LUISS

Corso di laurea in Giurisprudenza

Cattedra di Diritto Internazionale

La cooperazione giudiziaria internazionale in materia di reati informatici: il ruolo delle operazioni digitali sotto copertura

Prof. Roberto Virzo

RELATORE

Prof. Fulvio Maria Palombino

CORRELATORE

Chiara Guerrini
Matr. 168103

CANDIDATO

Anno Accademico 2024/2025

Impara nella vita a non finire mai

INDICE

INTRODUZIONE

Il presente elaborato si propone di analizzare l'attuale quadro della cooperazione giudiziaria internazionale in materia di reati informatici e il ruolo svolto dallo strumento investigativo delle operazioni sotto copertura in ambito digitale. I cosiddetti "*cybercrimes*" sono fattispecie di reato comparse con l'avvento delle tecnologie informatiche che, poiché caratterizzati da ampia diffusività e dalla natura prevalentemente transnazionale, hanno ridisegnato e modificato profondamente non solo il sistema penale nazionale degli ordinamenti interni ma anche il complesso di sistemi e meccanismi di cooperazione tra Stati in materia penale. In particolare, la natura prettamente extraterritoriale dei crimini informatici rende evidente la necessità di una cooperazione particolarmente intensa e uniforme al fine di contrastare efficacemente tale fenomeno. La cooperazione assume un ruolo centrale soprattutto in ambito investigativo per la crescente difficoltà di individuare gli autori dei reati e di ricostruirne le modalità operative. Tra gli strumenti ritenuti più efficaci, si collocano le operazioni sotto copertura nel cyberspazio, le quali, tuttavia, essendo qualificate come strumento atipico, implicano numerose criticità nel loro impiego, ulteriormente accentuate dal contesto digitale.

Il primo capitolo intende esaminare l'evoluzione della cooperazione giudiziaria internazionale in materia penale, che si fonda sull'esigenza comune di perseguire reati che, presentando elementi di transnazionalità, esigono un efficace coordinamento interstatuale. La cooperazione in materia penale, inizialmente sviluppatasi con riferimento al meccanismo dell'estradizione, ha subìto ad oggi un progressivo avanzamento verso le tecniche odierne di mutua assistenza giudiziaria e di scambio di informazioni investigative tra le forze di polizia.

Successivamente, verranno analizzate le caratteristiche peculiari del crimine informatico, le sue definizioni, e i soggetti coinvolti che consentono di comprendere le specificità della fattispecie di reato nel contesto digitale.

Sul piano internazionale, la Convenzione di Budapest sulla criminalità informatica del 2001 rappresenta lo strumento internazionale multilaterale più compiuto in materia. Le misure procedurali e gli strumenti di cooperazione internazionale in essa previsti assumono un particolare rilievo perché concepiti

specificamente per il *cybercrime* e, di conseguenza, finalizzati a garantire forme di mutua assistenza tempestive e celeri.

La mutua assistenza giudiziaria viene in rilievo in numerose Convenzioni internazionali e anche in ambito europeo, dove si assiste ad un'evoluzione progressiva che ha portato a un più intenso coordinamento investigativo. In materia di reati informatici, l'assetto cooperativo così delineato si completa con la predisposizione di un sistema organico concernente la cybersicurezza nazionale ed europea, che, grazie a strutture accentrate e a un quadro normativo uniforme, consente di delineare un'idonea protezione dell'ecosistema digitale statale e unionale, fondamentale per contrastare il fenomeno del *cybercrime*.

Nel secondo capitolo si analizzano gli strumenti investigativi delle operazioni sotto copertura, con riguardo alla loro natura e alla loro evoluzione, inizialmente focalizzandosi sul piano interno per poi approfondire il loro contributo nel quadro internazionale. La normativa italiana prevedeva una disciplina iniziale particolarmente frammentata, riunita parzialmente con l'introduzione dell'articolo 9 della legge 146 del 2006. In tema di infiltrazioni digitali sotto copertura, di particolare rilievo è l'introduzione della legge 137/2023 che prevede una serie di ampi poteri dell'agente nel cyberspazio, permessi dall'adozione di una scriminante complessiva per varie fattispecie di reato.

Al fine di contrastare efficacemente il *cybercrime*, il coordinamento deve partire dal livello nazionale, coinvolgendo in maniera integrata l'insieme degli attori istituzionali competenti. In tal senso, sono state svolte tre interviste con il Procuratore Nazionale Antimafia e Antiterrorismo Giovanni Melillo, con il Direttore Generale della Agenzia per la Cybersicurezza Nazionale il Prefetto Bruno Frattasi e con il Direttore del servizio di Polizia Postale e per la Sicurezza Cibernetica Ivano Gabrielli, che hanno evidenziato l'importanza del coordinamento tra dimensione istituzionale e tecnica, da un lato, e ambito giudiziario e investigativo, dall'altro.

Numerose sono poi le fonti internazionali in materia di *special investigation techniques*. Sebbene non tutte prevedono espressamente le operazioni sotto copertura, il loro richiamo contribuisce a riconoscerne l'utilità e l'efficacia quale strumento imprescindibile per indagare i crimini transnazionali.

In ambito europeo, la Direttiva 2014/41/UE prevede l'Ordine Europeo d'Indagine un meccanismo che garantisce il reciproco riconoscimento e l'esecuzione celere delle richieste di indagine tra degli Stati Membri dell'Unione Europea, anche con riferimento alle operazioni sotto copertura.

Sul piano operativo, meritano una speciale menzione le iniziative predisposte da Interpol, Europol ed Eurojust idonee sia a prestare supporto a Paesi che necessitano di una corretta implementazione di politiche di contrasto al *cybercrime*, sia a garantire il coordinamento operativo con attori pubblici e privati e a potenziare i meccanismi di contrasto. Infine, vengono prese in esame alcune tecniche investigative generalmente utilizzate ai fini dell'attività digitale sotto copertura e vengono analizzate due operazioni significative che hanno consentito, tramite la cooperazione di Stati, autorità operative e agenzie internazionali, di smantellare due dei principali *marketplace* illegali nel *Dark Web*, Alphabay e Hansa Market.

Il terzo capitolo pone l'attenzione sugli aspetti controversi delle operazioni sotto copertura che risultano più evidenti nel terreno digitale. Le principali criticità attengono alla definizione delle finalità delle operazioni e al loro inquadramento come mezzo di ricerca della prova, nonché al regime di utilizzabilità delle risultanze probatorie derivanti da tale peculiare attività investigativa. La questione più delicata e maggiormente discussa concerne il difficile inquadramento dell'operazione sotto copertura come attività lecita, evitando che la stessa si tramuti in un'ipotesi di provocazione al reato. In tal senso, viene presa in esame un'ampia giurisprudenza della Corte di Strasburgo che, partendo dalla necessità di garantire il giusto processo ai sensi dell'art.6 CEDU, vuole dettare i criteri distintivi tra le condotte dell'agente infiltrato scriminate e quelle inerenti *l'entrapment*, vietate.

Vengono analizzati, inoltre, gli ostacoli alla cooperazione in materia di operazioni sotto copertura. Si pone l'attenzione sulle diversità normative tra ordinamenti nazionali soprattutto in materia di provocazione al reato, passando poi ad analizzare i limiti rinvenuti negli strumenti di cooperazione adoperati ai fini investigativi, sia con riferimento ai meccanismi tradizionali, sia ponendo l'attenzione sugli aspetti critici di forme innovative quali le JITs e la rete 24/7. Inoltre viene evidenziato come gli strumenti di *law enforcement* di contrasto al crimine informatico incidano particolarmente sul diritto alla privacy e sulla protezione dei dati personali.

In conclusione, la particolare invasività del crimine informatico richiede l'implementazione di forme di rafforzamento della cybersicurezza italiana e, soprattutto, europea per la quale si auspica la definizione di una difesa cibernetica comune agli Stati Membri, in modo tale da consentire all'Unione Europea di potersi inserire in un quadro di super potenze cibernetiche.

In tale contesto, è necessario implementare, in ambito investigativo e tecnico, strumenti innovativi di contrasto al *cybercrime*, anche attraverso l'impiego delle nuove tecnologie, tra le quali l'intelligenza artificiale riveste un ruolo centrale.

In un'ottica di maggiore cooperazione, la Convenzione delle Nazioni Unite contro il *cybercrime* assume un rilievo determinante. La stessa è finalizzata a introdurre normative comuni per il contrasto al crimine informatico che siano idonee ad un'applicazione globale. Tale finalità, per lungo tempo prospettata nel quadro internazionale, viene, tuttavia, indebolita dagli aspetti controversi emersi durante i lavori preparatori alla Convenzione, in particolare con riferimento alla difficoltà di costruire un adeguato bilanciamento tra le esigenze di prevenzione e repressione del fenomeno e le garanzie dei diritti fondamentali dell'individuo.

Capitolo I.

Quadro giuridico della cooperazione giudiziaria internazionale in materia di criminalità informatica

SOMMARIO: 1. Profili generali della cooperazione giudiziaria internazionale penale 1.1 Definizione giuridica e finalità della cooperazione 2. Reati informatici e cibernetici: una nuova sfida per il diritto penale 3. Diritto internazionale e diritto comunitario: fonti normative 3.1 Convenzione del Consiglio d'Europa sulla criminalità informatica 3.2 Le Convenzioni delle Nazioni Unite e altri strumenti multilaterali 3.3 L'evoluzione della cooperazione nel diritto dell'Unione Europea 3.3.1 La *cybersecurity* nel diritto dell'Unione Europea 4. Quadro normativo italiano 4.1 Disciplina interna in materia di criminalità informatica 4.2 L'informatica forense e *digital evidence* 4.3 Coordinamento investigativo nazionale

1. Profili generali della cooperazione giudiziaria internazionale penale

La cooperazione giudiziaria internazionale in materia penale costituisce una delle modalità di repressione di reati la cui natura, dimensione e modalità di attuazione travalicano i confini nazionali. Ed è proprio in un contesto attuale di globalizzazione, caratterizzata da una sempre più comune interconnessione economica, sociale e soprattutto tecnologica che si insinua la possibilità che condotte criminali commesse in uno stato determinino conseguenza in altri.

Questo accresce la necessità di un più frequente coordinamento intenso e strutturato tra Stati, organizzazioni internazionali e sovranazionali. L'azione repressiva non può essere più isolata e interna ma necessità di modalità tipiche di assistenza transfrontaliera.

1.1 Definizione giuridica e finalità della cooperazione

Bassiouni definisce la cooperazione interstatuale in materia penale come "*modalità con cui gli Stati danno esecuzione, nelle loro relazioni bilaterali, alle prescrizioni delle rispettive legislazioni penali*"[1] affermando che questa si riferisce

[1] Bassiouni, M.C. (2005). *La cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo.* Giuffrè pp.33

principalmente ai reati interni e differenziandola rispetto al "*sistema di esecuzione indiretta*" che indica invece l'attuazione del diritto penale internazionale attuato attraverso gli Stati. Pur differenziandoli, l'autore asserisce tuttavia che entrambi gli istituti sono accomunanti dalle medesime modalità di attuazione della cooperazione: l'estradizione, la mutua assistenza giudiziaria, l'esecuzione di sentenze penali straniere, il riconoscimento di giudizi penali stranieri, il trasferimento di procedimenti penali, il sequestro e la confisca dei beni derivanti dalle attività criminose, lo scambio di informazioni di intelligence e di forze di polizia e la creazione di "spazi giudiziari" regionali e sub regionali[2].

La cooperazione in materia penale è tradizionalmente caratterizzata dalla dicotomia tra esigenze contrapposte: da un lato la tutela della sovranità statale e dall'altro l'interesse comune degli Stati nel contrasto della criminalità, interesse che richiede fiducia reciproca tra i diversi sistemi legali.

