportunità di procedere ad un "dump" della RAM o alla messa in "ibernazione" del dispositivo; effettuare tali considerazioni, procedere allo spegnimento; sulle modalità di spegnimento esistono varie "teorie" valide e meritevoli di attenzione, tanto da poter affermare che non ne esiste una più consigliata di altre. Il dibattito su come spengere il pc è tutt'altro che sopito tra gli esperti. I motivi si attestano sostanzialmente tra una posizione prudente, volta alla tutela dell'hardware e software del PC, tanto da consigliare sempre lo spegnimento attraverso le procedure "ordinarie", che si scontra con altra prudenzialmente volta ad impedire che attraverso lo spegnimento "canonico"/"ordinario" si possano attivare procedure di "erase" (cancellazione sicura dei dati) dei dati con ovvie irreparabili conseguenze sul piano della successiva acquisizione "probatoria"; tra i due estremi compaiono

poi diverse tecniche “intermedie” che cercano di mediare le criticità dell’una e dell’altra. Esistono diverse tecniche di spegnimento che non utilizzano le procedure indicate dal S.O. (attraverso START); a titolo di esempio, alcune combinazioni di tasti o l’utilizzo di comandi da terminale/shell che impediscono di cadere nella trappola del tasto START (l’apertura di una consolle e la digitazione di una stringa, per esempio: # shutdown -h now .)

IPOTESI DI DEVICE SPENTO: a seconda dei contesti andrà valutata la necessità di procedere all’accensione ed esame sul posto del dispositivo; tale operazione dovrà essere effettuata da personale esperto, dotato delle necessarie attrezzature hardware e/o software. Tale procedura avverrà solo in quei casi in cui risulti necessario procedere all’immediato accertamento di fatti urgenti sul luogo delle operazioni. In tutti gli altri casi si procederà, come meglio successivamente descritto, al solo “repertamento” del dispositivo riservando le operazioni di esame ad una fase successiva.

Acquisizioni a seguito di perquisizione in scenario “post-mortem”
Si tratta, ferme restando le considerazioni nel prosieguo, della situazione di più facile risoluzione una volta superate le problematiche già precedentemente evidenziate di “individuazione del target”, in quanto il personale meno esperto si ritroverà soltanto a lasciare il dispositivo nell’attuale ”condizione” (spento) e procederà al suo repertamento e sequestro, riservando ogni altra attività tecnica a personale esperto in un fase successiva. L’acquisizione di un target dovrebbe quantomeno essere sempre accompagnata da ragionevoli sospetti o prove o indicatori di rischio, quand’anche indiretti, risultanti da meccanismi tradizionali di monitoraggio e sorveglianza, che ne giustifichino l’indagine e l’azione di sorveglianza preventiva; ne consegue che qualora vi sia la presenza di personale esperto, verrà di volta in volta valutata l’opportunità di procedere ad una “preview” dei dispositivi prima di sottoporli all’eventuale “sequestro” o acquisizione. Le digital evidence devono essere trattate con particolare cura ed in modo da preservarne il valore probatorio o indiziario, a cagione delle particolari caratteristiche insite nella loro natura. Tale principio vale sia per l’integrità fisica di un dispositivo (contenitore), ma anche per i dati digitali che esso contiene (contenuto). L’esperienza operativa consentirà di apprendere che le fonti di prova o gli indicatori di rischio digitali richiedono particolari modalità di “gestione” in termini di acquisizione, conservazione, trasporto, che tengano conto anche di eventuali danni o alterazioni che possono derivare da urti accidentali, dal logoramento fisiologico del supporto, da fonti di calore ed elettromagnetiche e da ogni altra “interferenza” meccanico-fisica che possa in qualche modo danneggiare/modificare/deteriorare la digital evidence. Appare opportuna un’ultima osservazione riguardo ad alcuni elementi, spesso sottovalutati perché non digitali, che possono rinvenirsi durante una perquisizione all’interno di camere di pernottamento nel corso di un evento critico o sulla scena del crimine. Innanzitutto, si richiama la necessità di un’attenta e minuziosa descrizione (foto, video, disegni) del luogo in cui viene rinvenuto il “target”; tali elementi, talvolta apparentemente superflui, possono poi rivelar-

si “strategici” allorquando vi sia la necessità di pervenire ad una più precisa “identificazione” del sospetto. Inoltre, tale modalità di “ricognizione” indiretta permetterà, ex post, di rilevare abitudini, passioni ed altre caratteristiche che potrebbero rivelarsi molto utili per risalire ad un dizionario di parole da utilizzarsi per un password-cracking. Talvolta un’attenta “ricognizione” dei luoghi permette di risalire con immediatezza ad appunti, post-it, note in agende ed altri supporti cartacei contenenti le password ricercate. Si richiama altresì l’importanza della disposizione dei dispositivi, anche per rilevazioni che hanno più che a vedere con la cosiddetta “Polizia Scientifica” (impronte digitali, DNA) che in taluni scenari potrebbero divenire determinanti per l’individuazione dell’autore.

Acquisizioni a seguito di perquisizione giudiziaria o amministrativa in scenario “live-forensics”

Oggi la digital forensics predilige il mantenimento in stato di accensione dei dispositivi oggetto d’indagine ed analisi. Un aumento delle capacità delle RAM, un esponenziale incremento delle velocità di connessione sulla rete e, non da ultimo, un ormai universale interesse da parte degli utenti a mantenere criptati i propri dati per motivi di privacy e sicurezza da potenziali furti e smarrimenti, consigliano di non staccare l’alimentazione. Ciò potrebbe infatti comportare la perdita dei dati comunemente noti come “volatili”, l’interruzione delle connessioni attive in quel momento e il blocco dei file e dei volumi aperti che sono soggetti a crittografia. Considerato il problema, ovvero il rischio di perdita di tali dati, che potrebbero essere strategici per l’indagine e l’azione di sorveglianza preventiva, occorre anche considerare che le possibilità di alterare o sovrascrivere gli elementi di prova su di un sistema “live” è talmente elevata che le operazioni in “live-forensics” devono essere poste in essere a cura di personale esperto in materia. Invero, pur essendo scontato che le procedure adottate vanno ad impattare sul sistema, queste sono le uniche ad oggi conosciute e praticabili per la salvaguardia dei dati “volatili”, delle connessioni attive e dei files e volumi criptati di interesse investigativo. Proprio a cagione dell’inevitabile impatto sul sistema, è buona prassi non solo documentare precisamente le azioni intraprese ma, ove possibile, documentarle al meglio con altri mezzi quali foto e video, che potranno tenere traccia delle operazioni svolte e delle modifiche da queste apportate allo specifico sistema. Alla luce di tali fondamentali considerazioni, appare evidente come pur non essendo più al passo con i tempi lo spegnimento “tout court” del sistema, in assenza di personale esperto ci si limiterà alla realizzazione di foto e video del sistema in funzione e quindi si procederà (ove possibile) al suo spegnimento senza provvedere altrimenti, ritornando di fatto alla situazione del sistema “spento” già trattato in precedenza. Per evidenziare l’importanza del contenuto delle memorie volatili si riporta un elenco dei dati non esaustivo delle informazioni che possono rinvenirsi:

- Utenti connessi;
- Servizi in esecuzione;

- Informazioni di sistema;
- Processi in esecuzione;
- Porte di comunicazione aperte o in ascolto;
- Informazioni di avvio automatico;
- Informazioni del registro di sistema non ancora scritte su disco;
- Documenti non salvati; Codice binario dei processi, compresi i malware che risiedono solo in memoria.

Le memorie possono anche rivelare informazioni utili come le password o le applicazioni decifrate (utili se sul dispositivo sono installati software di crittografia) e, a volte, anche codici maligni che non sono salvati su disco, ecc. Considerata l'importanza di riflettere attentamente in caso di un sistema acceso, onde non incorrere nella perdita di dati spesso di grande importanza, in assenza di personale esperto si adotteranno le seguenti azioni finalizzate a ridurre al minimo il rischio di perdita di dati e informazioni in attesa, ove possibile, dell'intervento di uno specialista ovvero di un suo possibile supporto, anche da remoto, nella gestione del caso.
Occorre preliminarmente procedere alla messa in sicurezza del luogo e, attraverso foto e video, documentare lo stato del dispositivo contenente i dati volatili, in attesa dell'intervento dello specialista. Ogni situazione rappresenta dunque un caso a sé e non esistono procedure standardizzate che assicurino il successo in ogni contesto.
A seconda dei dati che potrebbero andare dispersi dopo lo spegnimento del dispositivo, vi sono tecniche quali il "dump" della RAM o anche sistemi più ordinari ma efficaci come quello di acquisire i files fintanto che questi risultano accessibili sul "cloud" o sono in "chiaro", in quanto decriptati. Ad ogni buon conto, il consulto con uno "specialista" è sempre consigliato, atteso che qualsiasi operazione effettuata su un sistema acceso provoca "modifiche" e potrebbe condurre ad invalidare la "digital evidence" acquisita.
In sintesi, la presenza di un sistema acceso dovrà sollecitare maggiore attenzione in capo agli operatori, diretta da un lato alla gestione di un dispositivo in continua "modificazione", dall'altro ad evitare che si proceda all'immediato spegnimento dello stesso con una perdita "irreversibile" di informazioni e dati. Infine, si rammenta che le operazioni svolte su sistemi accesi non andranno mai memorizzate sul medesimo "target" con conseguente modifica dell'originale e cancellazione per sovrascrittura di dati che potrebbero rivelarsi strategici. Pertanto, le eventuali operazioni di dump della RAM o di copia di files andrà effettuata su supporti "terzi", messi a disposizione dagli investigatori penitenziari, ove possibile e realizzabile. L'acquisizione di dati da sistemi accesi consente anche di introdurre il tema dell'acquisizione dei dati da sistemi che non possono essere mai spenti o sottoposti a sequestro, ovvero prelevati dal luogo in cui si trovano in funzione. Quanto evidenziato in precedenza è riconducibile al classico caso del PC acceso/PC spento, che oggi ancora si presenta di frequente nei contesti operativi "domiciliari" connaturati dalla presenza di uno o più dispositivi collegati in "rete" tra loro. Tuttavia, la realtà operativa spesso presenta situazioni che coinvolgono: infrastrutture di rete dove i dati

degli utenti sono salvati su server centralizzati suddivisi in gruppi di condivisione all'interno di un gruppo di reti; sistemi che non possono essere spenti e rimossi per ragioni di sicurezza medico-sanitaria, giudiziaria, di lavoro penitenziario o di sicurezza, etc., ovvero sistemi il cui funzionamento non deve essere mai interrotto, si pensi ai sistemi di controllo e di sicurezza all'interno del penitenziario medesimo; sistemi che non possono essere facilmente rimossi e trasportati quali mainframe, server di rilevanti dimensioni, server ubicati in spazi extraterritoriali; dati conservati sul "cloud".

Nuovi modelli di collaborazione pubblico-privata: E' evidente come al di là della "volatilità" dei dati, gli stessi non siano conservati solo in locale, ovvero sulla macchina "host" individuata, ma possono anche essere conservati su altri dispositivi collegati alla medesima rete ed in ogni caso conservati su dispositivi che potremo definire "intrasportabili" o che non possono essere facilmente spenti. Basti pensare ad un detenuto sottoposto alla misura di messa alla prova o in misura alternativa che operi in un'azienda di piccole-medie dimensioni, oggi caratterizzata dalla presenza di diversi PC, collegati tra di loro ed anche da un sistema "server" o "NAS", o ad un detenuto monitorato che svolga attività di formazione a distanza attraverso un learning management system gestito da un'università, con migliaia di studenti e un server esterno. Nella maggior parte dei casi i server dell'azienda o dell'università non possono essere spenti e sequestrati a causa dei vincoli esterni, così come le quantità di dati presenti nei vari sistemi sconsigliano o rendono difficile l'acquisizione "integrale" dei dati. Peraltro, in tali contesti l'operatore di polizia penitenziaria si espone all'accusa di 'superamento del sequestro', allorquando lo stesso non si sia limitato all'acquisizione di dati riconducibili al procedimento in trattazione, ma abbia acquisito anche dati di terzi di varia natura (industriali, marchi, brevetti, persone naturali, etc). In tali contesti si rende spesso indispensabile la collaborazione degli amministratori di sistema, che non è finalizzata alla sola conoscenza della "rete locale". Una partecipazione proattiva di soggetti terzi alle operazioni di monitoraggio finalizzate alla prevenzione o alle indagini, contribuisce ad ottenere "permessi" altrimenti difficilmente acquisibili per accedere alla rete ed effettuare le necessarie operazioni. Si tratta di un caso specifico di come la collaborazione pubblico-privata costantemente proposta dall'UE nell'attività di prevenzione e contrasto della radicalizzazione e del terrorismo, possa trovare nuovi modelli applicativi nell'ambito della prevenzione digitale. Una situazione tutt'altro che infrequente è inoltre quella relativa all'acquisizione della posta elettronica che, oltre alle credenziali dell'utilizzatore della casella, potrebbe richiedere ulteriori autorizzazioni rimesse agli "amministratori" ed in assenza delle quali le operazioni risulterebbero impossibili. Le stringenti normative sulla privacy (GDPR), specialmente laddove si operi in regime amministrativo ed in assenza di delega giudiziaria, tendono ormai a rappresentare un costante elemento che l'operatore dei nuclei investigativi penitenziaria deve continuamente considerare. In alcuni casi, il ricorso agli amministratori di rete o alle società che gestiscono i dati, sulla base dei loro contratti di natura privata, può contribuire a superare alcuni di questi ostacoli.

E' indispensabile, altresì, tenere conto delle informazioni non così facilmente acquisibili che si possono ottenere attraverso la collaborazione con tali figure. Si tratta di dati che possono aiutare l'investigatore penitenziario a "concentrare" la propria attenzione sugli aspetti più direttamente collegati all'indagine ed all'azione di sorveglianza preventiva, tralasciando quelli più marginali. Invero l'attuale contesto presenta spesso situazioni che vedono la presenza di centinaia di dispositivi, centinaia di TB di dati e reti "cloud" nell'ambito dei quali, senza un'attenta analisi e selezione dei target di interesse, si rischia di perdere la focalizzazione. Menzione particolare merita il "cloud", ricomprendendovi la moltitudine di archivi online, ovvero che non si trovano "fisicamente" presso gli spazi aziendali. Tali archivi online sono servizi che stanno assumendo sempre maggiore importanza a ragione della loro convenienza. In presenza di un sistema acceso collegato ad una rete sarà quindi necessario verificare la presenza di questi servizi o archivi "cloud", attraverso la presenza di eventuali icone riconducibili ai principali servizi e software cloud. In tal caso sarà importante non fidarsi della "sincronizzazione" spesso attiva sul target (cartella DROPBOX, ad esempio) ma verificare che i dati conservati "in cloud" siano effettivamente sincronizzati, provvedendo laddove non lo siano ad acquisire anche quest'ultimi, prima di procedere allo spegnimento del target. Terminate le operazioni di acquisizione dei dati volatili, dei dati cloud e di rete si potrà procedere allo spegnimento del target. Si ribadisce che le operazioni sopra tratteggiate sono patrimonio di personale "esperto" ed appositamente addestrato, non rimesse alla generalità degli operatori di polizia, i quali potranno, ferme restando le osservazioni e i suggerimenti sopra indicati, procedere a richiedere l'intervento di personale esperto, ossia procedere dopo le prescrizioni suindicate allo spegnimento del target.

Repertamento del Target: Sia nel caso in cui il target venga rinvenuto spento, sia nel caso sia rinvenuto acceso e solo successivamente spento, qualora si tratti di dispositivi che possono essere fisicamente sottratti all'utilizzo di chi ne dispone (sequestro o acquisizione amministrativa) occorrerà procedere ad un attento repertamento degli stessi. Tale fase può definirsi la "genesi" di ogni indagine ed azione preventiva. Senza un efficace repertamento la catena di custodia ha avvio con un anello debole, quasi spezzato e destinato a rompersi in occasione di quella delicata fase procedurale in cui le misure di prevenzione o l'indagine siano costrette a confrontarsi in contradditorio o in dibattimento. Senza un buon repertamento, la catena di custodia non ha inizio. Sempre più spesso nel corso del contradditorio e del dibattimento le difese fanno valere difetti nella catena di custodia. Questi non sono quasi mai dipendenti dal consulente o esperto chiamato ad analizzare i reperti, ma strettamente legati all'esperienza e preparazione di coloro che nella primissima fase si sono occupati della gestione, sequestro e repertazione dei supporti informatici, ovvero il personale penitenziario che ha effettuato il sequestro, gli ufficiali ed agenti di polizia giudiziaria che pur affidandosi al buon senso e alla loro esperienza non sempre sono riusciti a forgiare un primo e robusto anello di tale catena. Le criticità principali riguardanti il repertamento, e quindi la catena di custodia,

senza pretesa di esaustività possono riguardare :

- Il dossier fotografico: può essere realizzato con un semplice smartphone, che può aiutare il consulente/esperto ad associare compiutamente la descrizione messa a verbale con il corrispondente reperto. É il caso delle acquisizioni effettuate in ambito extramurario, per esempio presso una cooperativa, ove è probabile rinvenire più reperti della stessa marca e modello. La sola descrizione a verbale renderebbe difficile l'identificazione del reperto da parte del consulente. In particolare, il problema si pone laddove i reperti non presentino segni "distintivi" facilmente individuabili; in tali contesti solo un'"etichettatura" e il successivo report fotografico da parte degli operatori addetti al sequestro potrà impedire che si crei disordine tra reperti simili. Un caso analogo riguarda la moltitudine di SIM telefoniche i cui identificativi sono stati abrasi. Non vanno poi sottovalutati gli errori conseguenti a sviste nelle trascrizioni, dettati e ortografia compiuti dai verbalizzanti. La fotografia del reperto nel suo complesso e, ove presenti, dei suoi dati identificativi "esterni" - quali targhette, marca e modello - possono agevolare nel risolvere tale criticità, nonostante sia sempre preferibile etichettare i reperti con targhette adesive (possibilmente con intestazione del reparto operante). Inoltre, va ricordata l'importanza di tale etichettatura, effettuata con lettere e numero progressivo (A1, A2, A3, ecc) allorquando si proceda al sequestro di più componenti di un unico dispositivo; nel caso di sequestro di un telefonino in carcere corredato da accessori o da più SIM, tale etichettatura permetterà di ricondurre anche a distanza di tempo le componenti, compresi i cavi, ai corrispondenti dispositivi. Inoltre, qualora si effettui il report fotografico sarà sempre opportuno, al termine alle operazioni, comprimere tutte le foto in una cartella in formato .zip, .rar, etc., e calcolarne l'algoritmo di hash che andrà inserito nel verbale. Si eviteranno in tal modo contestazioni e modifiche al dossier/report fotografico;

- Le indicazioni minime utili ad identificare i reperti: erroneamente, sovente vengono confusi e descritti in maniera approssimativa i reperti, ed è pertanto necessario istruire gli addetti ai lavori in merito alle indicazioni che devono essere fornite per una completa e precisa identificazione del reperto, fornendo ove possibile un prestampato con spazi da compilare, che induca gli operatori penitenziari a completare il modello con le indicazioni necessarie. Fra queste, una descrizione sommaria del reperto (forma, colore, tipologia di dispositivo corredata, ove rinvenibile, da un numero seriale, facendo attenzione a non indicare il product key o altri seriali "generici" e non univoci, o altri codici che potrebbero solo ingenerare confusione). Accade talvolta che i numeri seriali siano erroneamente interpretati (zero per "O" e viceversa) o vengano letti e dettati con errori. Qualora si tratti di prodotti assemblati, spesso privi di segni identificativi univoci, ci si dovrà necessariamente affidare ad una "repertazione" fotografica accompagnata da un supporto, anche "di fortuna" (foglio, post-it, scotch di carta), che attribuisca al reperto un numero o lettera identificativa, che dovrà anche

essere “autenticata” attraverso la sottoscrizione dell’apposito verbale. Tra le indicazioni utili ad identificarlo vanno contemplate anche quelle riguardanti il luogo preciso in cui è stato rinvenuto il reperto e il soggetto da cui viene solitamente utilizzato. Si consideri che oggi molti telefonini svolgono ‘funzioni di sezione’, cioè sono utilizzati da più detenuti. Dunque, l’acquisizione di un determinato telefonino non necessariamente indica l’unicità del suo utilizzatore. Pertanto, al di là degli utilizzatori memorizzati dal sistema, è necessario ricondurre l’effettivo utilizzo del reperto anche attraverso altri elementi ed indizi, non potendosi escludere che attraverso un medesimo “user” agiscano sul sistema più persone utilizzando le medesime credenziali di accesso. Non va inoltre sottovalutato, come verrà più approfonditamente sottolineato in seguito, che fotografare “lo stato delle cose” (posizione degli oggetti e loro stato) prima di procedere al repertamento e sequestro dei dispositivi, può risultare, se non determinante, spesso strategico. Lo stato di acceso/spento: come evidenziato in precedenza, lo stato del dispositivo (acceso/spento/non noto) è un elemento fondamentale. La condizione non nota è una soluzione da adottare quando non si è in grado di stabilire se il dispositivo sia acceso o spento, alla luce delle proprie conoscenze. Si rammenta che proprio dallo stato del dispositivo discendono le scelte tecnico-informatiche-operative utili a salvaguardare le informazioni da acquisirsi nel rispetto delle linee guida internazionali. Invero, sarà necessario di volta in volta, attraverso lo “stato” del dispositivo, corroborare/giustificare le azioni tecniche intraprese, non sussistendo una regola generale che imponga lo spegnimento di un dispositivo o la sua accensione durante le operazioni di P.G. L’eventuale presenza di password, invece, oltre ad essere indicata nel verbale, dovrebbe costituire elemento di attenzione e sollecitazione per gli operatori penitenziari che dovrebbero cercare di ottenerle ognuno secondo le proprie tecniche. E’ opportuno evidenziare che le molteplici tecniche finalizzate all’ottenimento delle password e credenziali devono far parte dell’esperienza e capacità dell’operatore penitenziario, al pari delle capacità necessarie a condurre una perquisizione o un colloquio con il detenuto. Un buon report fotografico d’ambiente, inoltre, può essere d’aiuto, se non nell’individuazione diretta delle password, almeno a tracciare un profilo del soggetto, predisponendo magari “librerie” di password ad hoc con cui effettuare tentativi attraverso tecniche di “brute force” (titoli di libri, frasi apparentemente senza senso appuntate sulla scena, poster di film, squadre del cuore, foto di cani e gatti. etc., fotografate nella cella o sulla “crime scene”). Quest’ultimo aspetto è molto importante ed assume sempre maggior rilevanza alla luce del fatto che oggi i dispositivi risultano protetti da sistemi difficilmente by-passabili e che, a cagione degli algoritmi utilizzati (ad esempio AES256) sarebbero richiesti tempi lunghi per un crack-password. Quest’ultimo problema è fortemente avvertito, tanto che l’interconnessione dei dispositivi consiglia oggi di acquisire tutti i dispositivi presenti, in particolari in situazioni extramurarie, al fine di tentare, attraverso questi, di ottenere spunti, indizi o le vere e proprie password magari utili a sbloccarne altri.