Il principio di eguaglianza sovrana, trova esplicito riconoscimento nell'art.2(1) della Carta delle Nazioni Unite e dovrebbe significare che gli Stati sono tutti uguali nella loro sovranità e nella loro reciproca non subordinazione[3]. Di conseguenza, la cooperazione avviene a livello orizzontale ed è rimessa alla volontà degli Stati, i quali possono subordinare l'assistenza a requisiti di reciprocità o, in alternativa, rifiutarla al ricorrere di determinate circostanze.

In tal senso è di fondamentale importanza il principio di reciprocità, secondo il quale lo Stato richiesto presta assistenza allo Stato richiedente assumendo l'impegno di ricevere, in casi analoghi, un livello equivalente di cooperazione. Tale principio, spesso incorporato in trattati bilaterali e multilaterali, è considerato prevalente negli ordinamenti di *civil law*, mentre nei sistemi di *common law* non assume carattere obbligatorio, pur costituendo sovente una condizione preliminare per la concessione dell'estradizione. A titolo esemplificativo, la Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale menziona espressamente la reciprocità

[2] Ibidem

[3] cfr. Koskenniemi, M., & Kari, V. (2020). *Sovereign Equality*. In J. E. Viñuales (Ed.), *The UN Friendly Relations Declaration at 50: An Assessment of the Fundamental Principles of International Law*. Cambridge: Cambridge University Press. p. 166

all'art. 18 par.1[4] quale fondamento dell'assistenza, imponendone il rispetto in assenza di uno specifico trattato tra gli Stati interessati[5].

Tuttavia, nel passato, non sempre il metodo classico basato su reciprocità, canali diplomatici e formalismi procedurali si è dimostrato efficace. Spesso la diversità tra legislazioni nazionali, le condizioni restrittive da parte dello Stato richiesto e la lentezza delle procedure, non consentivano allo Stato richiedente di produrre risultati utili e efficaci. Per ovviare a tali criticità, si è progressivamente ammesso che lo Stato richiedente potesse indicare requisiti procedurali specifici e/o partecipare all'esecuzione delle misure nello Stato richiesto[6].

Tale evoluzione rispecchia anche quella avvenuta in relazione al principio di *locus regit actum* : se in origine l'esecuzione delle richieste di assistenza era regolata esclusivamente dalla legge dello Stato richiesto (*lex loci*), oggi si tendono ad applicare, come regola, le formalità e le procedure indicate dallo Stato richiedente (*lex fori*), purché compatibili con i principi fondamentali dell'ordinamento dello Stato richiesto secondo il principio del *forum regit actum*[7]. Parallelamente, si è registrato un cambiamento dei soggetti tenuti a effettuare le misure di cooperazione: dai tradizionali canali diplomatici, ritenuti spesso inefficaci, si è passati alle autorità centrali, usualmente collocate presso i Ministeri di giustizia o dell'interno, e più recentemente a forme di comunicazione diretta tra autorità giudiziarie.

In questo quadro l'Unione Europea ha compiuto un passo ulteriore introducendo il principio del "*mutuo riconoscimento*" delle decisioni giudiziarie, divenuto la pietra angolare della cooperazione legale tra gli Stati membri[8]. Tale principio consente di ottenere il riconoscimento e l'esecuzione automatica delle decisioni e delle richieste provenienti da un altro Stato membro, riducendo al minimo le formalità.

---

[4] United Nations. (2000). *United Nations Convention against Transnational Organized Crime and the Protocols Thereto*. New York: United Nations. art.18

[5] United Nations Office on Drugs and Crime. (2012). *Manual on mutual legal assistance and extradition.* United Nations. p. 23

[6] Cryer, R., Robinson, D., & Vasiliev, S. (2019). *State Cooperation with Respect to National Proceedings. In an Introduction to International Criminal Law and Procedure* chapter, Cambridge: Cambridge University Press. pp. 71–90

[7] Karsai, K. (2019). *Locus/forum regit actum - A dual principle in transnational criminal matters.* Hungarian Journal of Legal Studies, 60(2) pp. 155–172.

[8] European Union. (2012). *Treaty on the Functioning of the European Union*. *Official Journal of the European Union*, C 326. art.81,82

Strettamente connesso al principio di reciprocità, nonché corollario del principio di legalità per cui *nullum crimen sine lege,* è il principio di doppia incriminazione, secondo cui la condotta oggetto della domanda di cooperazione deve costituire reato sia per lo Stato richiedente sia per lo Stato richiesto. Tale assunto, tuttavia, può costituire un ostacolo significativo ad un'efficace cooperazione, soprattutto quando viene applicato sulla base di criteri interpretativi differenti. Alcuni Stati richiedono l'identità della qualificazione giuridica o che i reati siano sufficientemente gravi da consentire l'estradizione; altri ritengono che le giurisdizioni penali applicabili debbano coincidere, ovvero collegano la verifica della doppia incriminazione al momento della commissione del fatto e non al momento in cui viene inoltrata la richiesta di cooperazione. Le tendenze più recenti mirano a ridurre la portata di tale requisito: emblematico è il mandato d'arresto europeo che esclude la necessità della doppia incriminazione per una classifica di reati tassativamente determinati, purché puniti, nello Stato membro emittente, con una pena detentiva di almeno tre anni[9].

Altro principio essenziale è quello di specialità, secondo cui lo Stato richiedente può perseguire la persona consegnata solo in relazione ai reati per i quali l'estradizione è stata concessa. In caso contrario, verrebbero aggirati i presupposti fondamentali relativi all'estradizione e alla doppia incriminazione. Tale regola può comunque venire meno nel caso in cui lo Stato richiesto presti il suo consenso o nel caso in cui strumenti convenzionali, come quelli previsti nell'Unione Europea e nel Consiglio d'Europa, prevedano presunzioni di consenso in presenza di determinate condizioni.

Infine, assume rilievo il principio del *ne bis in idem*, tradizionalmente limitato allo Stato richiesto, in base al quale veniva negata l'estradizione qualora quest'ultimo avesse già emesso una sentenza definitiva nei confronti dell'imputato. L'evoluzione recente, soprattutto in Europa, tende ad ampliare la portata del principio sulla base del mutuo riconoscimento delle decisioni giudiziarie. Infatti, nell'ambito del mandato d'arresto europeo, gli Stati membri possono rifiutare l'esecuzione dello stesso qualora

[9] Council of the European Union. (2002). *Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States*. Official Journal of the European Union, L 190, 1–20.

il soggetto sia stato già giudicato in via definitiva da uno Stato terzo estraneo alla richiesta di cooperazione. Nel diritto internazionale, tuttavia, non esiste una regola generale che impedisca l'estradizione di una persona sulla base di una sentenza pronunciata da uno Stato terzo[10].

1.2 Origine ed evoluzione

Passaggio imprescindibile nell'evoluzione storica della cooperazione giudiziaria, è rappresentato dal principio fondante "*aut dedere aut iudicare*" enunciato per la prima volta da Hugo Grotius nel 1624. Enunciato inizialmente da Grotius come "*aut dedere aut punire*"[11], è stato successivamente rielaborato nel 1973 sostituendo il termine "*punire*" con "*iudicare*" per sottolineare la necessità che l'accertamento giurisdizionale della colpevolezza sia preliminare rispetto alla punibilità. La massima groziana si inserisce nel sistema di esecuzione indiretta del diritto penale internazionale e rappresenta oggi una pietra miliare anche del sistema di cooperazione interstatale. L'idea di fondo è che gli Stati condividano un interesse comune nel reprimere i crimini più gravi, evitando che la mancata collaborazione generi impunità.

Nel XVII secolo il principio trovò attuazione esclusivamente per l'estradizione, principale forma di cooperazione fino al XX secolo, estendendosi successivamente a tutti gli strumenti di cooperazione ad oggi esistenti. La sua *ratio* si fonda sull'idea che lo Stato richiedente, attraverso l'estradizione, persegua l'obiettivo di assicurare l'effettività della propria giurisdizione penale, mentre lo Stato richiesto, pur non avendo sempre un interesse diretto nel procedimento, contribuisce a prevenire l'impunità sostenendo così l'efficacia complessiva del sistema penale internazionale.

Per i crimini internazionali, invece, vige un più solido fondamento di cooperazione fondato sul concetto di *civitas maxima*[12], secondo cui il dovere morale

[10] Cryer, R., Robinson, D., & Vasiliev, S. *An Introduction to International Criminal Law and Procedure*. cit., pp. 89–112
[11] Grotius, H. (1625). *De jure belli ac pacis libri tres*. Parisiis: Nicolaum Buon.
[12] Onuf, N. G. (1994). *Civitas Maxima: Wolff, Vattel and the Fate of Republicanism. The American Journal of International Law*, 88(2), pp. 280–303.

e giuridico di estradare o di procedere direttamente si basa su di un interesse comune e reciproco degli Stati a reprimere tali crimini[13].

Accanto all'estradizione un ruolo centrale è svolto dall'assistenza giudiziaria o *mutual legal assistence.* Questa pratica originariamente si configurava come una relazione interstatale di tipo diplomatico, attuata tramite le commissioni rogatorie (*Letters Rogatory*). Le rogatorie consistevano nella trasmissione, fondata sul principio della cortesia (*comity*)[14], di un'istanza unilaterale con la quale l'autorità giudiziaria di uno Stato chiedeva a quella di un altro Stato di compiere una o più azioni specifiche quali ad esempio l'assunzione di una testimonianza o il reperimento di prove materiali.

Tali richieste, trasmesse tramite canali diplomatici, potevano essere autorizzate qualora l'informazione fosse ritenuta rilevante e non reperibile nel territorio in cui si svolgeva il procedimento. Inoltre, lo Stato richiedente doveva dimostrare che quanto domandato fosse compatibile con l'ordinamento e le leggi dello Stato richiesto. Tuttavia, la procedura si rivelò nella prassi particolarmente lenta perché appesantita da formalità che, in contesti investigativi complessi, rischiavano di compromettere l'efficacia delle indagini.

Per ovviare a tali criticità, si svilupparono i Trattati di mutua assistenza giudiziaria (MLATs) che introducono obblighi specifici per la raccolta delle prove in relazione a specifici crimini transnazionali. Diversamente dalle rogatorie, la richiesta di assistenza viene rivolta dall'autorità competente dello Stato richiedente direttamente all'autorità centrale dello Stato richiesto, superando così i tradizionali ma inefficaci canali diplomatici e assicurando maggiore speditezza e certezza nell'assistenza.

La Convenzione europea del 1959 sull'assistenza giudiziaria in materia penale del Consiglio d'Europa, ha svolto un ruolo fondamentale per la modernizzazione di tale cooperazione. La Convenzione ha introdotto l'obbligo di assistenza reciproca, ha definito l'estensione dell'assistenza stabilendo condizioni e limiti e ha infine creato un modello ripreso poi nei trattati bilaterali, regionali e multilaterali[15].

---

[13] Bassiouni, M. C. *La cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo.* cit. pp.34-38
[14] *Ibidem* p.55
[15] Boister, N. (2018). *An introduction to transnational criminal law* (2nd ed.). Oxford University Press pp.311-314

Un'ulteriore forma di cooperazione tra Stati riguarda lo scambio di informazioni tra forze di polizia e servizi di intelligence finalizzato al contrasto dei crimini transnazionali. In tale ambito, la collaborazione si fonda su relazioni fiduciarie, su reti di operatori e contatti informali tra forze di polizia[16] che costituiscono il presupposto dell'azione di organismi dedicati alla cooperazione quali Interpol e Europol. L'Organizzazione Internazionale di Polizia Criminale (Interpol), istituita nel 1923 a Vienna e riorganizzata nella sua forma nel 1956, ha il compito di "*assicurare la più ampia possibile mutua assistenza tra Autorità di polizia criminale, nei limiti delle leggi esistenti nei diversi paesi e dello spirito della Dichiarazione Universale dei diritti umani*"[17].