- La descrizione analitica del reperto: il riferimento è alle descrizioni analitiche che possono riguardare eventuali danni, abrasioni, malfunzionamenti, nonché eventuali accessori che accompagnano il target (cavi, alimentatori, trasformatori, etc.). Vale la pena rilevare che il collegamento di un dispositivo ad un alimentatore/ trasformatore non corrispondente può provocare gravi danni. Per taluni dispositivi, inoltre, non è agevole reperire accessori compatibili. Inoltre i reperti vengono spesso consegnati "imballati" e sigillati al consulente o esperto e questi talvolta non ha modo di verificarne in dettaglio il contenuto, rendendosi conto solo dopo l'apertura del plico che si tratta di reperti danneggiati, abrasi o rotti, senza che ciò sia stato evidenziato in appositi verbali al momento del repertamento. Questo inconveniente, che interesserà maggiormente la fase del cosiddetto "dissequestro" e restituzione dei reperti all'avente diritto, pur emergendo successivamente può essere talvolta fonte di conseguenze anche gravi (richieste di risarcimento danni, denunce di danneggiamento etc.).

- imballaggio: non è raro, purtroppo, assistere al deterioramento delle evidence o meglio all'impossibilità di poterle "recuperare" dal contenitore che le conserva. Ciò non a causa della loro elevata "volatilità" e "fragilità", quanto per l'impossibilità, a causa dei danni subiti dal "contenitore" a seguito di cadute, esposizione alle fonti di calore o gelo, infiltrazioni di acqua e diversi altri fattori, di accedere alle stesse. Non è raro rinvenire, all'interno di istituti penitenziari, telefonini o smartphone sequestrati in modalità "acceso" e "online", conservati per lungo tempo in locali esposti a rischi e risultati dunque ossidati, soprattutto se alimentati con batterie non tempestivamente rimosse. Il "contenitore", al pari delle evidences che contiene, va trattato con la massima attenzione e, pur apparendo in taluni casi "robusto" o "resistente" a fattori esterni, richiede di essere protetto e trasportato con estrema cautela proteggendolo da urti e cadute accidentali. Un hard disk meccanico (HDD), a discapito dell'aspetto, non è resistente come ferro; una pen drive si può danneggiare irrimediabilmente, soprattutto le versioni a forma di carta credito o con connettori morbidi; un pc desktop *all in one* va trattato con più cura rispetto ad un case di un pc desktop tradizionale, senza il relativo monitor; i dvd, cd, blue ray etc, sono molto fragili e più sensibili di altri supporti al calore e ai raggi del sole. Quasi tutti i dispositivi sono soggetti a rischi elettromagnetici, provenienti da fonti per di più sconosciute o inimmaginabili. Va anche ricordato che tutto ciò che è connesso più o meno stabilmente ad una rete di trasmissioni richiede anche l'adozione di particolari tecniche e modalità di "isolamento" dalle stesse, al fine di sottrarre il reperto da modifiche ed influenze esterne e da remoto che potrebbero invalidare l'acquisizione successiva delle evidences. Per questo motivo esistono "airplane-mode" (modalità aereo) ma anche modalità di "isolamento" fisico (gabbie di Faraday) in grado di proteggere da tali evenienze. Quanto appena rappresentato in termini di imballo e trasporto richiede di essere applicato a ciò che non è "target" (il dispositivo originale) ma anche ai supporti messi a disposizione dagli ope-

ratori penitenziari per la conservazione delle eventuali *bit stream image* o copie bit to bit realizzate sul luogo del ritrovamento del target. Accade ancora, purtroppo, che incautamente la realizzazione della bit stream image tenda a "sollevare" gli operatori da tutte quelle cautele, attenzioni e cure riservate ai reperti "originali". Va ricordato, a tal proposito, che i supporti contenenti la bit stream image assurgono a reperti veri e propri ed è necessario che gli stessi vengano custoditi, trasportati ed inseriti in un'apposita catena di custodia, al pari degli altri reperti, al di là della loro "assunta" immodificabilità, identicità e autenticità garantite dal match dell'algoritmo di hash tra "sorgente" (reperto origine) e "destinazione" (disco contenente l'immagine forense in formato .dd, .eo1, etc. del sorgente). In merito alle modalità di imballaggio preme evidenziare come esistano prodotti specifici per ogni tipologia di reperto, che prevedono anche la possibilità di repertazione attraverso apposite etichette. Per quanto riguarda gli hard disk, è possibile acquistare apposite scatole in plastica che garantiscono efficace protezione e possono essere facilmente sigillate e cautelate. Ad ogni buon conto, al di là delle tecniche e dei materiali utilizzati, è sempre importante conferire adeguata importanza all'apposizione dei sigilli, poiché, soprattutto in caso di accertamenti differiti, l'apposizione del suggello costituirà, per le parti interessate, un elemento fondamentale, in quanto attesterà che dal sequestro alla data di effettuazione dell'accertamento il reperto non è stato nella disponibilità di alcuno. Evidentemente, il suggello integro potrà attestare che il reperto non è stato aperto. Al fine di garantire la catena di custodia, le fasi di imballaggio, trasporto e conservazione devono essere sempre adeguatamente registrate (documentate) attraverso i verbali che il personale penitenziario redige, o attraverso appositi moduli che dovranno sempre indicare chi, cosa, come e quando le operazioni sono state effettuate. Dovranno quindi registrarsi tutte le azioni intraprese sul reperto dal momento della sua acquisizione presso il luogo di rinvenimento, alla sua restituzione al termine dell'indagine dell'azione preventiva, fino alla restituzione finale del reperto al legittimo possessore. Tutta la vita del reperto in quest'arco di tempo andrà opportunamente documentata e tracciata in verbali o altri modelli, o con altre modalità (alcuni Uffici di alta specializzazione si sono dotati di modalità di registrazione attraverso bar-code sia delle azioni intraprese sul reperto sia delle persone intervenute, delle date, luoghi ed orari, indicando anche sommariamente le operazioni intraprese sullo stesso in modalità registrate elettronicamente, delle quali è possibile ottenere uno specifico "report" a documentazione delle stesse).

III.6 - COPIA FORENSE

Nell'ambito della Digital Forensics, il termine "copia bitstream" o "copia bit to bit" indica una copia "esatta", un "clone" di una evidenza digitale. Bit to bit non significa la semplice copia o duplicazione del file, in quanto tale "copia forense" risulta composta da tutte le zone del disco, anche quelle che non contengono alcun file direttamente visibile all'utente, quali lo spazio non al-

locato. Nella maggior parte dei filesystem la cancellazione di un file implica semplicemente la cancellazione dell'indice che contiene la posizione del file su disco, cioè la perdita del suo indirizzo; la possibilità di avere accesso alle aree non allocate permette dunque il recupero di file cancellati o di informazioni ormai non più disponibili all'utilizzatore del sistema. La copia forense è realizzabile tramite la cosiddetta " clonazione" o tramite la creazione di un "file immagine". La prima effettua una copia bit a bit del dispositivo sorgente su un altro di destinazione, con il risultato che il disco di destinazione risulterà identico (bit to bit) a quello sorgente; tale metodo, se da un lato permette di ottenere un clone immediatamente avviabile e sul quale si potrà senza altre operazioni procedere ad analisi, presenta due svantaggi:

1 Il clone di un disco richiede un disco di capacità pari o superiore al disco sorgente, che non potrà ospitare altri target. Tale processo "one to one" richiede elevate risorse in termini di dischi;

2) Per essere analizzato, il "clone" andrà sempre utilizzato attraverso appositi "drive-blocker" che ne impediscano operazioni di scrittura in quanto eventuali successivi accessi allo stesso potrebbero modificare i files in esso contenuti e, conseguentemente, modificare "irreversibilmente" l'autenticità dello stesso, come si vedrà in seguito quando verrà affrontato il tema dell'algoritmo di HASH. La seconda effettua una "image" del supporto. La creazione di un'immagine del disco comporta la copia del disco sorgente in un file all'interno del filesystem del disco destinazione.

In tal caso la creazione di un file immagine, ovvero gli "n" byte di cui è composto il disco sorgente, verranno salvati in un file o più files sul disco destinazione, con dimensione variabile in base al tipo di codifica e compressione scelta. Nel caso di immagine detta *raw* (grezza) (DD), il file sarà della stessa dimensione degli "n" bit che saranno copiati uno ad uno, senza alcuna compressione o codifica dei dati. Tuttavia, è possibile utilizzare modalità che provvedono anche ad una compressione ed organizzazione degli "n" bit, quali ad esempio E01, EWF, AFF; in tal caso l'immagine sarà di dimensioni ridotte rispetto alle dimensioni del "sorgente". Inoltre, sarà possibile:

- caricare più immagini di diversi device sullo stesso disco destinazione;

- Le immagini per essere analizzate richiedono di essere "montate" e non necessitano di essere gestite attraverso "write-blocker".

Pertanto, i principali vantaggi di tale processo si sostanziano nella possibilità di salvare diverse immagini di dischi sorgente differenti, in quanto ogni immagine corrisponderà a un file (o a più file di dimensione ridotta, in caso di suddivisione in più split), e nel fatto che utilizzando formati compressi sarà possibile economizzare lo spazio di destinazione, limitando le risorse necessarie a tale scopo. Gli strumenti utilizzati per generare copie forensi "clone" o "file

immagine" sono di due tipi: copiatori forensi (hardware) e software di clone/copia utilizzati in congiunzione con write-blocker di tipo software o hardware. Tra i copiatori hardware si citano Tableau TD3, Logicube Falcon, CRU Ditto. Il loro funzionamento è alquanto semplice ed intuitivo: prevedono un lato al quale viene collegato il disco "sorgente" ed un altro al quale viene collegato, con appositi adattatori, il disco destinazione. Le operazioni vengono settate dall'operatore attraverso una "consolle" digitale, che permette di impostare i dati necessari per identificare la copia e avviare l'operazione che verrà svolta interamente dal dispositivo. Tali dispositivi prevedono un "blocco hardware" sul lato di collegamento del disco sorgente che ne impedisce modifiche accidentali. Per quanto concerne l'altra tipologia più approfonditamente descritta nel prosieguo, esistono distribuzioni Linux live (es. DEFT, Caine, Tsurugi, etc...) che permettono di:

- essere lanciate in live sul "target" per accedere in modalità "sola lettura" al disco sorgente e quindi attraverso appositi software in versione GUI o, da linea di comando, procedere ad effettuare un clone o un file immagine su di un disco destinazione collegato in "lettura/scrittura" allo stesso target;

- essere lanciate sempre in live e fungere da duplicatore su di una workstation forense, collegando a questa il disco sorgente ed il disco destinazione nelle modalità già sopra indicate e procedendo quindi allo stesso modo. L'acquisizione forense non è limitata ai supporti di archiviazione di dati quali hard disk HDD o SSD, CD e DVDROM, Blu Ray, SD e MicroSD, PendDrive USB etc, ma tende oggi sempre più ad interessare ambiti sempre più diversificati e complessi, quali il cloud (Google Drive, Dropbox, I-Cloud etc.) e lo spazio web ove ormai si tende a gestire e conservare la posta elettronica (webmail) e dove vengono conservate pagine, siti web o altri documenti (ad esempio le pagine dei vari social dai quali si potrebbero dover acquisire numerose informazioni che potrebbero andare a costituire possibili elementi probatori, per i quali si deve procedere attraverso procedure "forensi" che ne assicurino una corretta "cristallizzazione" a fini legali). E' evidente, in base a quanto sopra descritto, come con "copia forense" si intenda qualcosa di più complesso e completo della semplice copia di un file, di un hard disk o il download di una pagina web, e ciò perché la copia forense implica diversi requisiti. Volendo elencarli senza pretesa di esaustività, se ne richiamano alcuni con la finalità di evidenziare quelli che, a parere degli scriventi, si ritengono indispensabili per poter definire "forense" la copia di un "sorgente":

1 la copia forense, indipendentemente dalla sua "natura" di clone o file immagine, deve avere impatto minimo, se non nullo, e deve essere realizzata "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" come prescritto dalla Legge 48 del 2008;

2 la copia forense deve essere "identica" all'originale (sorgente), identità che deve essere dimostrata attraverso metodologie scientifiche come prescritto dalla Legge 48 del 2008 che stabilisce che le copie forensi devono essere eseguite "con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.";

3 la copia forense deve essere il più completa possibile e riprodurre il dato originale acquisendone non soltanto i contenuti, ma anche eventuali metadati e le altre informazioni (nome file, attributi, data di creazione, modifica e accesso ai file) unitamente a tutte le aree non allocate del sistema dalle quali sarà poi possibile, con opportuni tools, recuperare eventuali file cancellati e non ancora completamente sovrascritti;

4 le modalità di acquisizione della copia forense devono essere dettagliatamente descritte e verbalizzate al fine di poter replicare ad eventuali opposizioni su metodi, strumenti o tecniche adottate. Si rammenta altresì che devono essere indicati, con riferimento alla copia forense realizzata, tutti i dati relativi alla catena di custodia e alla sua conservazione, nonché il corrispondente algoritmo di hash che sarà buona prassi indicare, per ciascuna immagine o clone realizzato, anche nel verbale delle operazioni compiute, al di là che lo stesso sia riportato nei "report" prodotti dai software dedicati alla realizzazione delle immagini e cloni "forensi";

5 la copia forense deve assicurare che eventuali, quand'anche accidentali, modifiche o alterazioni intervenute successivamente sulla stessa, devono poter essere rilevate ed identificate. Tale requisito[43] è assicurato tramite il calcolo di funzioni matematiche chiamate "hash" sul dato originale e sul dato acquisito, con verbalizzazione delle attività e confronto dei valori hash calcolati sui due supporti.

L'Agoritmo di HASH: ai fini di un approfondimento di quanto sopra accennato in merito alll'algoritmo di HASH, si evidenzia che ogni acquisizione (clone o immagine forense) deve prevedere la verifica della congruità del dato copiato con il dato originale. La funzione di hash è una funzione univoca che, dato un input di lunghezza arbitraria, fornisce un output (hash) di lunghezza fissa. Viene detta "univoca" in quanto dall'hash non è possibile risalire al dato originale ed una minima variazione nel dato originale si traduce in una grande variazione del risultato. Queste proprietà rendono le funzioni di hash lo strumento ideale per la verifica di una copia forense.
Una volta acquisita la copia bit-a-bit, si calcolano l'hash dell'originale e quello della copia. Se coincidono, allora anche originale e copia coincidono.

43 Legge 48 del 2008

Tale operazione, che può essere eseguita “manualmente” dall’operatore, solitamente viene svolta in modo automatico da parte dei software dedicati alle operazioni di “clone/copia forense” allorquando questi vengono correttamente settati in modo tale che al termine dell’operazione di copia clone venga effettuata la cosiddetta “verifica” ovvero il riscontro (match) tra l’hash del sorgente e quello del clone o immagine forense realizzata. A livello internazionale, le best practices prevedono che la cosiddetta “verifica” venga eseguita obbligatoriamente , in quanto unico elemento capace di assicurare “scientificamente” l’identicità tra la sorgente e la destinazione, ovvero che la copia ottenuta è identica (bit to bit) al target. Pertanto, al di là della scelta effettuata circa l’uno o l’altro software o hardware utilizzato per le operazioni di copia clone, l’operatore dovrà sempre ricordare di procedere all’operazione di “verifica” attraverso il riscontro degli algoritmi di hash calcolati sul target e sul clone o immagine forense realizzati. Come già anticipato, sia gli apparati hardware che software dedicati a tali operazioni provvedono a documentare il calcolo degli algoritmi di hash e il loro riscontro in appositi “report” a corredo delle immagini forensi realizzate. Si rammenta che è sempre buona norma riportare l’hash del sorgente e dell’immagine forense realizzata anche nei verbali, a documentazione delle operazioni svolte. Inoltre, poiché sono state documentate dal mondo scientifico remote possibilità di “collisione” degli hash (ovvero dati due input differenti, questi generano lo stesso hash), è consigliabile verificare i dati applicando due differenti funzioni di hash, o avvalersi di algoritmi per i quali non sono state ancora palesate possibili “collisioni” (es. SHA256). In merito, occorre ricordare che molti dei software dedicati alla Digital Forensic ed anche numerose apparecchiature hardware (copiatori/clonatori, già menzionati) utilizzano di default gli algoritmi MD5 e SHA1 in combinazione per i motivi anzidetti, o utilizzano unicamente SHA256 che alla stato non ha evidenziato problematiche di collisione.

III.7 - L’ANALISI FORENSE DEI DATI

Il tema dell’analisi forense dei dati è molto esteso e complesso; ogni sistema operativo, infatti ha particolarità che lo contraddistinguono da tutti gli altri e molto spesso le tecniche di analisi dei dati muovono proprio da tale presupposto. Per tale motivo sono stati pubblicati volumi dedicati alle tecniche di analisi di ogni sistema operativo. E’ evidente, infatti, come il “registro” di Windows possa fornire informazioni che altri sistemi operativi non forniscono, e viceversa. Inoltre, le tecniche di analisi o i software dedicati alle stesse non sempre sono di tipo “multi SS.OO.”, multi sistemi operativi, con il risultato che ciò che era adatto per l’analisi di diversi sistemi operativi e filesystems fino a poco tempo fa, oggi non lo sia più, o richieda di essere aggiornato per essere efficiente (ad esempio l’introduzione di APFS che ha obbligato molti dei software dedicati all’analisi a continui aggiornamenti). Per quanto riguarda il tema dell’analisi dei dati, le due cose procedono fianco a fianco, come per la realizzazione di cloni e immagini forensi software “one click” che permettono all’analista, impostati i necessari parametri, di ottenere un’analisi completa

del target ed altri cosiddetti "specifici", che invece permettono l'analisi di solo alcuni artefatti o files. In merito occorre segnalare che i cosiddetti "one-click", se sono utili per la maggior parte delle esigenze di analisi, in taluni casi potrebbero fallire nel loro compito, rendendo preferibile il ricorso a software e tecniche specifiche; ad esempio, molti software one-click non effettuano il "parsing", come si indica nel linguaggio tecnico, file di particolari estensioni, relegando la loro attività a quelli di più frequente uso ed escludendo quelli che hanno particolari estensioni. In tali casi è sempre bene verificare le caratteristiche del software utilizzato e, qualora non ricomprenda l'estensione dei file oggetto d'indagine ed all'azione di sorveglianza preventiva, ricorrere ad altre soluzioni. Premesso questo, occorre tuttavia evidenziare che esistono, nell'ambito dell'analisi dei dati forensi, alcune regole che devono essere sempre rispettate:

1) le prove o indicatori di rischio informatici digitali che si ottengono al termine dell'analisi dei dati devono essere ricavate attraverso una procedura tecnica rispettosa delle normative locali e delle cosiddette best practices. Pertanto, le procedure adottate nel corso dell'analisi dovranno essere sempre documentate adeguatamente e rispettare i principi fondamentali della Digital Forensics (catena di custodia, verifica dell'hash, etc.). Sarà importante, pertanto, oltre ad un'attenta gestione dei reperti, procedere in sede di analisi ad un'altrettanto attenta rilevazione dei dati relativi al target, quali la sua precisa identificazione, time-stamp, indicazione specifica della "path" relativa ai file di interesse e loro precisa "identificazione" (algoritmo di hash);

2) minimo trattamento dei dati e, ove possibile, effettuazione delle analisi su "copie" del target. La situazione ideale è quella che prevede di lavorare su una copia forense del target, al fine di rendere nulle tutte le potenziali probabilità di alterazione dei dati in origine. Purtroppo questo è non sempre possibile, ossia non è possibile realizzare copie complete del target per diversi motivi e pertanto è necessario operare direttamente sul reperto originale. In questa situazione è sempre necessario svolgere tutte quelle operazioni minime indispensabili a scopo forense che garantiscano la minima alterazione possibile del target;

3) con richiamo al punto 1), tutte le attività svolte durante l'analisi forense devono essere accuratamente registrate al fine di permettere in sede di "contro-analisi" di confermare o confutare quanto ottenuto. Ciò sarà particolarmente rilevante nel caso in cui l'accertamento di analisi svolto diventi "irripetibile", richiedendo l'adozione di particolari procedure a seconda degli ordinamenti vigenti che assicurino alle parti processuali pari diritti ed opportunità. Fermi restando tali principi, appare evidente come un'attenta e precisa documentazione delle tecniche, procedure e software utilizzati per pervenire ad un risultato permetta di fatto in base a tale impostazione di poter ricorrere, nel rispetto di quanto descritto, a qualsiasi tecnica,

software o mezzo. Assume grande rilevanza anche la presentazione in giudizio delle prove o indicatori di rischio informatici ottenute a seguito dell'analisi.

III.8 - PRESENTAZIONE DEGLI ELEMENTI DI RISCHIO O DELLE EVIDENZE RACCOLTE

Scopo delle attività esaminate è l'esposizione di indicatori di rischio o indizi nell'ambito di un procedimento preventivo di tipo giudiziale o del dibattimento processuale, con la finalità di dimostrare alle autorità preposte all'adozione di misure di prevenzione o di sicurezza tutti gli elementi di fatto riferiti ai dati digitali rinvenuti. Errori nella fase "espositiva", al pari di quelli che possono essere commessi nelle fasi di "identificazione", "acquisizione" ed "analisi", rischiano di vanificare gli sforzi fino a quel momento compiuti. Ad esempio, in un contesto in cui le prime tre fasi si sono svolte senza censure, se in sede di "presentazione" dei risultati vengono commessi errori, potrebbero accadere che le autorità preposte non comprendano adeguatamente e correttamente gli elementi acquisiti. La presentazione delle prove o indicatori di rischio informatici digitali ottenuti avviene attraverso relazioni tecniche quasi sempre corredate da altri elementi rilevati nell'osservazione penitenziaria o nelle relazioni di sintesi. Una valida e completa relazione tecnica deve essere corredata dalla sintesi dei principi scientifici su cui l'analisi ed il repertamento si basano, dalla catena di custodia dei reperti, dalla loro precisa ed accurata descrizione, dalla descrizione delle operazioni tecniche svolte, dall'esito finale con specifico riferimento ad eventuali quesiti posti dall'organo competente e da tutte le altre indicazioni utili a comprendere se il risultato ottenuto possa essere ripetuto o meno, quali siano stati gli strumenti di "validazione" adottati a conferma del risultato ottenuto. In merito a tale ultimo punto occorre precisare che è buona prassi procedere in sede di analisi ad effettuare la stessa sempre attraverso due o più software differenti. Ciò implica due vantaggi:

- poter affermare che il risultato ottenuto non è frutto di un unico software utilizzato;

- limitare incisivamente "opposizioni" circa i risultati ottenuti atteso che se due o più software forniscono il medesimo risultato, sarà molto più difficile contestarne il risultato adducendo esclusivamente difetti sui software utilizzati.

L'esito finale che verrà presentato dovrà pertanto essere sintetico, semplificato e asettico. Sintetico in quanto dovrà contenere solo gli aspetti tecnico-giuridici di interesse nello specifico caso in analisi. Dovranno pertanto essere evitati rinvii ad altri casi, o rinvii a documenti tecnici che potrebbero "fuorviare" l'attenzione delle competenti autorità. Andranno in sintesi indicati i software utilizzati, le tecniche adottate ed una precisa "catena di custodia" che possa in ogni momento indicare precisamente la vita"del reperto, sin dalla fase di ap-

prendimento da parte della P.G. Anche se redatto da un tecnico della materia, dovrà essere semplificato per essere compreso anche da chi non possiede tale tecnicità, dunque compilato con un linguaggio semplice, ma allo stesso tempo completo e preciso, in grado di far comprendere anche ai non addetti ai lavori come si sia sviluppata l'analisi e quali siano stati i suoi risultati. Linguaggi eccessivamente tecnici ed il fatto di ritenere scontati alcuni principi, potrebbe condurre a non comprendere fino in fondo l'efficacia ed efficienza della relazione in esame. Infine, dovrà essere asettico, ovvero scevro da giudizi personali di colui che ha effettuato l'analisi.

III.9 - TOOLS PRATICI DELLA DIGITAL FORENSIC PENITENZIARIA

All'interno del laboratorio forense dell'Amministrazione Penitenziaria di Padova, competente per il Triveneto, leader del progetto europeo J-SAFE e partner del progetto MINDb4ACT, vengono testati diversi software e soluzioni funzionali alla attività di digital forensics. Di seguito presenteremo alcune delle soluzioni derivanti dal risultato di tali progetti, quali suggerimenti per i first-line practitioners e le loro amministrazioni.

III.9.A - TSURUGI HTTPS://TSURUGI-LINUX.ORG/

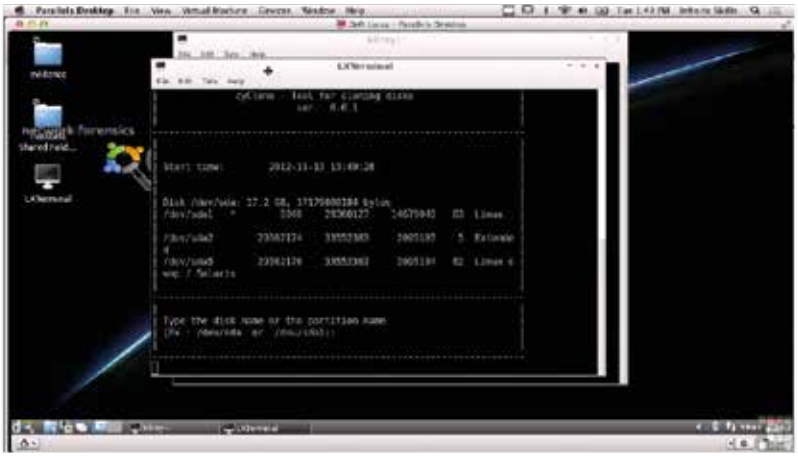
Tsurugi-Linux viene distribuito in due versioni distinte, con finalità diverse, integrate da una raccolta di strumenti destinati ad attività Digital Forensic, Incident Response, Malware Analisys, Open Source Intelligence e nelle future distribuzioni (Computer Vision e Facial Recognition):
Tsurugi Lab: piattaforma dedicata all'informatica forense (acquisizione e analisi), OSINT e analisi malware, avviabile direttamente su DVD o su pendrive, distribuita come ISO, installabile sui Personal Computer o macchine virtuali per la creazione di un laboratorio interno di analisi delle evidenze digitali, basato su Linux Ubuntu Mate LTS con Kernel 4.18.5 a 64 bit;
Tsurugi Acquire: sistema dedicato alla sola fase di acquisizione forense, con possibilità di eseguire limitati triage e verifiche di copie forensi, basato su Linux Ubuntu Mate LTS con Kernel 4.18.5 a 32 bit per maggiore compatibilità

con dispositivi obsoleti; Bento: raccolta di tool per Windows, Mac e Linux, da utilizzare su sistemi accesi e avviati per attività d'incident response o analisi forense sul campo, viene utilizzata principalmente dai Digital Forensic o First Responder in attività urgenti di acquisizione delle evidenze volatili (dump memory, process list, network connection, dump).

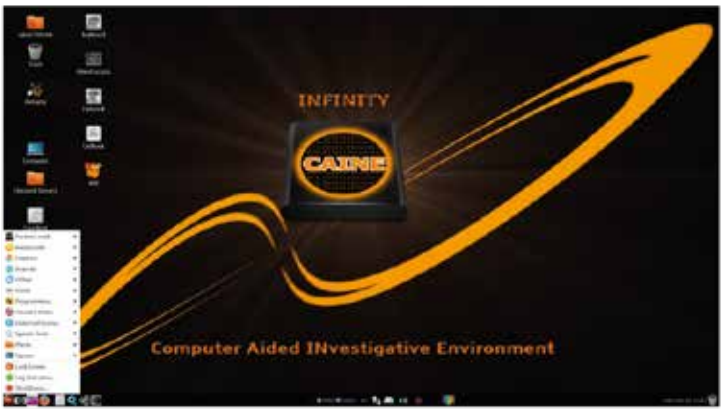
III.9.B - DEFT HTTP://WW.DEFTLINUX.NET/

Distribuzione nata da un idea di Stefano Fratepietro, DEFT (acronimo di Digital Evidence & Forensic Toolkit) è una distribuzione dedicata alla Digital Forensic e all'Incident Response, con possibilità di esecuzione in live nei sistemi senza scrivere o corrompere la prova digitale (hard disk, pendrives, etc) avviabile su PC/Mac quando si avvia il processo di boot sul sistema. Il sistema DEFT è basato su GNU Linux, si può avviare live (via DVD, ROM o USB pendrive) o in una macchina virtuale Vmware. DEFT è orientato ad implementare è sviluppare applicazioni che saranno rilasciate, in ausilio alle attività di Digital e Mobile Forensic, per essere utilizzate dalle società di consulenza, Forze di Polizia e investigatori pubblici e privati. DEFT è attualmente utilizzato in diversi luoghi e da diverse persone quali ad esempio: Military and Government Officers, Law Enforcement, Investigators, Expert Witnesses, IT Auditors, Universities, Individuals. DEFT è creato al 100% in Italia ed è un progetto gestito da R&D office di Tesla Consulting Srls.

III.9.C - CAINE HTTPS://WWW.CAINE-LIVE.NET/



CAINE (Computer Aided INvestigative Environment) è una distribuzione italiana creata come progetto di Digital Forensics. CAINE offre un ambiente completo organizzato per integrare i software esistenti in moduli e fornendo interfacce grafiche intuitive. I principali obiettivi di progettazione che CAINE mira a garantire sono:



- un ambiente interattivo che supporta lo sperimentatore digitale durante le quattro fasi dell'indagine ed all'azione di sorveglianza preventiva digitale;

- un'interfaccia grafica semplice;

- software di facile utilizzo. E' consigliata la lettura della pagina relativa alle politiche di CAINE. CAINE incarna pienamente lo spirito della filosofia Open Source, ed il sistema è completamente accessibile. La distribuzione è open source, il lato Windows è freeware e la distribuzione è installabile, dando così l'opportunità di ricostruirla in una nuova versione di marca, attribuendo così lunga vita a questo progetto.

III.9.D - PALADIN HTTPS://SUMURI.COM/SOFTWARE/PALADIN/

PALADIN è una distribuzione Linux live modificata basata su Ubuntu che semplifica le varie attività forensi in modo scientificamente corretto tramite PALADIN Toolbox. PALADIN è disponibile nelle versioni a 64 e 32 bit. PALADIN è diventata la suite forense numero uno nel mondo, utilizzata da migliaia di esaminatori forensi digitali delle forze dell'ordine, delle agenzie militari, fe-

derali, statali e aziendali. Molte altre distribuzioni Linux molto efficaci e ben supportate, nate ed utilizzate dagli Ethical Hacker nelle loro attività di Incident Response, Penentration Testing e, più in generale, in tutte le attività afferenti la sfera della Cyber Security, possono essere utilizzate nelle attività di Digital Forensic come First Responder. Se ne elenca qualcuna a titolo semplicemente esemplificativo e non esaustivo:

- https://linux.backbox.org/
- https://www.kali.org/
- https://www.parrotsec.org/
- https://digital-forensics.sans.org/community/downloads ▪ https://blackarch.org/
- https://sourceforge.net/projects/samurai/files/
- https://www.pentoo.ch/download/
- https://sourceforge.net/projects/nst/files/
- http://bugtraq-team.com/

Le distribuzioni Gnu-Linux sono ormai diventate centinaia e sono supportate ed implementate da vere e proprie comunità, che hanno al centro un motore software "Kernel" Open Source, la cui creazione e prima ideazione si deve attribuire a Linus Torvalds https://it.wikipedia.org/wiki/Linus_Torvalds, scaricabile gratuitamente su https://www. kernel.org/, implementato dalla comunità centrale https://www.linuxfoundation.org/ ed avente licenza Gnu-Linux https://it.wikipedia.org/wiki/GNU_General_Public_License. Il concetto dell'Open Source è quello di software libero aperto a tutti, con codice sorgente aperto leggibile, scaricabile, riutilizzabile da chiunque, con l'unico obbligo di reimettere tale codice alla libera disponibilità della comunità mondiale. Secondo tale paradigma, ognuno avrà la possibilità di guadagnare vendendo la propria professionalità acquisita. Tali software permettono a chi inizia, studia o non ha a disposizione importanti budget di investimento, di avvicinarsi ed approfondire le proprie conoscenze informatiche e di godere appieno di tali potenzialità nelle proprie attività lavorative, oltre a poter approfondire meccanismi e funzionamento del software. Tali concetti si contrappongono alle comunità di sviluppo software "Cloused Source", non meno diffuse ed importanti, nonché meglio supportate, e con garanzie sul software attuale e futuro. Un addetto al dominio dell'informatica o più specificatamente alla sicurezza informatica (Digital Forensics, First Responder, Penetration Testing, Ethical Hacking, etc.), non può prescindere dalla dotazione di strumenti professionali hardware e software Cloused Source e software Open Source, al fine di riuscire a risolvere difficoltà e scenari che si presenteranno nell'attività lavorativa o di studio.

III.10 - INFORMATICA FORENSE: QUESTIONI RELATIVE ALLE VALUTAZIONI URGENTI E ALLE OPERAZIONI RIPETIBILI /IRRIPETIBILI

Basati su un approccio top-bottom, i sistemi di giustizia penale in **Grecia** sono

disciplinati da pertinenti cornici previste dal diritto internazionale e, in particolare, dagli standard minimi previsti per i detenuti. Conformemente, la Costituzione in vigore comprende disposizioni che bilanciano le azioni preventive con i diritti umani, le libertà e i diritti civili. Restringendo la portata giuridica, in Grecia l'informatica forense come prova è fondata negli articoli 177, 178, 183, 187 e 265 (dati recenti: confisca di informatica forense durante un'indagine penale o ordinata dalla Corte) del codice di procedura penale. L'informatica forense in generale si riferisce a una serie di crimini, anche con giurisdizione all'interno delle carceri e strutture di correzione, oltre che alle disposizioni speciali individuate nel codice penitenziario. Tali casi sono descritti principalmente negli articoli 337, 348, 348A, 370A, 370C, 370D, 381A, 386A, 292B del codice penale greco, che fanno riferimento al reato commesso con mezzi tecnologici. Più specificamente, in tali casi e nel corso della procedura penale, sono considerati il quadro giuridico esistente per l'eliminazione della riservatezza delle comunicazioni (Legge 2225/1994 modificata con legge 4411/2016 e legge 4416/2016, e decreto presidenziale 47/2005), così come la protezione dei dati personali (EU 679/2016, EU 680/2016, legge 2472/1997, e legge 3471/2006).

In Bulgaria, i detenuti hanno diritto alla corrispondenza telefonica in linea con le norme e le procedure stabilite dal Direttore Generale della Direzione Generale "Esecuzione delle sentenze" (art. 86 (1), Atto di Esecuzione di Sanzioni Penali e Detenzione in Custodia). Ai detenuti non è consentito possedere telefoni cellulari, dispositivi audio o di videoregistrazione o loro parti (art. 97 (3), Atto di Esecuzione di Sanzioni Penali e Detenzione in Custodia).

In **Germania** le telecomunicazioni di un sospetto o di una persona condannata sono generalmente consentite ma, a seconda delle normative degli Stati federali, vincolate a determinate condizioni. Per i detenuti in custodia cautelare in Baviera, le telefonate sono possibili se il capo dell'amministrazione penitenziaria lo consente. La condizione principale è che la sicurezza della prigione non sia compromessa. Normalmente la telefonata dovrebbe essere fatta poco dopo la detenzione (BayU- VollzG Art. 21, paragrafo 1). La possibilità di utilizzare dispositivi mobili privati non esiste. I detenuti regolari possono effettuare chiamate telefoniche solo in casi urgenti su richiesta speciale. Se è necessario sorvegliare la chiamata, è obbligatorio informare la persona chiamata direttamente dopo che il personale del carcere ha stabilito il collegamento. Il prigioniero deve inoltre essere informato in anticipo della sorveglianza della chiamata (BayStVollzG, punto 35). L'amministrazione penitenziaria è autorizzata a utilizzare dispositivi tecnici per bloccare le frequenze e impedire ai detenuti di utilizzare dispositivi privati illegali.

In **Italia**, i colloqui telefonici dei detenuti sono regolati dall'art.18 della Legge 26 luglio 1975, n.354 e dall'art.39 del D.P.R. 30 giugno 2000, n.230. Le persone detenute possono essere autorizzate a telefonare a congiunti e conviventi e, quando ricorrano ragionevoli e verificati motivi, con persone diverse.

I detenuti possono usufruire di un colloquio telefonico alla settimana, della durata massima di dieci minuti. I detenuti per i reati previsti dal primo periodo del primo comma dell'art. 4 bis dell'Ordinamento Penitenziario (L. 26 luglio 1975, n.354) possono usufruire di due colloqui telefonici al mese. Può essere concesso un numero maggiore di colloqui in occasione del rientro dal permesso oppure in considerazione di motivi di urgenza o di particolare rilevanza, se la corrispondenza telefonica si svolge con prole di età inferiore ad anni dieci, nonché in caso di trasferimento del detenuto. I detenuti che vogliono intrattenere corrispondenza telefonica devono rivolgere istanza scritta all'Autorità competente, indicando il numero telefonico e la persona con cui corrispondere. Il contatto viene stabilito dal centralino dell'istituto. La corrispondenza telefonica è a spese del detenuto: la contabilizzazione avviene per ciascuna telefonata. In molti istituti sono disponibili carte telefoniche prepagate con cui è possibile telefonare solo a familiari o alle terze persone autorizzate. Il detenuto può ricaricare la scheda quando si è esaurita, il contatto viene comunque effettuato tramite centralinista dell'istituto, secondo i tempi e la durata previsti, nelle fasce orarie previste in ciascun istituto penitenziario. E' consentito ai detenuti chiamare i telefoni cellulari quando non effettuino da almeno 15 giorni alcun tipo di colloquio e quando non abbiano altra possibilità di contatto con i congiunti. E' sempre escluso per le tipologie detentive di maggiore pericolosità (41 bis e Alta Sicurezza). Non sono ammesse chiamate dall'esterno, a meno che la chiamata non provenga da congiunto o convivente detenuto, purché entrambi siano stati regolarmente autorizzati. In quanto espressione di principi fondamentali dell'ordinamento giuridico, il diritto dei detenuti al colloquio con i familiari non può essere negato (semmai limitato in presenza di altri interessi costituzionalmente garantiti). Peraltro, la negazione del diritto al mantenimento delle relazioni familiari si porrebbe in contrasto con il senso di umanità che deve presidiare l'esecuzione delle pene detentive, oltre che con la finalità educativa (art.27, comma 3, Cost.). Garantiti tali diritti, è necessario che sia perseguito il possesso non autorizzato di apparati idonei ad effettuare comunicazioni con l'esterno degli istituti penitenziari, ai fini di tutela dell'ordine, della sicurezza e della legalità pubblica, non permettendo a taluni detenuti di continuare a dare disposizioni e ordini per commettere ulteriori reati, per evitare che i reati già commessi siano portati ad ulteriori conseguenze o che possano essere date indicazioni finalizzate a inquinare e occultare le prove. Fino all'entrata in vigore del nuovo Decreto Legge sicurezza, varato in data 5 ottobre 2020 dal Consiglio dei Ministri, che ha introdotto una nuova figura di reato che vieta e sanziona l'introduzione di telefonini all'interno degli istituti penitenziari, il possesso di un cellulare da parte di un detenuto era sanzionato a livello amministrativo ex art. 77 commi 8 e 16 del Regolamento di Esecuzione (DPR 230/2000), a parte la possibilità di far rientrare tale possesso nella mancata osservanza di un provvedimento legalmente dato dall'autorità ex art. 650 c.p. "inosservanza dei provvedimenti dell'Autorità.