L'ufficio di Polizia europeo (Europol) è stato istituito nel 1995 con la Convenzione Europol nell'ambito della cooperazione in materia di Polizia e Giustizia riconducibile al III pilastro del Trattato di Maastricht. Oggi la sua disciplina è contemplata all'interno dell'art 88 TFUE nel quale si afferma che l'Europol "*ha il compito di sostenere e potenziare l'azione delle autorità di polizia e degli altri servizi incaricati dell'applicazione della legge degli Stati membri e la reciproca collaborazione nella prevenzione e lotta contro la criminalità grave che interessa due o più Stati membri, il terrorismo e le forme di criminalità che ledono un interesse comune oggetto di una politica dell'Unione*"[18]. Le attività originariamente svolte da Europol rappresentano un'applicazione *ante litteram* delle squadre investigative comuni[19] che si sostanziano nella compartecipazione delle autorità competenti di entrambe i paesi coinvolti ad attività di indagine. La costituzione delle *Joint Investigation Teams* (JITs), prevista nell'ordinamento italiano all'art 729-quinquies c.p.p., ha ricevuto un forte impulso dalla Convenzione di Bruxelles del 2000, le cui disposizione sono state successivamente inserite nella decisione quadro 2002/465/GAI. L'art.1 di quest'ultima stabilisce che la squadra investigativa comune

[16]Hufnagel, S., McCartney, C., Hufnagel, S.; McCartney, C. (2017). *Trust in International Police and Justice Cooperation* (1st ed.). Hart Publishing. p. 3

[17] International Criminal Police Organization – INTERPOL. (1956). *Constitution of the ICPO–INTERPOL*. art.2

[18] European Union. 2012. *Treaty on the Functioning of the European Union*. *Official Journal of the European Union*, C 326. art.88

[19] Paolucci, C. M. (2011). *Cooperazione giudiziaria e di polizia in materia penale*. UTET. pp.468-471

può essere costituita di comune accordo tra due o più Stati membri della UE "*per uno scopo determinato e una durata limitata che può essere prorogata con l'accordo di tutte le parti, per svolgere indagini penali in uno o più degli Stati membri che costituiscono la squadra*"[20].[21]

Su questa direttrice si colloca anche Eurojust, istituita con la decisione 2002/187/GAI. Essa opera su un duplice livello: il miglioramento delle forme tradizionali di cooperazione giudiziaria penale tra autorità giudiziarie e il rafforzamento del coordinamento delle indagini e delle azioni penali tra gli Stati membri. L'agenzia europea Eurojust svolge la sua attività in stretta correlazione con Europol, pur operando la prima in ambito giudiziario e la seconda su quello di polizia[22]. Nel loro insieme le Agenzie dimostrano la progressiva evoluzione della cooperazione nella repressione dei reati attraverso la facilitazione dello scambio di informazioni e la promozione di idonee forme condivise di indagine e raccolta delle prove.

In questa prospettiva, è opportuno precisare che la cooperazione tra Stati basata sul principio "*aut dedere aut iudicare*" è prevista nei trattati, solo con riferimento ai cosiddetti "*crimini transazionali*". A tal riguardo, bisogna effettuare una distinzione tra questi e i crimini internazionali.

Come sostiene il Procuratore Rosario Aitala, i reati transnazionali hanno "*la caratteristica di essere commessi in più Paesi e di comportare effetti geopolitici e di sicurezza per la comunità internazionale nel suo complesso, che ha conseguentemente sviluppato forme rafforzate di cooperazione intergovernativa, investigativa e giudiziale per prevenirli e punirli*"[23]. In relazione a tali reati, il principio "*aut dedere aut iudicare*" trova applicazione poiché la loro natura è più propriamente interstatale e intergovernativa e solo in parte internazionale.

La principale distinzione rispetto ai reati internazionali si fonda sull'assunto che per i crimini transnazionali la punibilità discende dal diritto nazionale, quindi i

[20] European Union. (2002). *Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams.* Official Journal of the European Union, L162, 1–3.
[21] Perduca, A., & Chiavario, M. (2022). *Cooperazione giudiziaria internazionale in materia penale*. Giappichelli. pp. 177-208
[22] Nicastro, G. (2006). *Eurojust* in *Diritto penale europeo e ordinamento italiano*. Giuffrè Editore. pp. 63-98.
[23] Aitala, R., & Severino, P. (2021). *Diritto internazionale penale*. Le Monnier. p.4

trattati non criminalizzano direttamente le azioni o omissioni dei soggetti, ma vincolano gli Stati al perseguimento di obiettivi di politica criminale o all'osservanza di requisiti tecnici. I crimini internazionali sono, invece, per loro stessa natura sovranazionali, rientrano nella maggior parte dei casi nello *ius cogens* e la loro punibilità deriva direttamente dal diritto internazionale[24].

Partendo da questa distinzione, è possibile comprendere come l'evoluzione della cooperazione internazionale abbia portato alla nascita di forme radicalmente nuove di collaborazione. La cooperazione giudiziaria internazionale si è sviluppata inizialmente in senso orizzontale, configurandosi come relazione reciproca tra gli Stati e le loro magistrature. Tale modello si è poi ampliato e arricchito con la nascita di nuove forme di cooperazione che hanno reso i meccanismi di assistenza reciproca tra Stati sempre più forti e coesi.

La prima espressione di questa evoluzione è la giustizia penale internazionale, il cui esempio emblematico è rappresentato dalla Corte penale internazionale (CPI). La Corte si distingue per la composizione multinazionale dei suoi giudici e degli orientamenti giuridici interessati e per la sua giurisdizione complementare rispetto agli ordinamenti nazionali[25]. La *International Crime Court* ha giurisdizione esclusiva in materia di crimini internazionali, ossia per le violazioni più gravi dei principi e valori considerati essenziali per la comunità internazionale, la cui punibilità, come detto in precedenza, discende direttamente dal diritto internazionale. In particolare, tali crimini sono definiti nell'art.5 dello statuto di Roma che include: crimini di guerra, crimini contro l'umanità, genocidio e, in seguito all'emendamento di Kampala, il crimine di aggressione[26].

La seconda forma innovativa di cooperazione giudiziaria è la giustizia penale sovranazionale, sviluppatasi a livello europeo con strumenti volti a tutelare gli interessi finanziari dell'UE. In questo modello, diversamente da quanto accade per la CPI, la giurisdizione penale è affidata alle autorità nazionali mentre le funzioni di pubblico ministero sono esercitate dalla Procura europea[27].

---

[24] *Ibidem* pp.43-44
[25] United Nations. (1998). *Rome Statute of the International Criminal Court*, July 17, 1998, 2187 U.N.T.S. 3 (entered into force July 1, 2002), art. 1.
[26] Ibidem, art. 5, art.8 bis
[27] Perduca, A., & Chiavario, M. *Cooperazione giudiziaria internazionale in materia penale*. cit. pp. 1-32

2. Reati informatici e cibernetici: una nuova sfida per il diritto penale

La rivoluzione informatica e cibernetica ha modificato profondamente l'approccio del diritto penale, non configurandosi come la mera costituzione di un nuovo ramo sostanziale, quanto come una vera e propria ridefinizione della realtà sociale e dei rapporti tra individui.

Tale mutamento implica sicuramente la nascita di nuovi diritti definiti come "*digitali*", la cui garanzia diventa imprescindibile, ma anche l'emersione di nuovi comportamenti illeciti che richiedono un differente approccio normativo.

In questo scenario, un concetto fondamentale è quello di cyberspazio, definito da Lorenzo Picotti, come un'associazione tra cibernetica [28]e nozione di spazio, volta a far intendere *"l'estensione pervasiva del nuovo mondo nel quale, singolarmente e collettivamente, siamo tutti realmente immersi, in quanto ormai permanentemente connessi ed interagenti, se non anche dipendenti".* Ed è proprio in questa nuova realtà che si innestano i nuovi crimini e illeciti, i quali assumono caratteristiche peculiari rispetto ai reati tradizionali.

Negli anni Novanta, con la diffusione di Internet al grande pubblico, si assiste ad un'evoluzione del concetto di reati informatici. Inizialmente, tali reati venivamo definiti come "*computer crimes*", ossia illeciti realizzabili in un sistema *stand alone* caratterizzato dall'utilizzo, per il compimento di tali reati, di dispositivi autonomi ovvero non collegati alla rete Internet. In questo senso la definizione era rivolta principalmente allo strumento tecnologico utilizzato. Ad oggi, invece, possiamo distinguere i reati informatici in due categorie. I reati informatici in senso stretto sono quelli che presentano almeno un elemento essenziale o circostanziale riferito alle Tecnologie dell'informazione e della comunicazione (TIC). Sono invece reati in senso ampio quelli che possono realizzarsi anche mediante le TIC ma tali tecnologie non sono imprescindibili per la consumazione del reato.

Mentre con l'avvento di Internet e del cosiddetto "*cyberspace*" si consolida la nozione di "*cyber crimes*" definiti da taluna dottrina come tutti quei reati "*che si*

[28] Il termine "cibernetica" fu coniato dal matematico Norbert WIENER: *Introduzione alla cibernetica. L'uso umano degli esseri umani* (1953), Torino, 1970 – che lo derivò dalla parola greca kyber, che significa "timoniere o pilota". La cibernetica studia i meccanismi con cui uomini, animali e macchine comunicano con l'ambiente esterno e lo controllano.

commettono o si possono commettere in rete o nel web, o meglio nel cyberspace" in quanto la formulazione legale delle relative fattispecie incriminatrici contiene un elemento essenziale o circostanziale che espressamente richiama la rete (reati cibernetici in senso stretto) ovvero prevede elementi di tipizzazione del fatto di reato che solo implicitamente o in via ermeneutica sono compatibili con la concreta realizzazione nel *cyberspace* (reati cibernetici in senso ampio)"[29] [30].

Per quanto concerne il rapporto tra reati cibernetici e reati informatici possiamo affermare che i primi, in senso stretto, costituiscono una *species* del *genus* dei secondi, nel senso che presuppongono necessariamente l'utilizzo di TIC. Mentre non tutti i reati informatici in senso stretto sono anche cibernetici, poiché quest'ultimi implicano sempre la commissione dell'illecito "*in rete*". Al contrario, quelli informatici possono essere commessi anche senza l'utilizzo di rete Internet, ovvero con sistemi chiusi o *stand-alone*.

A prescindere dalla definizione specifica, i reati cibernetici si distinguono rispetto i reati "*offline*" per varie caratteristiche che rendono evidente la necessità di una regolamentazione specifica. In prima battuta, una differenza sostanziale riguarda l'ampiezza delle vittime e degli autori che possono essere coinvolti. Un esempio significativo è rappresentato dalle frodi online e dal *phishing*, che consiste nell'essere indotti con l'inganno a fornire i propri dati personali: anche se non vengono colpite tutte le persone raggiunte dai messaggi ingannevoli, il numero potenziale di vittime che potrebbero subire questo tipo di attacco è enorme. Altro discrimine è rappresentato dalla facilità di accesso alle risorse informatiche, ormai diffuse globalmente. Ciò offre ai criminali informatici la possibilità di poter colpire soggetti in ogni parte del globo.
La terza differenza è l'anonimato: pur essendo presente anche nei reati tradizionali, nel cyberspazio è più semplice agire senza lasciare tracce. L'uso di strumenti come VPN, Tor o proxy ostacola l'identificazione del soggetto da parte delle forze di polizia, complicando le indagini e la raccolta di prove digitali.
La portabilità e la trasferibilità rappresentano un'ulteriore criticità dei reati cibernetici. I moderni sistemi di archiviazione e le tecnologie *cloud*, caratterizzati dalla presenza

[29] Picotti, L. (2023). Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme. in Cybercrime (2. edizione.). UTET Giuridica. p.79
[30] Ivi. pp. 76- 81

di server fisicamente distribuiti in vari Paesi, hanno reso difficile e complesso rintracciare gli autori dei reati. Ciò significa che la prova può trovarsi anche al di fuori della giurisdizione dello Stato in cui il reato è stato commesso, rendendo complessa l'attività di indagine e necessaria la cooperazione giudiziaria internazionale.

Ciò si collega anche al quinto elemento distintivo: la portata globale dei reati cibernetici. Tale caratteristica rende spesso difficile determinare quale sia la giurisdizione competente, quale legge debba essere applicata e quale autorità giudiziaria debba trattare il caso concreto [31].

Per svolgere una trattazione completa dal punto di vista tecnico-giuridico, occorre analizzare i soggetti del reato informatico sia sul versante delle vittime anche dette "*attaccati*" sia per ciò che riguarda gli attori o anche detti "*attaccanti*". Le vittime possono essere i singoli utenti della rete, le aziende, le autorità nazionali e, in misura limitata, anche le organizzazioni internazionali. I singoli utenti risultano particolarmente esposti a frodi informatiche, furti di identità e *malware* ossia dei software progettati per alterare il normale funzionamento di un dispositivo IT, o per infettare, rubare o distruggere le informazioni in esso contenute. Tali attacchi si verificano spesso a causa di misure di sicurezza mancanti nei sistemi individuali come l'assenza di aggiornamenti o di adeguati sistemi antivirus. Nonostante ciò, le vittime più frequentemente colpite restano le aziende poiché gli attacchi mirano a sottrarre informazioni commerciali da rivendere a terzi o a raccogliere dati per finalità estorsive. Le autorità nazionali, invece sono bersaglio privilegiato nei fenomeni di *cyber-terrorism*, volti a ottenere informazioni riservate allo scopo di intimidire, costringere o comunque esercitare pressioni politiche o sociali nei confronti di un governo o dei suoi cittadini[32] e di *cyber-warfare* consistente in attività informatiche aventi lo scopo di conseguire un vantaggio operativo militare[33].

Gli "*attaccanti*", invece vengono comunemente identificati come *hacker*, ossia soggetti dotati di elevate conoscenze e capacità tecnico-professionali che, individualmente o in gruppo, per motivi economici o politici, compiono

[31] Gillespie, A. (2026). *Cybercrime: key issues and debates* (3. ed.). Routledge, Taylor & Francis Group. pp15-17
[32] Marchetti, R., & Mulas, R. (2017). *La minaccia cibernetica*. In *Cyber security: hacker, terroristi, spie e le nuove minacce del web.* LUISS University Press. pp.66
[33] *Ibidem* p. 60

un'aggressione contro sistemi informatici o telematici. Tuttavia, si ritiene che sia più corretto parlare di *cracker* o *black hat hacker*[34] per riferirsi al soggetto che "*per scopi illeciti e criminosi, si introduce abusivamente nei sistemi automatizzati pubblici o privati, eludendo le misure di sicurezza, per diffondere virus, per esaminare, sabotare, alterare, manipolare e duplicare gli altrui patrimoni informativi o per captare informazioni riservate o per commettere ulteriori azioni illecite*"[35].

Il Consorzio Interuniversitario Nazionale per l'Informatica (CINI), ha elaborato una classificazione delle diverse tipologie di *hacker*, evidenziando come gli attacchi informatici possano provenire da una pluralità di soggetti: dai singoli individui o piccoli gruppi di cyber-criminali, fino a organizzazioni più complesse e strutturate, passando per veri e propri cyber-terroristi, per cyber-criminali riconducibili ad autorità governative o per i cosiddetti cyber-attivisti. Questi attori possono presentare livelli di professionalità molto diversi: si va da soggetti con competenze tecniche limitate, orientati principalmente ad ottenere beni finanziari, fino ad attori altamente qualificati, capaci di colpire in modo efficace individui, aziende o enti governativi[36].

3. Diritto internazionale e diritto comunitario: fonti normative

Nell'era attuale, i quadri giuridici nazionali faticano a regolamentare efficacemente le interazioni che avvengono nel cyberspazio, le quali presentano caratteristiche globali o internazionali. La rapidità dell'evoluzione tecnologia e la sua natura transnazionale rendono questa materia una delle sfide più complesse dell'ordinamento giuridico internazionale.

Tale difficoltà è ulteriormente aggravata dall'eterogeneità degli ordinamenti statali aventi sistemi giuridici, priorità normative e livelli di sviluppo tecnologico profondamente differenti, rendendo arduo individuare standard comuni per disciplinare il cyberspazio. La regolamentazione varia notevolmente tra le diverse regioni riflettendo la diversa percezione delle minacce e le differenti esigenze di sicurezza nazionale. Nell'Unione Europea il quadro regolamentare e normativo risulta

[34] *Ibidem* pp.66-68
[35] Corona, F. (2021). *Reati informatici e investigazioni digitali: diffamazione via web, prove digitali, sex crimes, cyberstalking, cyberbullismo, reati privacy*. Pacini giuridica. p.22
[36] Marchetti, R., & Mulas, R. *La Minaccia cibernetica*. In *Cyber security: hacker, terroristi, spie e le nuove minacce del web.* cit. p. 71

particolarmente armonizzato grazie a strumenti quali il Regolamento generale sulla protezione dei dati (GDPR)[37] e la Direttiva sulla sicurezza delle reti e dei sistemi informativi (Direttiva NIS)[38] che hanno contribuito alla definizione di standard condivisi in materia di sicurezza digitale. In altre aree del mondo, invece, il quadro giuridico è frammentato e disomogeneo, di conseguenza risulta più arduo garantire coerenza nella regolamentazione e nell'applicazione delle norme in materia di *cybercrime.*

Nonostante tali divergenze, il coinvolgimento attivo degli Stati ha dato vita alla Convenzione di Budapest, il primo e principale trattato internazionale vincolante in materia di crimini informatici. Essa rappresenta il tentativo più riuscito di costruire un quadro legislativo globale, fondato sul consenso tra Stati caratterizzati da normative e tradizioni giuridiche differenti. La natura transnazionale del *cybercrime* richiede infatti un'azione concertata e una cooperazione strutturata che coinvolga auspicabilmente il più ampio numero possibile di Paesi[39].

Il cyberspazio non opera quindi in un'area di vuoto normativo; al contrario esiste un ampio consenso generale sulla validità delle norme e dei principi consolidati del diritto internazionale, il quale è pienamente vincolante in relazione all'uso e alla regolamentazione delle tecnologie dell'informazione e delle comunicazioni (ICT) da parte degli Stati , cosi come per la prevenzione e risposta alle azioni dannose realizzata in ambito transnazionale [40].

3.1 Convenzione del Consiglio d'Europa sulla criminalità informatica

[37] European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Official Journal of the European Union, L119, 1–88.

[38] European Union. 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Official Journal of the European Union, L194, 1–30.

[39]Buçaj, E., & Thaqi, A. (2025). *Global Regulation of Cybercrime through International Law and Cyberconventions.* Kriminologie - Das Online-Journal, no. 7. p.163

[40] Oğurlu, E. (2023). *International Law in Cyberspace: An Evaluation of the Tallinn Manuals*. Annales de la Faculté de Droit d'Istanbul, (73). pp. 327-344.

Il primo e più importante Trattato internazionale in materia di reati informatici è la Convenzione sulla criminalità informatica nota anche come Convenzione di Budapest in onore del luogo in cui fu sottoscritta nel 2001[41].

Tuttavia, già prima del 2001 l'evoluzione tecnologica e informatica ha indotto la comunità internazionale a elaborare interventi coordinati in risposta al crescente fenomeno dei reati informatici. Nel 1986 l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) rilasciò un rapporto intitolato "*Computer-Related Crime: Analysis of Legal Policy*"[42] nel quale venivano analizzate le differenti proposte normative degli Stati Membri volte a contrastare la criminalità informatici.

Successivamente, nel 1989 il Consiglio d'Europa emanò una Raccomandazione sulla criminalità informatica in cui tentò di individuare una prima classificazione dei reati informatici, distinguendo una lista minima di condotte da criminalizzare obbligatoriamente e una facoltativa la cui punibilità veniva lasciata alla discrezionalità degli Stati. Con la Raccomandazione del 1995 emerse, inoltre, l'esigenza di imporre ai *Service Providers* l'obbligo di garantire e permettere sia l'intercettazione delle telecomunicazioni sia l'identificazione degli utenti.

Tali iniziative costituirono le premesse per l'avvio dei lavori preparatori volti a redigere una bozza di convenzione internazionale in materia di reati informatici. Il compito fu affidato ad un gruppo di esperti della criminalità nel Cyberspazio. Al termine di quattro anni di lavori preparatori, la Convenzione sul Cybercrime fu adottata il 23 novembre 2001 ed entrò ufficialmente in vigore nel 2004. Una caratteristica peculiare fu rappresentata dalla significativa partecipazione di Paesi extraeuropei, come Stati Uniti, Canada, Giappone e Sud Africa, che inizialmente ottennero lo status di osservatori e, in seguito, ratificarono anch'essi la Convenzione. Questo coinvolgimento costituì fin da subito un elemento distintivo di tale strumento internazionale, confermandone l'impostazione marcatamente globale e la volontà di promuovere una cooperazione che travalica i confini europei.

Ad oggi , la Convenzione continua a rappresentare lo strumento internazionale di riferimento nella lotta al *cybercrime*, in quanto giuridicamente vincolante e di

[41] Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). Budapest: Council of Europe.
[42] Organisation for Economic Cooperation and Development. (1986). *Computer-related crime: Analysis of legal policy.* Paris: OECD.

portata multilaterale[43]. Per quanto concerne il suo ambito di applicazione *ratione materiae*, la Convenzione non si applica esclusivamente ai reati in essa espressamente menzionati, ma si estende a tutti i crimini commessi mediante l'utilizzo di strumenti informatici, nonché a ogni fattispecie in cui sia possibile raccogliere prove in formato elettronico[44].

La Convenzione di Budapest si articola in 4 parti principali e affronta il tema del *cybercrime* sia sul piano sostanziale, sia su quello processuale, sia, soprattutto, sul piano della cooperazione internazionale. Per quanto riguarda la qualificazione delle diverse fattispecie criminose, tutte le disposizioni, ad eccezione di quelle in materia di diritto d'autore, hanno un elemento in comune: il reato deve essere commesso "*senza diritto*" ossia in violazione delle norme interne degli Stati Parte e deve essere realizzato "*intenzionalmente*".

L'articolo 1 fornisce le definizioni fondamentali, ai fini dell'applicazione della Convenzione, di sistema informatico, dati informatici, service provider e di trasmissione di dati[45]. Il secondo capitolo si concentra sulla parte sostanziale e definisce un elenco minimo di reati che gli Stati si impegnano a incriminare, articolandoli in quattro titoli. Il primo comprende i reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici, qualificati come "*cybercrime puri*" in quanto emersi esclusivamente con lo sviluppo tecnologico e legati intrinsecamente ad esso. Si tratta, infatti, di una categoria di illeciti inesistente

[43] Cadoppi, A. (2023). Cybercrime (2. edizione.). UTET Giuridica. pp. 109-113
[44] Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185), art. 14.
[45] *Article 1 – Definitions*
For the purposes of this Convention:

a) "*computer system*" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b) "*computer data*" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c) "*service provider*" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d) "*traffic data*" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

nel diritto penale tradizionale. In questa classificazione rientrano diverse fattispecie: l'accesso non autorizzato ai sistemi informatici (c.d. *Hacking*) all'art. 2; l' intercettazione illecita di trasmissione non pubbliche di dati informatici (art..3); il danneggiamento, la modifica o soppressione di dati informatici, riconducibili ai fenomeni di *Malware* o *virus* informatici (art.4); nonché l' impedimento del corretto funzionamento di un sistema informatico e l'abuso di apparecchiature o di password idonee a facilitare l'abuso informatico (c.d. *misuse of devices*) di cui all'art.6 [46].