In **Spagna**, il regolamento penitenziario prevede una serie di norme per le comunicazioni e le visite in carcere (art. da 41 a 49 del Regio Decreto Legge

190/1996, 9 febbraio). I detenuti hanno il diritto di comunicare (per iscritto o verbalmente) con la famiglia, gli amici o i rappresentanti delle istituzioni competenti e con gli avvocati. Per quanto riguarda le comunicazioni verbali, i detenuti hanno diritto a due comunicazioni settimanali, preferibilmente durante i fine settimana. I visitatori che sono parenti dovrebbero certificare la loro parentela e gli altri visitatori dovrebbero ottenere un'autorizzazione dal Direttore del carcere. Le comunicazioni potrebbero essere sospese in due circostanze (Art. 44): a) quando vi sono ragionevoli motivi per ritenere che sia in corso la preparazione di un'azione contro la sicurezza della struttura; b) quando i detenuti non adottano un comportamento corretto. Le comunicazioni telefoniche possono essere autorizzate nei seguenti casi (art. 47):
a) quando i parenti vivono lontano dal carcere o non sono in grado di recarvisi per comunicazioni verbali;

b) quando i detenuti hanno necessità di comunicare una questione importante ad avvocati o parenti. In questi casi, hanno diritto a cinque chiamate al massimo. Durante le comunicazioni, il personale penitenziario dovrebbe essere presente e dispone della possibilità di estendere le comunicazioni fino a cinque minuti.

Esiste un sistema di controllo delle comunicazioni telefoniche, utilizzato per monitorare il rispetto delle regole, ad esempio numero massimo delle chiamate effettuate dai detenuti, orario, limitazioni introdotte per alcuni detenuti e sorveglianza obbligatoria sulla base di mandati legali forniti dai giudici.

In caso di comunicazione con avvocati o autorità professionali, è richiesta l'autorizzazione del detenuto per la comunicazione.

Nelle prigioni spagnole non è consentito l'accesso a cellulari o a internet. Inibitori e scanner installati in ogni carcere impediscono che i telefoni cellulari vengano utilizzati all'interno.

In occasione del ritrovamento di un telefono cellulare all'interno di un istituto penitenziario, che può avvenire nei casi di perquisizioni ordinarie, straordinarie, o durante il servizio di vigilanza e osservazione, il personale di Polizia Penitenziaria provvede immediatamente al ritiro dell'oggetto non consentito, che viene messo a disposizione dell'Ufficio Comando e conservato presso una cassaforte all'interno della struttura penitenziaria o, in ogni caso, conservato con le necessarie cautele. Nel caso in cui il detenuto acconsenta, lo stesso viene escusso a verbale di spontanee dichiarazioni e viene redatto verbale di sequestro, trasmesso poi alla locale Procura della Repubblica, competente per la successiva convalida. Una copia del verbale di sequestro viene consegnata al detenuto e una resta conservata agli atti dell'istituto penitenziario.

Posto che la comunicazione alla competente Autorità Giudiziaria in merito al ritrovamento viene sempre assicurata, soprattutto nel caso in cui vi sia il

concreto sospetto che attraverso l'utilizzo del telefono cellulare si siano configurati ulteriori reati (gestione di traffico di stupefacenti, stalking, omicidi su commissione, terrorismo, etc), sarà la stessa A.G. a stabilire se il dispositivo dovrà essere sottoposto ad analisi forense e dei tabulati telefonici.
Tuttavia, in casi particolari, ad esempio allorquando non sia stato possibile risalire al possessore del telefono cellulare o in casi di urgenza, la Polizia Penitenziaria potrà procedere d'iniziativa ad effettuare gli accertamenti ritenuti necessari.
Al detenuto viene elevato rapporto disciplinare con contestazione dell'infrazione prevista dall'art. 77 del Regolamento di Esecuzione (D.P.R. n.230/2000). Il Consiglio di Disciplina, visti gli art.77, 78, 79, 80 e 81 del D.P.R. n.230/2000 e gli art. 39 e 40 dell'Ordinamento Penitenziario irroga la sanzione disciplinare ritenuta adeguata alla violazione considerando di volta in volta le circostanze del caso.

Pertanto, non configurandosi come diretta ipotesi di reato, il possesso di un telefono cellulare deve essere soggetto alle normali procedure amministrative. Solo la connessione tra la detenzione di un dispositivo mobile ed altri elementi concernenti sospetti di radicalizzazione o terrorismo può rappresentare una valida ragione per avviare un approfondimento, che dovrà avvalersi dell'Autorità Giudiziaria per il rilascio delle relative autorizzazioni. Tuttavia, è importante sottolineare che alcuni indicatori di rischio o elementi di prova sono soggetti a test non ripetibili. Questa parte dell'informatica forense è strettamente legata al quadro legislativo nazionale. Nelle note che seguono, ci riferiamo al quadro legislativo italiano, anche se si ritiene che la questione debba trovare una propria armonizzazione europea, poiché riguarda direttive fondamentali, come l'Ordine Investigativo Europeo, ed è rilevante per l'intero dibattito sulle prove elettroniche. A seguito delle modifiche apportate al Codice di Procedura Penale italiano dall'art. 9 della legge 48/2008, in particolare a seguito della modifica dell'art. 354 del Codice di Procedura Penale italiano (indagini urgenti su luoghi, cose e persone e sequestro) con specifico riferimento alla legislazione nazionale italiana, è stato avviato un acceso dibattito sulla ripetibilità o irripetibilità delle valutazioni scientifiche digitali. Occorre innanzitutto chiarire che l'elenco delle cosiddette indagini urgenti ai sensi dell'articolo 354 del Codice di Procedura Penale italiano, che comprende le operazioni tecniche effettuate durante le attività della polizia giudiziaria, mirava in generale alla mera individuazione e conservazione degli elementi riscontrati, in attesa dell'intervento del Pubblico Ministero, al punto che l'articolo che li disciplina stabilisce che:

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.

2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la

direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.

3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone, diversi da ispezioni personali [245].

Vedremo nel prosieguo che gli accertamenti urgenti ex art. 354 c.p.p. prevedono in concreto l'effettuazione di operazioni "ripetibili" ma molto più spesso "irripetibili", ma in tal caso, stante "l'urgenza", non scontano il particolare regime previsto rispettivamente dall'art. 359 c.p.p. (Consulenti Tecnici del Pubblico Ministero) in gergo definiti accertamenti "ripetibili", e dall'art. 360 c.p.p. (Accertamenti tecnici non ripetibili) in gergo definiti accertamenti "irripetibili". Si tratta dunque di tre aspetti diversi disciplinati da tre differenti articoli ed ogni loro tentata commistione è tutt'ora oggetto di aspri dibattiti tra polizia giudiziaria, magistrati, consulenti tecnici, dottrina e mondo accademico, ognuno con le proprie convinzioni che non permettono, ad oltre dieci anni dalla Legge 48/2008, di arrivare ad una linea condivisa sulla natura di detti accertamenti.

Invero, l'inarrestabile progresso tecnologico caratterizzato dalla comparsa sulla "scena del crimine" di nuovi e sempre più complessi dispositivi, ha dissolto le scarse "considerazioni tecnico-logico-giuridiche" comuni che si erano formate e sembravano aver portato a risoluzione alcuni aspetti. Un esempio potrà chiarire la problematica: se fino a qualche anno fa risultava assodata, tra gli attori, la "ripetibilità" di un accertamento su un hard-disk di tipo meccanico, oggi, a seguito della massiccia diffusione dei dischi solidi (SSD) si evidenzia come l'accertamento su tali dispositivi tenda a rientrare, a cagione della loro "modificabilità intrinseca", nel novero degli accertamenti "irripetibili". Tuttavia,evidenziando che con "ripetibilità" ed "irripetibilità" degli accertamenti si fa riferimento alle fasi della consulenza tecnica, laddove l'organo Requirente, anche previa estrazione di una copia forense del dispositivo, chiede di "valutare" gli elementi di prova.

Nel fare rimando al testo degli articoli 359 e 360 c.p.p. preme evidenziare, al di là della profonda "differenza" procedurale sui due istituti, come per "ripetibilità" si intenda la possibilità di ripetere più volte l'accertamento sul medesimo materiale pervenendo allo stesso risultato, a mente dei concetti di integrità e

immodificabilità, in quanto la distruzione del materiale o la sua modificabilità non condurrebbe ai medesimi risultati. Viceversa, con "irripetibilità" potremmo definire la situazione in cui il "risultato" di quell'accertamento è ottenibile una sola ed unica volta, in quanto a seguito dello stesso il materiale subisce modifiche tali da rendere impossibile il medesimo risultato. Sul piano operativo è possibile affermare che non è possibile oggi, ad eccezione di alcuni casi, stabilire con assoluta certezza cosa possa definirsi accertamento informatico ripetibile o irripetibile, tanto che la pratica "operativa" consiglia di valutare di volta in volta il caso rimettendo al "dominus" delle indagini ed all'azione di sorveglianza preventiva (il Pubblico Ministero) la scelta dell'uno o dell'altro accertamento. In merito si richiama un esempio tipico, si ricorda che se da un lato l'accertamento su un hard-disk meccanico è considerato sempre ripetibile, anche per giurisprudenza ormai ampiamente consolidata, la dottrina continua a citare l'esempio dell'hard-disk meccanico in pessimo stato di conservazione, che si danneggia irrimediabilmente a causa della copia forense e quindi di fatto rende "irripetibile" l'accertamento in corso, in quanto una volta realizzata quella copia non sarà più possibile ripetere lo stesso accertamento con i medesimi risultati. Con riferimento all'acquisizione di un hard-disk SSD è noto che se la sua ripetibilità/ irripetibilità è rimessa all'hash SHA256 dell'immagine in formato .dd realizzata all'acquisizione, non può escludersi che a seguito di tale operazione e di un certo lasso di tempo lo stesso, a causa di diversi fenomeni imprevedibili (TRIM), vada a "modificare" lo stato del disco fornendo un hash diverso. Rispetto a tale problematica, ciò che aiuta a uscire da empasse difficilmente risolvibili è la distinzione tra "dato" e "contenitore", o meglio all'individuazione di quale tra i due venga effettivamente a subire una "irrimediabile" modifica/alterazione, con le conseguenze previste e risolte dall'art. 360 c.p.p. Con riferimento all'esempio, se è vero che l'hash dell'immagine .dd del disco SSD potrebbe essere diversa dalla successiva immagine, è altrettanto vero che i singoli file nello stesso contenuti, o meglio i file che generalmente interessano l'indagine e l'azione di sorveglianza preventiva, non hanno subito alcuna modifica/alterazione. Tale concetto di "dato"/"contenitore" sta assumendo sempre maggiore importanza, come emergerà nel prosieguo, anche in materia di Mobile Forensics. Anche in questo caso, se è vero che ad ogni riavvio del dispositivo mobile molti file (per esempio quelli di log) subiscono importanti modificazioni, è altrettanto vero che la maggior parte dei file (foto, documenti, video, file office, pdf, etc.) non subiscono alcuna modifica. A soluzione del problema dunque interviene "l'oggetto dell'indagine e dell'azione di sorveglianza preventiva". E' evidente che se il dispositivo dovrà fornire notizie riferite all'ultima volta che è stato acceso, o a dove si trovava prima dello spegnimento, andranno poste in essere tutte le attenzioni imposte dall'art. 360 a genuinità e attendibilità dell'accertamento effettuato; viceversa, tali attenzioni potranno venire meno qualora l'attenzione sia invece focalizzata su file, quali foto, video, documenti office, pdf, etc., che non subiscono cambiamenti nonostante le modifiche al "contenitore". Nella realtà operativa accade che durante il dibattimento venga contestata dinanzi al giudice una violazione circa un accertamento effettuato ai sensi dell'art. 359 che doveva essere ef-

fettuato invece ai sensi dell'art. 360 (connaturato da ben più stringenti garanzie). In tali casi occorrerà "convincere" il giudicante circa l'affidabilità della tesi dato/contenitore, pena la perdita di strategici elementi probatori. Dunque appare conveniente (salvo diverso avviso del Pubblico Ministero) propendere per l'effettuazione di accertamenti ex art. 360 c.p.p. laddove si possa palesare l'ipotesi che per la natura del dispositivo e dell'accertamento, lo stesso rientri in tale contesto. Eventuali azzardi potranno subire, anche in presenza di una valida e precisa esposizione delle tesi dato/contenitore, una pesante censura che in taluni casi potrebbe disperdere la cosiddetta "prova regina" al dibattimento. Ne consegue pertanto che, laddove possibile e realizzabile, è conveniente in termini praticooperativi anticipare (se il contesto in termini giuridici lo consente) l'estrazione della cosiddetta copia forense del dispositivo già in sede di "perquisizione" (ex art. 247 c.p.p.) o di accertamenti urgenti ex art. 354 c.p.p. A tal proposito si rappresenta come la "perquisizione" sia già di per sé atto "irripetibile" e pertanto le operazioni svolte, quand'anche di natura "irripetibile", non scontano il particolare regime dell'art. 360 c.p.p. Dunque, nell'ambito della "perquisizione" sarà possibile svolgere quegli accertamenti ontologicamente rientranti nel novero degli "irripetibili" (ad esempio l'acquisizione di uno smartphone) evitando la procedura prevista dall'art. 360 c.p.p., che evidentemente non sarà più realizzabile a seguito del "sequestro" del dispositivo con rinvio degli accertamenti ad una fase diversa dalla "perquisizione". La medesima copertura è assicurata nell'ambito dell'art. 354 c.p.p., attività di iniziativa della P.G., in base al quale in attesa dell'intervento del Pubblico Ministero si gode della stessa copertura qualora si rendano necessari accertamenti urgenti. E' evidente come tali "accertamenti urgenti" debbano essere sempre corredati, a cura degli operanti, da elementi che li facciano rientrare tra i "presupposti" dell'art. 354 c.p.p., ovvero di urgenza (realizzazione di un "dump" della memoria RAM) o alla necessità di realizzare una copia del target per l'effettuazione di accertamenti urgenti sul posto, utili al prosieguo delle indagini o ancora alla necessità, in adempimento all'art. 354 c.p.p., di " assicurarne la conservazione e impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità..." in attesa dell'intervento del P.M.

III.11 - INTRODUZIONE ALLA MOBILE FORENSICS

La Mobile Forensics, nell'ambito delle più ampie attività di Digital Forensic, riguarda in particolare tutto ciò che è eseguito sui dispositivi mobili quali smartphone, telefoni cellulari, tablet, smartwatch, etc. ed in particolare sulle loro memorie interne ed esterne, ma anche sulle loro sim. Anche la Mobile Forensic, generalmente, segue l'intero ciclo delle fasi generali della Computer Forensic con alcune differenze e particolarità. La loro precisa identificazione e copia forense avviene attraverso tecniche e modalità differenti, in quanto per loro natura i dispositivi mobili sono soggetti a continue modifiche dovute alla necessaria interazione con la rete per il loro funzionamento. In molti casi, le

operazioni svolte sugli stessi vengono associate ad attività irripetibili in quanto, nella maggior parte dei casi, non è possibile accedere ad una memoria di telefono cellulare in modalità "post mortem", come accade per gli hard-disk. Solo le memorie esterne SD o Micro SD dei dispositivi mobili risultano assimilabili agli hard disk e possono essere quindi acquisite con modalità ripetibili. In tutte queste attività e nel passaggio dei reperti, estrema importanza riveste la catena di custodia che ha sempre avvio con la precisa identificazione del reperto mobile sul luogo di ritrovamento o sequestro o consegna e della precisa identificazione di tutti gli utilizzatore e proprietari, quando possibile. Si consideri che all'interno degli istituti penitenziari un apparecchio mobile può essere in dotazione a più detenuti, che in vari casi si è visto disporre di proprie SIM. Occorre poi tener conto che se lo stesso è stato acquistato o è entrato in carcere come nuovo od usato, ma soprattutto, a cagione dei sofisticati sistemi di protezione adottati dai produttori a tutela della privacy degli utenti, ci si dovrà prodigare in ogni sforzo diretto all'ottenimento delle password di sblocco del dispositivo, in assenza delle quali su determinati modelli risultano alquanto limitate le operazioni di effettuazione di copia ed analisi.

III.11.1 - PROBLEMATICHE LEGATE AGLI ACCERTAMENTI URGENTI ED ALLE OPERAZIONI RIPETIBILI/IRRIPETIBILI

Il tema è di particolare attualità in quanto la copia logica o fisica (bit to bit) di un dispositivo mobile richiede che esso sia acceso. L'operazione di accensione del dispositivo quand'anche disconnesso da ogni connessione di rete GSM, 3G, 4G, wi-fi, bluetooth, etc (cosiddetta modalità Aereo) comporta che alcuni file dedicati al funzionamento del sistema operativo, e più comunemente i cosiddetti file di log, possano modificarsi rendendo "irripetibile" uno specifico accertamento. La riaccensione del dispositivo va a modificarne lo stato preesistente, ma è altrettanto vero che la maggior parte dei file che costituiscono interesse per l'operatore penitenziario (foto, file di testo, chat) non subiscono alterazioni o modifiche rilevanti a seguito di tale accensione. In sintesi, si richiama il concetto di contenitore (il dispositivo mobile) e contenuto (i dati di interesse). Se il contenuto è costituito da file che non subiscono modifiche dall'accensione e spegnimento del dispositivo, si ritiene che accertamenti sugli stessi possano essere effettuati con modalità "ripetibili". Per questo motivo alcune autorità fanno eseguire anche le operazioni riguardanti la Mobile Forensic in regime di "Accertamenti ripetibili". Ad ogni buon conto si ritiene, come già rappresentato, che tali decisioni "strategiche" per le sorti delle evidences vadano rimesse al "dominus" dell'azione di sorveglianza preventiva da individuarsi nell'autorità competente in base alle norme nazionali.

III.11.2 - ASPETTI OPERATIVI DELLA MOBILE FORENSICS

Il dispositivo mobile dispone spesso di un blocco di sicurezza all'avvio indipendente dal PIN/PUK della sim, o che potrebbe essere costituito da una password alfanumerica, da un numero di 4 o più cifre, dalla sequenza di un segno

su disegno geometrico quadrato a 9 pallini, dalle impronte digitali del proprietario di una o più dita, dal riconoscimento facciale, etc. Per tale motivazione è importante disporre della password di accesso e di eventuali altre password di restrizione presenti nelle impostazioni dei dispositivi, sia con sistema operativo IOS che del sistema operativo Android, nonché degli altri disponibili. Una memoria criptata, anche se estratta con metodi avanzati ("chip-off/Jtag"), permarrà nel medesimo stato di copia integrale bit-streaming criptata, a meno che non venga rinvenuta la password successivamente alla copia attraverso una "escalation" su altri dispositivi a seguito di analisi, oppure a seguito di attività di indagini ulteriori da parte della Polizia Penitenziaria. Un ulteriore fattore da tenere in considerazione durante la fase di identificazione dei dispositivi mobili è la precisa identificazione del dispositivo, anche tramite documentazione fotografica e il rilievo dei numeri seriali e IMEI Mac-Address. Di solito tali dati sono posti sotto la batteria, quando è accessibile ed è possibile smontare il dispositivo, oppure sono indicati nelle informazioni generali del software o ancora sono producibili attraverso la digitazione del codice (*#06#). Si evidenzia che l'identificazione del dispositivo comprende anche la sua collocazione fisica ed ogni altra notizia utile a conoscerne gli attuali e passati utilizzatori. Le effettive e le presunte password eventualmente rinvenute nelle confezioni, sulle schede sim o in appunti andranno annotate in appositi report e qualora costituite da gesture andranno adeguatamente annotate.

III.11.3 - BEST PRACTICES PER IL PRIMO INTERVENTO

Le operazioni di primo intervento nell'ambito delle operazioni di Polizia Penitenziaria riguardano la fase dell'identificazione dei dispositivi mobili all'interno degli istituti penitenziari o con riferimento a individui sospetti che beneficino di misure alternative o messa alla prova all'esterno. Oltre all'identificazione fotografica, è importante cercare di identificare l'utilizzatore o gli utilizzatori, proprietario o proprietari, del dispositivo mobile nella sua storia, nel luogo e data del sequestro, ritrovamento o consegna, e nel repertamento dello stesso con le precise indicazioni indicate nel foglio "chain of custody", da allegare al reperto. Successivamente, a seguito di passaggio di consegna ed implementazione della "chain of custody", il dispositivo sarà copiato, analizzato e le evidence saranno presentate, verbalizzate e depositate alle autorità competenti in base alle procedure adottate. In questa fase occorre anche accertarsi dello stato di acceso o spento del dispositivo, ponendo particolare attenzione agli stati di stand-by che potrebbero trarre in inganno l'operatore penitenziario. Qualora il dispositivo sia effettivamente spento, le operazioni si riducono al suo repertamento previa acquisizione delle eventuali password, allorquando fornite dal detenuto o dai detenuti. In merito alla fase di repertamento, si sottolinea che:

- può essere sempre utile acquisire gli imballi originali, ove presenti, unitamente ai cavi, in quanto talvolta possono rinvenirsi dispositivi aventi cavetteria "proprietaria" non comune o comunque non internazionale di difficile

reperimento per le successive operazioni.

- è fondamentale procedere ad una sempre attenta e precisa descrizione dello stato del dispositivo (meglio se fotografica) onde poter sostenere le proprie ragioni su eventuali contestazioni di danni provocati allo stesso successivamente al suo rinvenimento.