Il titolo seguente è dedicato ai cosiddetti "*computer related offences*", ossia reati tradizionali che possono essere commessi a mezzo di computer. La Convenzione prevede solo due fattispecie: la falsificazione informatica (c.d. *computer related frogery*) che consiste nella creazione o modifica di dati falsi destinati ad essere usati come autentici ai fini legali (art. 7), e la frode informatica, che si realizza quando, attraverso sistemi digitali, si cagiona un danno patrimoniale a terzi (art.8).

La terza categoria di reati comprende i "*content related offences*" e include un'unica fattispecie: la pornografia minorile (art.9) riconosciuta come reato a livello internazionale.

Infine, il quarto titolo obbliga gli Stati a prevedere reati a tutela della proprietà intellettuale e dei diritti connessi, richiamando gli obblighi assunti dalle parti derivanti dalla Convenzione di Berna, dall'accordo TRIPS e dai trattati WIPO (art.10)[47].

La seconda sezione della Convenzione si riferisce agli aspetti processuali della materia. La rivoluzione tecnologica, infatti, richiede una revisione della normativa non solo sul piano sostanziale, con l'introduzione di nuove fattispecie di reato, ma anche su quello procedurale. Ed è proprio nella dimensione processuale dei nuovi reati che emergono le principali sfide per il diritto penale, a causa della difficoltà di identificare gli autori dei *cybercrime*, della portata e ampiezza dei beni giuridici lesi, nonché per la facilità con cui si possono modificare o addirittura eliminare i dati informatici.

La Convenzione ha adattato le procedure di ricerca della prova tradizionali alle nuove tecnologie, distinguendo tra tre tipologie di dati: i dati di traffico, i dati di

[46] Clough, J. (2012) *The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World.* Crime Law Forum 23, pp.363–391.
[47] Council of Europe. (2001, November 8). *Explanatory Report to the Convention on Cybercrime* (ETS No. 185). pp. 15-19

contenuto e i dati relativi agli abbonati. Questi dati possono essere già conservati o in corso di trasmissione.

Le misure procedurali imposte agli Stati Parte devono essere applicate nel rispetto degli ordinamenti interni e, soprattutto, bilanciando l'interesse alla ricerca della prova con la tutela dei diritti umani e delle garanzie fondamentali contenute negli strumenti internazionali in materia tra cui la Convenzione europea dei diritti dell'uomo, la Convenzione americana sui diritti umani, la Carta africana dei diritti dell'uomo e dei popoli e il Patto internazionale sui diritti civili e politici (art.15).

Per quanto concerne le norme in senso stretto, l'articolo 16 è volto a garantire la conservazione rapida di dati informatici già memorizzati per una specifica indagine o procedimento penale. In questo senso per "*conservazione*" si intende la possibilità per le autorità competenti di ordinare ai fornitori di servizi di impedire che i dati subiscano qualsiasi forma di alterazione, deterioramento o cancellazione, soprattutto quando si tratta di dati ritenuti particolarmente vulnerabili. Tale misura corrisponde alla *data preservation* che si deve distingue dalla *data retention*: mentre la prima si riferisce alla conservazione mirata di dati già esistenti, la seconda comporterebbe, per il service providers, un obbligo generalizzato e preventivo di raccolta di tutti i dati informatici.

La Convenzione lascia ampia discrezionalità agli Stati nel determinare gli strumenti con i quali imporre la conservazione, purché siano efficaci per il raggiungimento dell'obiettivo. Se la misura è disposta tramite un ordine, il soggetto destinatario ha l'obbligo di proteggere l'integrità dei dati per un periodo necessario, comunque non superiore a novanta giorni rinnovabili, così da consentire la successiva divulgazione alle autorità competenti. Ai *service providers* è inoltre imposto l'obbligo di riservatezza in merito all'ordine di conservazione ricevuto, volto sia a salvaguardare l'efficacia dell'indagine, evitando che il presunto autore del reato possa venirne a conoscenza e distruggere le prove, sia a garantire la privacy delle persone coinvolte[48].

Su un piano operativo analogo si colloca l'art. 29, intitolato "*conservazione rapida di dati informatici immagazzinati*". A differenza dell'art 16, che impone obblighi da applicare nel territorio nazionale di ciascuno Stato parte, l'art.29 si riferisce alla conservazione di dati finalizzata a garantire un'efficace cooperazione

[48] Ivi pp.21-27

internazionale. Ne consegue che la sua attuazione risulterà nella pratica molto più complessa. Differisce anche la durata della conservazione: mentre l'art. 16 prevede un termine massimo di novanta giorni, l'art.29 richiede un periodo non inferiore a sessanta giorni, volto ad assicurare una maggiore stabilità della cooperazione, che può richiedere tempi lunghi per la sua effettiva attuazione. In aggiunta, l'art.29 stabilisce il principio della doppia incriminazione, secondo il quale il reato, oggetto della richiesta di assistenza, deve essere qualificato come tale per ambedue gli ordinamenti giuridici coinvolti[49].

L'art.17 riguarda invece la conservazione di dati di traffico (*traffic data*) ossia dati relativi alla trasmissione di una comunicazione (origine, destinazione, percorso, ora, data, durata e tipo di servizio utilizzato). Queste dati sono cruciali per ricostruire il flusso comunicativo e per identificare l'autore del reato informatico per cui si sta indagando. Tuttavia, poiché sono conservati per periodi brevi e spesso distribuiti tra più fornitori di servizi, la Convenzione prevede la possibilità di richiedere la conservazione presso tutti i *providers* eventualmente coinvolti, così da permettere la rapida trasmissione dei dati interessati alle autorità nazionali competenti[50].

L'articolo 30, strettamente correlato all'art. 17, disciplina la rivelazione accelerata di dati sul traffico nel contesto della cooperazione internazionale. A differenza dell'art. 17, volto all'adozione di obblighi interni, l'art. 30 riguarda la cooperazione tra due Stati, e stabilisce che la parte richiesta può rifiutare l'assistenza solo per i motivi elencati nell'art. 27, par. 4, relativi alla tutela della sovranità, della sicurezza e dell'ordine pubblico[51].

All'interno del titolo III la Convenzione introduce poi l'ingiunzione a produrre, una misura investigativa meno invasiva della perquisizione e del sequestro, che consente alle autorità competenti di ottenere da privati o soggetti giuridici dati specifici in loro possesso, inclusi quelli sugli abbonati dei fornitori di servizi (c.d. *subscriber information*). Questa misura consente un'acquisizione rapida e mirata delle informazioni senza ricorrere a procedure più invasive e complesse, preservando così un equilibrio tra efficacia investigativa e tutela dei diritti fondamentali.

[49] Ivi pp. 50-52
[50] Ivi pp.28-29
[51] Ivi. p.52

L'art 19, intitolato "*Search and seizure of stored computer data*", disciplina le misure di perquisizione e sequestro di dati informatici memorizzati con l'obiettivo di adattare la legislazione nazionale alla natura immateriale dei dati digitali. Le Parti devono consentire alle autorità di perquisire e accedere ai sistemi informatici presenti sul territorio, nonché ai sistemi connessi qualora vi sia motivo di ritenere che ospitino dati rilevanti. Le autorità possono adottare tutte le misure necessarie al raggiungimento dello scopo fermo restando il rispetto degli artt.14 e 15 della Convenzione, relativi, rispettivamente all'ambito di applicazione delle disposizioni procedurali e alle condizioni e garanzie[52].

In ambito internazionale, l'articolo 31 disciplina l'assistenza reciproca relativa all'accesso ai dati informatici archiviati. Tale disposizione consente alla parte richiedente di sollecitare la parte richiesta a procedere alle misure di perquisizione e sequestro relative ai reati informatici. A differenza delle misure applicabili in ambito interno, i cui termini e condizioni sono stabiliti dall'art.14 e 19 della Convenzione, l'art.31 specifica che i presupposti e i limiti delle operazioni di perquisizione e sequestro nel contesto della mutua assistenza sono definiti dai trattati e accordi internazionali vigenti tra le Parti. Inoltre, mentre l'art.19 non specifica alcun obbligo di tempestività nell'adozione di tali misure, l'art 31 prevede espressamente una risposta accelerata da parte della parte richiesta, data la natura volatile e facilmente modificabile dei dati informatici[53].

Gli articoli 20 e 21 completano il quadro, disciplinando rispettivamente la raccolta in tempo reale dei dati sul traffico (*traffic data*) e l'intercettazione in tempo reale dei dati di contenuto (*content data*). Innanzitutto è necessario distinguere tra dati sul traffico e dati di contenuto. I primi si riferiscono alle informazioni riguardanti la comunicazione in sé, mentre i secondi riguardano il contenuto effettivo della comunicazione, ossia ciò che viene trasmesso tra le parti. Questa distinzione terminologica riflette la diversa invasività: i dati sul traffico, sono considerati meno invasivi e la loro intercettazione può essere effettuata per qualsiasi reato; mentre i dati di contenuto comportano un grado di intrusione più elevato nella sfera privata dell'individuo, per questo motivo l'intercettazione può essere autorizzata solo per reati

[52] Ivi. pp. 29-35
[53] Ivi p.52

particolarmente gravi, definiti tali secondo l'ordinamento interno di ciascuno Stato Parte. Gli Stati devono garantire gli strumenti tecnici necessari, imponendo obblighi di cooperazione ai fornitori di servizi[54].

Sul piano internazionale, gli art. 33 e 34 disciplinano l'assistenza reciproca tra Stati relativa alla raccolta in tempo reale di dati sul traffico e di dati di contenuto. Anche in questo caso, incombe l'obbligo di riservatezza in capo ai fornitori di servizi volto a garantire la corretta prosecuzione delle indagini[55].

Infine, per assicurare l'effettiva punibilità degli autori dei reati, gli Stati Parte devono stabilire la propria giurisdizione penale rispetto ai reati elencati dall'art.2 all'art.11 della Convenzione. In questo senso, si prevedere la possibilità per le Parti di apporre delle riserve nei casi di giurisdizione territoriale estesa, ossia quando il reato è commesso a bordo di una imbarcazione battente bandiera dello Stato o a bordo di un aeromobile registrato a suo nome, nonché nel caso di giurisdizione basata sul criterio della nazionalità del colpevole. Non sono invece ammesse riserve nei casi di giurisdizione territoriale ordinaria, ossia quando il reato è commesso all'interno del territorio di uno Stato Parte, ovvero nel caso in cui si applichi il principio "*aut dedere aut iudicare*", secondo cui il rifiuto dell'estradizione comporta l'obbligo di giudicare l'indagato.

Il paragrafo 5 dell'articolo 22 prevede, infine, la possibilità di consultazioni tra Stati in caso di concorso di giurisdizioni. Tuttavia, tale previsione non è assoluta e gli stati possono decidere di ritardare o negare la consultazione qualora ritengano che la stessa possa compromettere le indagini o il procedimento in corso[56].

Essendo i *cybercrimes* reati a carattere transnazionali, essi coinvolgono più Stati e, di conseguenza, più giurisdizioni. È quindi necessario, ai fini dell'instaurazione di procedimenti giudiziari completi ed efficaci, garantire la cooperazione internazionale. A tal fine, opera il capitolo III della Convenzione di Budapest sul Cybercrime che disciplina la cooperazione e la mutua assistenza nei casi di reati commessi mediante l'uso di mezzi e sistemi informatici; nell'ipotesi di reati ordinari

[54] Ivi pp. 35-40
[55] Ivi pp.53-54
[56] Ivi. pp.43-43

che coinvolgono prove elettroniche; nonché nel caso di crimini informatici cosiddetti "*puri*"[57].

La Convenzione tratta della cooperazione internazionale distinguendo due situazioni differenti: quando non esistono altri strumenti applicabili tra le Parti, essa costituisce il fondamento stesso della cooperazione; quando invece esistono altri trattati vincolanti, la Convenzione opera in via complementare, senza precluderne l'applicazione[58].

In quest'ottica, l'articolo 23 stabilisce che la cooperazione deve essere garantita "*nella più ampia misura possibile*" obbligando le parti a ridurre al minimo gli ostacoli che possano comprometterla e a consentire la massima assistenza reciproca per lo scambio delle informazioni e per l'attuazione delle misure operative[59].

Tra i meccanismi tradizionali di cooperazione, la Convenzione stabilisce, all'art.24, l'obbligo di estradizione per i reati previsti dall'articolo 2 all'articolo 11. Tali reati sono considerati "*estradabili*" solo se punibili in entrambi gli ordinamenti coinvolti e se sono sanzionati con una pena non inferiore a un anno di reclusione. Nel caso in cui vi siano accordi bilaterali o trattati multilaterali che prevedano soglie differenti, si applicheranno quest'ultimi. Resta fermo che la parte alla quale viene richiesta l'estradizione non è obbligata a concederla se ritiene che la stessa non soddisfi i requisiti richiesti dal diritto internazionale o dal proprio ordinamento interno. In tal caso, lo Stato richiesto che ritiene di avere giurisdizione nel caso concreto sarà comunque tenuto, su domanda della parte richiedente, a procedere nei confronti del presunto autore del reato, conformemente al principio di "*aut dedere aut iudicare*". [60]

Per quanto concerne la mutua assistenza, la Convenzione ribadisce il principio della massima cooperazione possibile, come descritto nell'art.25. Particolarmente rilevante è il paragrafo 3, che mira a facilitare e accelerare il processo di assistenza reciproca. Infatti, poiché i dati informatici sono per loro natura volatili e destinati ad

[57] COLOMBO E., (2009) *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in Ciberspazio e Diritto 2009, n. 3-4. pp. 285-304

[58] Ilarda, G., Marullo, G., & Osservatorio permanente sulla criminalità organizzata. (2004). *Cybercrime: conferenza internazionale: la Convenzione del Consiglio d'Europa sulla criminalità informatica.* Giuffrè. p.18

[59] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, cit., pp. 41-42

[60] Ivi pp.42-44

essere eliminati rapidamente, le Parti devono consentire alle proprie autorità competenti, in caso di urgenza, di utilizzare mezzi di comunicazione rapida, quali fax o posta elettronica, a condizione che sia garantita autenticità e sicurezza rispettivamente delle informazioni trasmesse e dei mezzi utilizzati. Simmetricamente, anche lo Stato richiesto è tenuto a fornire una rapida risposta, utilizzando mezzi che consentano la stessa facilità e tempestività. La mutua assistenza non è tuttavia assoluta. L'articolo 25 paragrafo 4, prevede che essa sia soggetta alle condizioni previste dai trattati in tema di mutua assistenza giudiziaria e dalle norme interne degli Stati, le quali assicurano il rispetto dei diritti fondamentali delle persone coinvolte.

La Convenzione introduce due rilevanti eccezioni a tali limitazioni. In primo luogo, le Parti sono tenute a predisporre nei loro ordinamenti interni le misure di cooperazione previste dalla Convenzione (conservazione dei dati, perquisizione, sequestro, rete 24/7) anche qualora, tali strumenti non siano previsti negli altri trattati internazionali[61].

La seconda eccezione riguarda quanto definito dall'art.27, il quale dispone che, in assenza di un trattato bilaterale o multilaterale in materia di mutua assistenza, la Convenzione funge da strumento sostitutivo, disciplinando le modalità e i limiti della cooperazione. A tal proposito, l'articolo 27 paragrafo 4, riveste un ruolo determinante, in quanto individua esplicitamente i casi in cui l'assistenza può essere rifiutata. La disposizione stabilisce, infatti, che oltre ai casi di cui all'articolo 25 paragrafo 4 riguardanti le specifiche limitazione previste dalle legislazione della parte richiesta, l'assistenza può essere limitata quando "*la richiesta riguarda un reato che la parte richiesta considera politico o connesso con un reato politico*" ovvero quando "*la Parte richiesta ritenga che l'esecuzione della richiesta possa recare pregiudizio alla sua sovranità, alla sua sicurezza e all'ordine pubblico o ad altri interessi essenziali*".

A completamento delle eccezioni definite dalla Convenzione, si prevede, da un lato, che la cooperazione non può essere limitata per i reati indicati negli articoli 2 – 11, anche qualora si tratti di reati fiscali[62], e dall'altro che, per quanto riguarda la conservazione dei dati non è richiesta la doppia incriminazione come precondizione,

[61] Council of Europe. (2001, November 23). *Convention on Cybercrime* (ETS No. 185), art. 25, para. 2.
[62] Ivi art.25 para. 4

in modo da accelerare lo scambio di informazioni[63]. In relazione a quest'ultima eccezione, l'art,29 paragrafo 4, stabilisce che uno Stato può riservarsi la facoltà di rifiutare la conservazione per i reati diversi da quelli contemplati dagli articoli 2-11, qualora abbia motivo di ritenere che, al momento della divulgazione, il requisito della doppia incriminazione non possa essere soddisfatto.

L'art 25 paragrafo 5 chiarisce poi che il requisito della doppia incriminazione deve ritenersi soddisfatto quando la condotta oggetto della richiesta è qualificata come reato nell'ordinamento della parte richiesta, anche se tale reato è inserito in una categoria diversa o descritto con una terminologia differente[64].

In attuazione del principio della massima cooperazione possibile, l'art 26 prevede la possibilità di trasmissione spontanea di informazioni, consentendo ad uno Stato di fornire ad un altro, di propria iniziativa, dati e informazioni che possono risultare utili ai fini di un'indagine o di un procedimento, anche in assenza di richiesta formale di assistenza[65] .

L'art.28 intitolato "*confidenzialità e limitazioni di utilizzo*", si applica, al pari dell'art.27, qualora non vi siano in vigore specifici accordi di mutua assistenza. Esso consente alla parte richiesta di poter subordinare la trasmissione di informazioni alla garanzia della loro riservatezza e alla limitazione del loro impiego esclusivamente ai fini del procedimento o delle indagini per le quali sono state fornite[66].

Di fondamentale importanza è, infine, l'art. 35 che istituisce la "*Rete 24/7*" ossia la creazione di punti di contatto e informativi funzionanti 24 ore su 24 e 7 giorni su 7 idonei a raccogliere richieste e fornire risposte celeri e immediate ai destinatari[67]. Tale meccanismo è considerato una delle principali novità della Convenzione in quanto il contrasto ai reati informatici, per essere realmente efficace, necessita di interventi tempestivi per i quali si rendono necessari canali di cooperazione e coordinamento efficienti e celeri. Tale Network, istituito originariamente sotto gli auspici del G8 del 1995, ha come obiettivo quello di facilitare le attività di prevenzione e indagine in materia di criminalità informatica. Ogni Stato Parte ha l'obbligo di

[63] Ivi art.29 par 3
[64] Council of Europe, *Explanatory Report to the Convention on Cybercrime*. cit. pp. 44-45
[65] Ivi p. 46
[66] Ivi pp. 49-50
[67] Colombo, E. *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali.* cit. pp. 285-304.

designare un punto di contatto 24/7, con libertà di decidere se accentrare tale Network in un'unica autorità ovvero decentrarlo in diverse zone territoriali e istituzionali. Le funzioni che devono essere garantite comprendono l'assistenza tecnica, la conservazione dei dati ai sensi degli art.29 e 30, la raccolta delle prove, la trasmissione di informazioni di carattere giuridico utili alla cooperazione e la localizzazione dei sospettati[68].

3.1.1 I protocolli addizionali alla Convenzione di Budapest

L'inadeguatezza della Convenzione del 2001 nel fronteggiare tutti gli aspetti dell'ampio ambito del cyberspazio emerse quasi immediatamente dopo la sua adozione. Gli stessi redattori della Convenzione, prevedendo la possibilità (o certezza) di un'evoluzione necessaria nel settore, hanno imposto agli Stati Parte l'obbligo di consultarsi periodicamente al fine di monitorare modificare e integrare la Convenzione stessa, sotto la guida del Comitato Europeo per i problemi della criminalità (CDPC)[69].

Un primo passo in tale direzione si ebbe nel 2003, con l'adozione del Primo Protocollo Addizionale[70], volto ad ampliare la categoria dei reati informatici legati al contenuto. In particolare, tale protocollo si riferisce ai reati di natura razzista e xenofoba commessi tramite Internet, rilevanti in considerazione del costante aumento delle manifestazioni di odio e di discriminazione via web[71].

Per quanto concerne invece l'aspetto procedurale della materia, le Parti si resero conto da un lato, della necessità di bilanciare con maggiore fermezza la protezione dei cittadini dagli attacchi informatici con la tutela dei diritti fondamentali, preservando lo stato di diritto nel cyberspazio. Era infatti essenziale evitare che la Convenzione potesse apparire come uno strumento di controllo di massa, garantendo

---

[68] Council of Europe, *Explanatory Report to the Convention on Cybercrime*. cit. pp.54-55
[69]Council of Europe. (2001, November 23). *Convention on Cybercrime* (ETS No. 185), art. 46
[70]Council of Europe. (2003, January 28). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (CETS No. 189). Strasbourg: Council of Europe.
[71]Polyzoidou, V. 2021. *Combatting the cybercrime: Thoughts based on the second additional protocol (draft) to the Budapest Convention on Cybercrime*. In T.-E. Synodinou, P. Jougleux, C. Markou, & T. Prastitou (Eds.), *EU Internet law in the digital single market*. Springer International Publishing. p. 360

invece che essa risultasse realmente funzionale agli obiettivi procedurali per cui era stata concepita. Dall'altro lato, esse riconobbero l'esigenza di assicurare un livello più elevato di cooperazione e di assistenza giudiziaria reciproca.

In tale contesto, nel settembre 2017 vennero avviati i negoziati per il Secondo Protocollo Addizionale alla Convenzione sulla criminalità informatica che si conclusero con l'apertura alla firma nel 2022[72]. Il protocollo introduce varie disposizioni a carattere tecnico volte a accelerare e rafforzare lo scambio di informazioni, riconoscendo il ruolo sempre più centrale dei fornitori dei servizi privati nel cyberspazio. La novità principale riguarda infatti le procedure di comunicazione diretta tra autorità statale e *service providers* finalizzata all'ottenimento di dati relativi agli abbonati, dei *traffic data* e delle registrazioni dei nomi a dominio. Le nuove disposizione, per tanto, non si limitano a disciplinare la cooperazione tra Autorità di paesi diversi, ma la estendono ai soggetti privati, i quali giocano un ruolo chiave, se non determinante ed esclusivo, nel mondo digitale[73].

Di altrettanta importanza, sono le altre innovazioni normative che mirano a rendere l'assistenza reciproca più efficiente, a chiarire il quadro normativo in relazione alle pratiche di accesso transfrontaliero ai dati e a rafforzare le garanzie in tema di requisiti di protezione dei dati[74]. Gli Stati Parte hanno riconosciuto che la sola maniera per contrastare la criminalità informatica, divenuta nel frattempo un fenomeno molto più intricato e complesso rispetto al 2001, consiste in una maggiore e costante interconnessione tra giurisdizioni e in una più profonda comprensione delle modalità di conservazione e trasmissione di dati.