- Ove possibile, si consiglia anche di scollegare la batteria. Se il telefono viene rinvenuto acceso bisognerà invece procedere con maggiore attenzione e cautele, atteso che in quello stato il dispositivo è in continua modificazione e si moltiplicano le possibilità di provocare accidentali o volontarie perdite di dati.

III.11.4 - MODALITÀ D'INTERVENTO CON DISPOSITIVO ACCESO

Il primo elemento di attenzione in caso di dispositivo accesso è l'ottenimento della password o gesture di "sblocco" per poter accedere alle impostazioni. Tuttavia, la maggior parte dei dispositivi prevede la possibilità di procedere ad un isolamento dalla rete e da altre connessioni (cd. modalità aereo) anche in assenza dello sblocco. Il primo punto è quindi l'isolamento del dispositivo, che potrà avvenire attraverso la procedura indicata o attraverso apposite gabbie di Faraday, che isoleranno il dispositivo da ogni interferenza. Ciò è importante per due motivi:

- si impediscono modifiche allo stato del dispositivo;

- si impediscono le operazioni di cancellazione dei dati che ormai quasi tutti i dispositivi prevedono in caso di furto o smarrimento; Una volta "isolato", l'opportunità di conservare il dispositivo acceso o di spegnerlo è rimessa a specialisti ai quali andranno fornite tutte le specifiche necessarie (modello, IMEI, etc). Va ricordato che in taluni casi, solo mantenendo il dispositivo accesso è possibile procedere ad alcune operazioni tecniche di acquisizione che potrebbero venire meno al suo spegnimento qualora non si sia in possesso delle password di sblocco. Pertanto è sempre consigliato, in caso di dispositivi mobili, un confronto con personale esperto che saprà, a seconda delle situazioni che di volta in volta si presentano, consigliare le preliminari modalità di intervento.

III.11.5 - COPIA FORENSE ED ESTRAZIONE DATI

La copia forense dei dati richiede strumenti hardware e software ormai consolidati ed universalmente utilizzati, che verranno di seguito illustrati, non soltanto nell'ambito della Mobile Forensic ma anche in casi di Incidente Response (incidente informatico). Gli stessi, a seguito di estrazione di tipo logico, fisico, file system o altro, saranno in seguito sottoposti nella loro interezza a doppi algoritmi hash che confermeranno la autenticità e veridicità del dato informatico

acquisito in quel preciso momento. Le difficoltà dell'acquisizione dipendono principalmente dalle credenziali di accesso al dispositivo mobile, considerando però che in alcuni modelli è possibile accedere al dispositivo senza credenziali di accesso (dispositivi sottoposti a root o jailbreak o acquisizione in modalità recovery mode, download mode). Una ulteriore difficoltà consiste nella tipologia del dato da acquisire e dell'interesse investigativo nella sua raccolta (tipologia di chat o altro dato informatico quale email, immagini, navigazioni web, contenuto in cloud, ecc).

III.11.6 - I TOOLS PIÙ COMUNI E IL MONDO OPEN SOURCE

Il panorama software/hardware nella Mobile Forensic è molto vario: si elencano di seguito alcuni tra i tool più comuni a titolo esemplificativo e non esaustivo:

- Cellebrite con le soluzioni Ufed Touch, Ufed Touch2, Ufed Ultimate, Ufed Forpc e altri della medesima azienda israeliana, che devono essere utilizzati di concerto ai software della medesima azienda Ufed Physical Analizer, Ufed Logical Analizer, Lynks analisys e ad altri della medesima azienda; - MSAB XRY;
- Oxygen Forensics;
- MOBILedit;
- SalvationData XLY;
- Magnet forensic;
- Encase forensics;
- Mobilyze BlackBagtech.

Software diversi conducono a risultati di estrazione leggermente diversi a seconda della potenzialità degli stessi, pertanto un buon laboratorio di Digital Forensics dovrà avere a disposizione diversi software ed hardware per disporre di maggiori possibilità di accesso ai dati informatici. Le procedure e le best practices sono le medesime: in particolare si menziona lo standard ISO 27037/IEC e le direttive per la Polizia Giudiziaria a seguito della ratifica della Convenzione di Budapest del 2001[44]. Tra gli strumenti a disposizione non va trascurato il mondo Open Source ed in particolare i tool liberamente disponibili e spesso già contenuti all'interno dei sistemi operativi Gnu-Linux, tra i quali: Gnu-Linux Tool Mobile Forensics In particolare tra i tool Open Source atti alla specifica attività di Mobile Forensic si menzionano:

a) il tool ADB "Android Debug Bridge" con il quale è possibile effettuare screenshot e registrazioni video dello schermo del dispositivo mobile per attività urgenti di Polizia Giudiziaria per le quali non è possibile attendere il pro-

44 In Italia il riferimento è la L. 48/2008.

cesso finale di estrazione e analisi del dispositivo, ad esempio negli ambiti della criminalità organizzata, terrorismo ed in genere attività di pubblica sicurezza, con lo stesso tool è possibile effettuare numerose operazioni sui telefoni cellulari supportati, tra cui il downgrade install App;

b) Apktool con il quale è possibile effettuare disassemblaggio di software .apk alla ricerca di malware e codici malevoli in genere;

c) BitPim con il quale è possibile accedere al contenuto logico dei telefoni cellulari supportati e, talvolta, al livello filesystem;

d) Fastboot con il quale, avviando i telefoni cellulari Android proprio in modalità FastBoot o Download Mode è possibile copiarne la memoria interna;

e) IDevice Backup2 con il quale è possibile, grazie ai driver e alle librerie per Iphone, copiare le memorie dei dispositivi con sistema operativo IOS;

f) Iphone backup analizyer con il quale è possibile analizzare i backup rinvenuti nelle memorie dei personal computer o effettuate quale scelta di copia estrazione del dato informatico per successiva analisi e ricerca delle evidence;

L'utilizzo di tali strumenti di estrazione richiede indubbiamente esperienza e competenza, acquisibili attraverso appositi corsi.

III.11.7 - ANALISI DEL DATO DIGITALE

L'esperto della polizia penitenziaria effettuerà le proprie ricerche sugli indicatori di rischio o sugli indizi attraverso una copia dei dati e non sull'originale acquisito, sulle stringhe, sui time-stamp dei file e quindi sulla timeline o sul contenuto anche esadecimale presente all'interno dei file o degli artefatti, facendo sempre riferimento alla posizione del dato informatico ed alle sue coordinate informatiche all'interno del file system o della posizione logica. La medesima ricerca deve essere ben documentata e ripetibile in procedimento anche con altri strumenti software. Molta importanza rivestono in questa fase i software che riescono ad indicizzare anche i contenuti stringa all'interno dei file binari (.docx, .xlsx, ecc) e ad effettuare in seguito una ricerca veloce sui dati. Gli strumenti per l'analisi (software forensi) risultano sempre più orientati verso la digital forensics ricomprendendovi anche la mobile forensics, volendo qui significare che ormai è uno standard di questi software la capacità di analisi anche di estrazioni (dump fisici o logici o file sytem) di dispositivi mobili. Questi si sono evoluti al punto che oggi risultano essere strumenti "multipiattaforma", in grado di analizzare anche estrazioni effettuate da software diversi da quelli cui si riferiscono. Esistono anche strumenti e programmi open source capaci di analizzare i dump di dispositivi mobili che sono in grado di effettuare analisi anche approfondite e specifiche con riferimento a singole app.

III.11.8 - REDAZIONE DEI REPORT

Per quanto concerne questo aspetto non sussistono particolari diversità rispetto a quanto già evidenziato nella computer forensics; i programmi e tool dedicati alla mobile forensics forniscono spesso la possibilità di ottenere dei report preconfezionati o a richiesta dello specifico caso, di facile consultazione e portabilità. Tuttavia la loro completezza va sempre rivalutata sui canoni di quanto già descritto circa la presentazione delle prove o indicatori di rischio informatici in dibattimento, che risultano strettamente legati alle caratteristiche di un idoneo report di analisi. Vengono illustrati di seguito alcuni software di analisi dei tabulati telefonici.

III.11.8.A - PHONELOG

SecurCube®PhoneLog è il software per l'analisi dei tabulati telefonici e correlazione degli stessi con altre prove o indicatori di rischio informatici digitali quali estrazioni da dispositivi mobili, tracce GPS, log di copertura reale delle celle telefoniche, ottenuti utilizzando la strumentazione forense SecurCube®BTS Tracker, e altri metadati; il tutto, per una completa ricostruzione e interpretazione della scena del crimine "digitale". In analisi disgiunte, le fonti permettono di evidenziare solo parzialmente i legami che intercorrono tra loro. Al contrario, se opportunamente collegate, possono fornire importanti spunti investigativi. Si prenda in esame il seguente esempio, estratto di un'analisi realizzata con l'applicativo PhoneLog: *"Il soggetto dichiarava di essere estraneo ai fatti. Affermava di essere rientrato nella sua abitazione alle 12:00 pm e di non averla più lasciata fino all'indomani. Dai tabulati telefonici però, alcuni eventi lo collocavano sotto la copertura di cella telefonica, lontana dal suo domicilio*" Il filtro creato propone criteri di ricerca idonei all'identificazione di talune attività nella fascia oraria collegata ai fatti, in copertura della cella che teoricamente rivolge la sua copertura altrove rispetto all'abitazione del sospettato (ping rosso in alto a destra) ma che in realtà ha registrato un gruppo di eventi oggetto di ulteriore verifica [Fig.1].

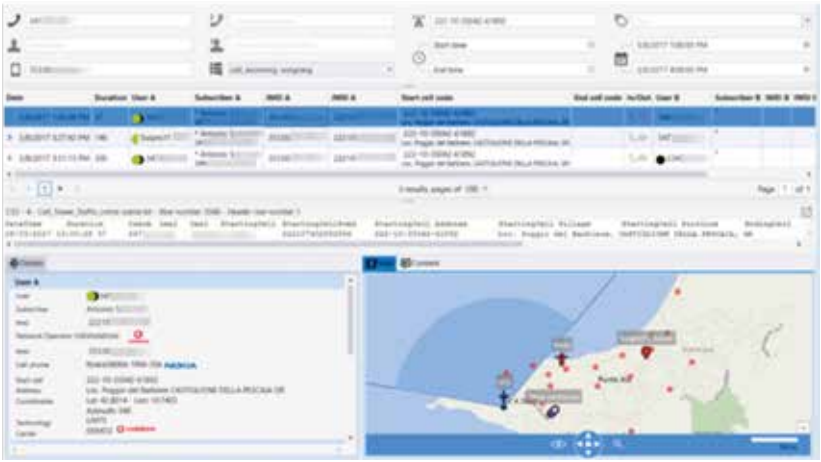


Fig. 1: ricerca degli eventi collegati all'utenza nella fascia oraria d'interesse[1]

A che prova forense digitale fanno capo i cerchietti rossi sulla mappa? La dichiarazione del sospettato, quindi il suo alibi, potrebbero trovare fondamento esattamente a seguito di quella prova. I punti mostrano il log di misurazione della strumentazione forense BTS Tracker, per la verifica della copertura reale delle celle telefoniche. L'attività, eseguita simulando condizioni temporali/ambientali/urbanistiche idonee alla ricostruzione dei fatti (giorno della settimana, fascia oraria, condizioni meteo, edifici ecc.) appura come, idealmente, il dispositivo del sospettato si sarebbe potuto agganciare alla cella target anche lontano dalla sua installazione e copertura teorica [Fig.2].

Fig. 2: dettaglio nell'analisi della copertura teorica e reale delle celle telefoniche

In base alla simulazione, la casa del sospettato è interessata dal fascio di copertura reale (linea retta che collega l'icona BTS al ping rosso dell'abitazione del sospettato). L'estrazione dati dai dispositivi entra in gioco per la verifica delle interconnessioni tra i soggetti, le loro abitudini ecc. I tabulati ricreano lo scenario nel quale collocare questi contenuti, evidenziando talvolta lacune ed aspetti di anti-forensics molto importanti [Fig. 3]:

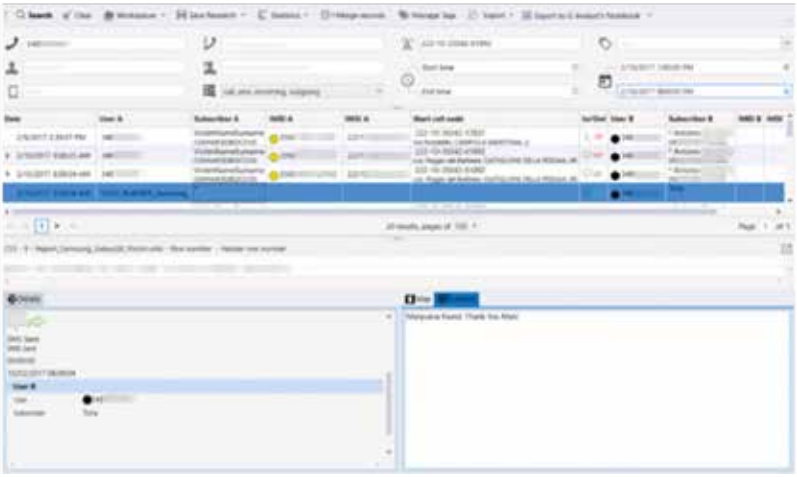


Fig. 3: comparazione dei record del tabulato con i dati estratti dal dispositivo

I dati estratti dal dispositivo mobile della vittima, in questo caso, presentano elementi utili a collegare il sospettato all'attività illecita della vittima. Qui, nello specifico, il record del tabulato si associa esattamente al contenuto estratto. A supporto di quanto emerso in quella data e da tal contenuto, dai dati estratti emerge anche un'immagine scattata e inviata (exif file recuperato) [Fig.4]:

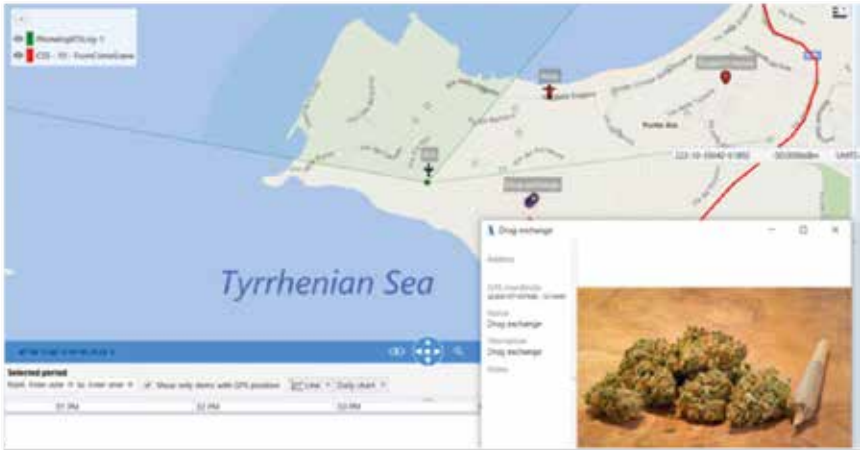


Fig. 4: Estrazione dati e correlazione con l'analisi della copertura teorica e reale delle celle telefoniche

La cella d'interesse è sempre la stessa. L'immagine è stata inviata in coda a quel messaggio [Fig. 3] per poi essere cancellata. Il percorso in rosso è la strada percorsa dal sospettato. Un secondo filone d'indagine e di azione di sorveglianza preventiva ha accertato che il veicolo dello stesso fosse transitato in quella data e in quell'orario della comunicazione (immagini di videosorveglianza dell'ufficio postale del Paese ubicato in via del Porto). Quanto raccolto è di per sé un esempio lampante di come i metadati, nell'informatica forense, necessitino di opportuna investigazione incrociata, al fine di evidenziare ogni tipo di relazione intercorsa, presente o passata, di vitale importanza per la confutazione o conferma dell'alibi.

III.11.8.B - NEW S.A.T. 32/64 BIT

S.A.T., acronimo di "Sistema Analisi Tabulati", è un database creato in Access ad uso esclusivo delle Forze dell'Ordine. Il programma si pone come obiettivo di semplificare e velocizzare l'importazione e l'elaborazione dei tabulati telefonici e telematici. L'interfaccia utente è piuttosto semplice ed immediata, infatti nella schermata principale si trovano le varie funzionalità dell'applicativo che, con estrema facilità, permette di aggiungere tabulati, anagrafiche e successivamente effettuare l'analisi e la correlazione dei dati utili ai fini dell'indagine ed all'azione di sorveglianza preventiva:

- Analisi Tabulati
- Analisi e Match su Imei
- Analisi Celle Telefoniche
- Analisi Anagrafiche Attive e Storico Utenza
- Modifica nomi Tabulati
- Eliminazione Tabulati
- Eliminazione Anagrafiche
- Importazione dati da versione precedenti

Importazione tabulati

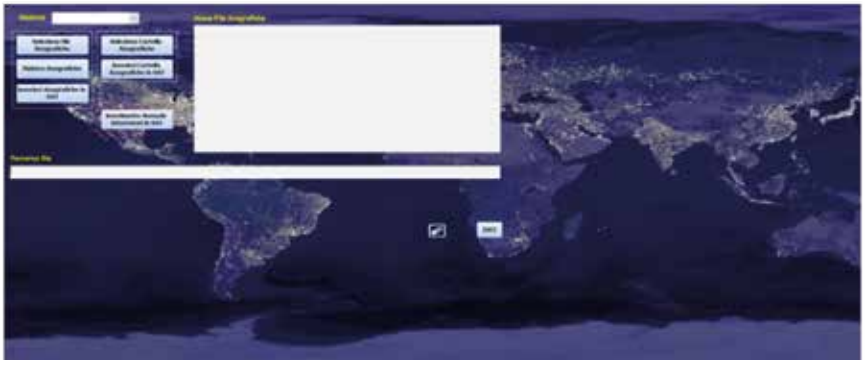
L'importazione dei tabulati telefonici e telematici, esclusivamente in formato

testo ".txt", non è altro che la normalizzazione per l'omogeneità dei dati ricevuti dai principali gestori telefonici italiani (TIM, VODAFONE, WIND/H3G, ILIAD, SPARKLE Italia)

Importa Tabulati

Come si può evincere dalla schermata "Importa Tabulati", l'importazione può avvenire selezionando sia un file singolo che l'intera cartella contenente tutti i tabulati, di tutti i gestori richiesti, relativi al nostro target. Il riconoscimento del Gestore avviene in modo automatico e senza apportare modifiche alla struttura dei file ad eccezione dei file ricevuti da Wind/H3g ed Iliad che dovranno essere precedentemente suddivisi utilizzando l'apposito pulsante. La presenza del pulsante "Cerca Tabulati Wind o Iliad da Dividere", infatti, serve per facilitare ed automatizzare la divisione tra i dati dei tabulati telefonici e le informazioni anagrafiche delle utenze contenute all'interno di un unico file. Importazione anagrafiche L'importazione delle anagrafiche, analogamente ai tabulati telefonici, può anch'essa avvenire con un'importazione singola o massiva.

Importa anagrafiche



Per l'importazione singola delle anagrafiche, ricevute unitamente ai tabulati,

va selezionato il Gestore Telefonico (Tim, Vodafone, Wind/H3g, Iliad, Lyca-Mobile, Telecom) mentre per le richieste effettuate tramite portale c'è da selezionare il relativo Gestore seguito dalla parola "portale". Per l'importazione massiva il riconoscimento avverrà in automatico. All'interno dell'applicativo saranno importate le anagrafiche attive e disattive, ma in "visualizzazione tabulato" verranno associate solo le informazioni anagrafiche delle utenze che risulteranno attive al momento della richiesta. Inoltre, è possibile inserire o modificare le informazioni anagrafiche di un'utenza in modo manuale.

Analisi tabulati

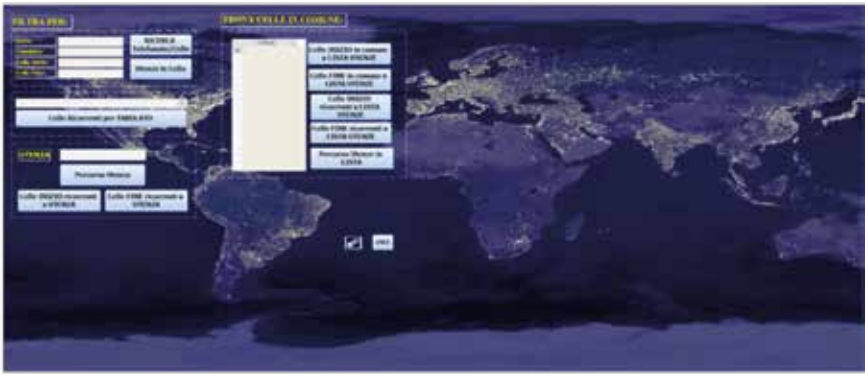
La schermata "Analisi Tabulati", come si può notare, è caratterizzata da varie possiblità di visualizzazione e di ricerca. Analisi Tabulati La visualizzazione Tabulati "Totale" o "Selezionato" dà la possibilità di constatare prontamente:

- Tipo Eventi (tipo di traffico, Generato/Terminato, non risposto, sms, segreteria)
- Durata Evento (timestamp dei dati traffico)
- Identità dei terminali ed utenze (codici IMEI ed IMSI)
- Informazioni Gestore (competenza Gestore in base all'IMSI)
- Luogo Evento (BTS "stazione radio base") La "Visualizzazione Avanzata" dei Tabulati "Totale" o "Selezionato, a differenza della precedente, aggiunge, se importati all'interno dell'applicativo, importanti e fondamentali informazioni investigative sull'utenza chiamante, ovvero:
- Intestatario Storico
- Indirizzo
- Stato Numero
- Imsi
- Data Attivazione / Disattivazione
- Codice Fiscale / P.IVA

Analisi e match su IMEI

In questo menù si potranno effettuare ricerche inverse, tra IMEI e UTENZA, e verificare rapidamente un'utenza a quanti apparati telefonici è stata abbinata o viceversa. Inoltre, è possibile effettuare ricerche multiple sui tabulati oppure visualizzare il percorso effettuato da una qualsiasi IMEI presente all'interno dei tabulati inseriti.