3.2 Le Convenzioni delle Nazioni Unite e altri strumenti multilaterali

[72] Council of Europe. (2022, May 12). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). Strasbourg: Council of Europe

[73] Buccarella M. (28 gennaio 2023). *Il Secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione internazionale in ambito digitale: Quali rischi per la protezione dei dati personali nell'Unione europea?* in I Post di AISDUE, V, n. 8, 28 gennaio 2023, AISDUE. pp. 187-188

[74] Polyzoidou V. *Combatting the cybercrime: Thoughts based on the Second Additional Protocol (draft) to the Budapest Convention on Cybercrime*. cit. pp. 355–375.

In materia di cooperazione giudiziaria internazionale, risulta opportuno richiamare alcune delle più importanti Convenzioni multilaterali che hanno contribuito a definire un quadro giuridico comune tra gli Stati. Questi strumenti internazionali contengono disposizioni in larga parte analoghe a quelle previste dalla Convenzione di Budapest, a testimonianza del consolidarsi di un consenso internazionale e di un'uniformità in materia di assistenza giudiziaria reciproca idonea sia a favorire la cooperazione ma anche a precisare i limiti della stessa.

La prima Convenzione di fondamentale rilevanza è la Convenzione europea di assistenza giudiziaria in materia penale, adottata dal Consiglio d'Europa nel 1959 ed entrata in vigore nel 1962 (CEAG)[75]. Si tratta del primo strumento multilaterale specificamente dedicato all'assistenza giudiziaria, nata dall'esigenza di separare tale disciplina da quella dell'estradizione. La distinzione si fonda sulla considerazione che l'assistenza giudiziaria comporta un minor impatto sulla libertà personale rispetto all'estradizione, consentendo di attenuare alcune limitazione proprie di quest'ultima, come, ad esempio, il principio della doppia incriminazione, che non si applica per l'assistenza giudiziaria. La Convenzione disciplina alcuni istituti tipici di cooperazione tra i quali: le commissioni rogatorie per l'audizione di testimoni o periti, la notifica di documenti ufficiali e di sentenze giudiziarie, la citazione di testimoni, periti o persone detenute e la trasmissione di informazioni dai registri giudiziari [76].

Un altro strumento multilaterale in questo senso è la Convenzione delle Nazioni Unite contro la criminalità organizzata (UNTOC o "*Convenzione di Palermo*") entrata in vigore nel 2003[77]. Nonostante sia stata concepita principalmente per contrastare fenomeni di criminalità organizzata transnazionale, la sua portata applicativa è più ampia in quanto mira, tra le altre cose, a promuovere la cooperazione internazionale in particolare attraverso l'estradizione, l'assistenza legale e le indagini congiunte. In questo senso è fondamentale l'art.18 di tale Convenzione intitolato

[75] Council of Europe. (1959). *European Convention on Mutual Assistance in Criminal Matters* (CETS No. 30).
[76] Council of Europe. (1959). *Explanatory Report to the European Convention on Mutual Assistance in Criminal Matters* (CETS No. 30) p.2.
[77] United Nations. (2000). *United Nations Convention against Transnational Organized Crime and the Protocols Thereto*. New York: United Nations.

"*assistenza giudiziaria reciproca*" che mira a stabilire la più ampia forma possibile di cooperazione volta a contrastare i reati contemplati dalla Convenzione [78].

Centrale in tema di MLA è la Convenzione delle Nazioni Unite contro la corruzione adottata nel 2003 ed entrata in vigore nel 2005[79]. Essa contiene norme particolarmente dettagliate in materia, che si estendono oltre i reati di corruzione, applicandosi per una vasta gamma di crimini economici e finanziari. L'art. 46 costituisce il punto focale della cooperazione reciproca in quanto afferma che le parti devono garantire la maggior assistenza giudiziaria in tema di indagini, azioni penali e procedimenti giudiziari relativi ai reati previsti nella Convenzione[80].

3.3 L'evoluzione della cooperazione nel diritto dell'Unione Europea

La cooperazione in materia penale tra gli Stati europei nasce negli anni Settanta, quando gli Stati Membri della Comunità Economica Europea avviarono le prime iniziative in tale ambito. Proprio in quegli anni, a seguito della crescente preoccupazione per le minacce terroristiche, fu fondato il cosiddetto "gruppo Trevi" considerato, ad oggi, l'origine della cooperazione penale nell'Unione Europea. In questo contesto, caratterizzato dalla necessità di rafforzare la collaborazione al fine di combattere fenomeni criminali, Giscard d'Estaing propose la creazione di uno "*Spazio giudiziario penale europeo*" volto a rafforzare e migliorare i meccanismi e le modalità di cooperazione.

Un ruolo di fondamentale importanza in questa evoluzione fu svolto dall'Accordo *Schengen*, relativo all'eliminazione progressiva dei controlli alle frontiere. Sebbene tale accordo fosse stato concluso al di fuori dell'ambito comunitario e dunque a livello intergovernativo tra gruppi di Stati diversi, esso mise in evidenza la necessità di evitare che l'abolizione dei controlli potesse essere sfruttata dagli autori di crimini come strumento per eludere le previsioni normative. Di conseguenza, si ritenne indispensabile adottare misure compensative nell'ambito Giustizia e Affari

[78] Council of Europe. (2013). *Mutual Legal Assistance Manual*. Belgrado: Council of Europe. p. 62-64
[79] United Nations. (2004). *United Nations Convention against Corruption*. New York: United Nations.
[80] Council of Europe, Mutual Legal Assistance Manual, cit., p. 64-69

Interni GAI) degli Stati membri, volte non solo a colmare il deficit di sicurezza derivante dalla libertà di circolazione ma anche a intensificare la cooperazione tra le autorità nazionali, garantendo un controllo efficace in uno spazio privo di frontiere.

A livello comunitario, un decisivo passo avanti si ebbe con il Trattato di Maastricht del 1992[81] che istituì il terzo pilastro dell'Unione dedicato alla cooperazione nei settori della GAI. Tale innovazione introdusse per la prima volta un coordinamento sovranazionale, seppur ancora acerbo ed embrionale, nella cooperazione giudiziaria e di polizia in materia penale.

Progressivamente, il Trattato di Amsterdam (1997)[82] segnò un'ulteriore evoluzione, ponendo tra gli obiettivi dell'Unione l'istituzione dello "*Spazio di libertà, di sicurezza e di giustizia*". Tale proposito portò ad una progressiva erosione del concetto di stretta territorialità in ambito penale, in favore di un impegno comune della neonata Unione Europea a garantire la sicurezza dei cittadini e la lotta alla criminalità.

Per concretizzare tali obiettivi, furono istituiti due programmi quinquennali di lavoro: il Consiglio europeo di Tampere e il programma de l'Aia. Il consiglio di Tampere stabilì un nuovo approccio nella gestione della cooperazione giudiziaria in materia penale basata sul principio di reciproca fiducia tra gli ordinamenti nazionali e sul principio del mutuo riconoscimento delle decisioni giudiziarie. Tampere pose anche le basi per l'istituzione dell'unità denominata "*Eurojust*", organo di coordinamento tra le autorità giudiziarie degli Stati membri. Il programma de l'Aja, invece, definì un'ulteriore principio fondante della cooperazione ossia il principio di disponibilità delle informazioni ai sensi del quale ogni agente di uno Stato membro che abbia necessità di disporre di determinate informazioni, nell'esercizio delle sue funzioni, ha diritto di ottenerle dalle autorità omologhe di un altro stato che le detengano.

[81] European Union. (1992, February 7). Treaty on European Union (Maastricht Treaty). Official Journal of the European Communities, C 191.
[82] European Union. (1997, October 2). *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts*. Official Journal of the European Communities, C 340.

Infine, con l'entrata in vigore del Trattato di Lisbona nel 2009[83], si procedette all'eliminazione della struttura in pilastri, di stampo prettamente intergovernativo, al fine di ricondurre la disciplina della cooperazione di polizia e giudiziaria penale sotto il metodo "*comunitario*". Quest'ultimo si caratterizza per l'adozione delle decisioni a maggioranza qualificata (e non più all'unanimità, che in precedenza garantiva un sostanziale potere di veto agli Stati nell'adozione di misure di cooperazione), per il rafforzamento del ruolo decisionale del Parlamento europeo e della Corte di Giustizia dell'Unione europea, nonché per l'applicazione, anche in tale contesto, dei principi generali dell'ordinamento comunitario quali la leale collaborazione e, soprattutto, la supremazia del diritto dell'UE sul diritto interno[84]. In questo nuovo contesto istituzionale, si assiste a un profondo rinnovamento degli strumenti di cooperazione in materia penale, volto a garantire una raccolta delle prove più efficiente e tempestiva all'interno di un quadro europeo sempre più integrato.

In materia strettamente investigativa, un ruolo significativo lo ha giocato la Direttiva 2014/41/UE[85] con la quale si è proceduto alla sostituzione del vecchio sistema di assistenza giudiziaria basato sugli strumenti rogatori introducendo l'ordine europeo di indagine penale (OEI) per l'acquisizione di prove transnazionali.

Prima della Direttiva, esistevano problematiche procedurali e incertezze circa la tipologia di prova che potesse ricadere nel precedente regime del "*mandato europeo di ricerca delle prove*" (MER). Con l'OEI, invece, l'Unione ha introdotto uno strumento univoco per l'acquisizione e la circolazione delle prove nel contesto europeo. L'OEI consiste in una decisione giudiziaria emessa da un'autorità competente di uno stato membro denominato "*Stato di emissione*" e volta a far eseguire attività di indagine o ad ottenere una prova già nella disponibilità di un altro Stato membro, definito come "*Stato di esecuzione*". L'obiettivo è sostituire le modalità

[83] European Union. (2007, December 13). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*. Official Journal of the European Union, C 306.
[84] Kostoris, R. E. (2017). *Manuale di procedura penale europea* (5ª ed.). Milano: Giuffrè Editore pp.315-341
[85] European Union. (2014). *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.* Official Journal of the European Union, L 130/1.

farraginose e complesse di cooperazione transfrontaliera, con un unico strumento standardizzato a carattere orizzontale applicabile per qualsiasi atto di indagine penale.

Una delle principali innovazione introdotte dalla Direttiva è la possibilità che l'OEI sia richiesto non solo dall'autorità giudiziaria, ma anche dalla persona sottoposta a indagini, dall'imputato o dal loro difensore, in virtù del rispetto dei diritti di difesa garantiti dagli ordinamenti nazionali e dal diritto dell'Unione Europea[86].

Inoltre, la direttiva stabilisce che "*l'adozione della decisione sul riconoscimento o sull'esecuzione e il compimento dell'atto di indagine hanno luogo con la stessa celerità e priorità usate in un caso interno analogo e, in ogni caso entro i termini previsti dal presente articolo*"[87].Tale strumento impone particolare celerità: la decisione sul riconoscimento e sull'esecuzione deve intervenire entro 30 giorni, prorogabili di ulteriori 30 in casi eccezionali. L'autorità di esecuzione deve poi compiere l'atto di indagine entro 90 giorni dall'adozione della decisione e deve trasmettere, senza indebito ritardo, le prove acquisite o già in suo possesso[88].