Analisi celle telefoniche



Nella schermata "Analisi Celle Telefoniche" è possibile effettuare con estrema facilità un'analisi del traffico telefonico e telematico rivolto alla localizzazione simultanea e reciproca di più utenze al fine di vagliare l'ipotesi di frequentazione o incontri tra i soggetti utilizzatori. Analisi Celle Telefoniche Sulla base delle informazioni emerse, una volta individuate una o più utenze telefoniche, è possibile verificarne:

- la presenza in un dato luogo e in un certo intervallo di tempo;
- la dinamica degli spostamenti singoli o multipli;
- la supposizione di incontro con altri soggetti; Si evidenzia che l'apparte-

nenza delle utenze ad operatori differenti ed i fattori casuali nei processi di aggancio di cella introducono diversi elementi di criticità che possono condurre ad una ricostruzione investigativa errata.

Analisi Anagrafiche Attive

Il menù "Analisi Anagrafiche Attive" oltre a contenere tutte le informazioni utili all'identificazione dei soggetti intestatari, se ricevuti dal gestore di appartenenza, permette di effettuare ricerche semplici mediante:

- Nome
- Cognome
- Codice Fiscale/P.IVA Oppure, tramite i sottomenù "Ricerca su Campi", di eseguire ricerche avanzate su:
- Indirizzo
- ICCID
- IMSI
- Data Attivazione/Disattivazione
- Data e Luogo di Nascita Anagrafiche Attive

Requisiti minimi di sistema

- CPU: 1 gigahertz (GHz) o superiore
- RAM: 2 GB per sistemi a 32 bit o 4 GB per sistemi a 64 bit
- OS: Windows 7/8/10 (32/64 bit)
- SOFTWARE: Office 2013 / 2016 / 2019 (32/64 bit)

III.12 - CENNI SUL SISTEMA DI LOCALIZZAZIONE TRAMITE RETE CELLULARE

Nelle telecomunicazioni una rete radiomobile cellulare è una rete di telecomunicazioni wireless che consente la radiocomunicazione tra terminali mobili sparsi su un territorio coperto da più celle radio, ciascuna servita da apparati

fissi di ricetrasmissione, denominati stazioni radio base. Essi sono dunque i sistemi che implementano la telefonia cellulare, che a sua volta fa parte della telefonia mobile. Il sistema di telefonia mobile è organizzato per celle che assicurano la copertura delle zone di territorio con una complessa struttura a nido d'ape in cui le celle rappresentano una zona coperta dal segnale di un'antenna radio chiamata BTS.
Ogni terminale acceso sul territorio viene quindi intercettato dall'antenna radio BTS che "copre" quell'area e, dopo essere stato individuato, l'associazione tra il terminale e la cella viene comunicata ad un database di gestione. Tale informazione è inserita sui tabulati telefonici richiesti agli operatori telefonici e rappresenta il dato utile per la ricostruzione della localizzazione nell'ambito del sistema di telefonia mobile.
RETE GSM: la singola centrale telefonica (MSC) della rete radiomobile GSM controlla un numero elevatissimo di celle, raggruppate in insiemi distinti definiti LOCATION AREA (LAC). Di conseguenza la rete GSM realizza un'architettura gerarchica, con la singola centrale telefonica (MSC) che controlla le varie LOCATION AREA, ognuna delle quali è costituita a sua volta da un insieme di celle ben definito.
CAMBI DI CELLA: il telefonino resta normalmente in modalità di ascolto (STANDBYNCELL SELECTION), e periodicamente identifica la cella telefonica migliore alla quale rimanere connesso. Tale selezione avviene in base all'analisi di diversi parametri. Il più importante tra questi è senza dubbio il parametro che identifica la "potenza del segnale". Più vicina è la stazione trasmittente (radio base), più alta sarà la potenza del segnale. Questo processo prende il nome di "CELL SELECTION (o RESELECTION)".
La cosiddetta modalita' "HANDOVER", invece, riguarda il sistema di scelta delle celle telefoniche da parte del provider telefonico quando e' già in corso una comunicazione. Nel caso della modalità standby, la rete radiomobile non tiene traccia normalmente della cella alla quale il cellulare è connesso, ma memorizza solo la posizione relativa alla Location Area.
CELL SELECTION: quando l'utente accende il terminale radiomobile, quest'ultimo passa in modalità standby (IDLE mode). Il dispositivo si mette in "ascolto" e si sintonizza sulla cella "migliore" appartenente al proprio operatore. La procedura di selezione della cella telefonica effettuata all'accensione del dispositivo radiomobile è denominato "CELL SELECTION". CELL RESELECTION: nel caso in cui in fase di IDLE il terminale radiomobile identifichi una nuova cella telefonica (ad esempio, a causa di uno spostamento dell'utente o di una variazione del segnale radioelettrico) il cellulare interrompe la connessione con la cella precedente ed inizia una connessione verso la nuova cella. L'operazione di cambio cella è definita
CELL RESELECTION. MODALITA' STANDBY (IDLE MODE): quando un cellulare è in modalità STANDBY (IDLE MODE), ossia acceso ma non attivo (nessuna comunicazione in corso) la rete radiomobile può determinare la sua posizione solo a livello di Location Area. In caso di chiamata o di sms entrante la rete effettua un'operazione chiamata PAGING: tutte le celle della Location Area in cui si trova l'utente irradiano una richiesta specifica di localizzazione, a cui il

terminale radiomobile dell'utente interessato deve rispondere inviando il codice della cella in quel momento "impegnata". La rete radiomobile ottiene quindi la localizzazione precisa a livello di cella dell'utente e procede indirizzando la comunicazione verso la cella precedentemente segnalata dall'utente. Nel caso di chiamata uscente, la richiesta di comunicazione da parte del telefonino chiamante permette alla centrale ed alla rete l'immediata conoscenza della cella alla quale il chiamante è connesso.

III.12.1 DEFINIZIONE BTS

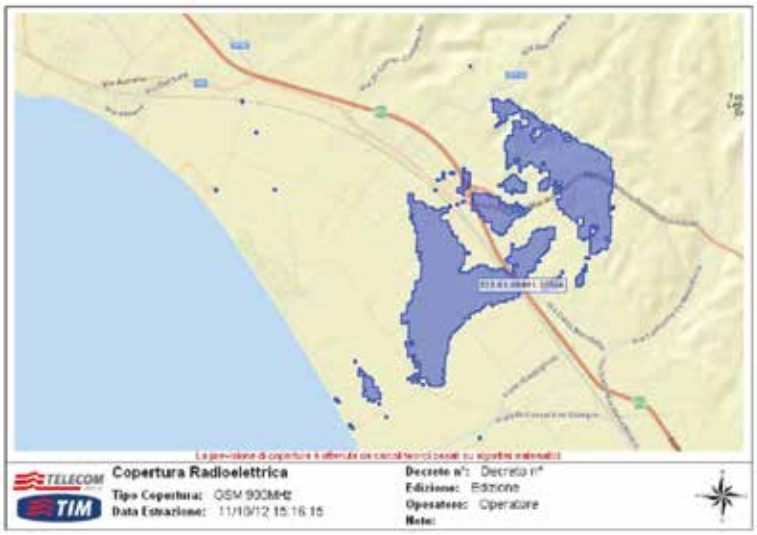
Nelle telecomunicazioni, nell'ambito delle reti cellulari, il termine stazione radio base, in sigla BTS (del corrispondente termine inglese "base transceiver station"), indica il sottosistema di ricetrasmissione di un segnale radio dotato di antenna ricetrasmittente che serve i terminali mobili di utente coprendo una determinata area geografica detta appunto cella radio.
Essa rappresenta, dunque, l'infrastruttura base della telefonia cellulare usata nei radiocollegamenti delle reti mobili cellulari nell'interfaccia radio del sistema cellulare. In genere chiamato ripetitore, in realtà non "ripete" alcun segnale, ma lo genera e lo trasmette in aria oppure lo riceve.
Definizione CGI: https://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_ Europe#Italy

Nel 2016 Wind Italy e 3 Italy (Tre) hanno raggiunto un accordo per completare la fusione durante il prossimo anno.
La fusione è stata approvata o gli indicatori di rischio informatici sono stati resi noti dalle autorità europee e nazionali. Un nuovo operatore, Iliad, è entrato nel mercato italiano nel maggio 2018 come conseguenza della fusione.

Rank	Operator	Technology	Ownership	MCC / MNC
		900/1800 MHz GSM (GPRS, EDGE)		
				22288
1	Wind Tre	900/2100 MHz UMTS, HSDPA, HSUPA, HSPA+, DC-HSPA+	CK Hutchison Holdings	(Wind) 22299 (Tre)
		800/1800/2100/2600 MHz LTE, LTE-A		
2	TIM	900/1800 MHz GSM (GPRS, EDGE) 900/2100 MHz UMTS, HSDPA, HSUPA, HSPA+, DC-HSPA+ 800/1500/1800/2600 MHz LTE, LTE-A VoLTE 3700 MHz 5G NR (Only in Rome and Turin)	Vivendi (24%)	22201

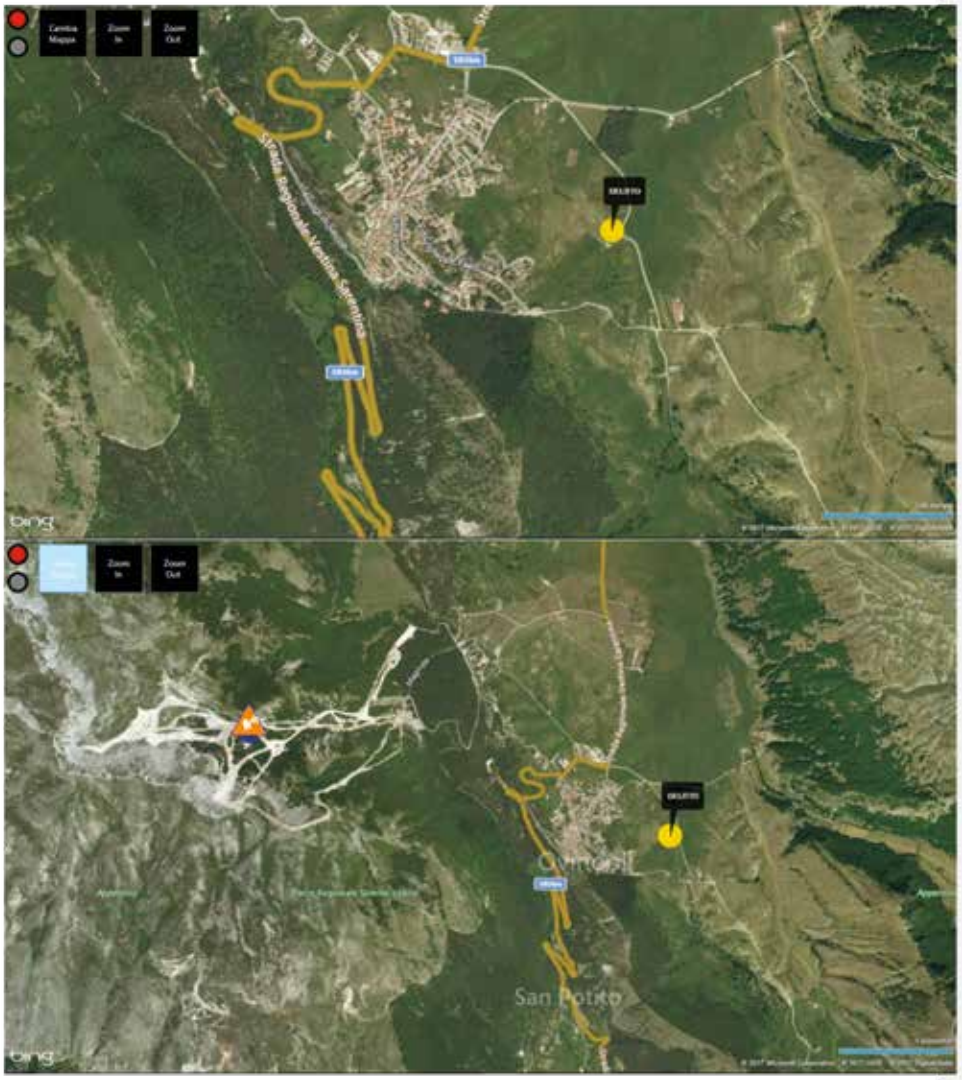
Cell Global Identity È usato per identificare le celle e quindi l'area dalla quale è stato sviluppato un certo traffico telefonico (voce-dati-sms) CGI = MCC – MNC – LAC – CID CGI 2G e 3G = 222-01-12345-12345 CGI 4G = 222-01-1234567-123 Previsione di Copertura Radioelettrica

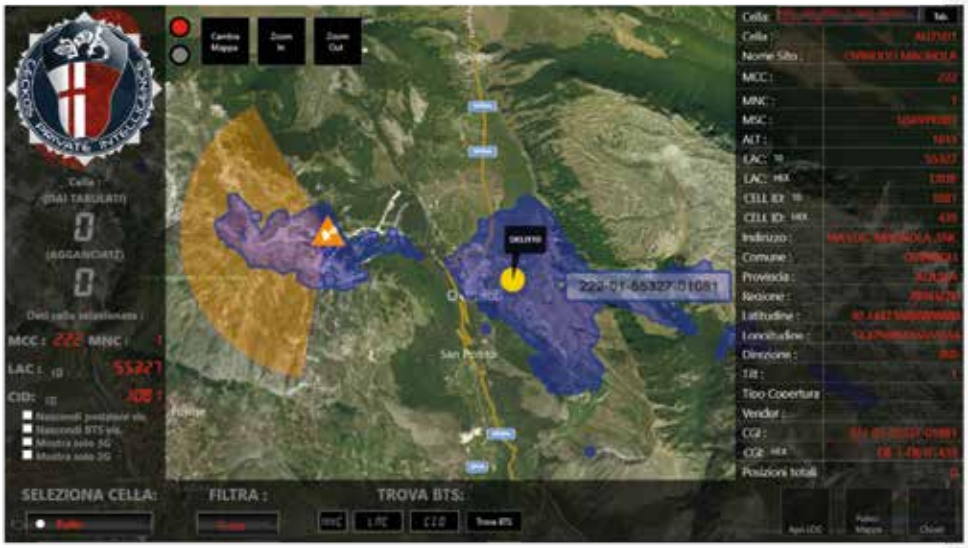
Mappe di servizio



III.12.2 - CASO PRATICO DEL VALORE DELL'ACQUISIZIONE DELLE COPERTURE RADIO ELETTRICHE

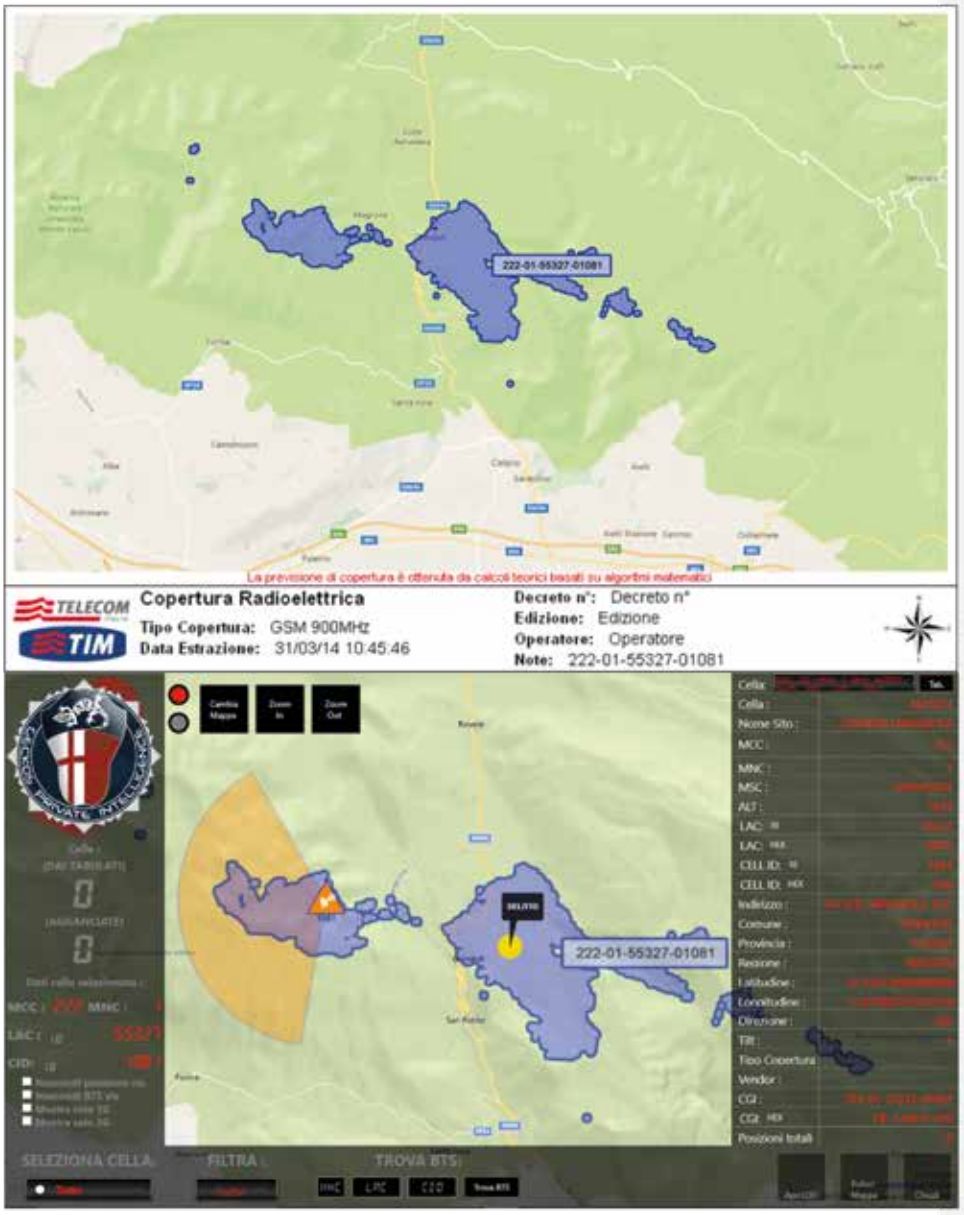
- L'indagato viene riconosciuto dalla vittima
- L'indagato viene interrogato dal Magistrato in presenza del difensore ▪ L'indagato dichiara di non ricordare che cosa avesse fatto in quel giorno e a quell'ora
- L'indagato viene sottoposto a fermo
- L'indagato viene rinviato a giudizio
- L'avvocato si attiva con le indagini difensive ed acquisisce i tabulati telefonici del proprio cliente
- Viene individuata una telefonata ricevuta dal proprio cliente della durata di 2'18'' compatibile con il giorno e l'ora dell'aggressione
- L'avvocato acquisisce le CGI per verificare la posizione della Cella 222-01-55327- 01081 agganciata
- L'avvocato durante il dibattimento dimostra che la cella agganciata dal cellulare del suo cliente è distante e soprattutto con direzione incompatibile con il luogo del delitto
- L'indagato viene assolto per non aver commesso il fatto


Cambia Mappa
Zoom In
Zoom Out
bing
Cambia Mappa
Zoom In
Zoom Out
bing

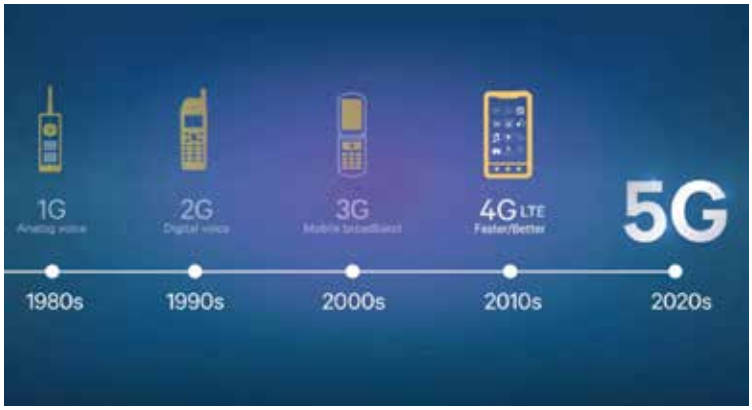

Cambia Mappa
Zoom In
Zoom Out
Cella :
(DAI TABULATI)
(AGGANCIATI)
Dati cella selezionata :
MCC : 222 MNC :
LAC :
CID :
SELEZIONA CELLA:
FILTRA :
TROVA BTS:
Cella :
Nome Sito :
MCC :
MNC :
MSC :
ALT :
LAC :
CELL ID :
Indirizzo :
Comune :
Provincia :
Latitudine :
Longitudine :
Direzione :
Tilt :
Tipo Copertura
Vendor :
Posizioni totali


Cambia Mappa
Zoom In
Zoom Out
Cella :
(DAI TABULATI)
(AGGANCIATI)
Dati cella selezionata :
MCC : 222 MNC :
LAC :
CID :
SELEZIONA CELLA:
FILTRA :
TROVA BTS:


Cambia Mappa
Zoom In
Zoom Out
San Potito
SELEZIONA CELLA:
FILTRA :
TROVA BTS:


222-01-55327-01081
La previsione di copertura è ottenuta da calcoli teorici basati su algoritmi matematici
TELECOM
TIM
Copertura Radioelettrica
Tipo Copertura: GSM 900MHz
Data Estrazione: 31/03/14 10:45:46
Decreto n°: Decreto n°
Edizione: Edizione
Operatore: Operatore
Note: 222-01-55327-01081
222-01-55327-01081
SELEZIONA CELLA
FILTRA
TROVA BTS

IL MOBILE PROFILING: Introduzione: L'avvento degli smartphone ha determinato a partire dal 2008 una vera rivoluzione tecnologica e sociale in costante evoluzione. Questi dispositivi hanno soppiantato i telefoni cellulari basati su standard GSM/GPRS, offrendo la potenza di un computer, una fotocamera ed una connessione ad alta velocità (3G/4G/5G), nel palmo di una mano. Al loro interno viene custodita la nostra vita.



Le semplici telefonate, hanno lasciato lo spazio a chat con contenuti multimediali, videochiamate, conferenze, scambio e condivisione di documenti e tanto altro, sfruttando applicazioni proprietarie del sistema operativo oppure successivamente scaricate ed installate sul dispositivo.

Gli sviluppatori, al fine di migliorare la *user-experience* mediante semplici interazioni sul touchscreen, hanno dovuto sviluppare soluzioni di funzionamento e sicurezza semplificate ed allo stesso tempo in grado di garantire stabilità e compatibilità con i classici servizi desktop.

Così, autorizzare un accesso ad un determinato servizio, non è più subordinato all'immissione di una password ma unicamente all'utilizzo dello smartphone associato all'istallazione della relativa applicazione.

Ogni applicazione avrà la necessità di utilizzare specifici servizi di base del sistema operativo subordinatamente all'accettazione da parte dell'utilizzatore di specifiche autorizzazioni di accesso.

Prima dell'ottobre del 2015 nel mondo Android (API level 23 - <Android 6.0), la concessione di tali permessi risultava inderogabile nelle fasi della prima installazione dell'app sul dispositivo che altrimenti non andava a buon fine. Successivamente è stata introdotta la possibilità di autorizzare specifici singoli permessi nel momento in cui lo stesso risultava necessario durante il funzionamento dell'app mediante la comparsa della notifica sullo schermo.

Ciononostante la necessità di utilizzare il servizio, quasi sempre indurrà l'utilizzatore a concederla senza troppi indugi, a maggior ragione nel momento in cui ne ha effettivamente bisogno.

Tutte queste soluzioni hanno di fatto permesso un uso più veloce della tecnologia ma di fatto ridotto la sicurezza complessiva dell'utente in quanto il semplice possesso del dispositivo, permette di gestire ed autorizzare una pluralità di azioni.

Inoltre la necessità di esser sempre online, ha portato gli sviluppatori a lasciare attive queste applicazioni in uno stato di backgruond, che di fatto ne nasconde apparentemente il costante funzionamento, ma non la condivisione e raccolta dei dati.

Le nuove tecniche d'indagine vanno proprio a sfruttare tale caratteristiche funzionali per ottenere dati ed indizi fondamentali nel corso delle attività d'indagine così da identificare il reale utilizzatore del dispositivo creando un impianto probatorio costituito da dati tecnici.

Questa tecnica prende il nome di **"Mobile profiling"**.

Partendo da informazioni personali quali ad esempio numeri di telefono, indirizzi email, account social network, titoli di credito, si potrà risalire alle relative informazioni personali dell'utente richiedendole direttamente alle società che le detengono per garantire il funzionamento dello smartphone e/o della specifica applicazione attenzionata nel corso delle indagini.

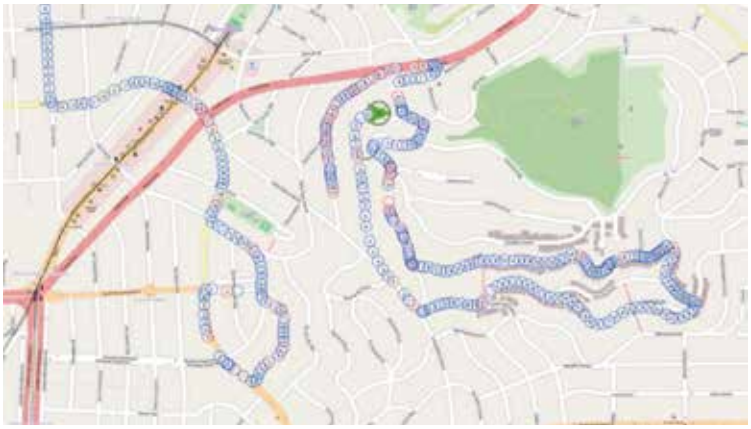
Infatti se si considera il mondo degli smartphone principalmente divisibile in due categorie, rispettivamente quelli basati su sistema operativo Android afferente alla Società Google LLC. e quelli basati su iOS relativi all'azienda Apple Inc., si potranno ottenere le informazioni di quasi tutti gli utenti del mondo direttamente rapportandosi, a norma di legge, con loro.

Attraverso l'emissione dell'A.G. competente di un decreto d'acquisizione traffico telematico riconosciuto bilateralmente (MLAT) si potranno ottenere dati anagrafici, e log di connessione del target mentre per tutti i contenuti quali ad esempio conversazioni, posizioni e quant'altro il loro ottenimento sarà subordinato ad un procedimento in rogatoria internazionale.

Analogamente, si potrà procedere nei confronti delle società proprietarie delle singole applicazioni installate sul dispositivo e/o in uso dal target.

L'analisi dei tabulati telefonici e telematici permette all'investigatore di avere una traccia approssimata del dispositivo d'interesse investigativo e ricostruirne grossolanamente gli spostamenti.

Sfruttando i dati condivisi dallo smartphone, si potranno invece compiere attività di mobile tracing più puntuali in quanto generate direttamente dal GPS cui corredati tali dispositivi (errore < 1 metro), ricavandole dal fornitore del servizio (“ ”). (“*server side*”).



A titolo esemplificativo si riporta la ricostruzione spazio temporale degli spostamenti di un sospettato effettuata sfruttando le posizioni acquisite dal social network Facebook dal funzionamento in background della relativa applicazione installata sullo smartphone del target.

Il fatto che tali posizioni siano associate ad un'identità virtuale, permette all'investigatore di giungere, attraverso attività di Open Source Intelligence (OSINT), ad una correlazione con il reale utilizzatore dello smartphone molto più agevolmente rispetto alle abituali tecniche d'indagine. Il mobile profiling risulta ancor più efficace quando si procederà in seguito ad un evento crimi-

noso alla ricerca dell'autore, non avendo alcun elemento d'indagine se non il reato stesso.

Sfruttando infatti le specifiche funzionalità dei sistemi operativi e delle applicazioni che sono installate sugli attuali smartphone ad esempio, si potrà ottenere una lista puntuale di tutti i dispositivi presenti nell'area geografica d'interesse ed ottenere elementi indiziari in capo ai loro proprietari e/o sulle persone che li stavano utilizzando sulla scena del crimine.

Inoltre, un'analisi approfondita dell'applicazione d'interesse investigativo, attraverso attività tecniche di reverse engineering, potrà aiutare l'investigatore a determinare tutte le specifiche funzionalità attivate così da individuare i dati

effettivamente condivisi con i server dell'azienda proprietaria anche in tutti quei casi in cui vengono utilizzate applicazioni improntate all'anonimato ed alla tutela della privacy.

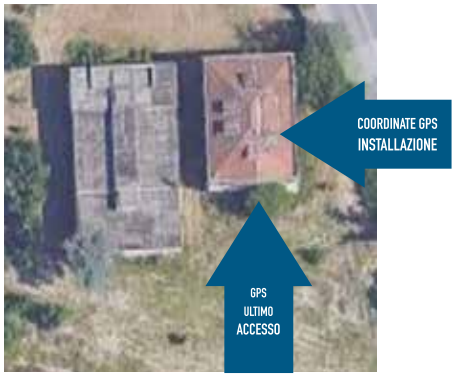
Esempio in un caso reale Reato ipotizzato:

Istigazione a pratiche di pedofilia – soggetto ricercato anche dall'FBI.

Fatti: Il reo, sfruttando un'applicazione di chat anonima, ove non c'era l'obbligo di fornire alcun dato all'atto della registrazione al servizio, riusciva a circuire delle vittime preadolescenziali fingendosi coetaneo di sesso femminile.

Dati tecnici: L'applicazione, sviluppata in un paese del sud est asiatico, era caratterizzata dalla possibilità di ricercare solo gli utenti prossimi territorialmente tra loro entro un determinato raggio (50 Km). Nessun dato veniva dichiaratamente acquisito.

Indagini: Veniva effettuata un'attività di reverse engineering volta a stabilire lo specifico funzionamento dell'applicazione determinando che vi fossero, tra i dati inviati durante il funzionamento, le coordinate GPS del dispositivo ove installata nonché la trasmissione delle caratteristiche stesse del device e degli account su di esso sincronizzati.
Attraverso l'analisi delle connessioni generate, veniva inoltre determinata l'ubicazione reale del data center ove riversati i dati esfiltrati dall'applicazione ed in seguito ad attività di Osint si giungeva all'individuazione degli sviluppatori dell'applicazione e del referente del data center.
Veniva instaurata una collaborazione transnazionale con l'ottenimento di tutti i dati in loro possesso tra cui rispettivamente un indirizzo email sincronizzato sullo smartphone, i dettagli tecnici del dispositivo (marca, modello ed IMEI) e due coordinate GPS pressoché coincidenti comprensive di data/ora relative all'installazione dell'applicazione ed al suo ultimo utilizzo.



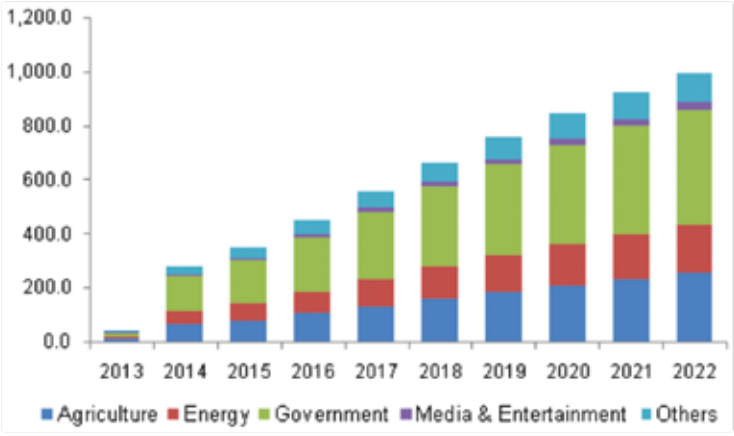
Esiti: In seguito ad un ulteriore attività info investigativa su tali dati, si poteva

stabilire che tali geo localizzazioni fossero riferibili ad un'abitazione specifica presso cui dimorava, unitamente ai familiari, un soggetto già pregiudicato per reati afferenti alla pedo pornografia. Procedendo a perquisizione, veniva trovato in possesso dello specifico smartphone individuato nonché rinvenuti elementi inequivocabili circa le responsabilità costituenti reato.

Conclusioni Come esplicato brevemente, infinite possono essere le possibilità d'indagine sfruttando e servendosi della tecnologia ma solo la conoscenza di tali potenzialità potrà permettere all'investigatore di aumentare le sue capacità critiche e d'analisi andando a ricercare le prove anche dove nessuno aveva mai pensato di cercarle.

DRONE FORENSICS

Il Drone Forense mira a identificare, acquisire e analizzare l'intero "Drone Ecosistema". Questo capitolo ha l'obiettivo di fornire orientamenti agli operatori per un approccio migliore alle indagini tecniche sull'ecosistema drone.



Il mondo dei droni o UAS (Unmanned Aerial System), attualmente agevolmente accessibile, dispone di un mercato sempre crescente rivolto ad un pubblico ampio, che coinvolge sia utenti inesperti che principianti, i quali, grazie alla tecnologia di volo altamente assistita e droni commerciali semplificati, acquistabili online o in vari negozi di elettronica già pronti al volo, fino a criminali esperti nell'uso illecito di tali potenti strumenti che non richiedono particolari abilità di volo, ma sono altamente versatili per capacità operativa. La divisione dei droni offensivi in due macro categorie, li identifica come segue:

1 UAS offensivo che può mettere in pericolo persone e/o infrastrutture e/o aeromobili;
2 UAS offensivo che può essere utilizzato come mezzo di consegna/contrabbando, anche nelle carceri.

Le due categorie sopra elencate sono le più comuni e ben note ai media, anche se la prevenzione e l'analisi dell'uso illecito di droni ha infiniti scenari criminali. È importante che i primi soccorritori e gli operatori digitali che intervengono per primi sulla scena del crimine sappiano come utilizzare i droni senza compromettere alcuna traccia digitale.

CATEGORIE DI DRONI

L'enorme numero di droni e la continua crescita delle tecnologie con relativo calo dei prezzi può rendere difficile identificare e classificare gli UAS. Di seguito si distinguono due macro categorie per identificare gli UAS e il loro campo di applicazione, specificando che tutti i modelli di aeromobili, anche multi-motore, che non dispongono di tecnologie e software per la gestione assistita o automatica del volo, non sono presi in considerazione, e che tutti gli UAS sono composti da un sistema RAP (Remote Aeromodel Piloting) e da un RPS (Remote Piloting System) che costituiscono insieme il RAPS (Remote Aircraft Piloting System).

UAV ricreativi e commerciali

Si tratta di tutti i droni di marca che possono essere acquistati online o in vari negozi di elettronica o di giocattoli. Tale tipo di drone può essere utilizzato sia a livello ricreativo (hobby) che commerciale e professionale, ed è generalmente dotato di una fotocamera e di volo assistito e automatico.

UAV su misura

Sono tutti droni autoprodotti o personalizzati che costituiscono la parte del mercato che non è regolamentata e quindi irrintracciabile perché non hanno prezzi di vendita e sono per uso non professionale. Generalmente i droni autocostruiti sono composti da:

Componenti fisici

Si tratta di tutti i componenti che compongono il drone, che vengono poi divisi e descritti nelle varie categorie:

Telaio di volo

La struttura di volo è il corpo del drone che può avere le seguenti configurazioni:

Controllore di volo

Il controllore di volo è il cuore del drone, composto da diversi giroscopi, bussole e barometri per la stabilizzazione del drone durante il volo: può essere gestito e controllato da un radiocomando (RAP) o direttamente dal software interno per voli automatici. Generalmente composto da una CPU, RAM, e memoria interna ed esterna e gestito da un sistema operativo proprietario (es. Pixhawk con ChibiOS).

Motori, eliche e regolatori di velocità
Sono i motori, le ESC (regolatori del motore per aumentare o ridurre la velocità del motore come necessario), e le eliche.

Custodia protettiva Questa è la copertura che protegge fisicamente l'elettronica sensibile e delicata del drone contro potenziali danni da impatto.

Ricevitore GPS GPS (Global Position System) che consente il posizionamento dell'UAS ed è generalmente collegato al controllore di volo.

Ricevitore Radio (RX) Il ricevitore è collegato al controllore di volo per gestire e pilotare il Drone (RX) tramite un radiocomando RPS.

Trasmettitore (TX) È il Radio Control (RPS) che consente di controllare e gestire il drone e i vari carichi trasportati dagli UAS.

Telemetria (RX e TX) È un modem radio collegato al controllore di volo e alla stazione di terra che consente di ricevere la telemetria UAS (altezza, velocità, carica della batteria rimanente, posizionamento GPS, registro delle operazioni, ecc e invia istruzioni o orari di volo).

Software Per il loro funzionamento, tutti gli UAS utilizzano applicazioni e sistemi per la gestione e la configurazione del drone. I sistemi commerciali di solito utilizzano sistemi chiusi con alcune personalizzazioni, mentre i sistemi di cui al presente paragrafo possono essere gestiti da Open Software e, quindi, personalizzati nella loro interezza e per l'esecuzione di un numero imprecisato di compiti. I pacchetti Open Software sono disponibili gratuitamente su internet e possono essere scaricati da chiunque.

Tra i più noti e utilizzati vi sono:

Indipendentemente dal sistema utilizzato o dalla configurazione di componenti hardware e software, le soluzioni software UAS possono essere classificate in due categorie principali:

Software di gestione del volo Questo software è installato nel controllore di volo e server per la gestione degli UAS, sia manualmente che automaticamente, e permette di controllare la stabilizzazione, il decollo e l'atterraggio del drone.

Software di controllo a terra Il sistema di controllo a terra del drone permette di controllare, comandare, dare operazioni, localizzare, pianificare missioni, ecc. Una stazione di terra può sostituire il controllo radio e può gestire un UAS via radio con diversi tipi di tecnologie di comunicazione (radio, radio criptata, WiFi, 2G, 3G, 4G e 5G). Pur mantenendo elevati livelli di sicurezza degli UAS, i sistemi Open Source sono più economici e possono essere scelti più facilmente per l'uso illecito in quanto possono essere costruiti secondo lo scopo previsto e generalmente utilizzare la stessa tecnologia per diverse configurazioni UAS (molti rotori, ala fissa, VTOL, elicottero, dirigibile).

DRONE PAYLOADS

Ci sono diversi carichi utili che possono essere installati e trasportati da un UAS commerciale o Open Source, e generalmente rientrano in una delle seguenti categorie:

Carichi utili di videocamere e video Si tratta generalmente di telecamere o di telecamere montate su stabilizzatori con 1, 2 o 3 assi chiamati gimbal che consentono registrazioni video stabilizzate in volo.

Carichi utili termici e infrarossi Si tratta generalmente di telecamere termiche o a infrarossi montate su stabilizzatori con 1, 2 o 3 assi chiamati gimbal che consentono registrazioni video stabilizzate in volo. Generalmente utilizzate in applicazioni che comportano indagini agricole, salute e sicurezza, applicazione della legge, e ricerca e salvataggio digitale.

Carichi utili di consegna Si tratta di un settore in continua espansione negli ultimi anni. Utilizza UAS per la consegna dei pacchi. Pionieri includono UPS, DHL e Amazon con Prime Air.

Agricoltura Carico di lavoro Agricola Spraying Drone: si tratta di carichi molto pesanti che possono essere trasportati da grandi droni per il mondo agricolo, al fine di distribuire prodotti per le colture.

Carichi utili delle armi UAS può trasportare armi o esplosivi per attacchi militari o terroristici. Essi possono anche essere utilizzati per fornire le strutture detentive. Grazie alla facilità d'uso e programmazione delle missioni, gli UAS possono essere utilizzati come strumenti per attacchi di precisione.

CAPIRE I DRONI E ALTRE FONTI DI PROVA ASSOCIATE

Gli UAS richiedono tecnologie diverse per supportare il loro funzionamento e mantenere una capacità operativa adeguata; di seguito si illustrano alcuni componenti di base per il funzionamento dei droni:

Telecomando (sistemi di pilotaggio remoto RPS - radiocomandi)

Va sottolineato che i sistemi Closed (commerciale) e Open (Open Source) richiedono sistemi IT per gestire gli UAS. In particolare, nei primi due sistemi di pilotaggio a distanza esiste un radiocomando con sistema Windows per la programmazione e la gestione degli UAS (informatica forense), mentre il secondo è un sistema commerciale di pilotaggio remoto con gestione degli UAS basato

su Android (Mobile Forensics). Sistemi di pilotaggio a distanza con supporto tablet Apple.

Sistema di pilotaggio remoto con sistema operativo Open Source OpenTX. Il sistema salva vari tipi di informazioni utili per gli investigatori in una memoria SD, installata nel Radio Control (Computer Forensics).

Schede di memoria Immagini, video, registri di gestione, registri di programmazione, registri di volo, ecc. possono essere recuperati nella memoria SD. La memoria SD dovrebbe essere acquisita attraverso la metodologia dettata dall'informatica forense e analizzata con il relativo software di gestione o con il software forense mobile che supporta la drone forensics (ad es. MSAB).

Archiviazione cloud Gli UAS possono utilizzare i servizi cloud per memorizzare dati di volo, foto e video nel cloud.

Personal Computer Molti sistemi utilizzano anche un personal computer per la gestione

e la programmazione di droni. I personal computer sono una fonte molto importante di tracce digitali in quanto possono memorizzare tutte le missioni effettuate. Generalmente i personal computer utilizzati per la gestione, la configurazione e la programmazione degli UAS, indipendentemente dal sistema operativo (Linux, Windows o osx), sono chiamati Ground Stations. Tutte le stazioni di terra sopra indicate sono personal computer con sistema operativo Windows.

Tutte le fonti di evidenza digitale illustrate sono, tuttavia, secondarie alla principale evidenza digitale che rimane sugli UAS. Tuttavia, è essenziale che tutte le secondarie dell'evidenza digitale siano trattate e gestite secondo i principi della scienza forense digitale. Il drone, che rimane la principale fonte di evidenza digitale nello scenario è un oggetto che si muove nei tre assi, quindi tutti gli eventi fisici e logici associati devono essere valutati (nonché le condizioni ambientali e i luoghi di interesse). Alcuni di questi elementi, che possono sembrare superflui in altre indagini, possono essere molto utili per il successo dell'indagine.

Dati Drone Come in tutti gli scenari in cui è interessata l'evidenza digitale, anche nel sistema UAS l'intero ecosistema drone dovrebbe essere valutato, così come i registri storici che possono essere recuperati da Ground Station, SD Memoria e Cloud.

Tipi di Dati Vi sono diversi tipi di dati che possono essere molto utili nelle indagini e scenari che coinvolgono UAS:

Contenuto Audio Visivo Una delle principali fonti di informazioni digitali in un UAS sono foto e/ o immagini video e, in alcuni casi, anche immagini audio memorizzate sulla memoria SD, installate negli UAS o inviate a dispositivi esterni e/ o cloud. Pertanto sarà necessario fare riferimento alle informazioni inviate da droni commerciali al cloud relativo del produttore o fornitore di servizi.

Altri contenuti creati dal carico utile In alcuni UAS i payload possono mantenere i dati di utilizzo o il log delle operazioni del payload stesso nella loro memoria.

Registri di uso automatizzati Gli UAS possono essere programmati per effettuare voli in orari specifici, con rotte precise; questi orari possono anche essere utilizzati più volte o possono essere salvati per un uso successivo. Le informazioni digitali che vengono spesso salvate dagli UAS sono anche i registri delle operazioni che possono fornire una grande quantità di informazioni, anche per i produttori che possono utilizzarli per migliorare/aggiornare il firmware UAS che può anche essere trasmesso al drone produttore di cloud. Tali informazioni sono spesso sconosciute all'utente finale e, purtroppo, anche agli investigatori. I dati del registro operativo generalmente contengono anche i dati relativi al consumo della batteria e alla carica residua, i dati GPS, i dati della missione, l'altitudine, la direzione, la velocità e tutte le informazioni tecniche utili al fabbricante per identificare eventuali malfunzionamenti.

DRONE ECOSYSTEM FORENSICS ACCESSO A DIVERSI SUPPORTI DI MEMORIZZAZIONE

DATI Come precedentemente descritto, ci sono molte fonti di prova che un Drone Ecosystem può offrire ad un investigatore. Negli UAS, le tracce digitali sono ricche di informazioni che possono portare gli investigatori a valutare correttamente l'attività svolta da un UAS. La peculiarità del sistema, come nella mobile health care forensics, presenta una certa complessità riguardo ai dati 'nascosti' all'intero dell'ecosistema ed è per questo motivo che nelle pagine seguenti verranno riportate una serie di linee guida essenziali per consentire agli investigatori di salvaguardare le tracce digitali utili per indagini, nella misura più ampia possibile. Per identificare correttamente tutte le fonti di dati che possono influenzare un ecosistema drone, va sottolineato che tutti gli ecosistemi sono diversi. È essenziale disporre di nozioni di "Digital Profiling" e, quindi, di un ampio profilo tecnico, in modo che possa essere effettuata la valutazione più puntuale possibile. Controllare il movimento delle persone e limitare il numero di persone che accedono alla scena del crimine è essenziale per mantenere l'integrità della scena, salvaguardare le prove e ridurre al minimo la contaminazione.

DRONE FORENSE E LE INDAGINI

In primo luogo, la sicurezza dell'operatore e il ritrovamento

I droni coinvolti in incidenti possono essere una grande fonte di informazioni digitali ma anche di rischi per gli operatori.

I droni possono essere eliminati in remoto. Rimuovere la batteria immediatamente.

Il drone ha un carico. Attenzione, può essere pericoloso.

Scienze Criminologiche e Forensi. Il drone può contenere impronte digitali, biologici, DNA, ecc. che possono aiutare gli investigatori nelle indagini.

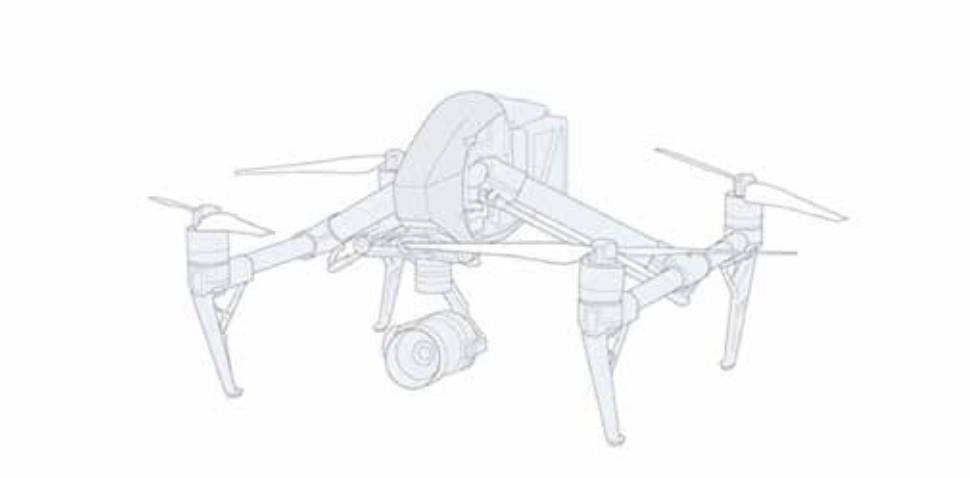
La batteria utilizzata per alimentare il drone può essere pericolosa se danneggiata. Manipolare con cura.

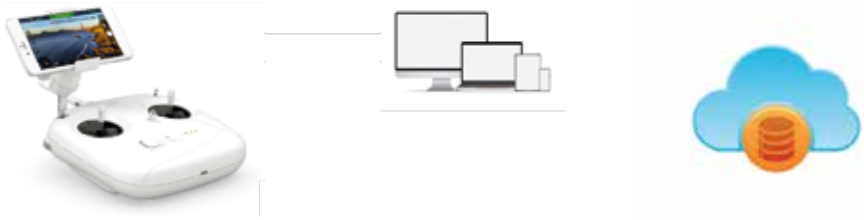
La batteria è un serbatoio di energia, ricordarsi di misurare la carica residua al fine di identificare la gamma del drone.

Non dimenticare di provare a localizzare il pilota. Per misurare la carica residua della batteria, il peso del drone e la motorizza- zione. È possibile calcolare un raggio operativo del drone, che rappresenta una traccia importante in merito all'ambito delle ricerche sull'operatore

DOVE SI POSSONO TROVARE I DATI DEI DRONI

DRONE



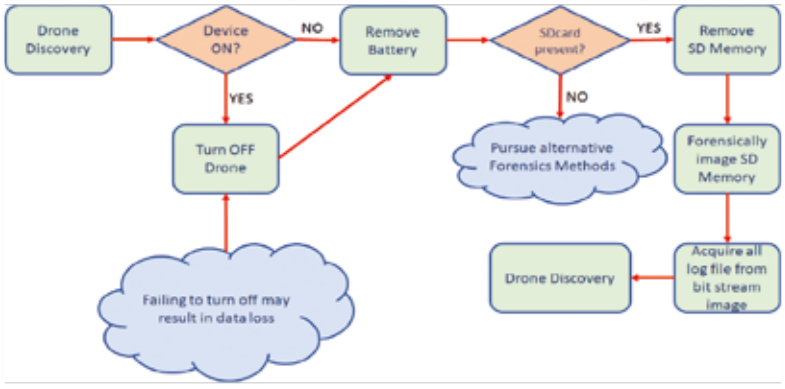


APP MOBILE
DESKTOP
REMOTE CONTROL CLOUD

Schema per la valutazione e il primo intervento su un UAS oggetto di indagine: Non dimenticare di provare a localizzare il pilota. Per misurare la carica residua della batteria, il peso del drone e la motorizzazione. È possibile calcolare un raggio operativo del drone, che rappresenta una traccia importante in merito all'ambito delle ricerche sull'operatore.

DRONI COMMERCIALI
La maggior parte dei sistemi commerciali di drone salvano i dati di volo e le immagini in genere all'interno di:

- **DRONE:** I dati contenuti nei droni commerciali sono generalmente quelli salvati in memoria SD rimovibile e, in alcuni casi, anche nella memoria interna degli UAS. Tutti i droni commerciali e open source, dotati di GPS, gestiscono la funzione "Fail Safe" e i dati di partenza "Home" vengono salvati nella memoria interna in modo da garantire che il drone possa rientrare alla base, anche nel caso in cui la memoria SD non sia in grado di farlo. Il drone deve essere acquisito tramite software forense come XRY da MSAB, UFED e OXYGEN FORENSICS.



- **MEMORIA SD**: è la memoria rimovibile che è generalmente installata nel drone o nel controllo di volo (Flight Control Unit). Le operazioni di acquisizione sono le medesime adottate in Computer Forensics. Si raccomanda di utilizzare i sistemi software XRY di MSAB, UFED o OXYGEN FORENSICS per l'analisi.

- **APP:** sono le varie applicazioni che possono essere installate in smartphone in modo che i droni possano essere gestiti e possano ricevere immagini e registri di telemetria. Le applicazioni installate in dispositivi mobili devono essere acquisite attraverso software forensi come XRY da MSAB, UFED o OXYGEN FORENSICS.

- **CLOUD:** alcuni droni commerciali inviano registri di volo e immagini al Cloud del produttore e/o Cloud che gestisce sistemi di analisi video. I Clouds sono accessibili per l'acquisizione forense tramite login e password o tramite un token che può essere ottenuto dall'analisi mobile. Le nuvole possono essere acquisite tramite il software forense OXYGEN FORENSICS.

- **COMANDO REMOTO:** Il radiocomando o RPS può memorizzare una serie di informazioni utili per gli investigatori, come il numero di serie o l'indirizzo mac del drone pilotato.

DRONI OPEN SOURCE

La maggior parte dei droni open source memorizzano i dati di volo generalmente in: **DRONE:** i dati contenuti nei droni con tecnologia Open Source sono generalmente salvati in memoria SD rimovibile e nella memoria interna del controllo di volo. Tutti i droni commerciali e open source, dotati di GPS, gestiscono la funzione "Fail Safe" e i dati di avvio "Home" vengono salvati nella memoria interna in modo da garantire la "Return home", così come nel caso in cui la memoria SD non vi riesca. Il drone dovrebbe essere acquisito tramite software forense come XRY da MSAB, UFED e OXYGEN FORENSICS.

- **MEMORIA SD**: è la memoria rimovibile che è generalmente installata nel drone o nel controllo di volo (Flight Control Unit). Le operazioni di acquisizione sono le medesime adottate in Computer Forensics. Si raccomanda di utilizzare sistemi software Open Source utilizzati per la gestione del controllo di volo relativo o software forense, come MSRY da MSAB, UFED e OXYGEN FORENSICS per analisi.

- **APP:** sono le varie applicazioni che possono essere installate in smartphone in modo che i droni possono essere gestiti e possono ricevere immagini e registri di telemetria. Apps generalmente salvare i log in database sqlite che possono essere letti e analizzati con diversi sistemi software di analisi. Le applicazioni installate in dispositivi mobili devono essere acquisite attraverso software forensi come XRY da MSAB, UFED e OXYGEN FORENSICS.

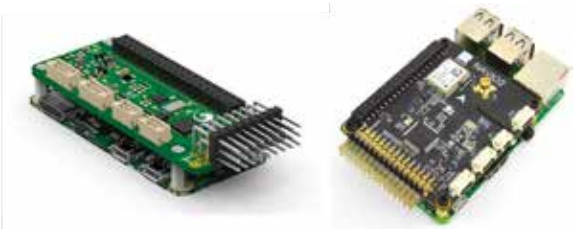
- **MEMORIA SD:** è la memoria rimovibile che è generalmente installata nel drone o nel controllo di volo (Flight Control Unit). Le operazioni di acquisizione sono le stesse adottate in Computer Forensics. Si raccomanda di utilizzare sistemi software Open Source utilizzati per la gestione del controllo di volo relativo o software forense, come MSRY da MSAB, UFED e OXYGEN FORENSICS per analisi.

- **APP:** sono le varie applicazioni che possono essere installate in smartphone in modo che i droni possono essere gestiti e possono ricevere immagini e registri di telemetria. Apps generalmente salvare i log in database sqlite che possono essere letti e analizzati con diversi sistemi software di analisi. Le applicazioni installate in dispositivi mobili devono essere acquisite attraverso software forensi come XRY da MSAB, UFED o OXYGEN FORENSICS.

- **DESKTOP – STAZIONE DI TERRA:** come descritto in precedenza, i sistemi Open Source sono gestiti e configurati utilizzando un software che può essere installato su personal computer. Molti software di gestione sono multi-piattaforma (Windows, OSX e Linux). Le operazioni di acquisizione sono le medesime adottate in Computer Forensics, mentre per l'analisi lo stesso software può essere utilizzato per gestire sistemi UAS.

- **COMANDO REMOTO:** Il radiocomando o RPS può memorizzare una serie di informazioni utili per gli investigatori, come il numero di serie o l'indirizzo mac del drone pilotato. Nei radiocomandi con software o tecnologia Open Source, possono essere salvate anche configurazioni o script per la gestione automatica degli UAS.

I seguenti sono alcuni dei comandi di volo più utilizzati:



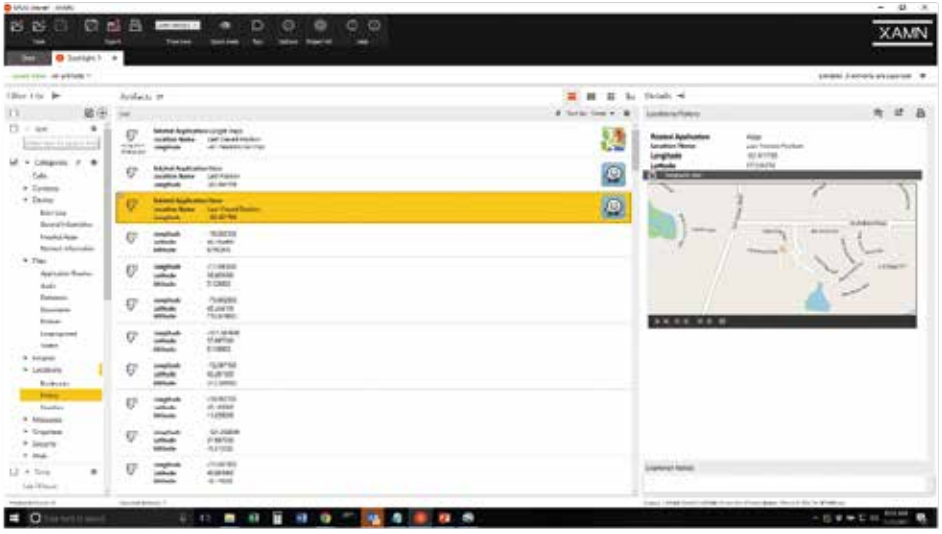
I comandi di volo di seguito sono basati su Raspberry e dovrebbero essere considerati e gestiti come se si trattasse di computer, con l'approccio descritto nel capitolo riguardante la Computer Forensics.

Il Pixhawk Cube Flight Control, illustrato di seguito, può contenere un Intel Edison "Companion Computer"; questo tipo di tecnologia di gestione drone dovrebbe analogamente essere gestito come fosse un computer (informatica forense).

Edison è il nuovo potente modulo Intel®.
Di dimensioni abbastanza ridotte per adattarsi a dispositivi indossabili, abbastanza versatile per gestire applicazioni IoT e sufficientemente potente per controllare le piattaforme robotiche.

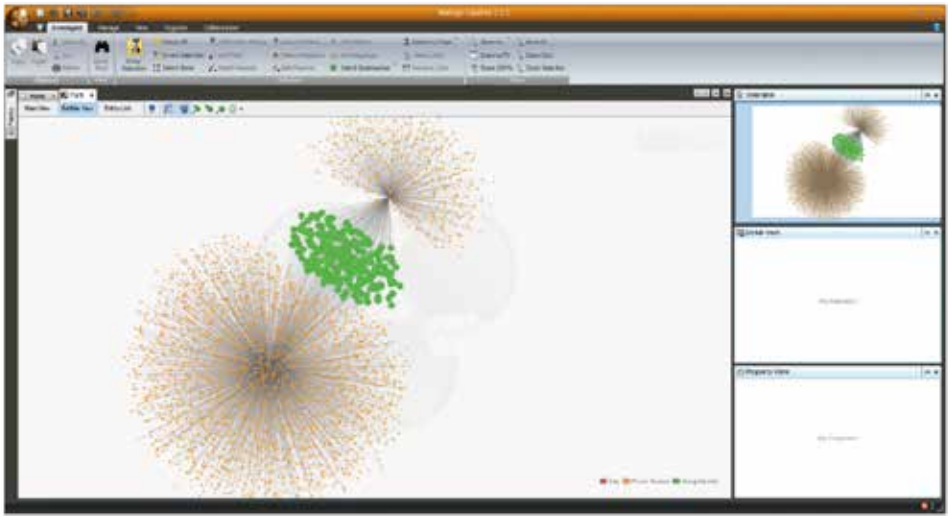
Edison include una serie di funzioni, tra cui WiFi (802.11a / b / g / n), Bluetooth (4.0 e 2.1 EDR), UART, I2C, SPI, USB ans 40 GPIO.
È pilotato da un processore a 32 bit Intel® Atom™ con clock a 500 MHz, supportato da 1 GB di RAM LPDDR3 e 4 GB di memoria flash eMMC.
Le applicazioni che possono supportare queste tecnologie possono r
iguardare "Terra, Acqua e Aria" Errore il controllo di volo, modello PIXHAWK, è acceso

L'"UAS Ecosystem" e Drone Forensics includono tutti i Digital Forensics descritti nei capitoli precedenti. L'ecosistema drone si apre a scenari che riguardano le indagini mobili con l'acquisizione e l'analisi di telefono cellulare annunci poiché, soprattutto nei droni commerciali, vengono utilizzati sistemi di comunicazione mobile come negli smartphone e nei tablet.



Un approccio corretto in uno scenario in cui i sistemi UAS sono utilizzati per il contrabbando di farmaci, telefoni cellulari o altro materiale illegale nelle prigioni, è un approccio fondamentale al profilo di indagine digitale.

Nell'esempio riportato di seguito, viene esaminato un modello di DJI Spark Drone, analizzato con il software XRY Forensic del MSAB, che ha effettuato diversi voli in aree lontane tra loro.
Dai dati acquisiti con XRY è stato possibile analizzare tutte le rotte effettuate dal sistema UAS e, soprattutto, è stato possibile acquisire tutte le posizioni di partenza (Take Off) e di arrivo (Landing) coincidenti tra loro. Acquisendo e analizzando il traffico della rete cellulare, gli investigatori sono stati in grado di ridurre il numero di possibili utenti del drone che si trovavano in vari luoghi al momento di interesse investigativo. Utilizzando un software chiamato Maltego Case File (gratuito e commerciale) è stato possibile evidenziare tutti gli utenti di telefoni cellulari compatibili con le aree di interesse.



Finito di stampare nel mese di dicembre 2020 in Italia, per conto di
agenzia NFC di Amedeo Bartolini & C. sas

www.agenzianfc.com - www.nfcedizioni.com

MANUALE FORENSE PER LA POLIZIA PENITENZIARIA

Il manuale è diviso in tre parti. La prima parte analizza i modelli di osservazione penitenziaria in diversi paesi. Attenzione particolare è stata riservata al modello italiano, in cui l'osservazione penitenziaria sul fenomeno della radicalizzazione si coniuga con il pre-esistente regolamento penitenziario riformato tra gli anni '70 e '80. La seconda parte si pone l'obiettivo di costruire un modello standard di analisi preventiva, partendo dal presupposto che la prevenzione della radicalizzazione, anche se quest'ultima non costituisce reato, richiede una solida base giuridica e procedurale, in linea con la più recente giurisprudenza della Corte dei Diritti dell'Uomo e con la dottrina emergente in Europa sulla differenziazione dei modelli di prevenzione giuridica, sociale e amministrativa. Nell'ultima parte il lavoro definisce linee guida sperimentali di una nuova digital forensics penitenziaria, partendo da esperienze acquisite attraverso casi specifici e il lavoro di simulazione tecnologica effettuato all'interno del laboratorio ELPeF.

9 788867 262755

NFC edizioni

Euro 18,00