3.3.1 La *cybersecurity* nel diritto dell'Unione Europea

La *cybersecurity*, termine derivante dalla crasi di due parole *cyberspace* e *security*, consiste "*nell'insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere dispositivi, dati e reti informatiche"*[89]. Questo concetto si riferisce alla tutela di 3 ambiti digitali: la protezione dei contenuti, dei dati e delle informazioni; la protezione dell'*hardware* ossia dei dispositivi fisici come PC, *smartphone*, *mainframe* o *server*; e, infine, la protezione degli aspetti *software* intesi come programmi, reti, *database*, archivi digitali e altre impostazioni tecnologiche. Accanto a tale definizione, è opportuno precisare cosa si intende invece per *cyberdefence*. Secondo il *Nato Cooperative Cyber Defence Centre of Excellence* (CCDCOE) è la *"misura proattiva per rilevare od ottenere informazioni su un'infrazione informatica, attacco informatico o imminente operazione informatica*

[86] Ivi art. 1, par. 3.
[87] Ivi art.12.
[88] Camaldo, L. (2014, 27 maggio). *La Direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*. DIRITTO PENALE CONTEMPORANEO.
[89] Mula, D.; Contaldo, A. (2020). *Cybersecurity Law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche* Pacini Editore.

ovvero per determinare l'origine di un'operazione che comporta l'avvio di una contromisura preventiva o informatica contro la fonte d'aggressione"[90].

La distinzione tra *cybersecurity* e *cyberdefence* è doverosa in quanto i due ambiti, pur condividendo il riferimento allo spazio digitale, rispondono a logiche e finalità differenti: la prima riguarda la protezione complessiva dell'ecosistema informatico, mentre la seconda attiene alla difesa nazionale e alla sicurezza informatica[91].

Sul piano della disciplina sostanziale, l'Unione Europea ha dato vita a un processo progressivo di armonizzazione volto a creare un quadro normativo uniforme per la sicurezza informatica e il contrasto al *cybercrime*. Prima fra tutti è la "*Strategia dell'Unione Europea per la cybersecurity*"[92] con la quale la Commissione Europea ha promosso l'adozione, da parte degli Stati membri, di normative nazionali orientate alla prevenzione e alla risposta agli incidenti, alle minacce e agli attacchi che possono colpire i canali di comunicazione europei. Tale strategia si fonda su determinati principi ispiratori: l'accessibilità e la gestione condivisa, democratica e efficiente del cyberspazio; il rispetto delle libertà e dei diritti sanciti dalla Carta dei diritti fondamentali dell'Unione Europea e la responsabilità condivisa tra tutti gli *stakeholders*. Essa persegue, da un lato, l'obiettivo di rafforzare la *cyber-resilience*, intesa sia come sviluppo di capacità cibernetiche all'interno degli Stati membri sia come promozione di una cooperazione strutturata tra autorità pubbliche e settore privato; e , dall'altro, la riduzione drastica del *cybercrime* attraverso l'adozione di una legislazione efficace e di adeguate politiche di finanziamento volte a sostenere gli Stati nel rafforzamento delle loro capacità investigative e di contrasto al crimine informatico. Accanto a tali finalità, la strategia contempla anche lo sviluppo di politiche e capacità di *cyberdefence* nel contesto della Politica di sicurezza e difesa comune con particolare attenzione alla protezione degli *asset* critici, e la promozione delle risorse industriali e strategiche nel settore della cybersicurezza. Infine, essa mira

[90] NATO Cooperative Cyber Defence Centre of Excellence, istituito il 14 maggio 2008.
[91] Mula, D.; Contaldo, A. *Cybersecurity Law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*
[92] European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2013, 7 febbraio). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Bruxelles.

alla definizione di una politica internazionale dell'Unione che colmi i divari normativi e consolidi la cooperazione con Paesi terzi e organizzazioni internazionali.

In tale contesto si inserisce la direttiva *Network and Information Security* (NIS) 2016/1148[93] che, impone agli Stati membri di innalzare il proprio livello di sicurezza informatica e di resilienza. In particolare, l'obbiettivo principale stabilito dalla Direttiva mira ad armonizzare le politiche nazionali di *cybersecurity* attraverso un rafforzamento dei sistema di sicurezza delle reti e dei sistemi informativi e mediante la creazione di una struttura di *governance* che attribuisca ruoli e responsabilità chiari per gli attori coinvolti [94].

Strettamente correlato alla Direttiva NIS, è il Regolamento (UE) 2019/881, il cosiddetto *Cybersecurity Act* (CSA)[95] che persegue due intenti principali. In primo luogo esso rafforza in modo significato il ruolo dell'ENISA, l'Agenzia dell'Unione Europea per la cybersicurezza. Istituita nel 2004 con mandato temporaneo, l'ENISA era inizialmente incaricata di assistere gli Stati membri e le istituzioni europee nell'elaborazione di politiche in materia di sicurezza delle reti e dei sistemi informativi Con il *Cybersecurity Act*, il suo ruolo viene potenziato mediante l'attribuzione di un mandato permanente e di compiti più ampi, tra cui il supporto nella gestione operativa degli incidenti informatici. In secondo luogo, il regolamento si propone di stabilire una cornice normativa e regolamentare in materia di certificazione della sicurezza informatica di prodotti, servizi e processi ICT.

Il regolamento persegue, inoltre, ulteriori finalità quali il rafforzamento della resilienza rispetto agli attacchi informatici, lo sviluppo di un mercato europeo della *cybersecurity* e l'incremento della fiducia dei consumatori nei prodotti e servizi digitali. Come affermato dalla parlamentare europea Angelika Niebler il Cybersecurity

---

[93] European Union. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Official Journal of the European Union, L 194, 1–30.

[94] Marchetti, R., & Mulas, R. *La governance internazionale della sicurezza cibernetica: L'Unione Europea*. In *Cybersecurity: hacker, terroristi, spie e le nuove minacce del web*. cit. pp.136-146.

[95] European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69.

Act *"...will enable the EU to keep up with security risks in the digital world for years to come. The legislation is a cornerstone for Europe to become a global player in cyber security. Consumers, as well as the industry, need to be able to trust in IT-solutions*"[96].

A completamento del sistema, la Direttiva (UE) 2022/2555, nota come NIS2[97], ha sostituito la precedente direttiva NIS ampliandone l'ambito di applicazione sia quanto ai settori interessati sia quanto ai soggetti obbligati. La direttiva prevede obblighi specifici in materia di misure di sicurezza e notificazione di incidenti, rafforza i poteri di vigilanza delle autorità competenti, introduce strumenti come la divulgazione coordinata delle vulnerabilità e potenzia il coordinamento e la cooperazione in materia *cyber* a livello nazionale e europeo[98].

4. Quadro normativo italiano

Sul piano strettamente interno, il legislatore italiano non ha ritenuto necessario l'introduzione di un corpus normativo organico volto a disciplinare in maniera unitaria il fenomeno dei *Cybercrimes*, preferendo invece una regolamentazione frammentaria, realizzata dislocando la materia in fattispecie incriminatrici inserite nel codice penale o in testi legislativi autonomi.

Sulla base di queste premesse, non appare corretto parlare di un vero e proprio "*diritto penale dell'informatica*" poiché, tanto con riguardo ai reati informatici in senso ampio, ossia quelli caratterizzati dall'utilizzo di materiale informatico come mezzo di aggressione (es. le fattispecie in tema di pedofilia), quanto con riferimento ai reati informatici in senso stretto, cioè le condotte illecite dirette verso un sistema informatico (es. accesso e danneggiamento di dati o sistemi), non è identificabile un bene giuridico unitario e specifico che consenta la trattazione sistematica e coerente della materia[99].

---

[96] Mula, D.; Contaldo, A. *Cybersecurity Law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*

[97] European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive*). Official Journal of the European Union, L 333, 80–152.

[98] Agenzia per la Cybersicurezza Nazionale. (2024). Portale NIS

[99] Corona, F. *Reati informatici e investigazioni digitali: diffamazione via web, prove digitali, sex crimes, cyberstalking, cyberbullismo, reati privacy*. cit. p.9

4.1 Disciplina interna in materia di criminalità informatica

La legge del 23 dicembre 1993 n.547[100] costituisce il primo intervento del legislatore italiano inteso a contrastare, in sede penale, la criminalità informatica. Tale intervento si rese necessario in considerazione dell'inadeguatezza delle fattispecie incriminatrici tradizionali di ricomprendere i comportamenti illeciti commessi a mezzo del computer o aventi come obbiettivo i sistemi informatici. Infatti, l'applicazione analogica delle disposizioni penali tradizionali a tali condotte avrebbe comportato un'interpretazione ermeneutica difficilmente compatibile con i principi fondamentali del diritto penale, in particolare con il principio di legalità e tassatività della norma incriminatrice, sanciti dall'art.25 c.2 della Costituzione e dall'art.1 del c.p. Di conseguenza, in mancanza di una normativa ad hoc, i crimini informatici rischiavano di rimanere privi di sanzione. La legge 547/1993 si propose di colmare tale carenza, introducendo specifiche fattispecie penali e adeguando la disciplina processuale alle condotte realizzate tramite strumenti informatici.

In ambito internazionale, a meno di 10 anni da tale riforma emerse l'esigenza di un rafforzamento normativo volto ad una più intensa repressione della condotta criminosa realizzata a mezzo di computer. Tale necessità nasceva dal rapido diffondersi delle comunicazioni telematiche e del personal computer, divenuto ormai uno strumento di uso quotidiano da parte di chiunque. Ciò mise in evidenza come le attività svolte mediante tale strumento, incluse quelle illecite, si collocassero sempre più raramente in un contesto territoriale ben preciso, avendo invece la potenzialità di estendersi oltre i confini nazionali in un breve lasso temporale.

Sulla base della consapevolezza della rilevanza internazionale del fenomeno, venne approvata la Convenzione di Budapest sulla criminalità informatica nel 2001[101]. La Convenzione fu ratificata in seguito dal Parlamento Italiano con la legge 18 marzo 2008, n.48[102], che comportò una totale riscrittura della disciplina previgente.

---

[100] Legge 23 dicembre 1993, n. 547, *modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*. (Gazzetta Ufficiale della Repubblica Italiana, n. 305, 2008).

[101] Amato, G. (2010). *I reati informatici: nuova disciplina e tecniche processuali di accertamento*. p. 1-3. Padova: CEDAM.

[102] Legge 18 marzo 2008, n. 48. *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*. Gazzetta Ufficiale della Repubblica Italiana, n. 80.

Con riferimento alle riforme della fattispecie criminose, le modifiche riguardano il falso informatico (art.491- bis c.p.), la falsa dichiarazione o attestazione al certificatore di firma elettronica (art.495-bis c.p.), la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere il sistema informatico o telematico (art.615-quinquies c.p.), il danneggiamento informatico (art.635-bis, 635-ter, 635-quater, 635-quinquies c.p.), e la frode informatica del soggetto che presta servizio di certificazione di firma elettronica (art.640-quinquies); risultano inoltre abrogati il secondo e terzo comma dell'art.420 c.p. relativo all'attentato agli impianti di pubblica utilità, in quanto tale previsione si considerano assorbite nell'art.635-quinquies.

Dal punto di vista processuale invece la legge 48/2008 ha modificato il codice di procedura penale, relativamente ai mezzi di ricerca della prova e alle indagini di polizia giudiziaria con l'indicazione di specifiche modalità di esecuzione per le ispezioni, perquisizioni e sequestri indicando apposite regole di conservazione, di intangibilità degli originali dati informatici e di conformità delle copie[103].

4.2 L'informatica forense e *digital evidence*

La prova del fatto-reato informatico o telematico presenta delle caratteristiche peculiari, in quanto il pubblico ministero, il difensore e il giudice devono operare in un contesto differente da quello fisico tradizionale, ossia l'ambiente digitale.

Lo studio delle modalità di formazione e acquisizione della prova in questo ambito viene definito come *computer-forensic* o *digital-forensic*, disciplina che si occupa della preservazione, dell'identificazione e della documentazione dei contenuti dei sistemi informatici al fine di acquisire elementi probatori idonei ad essere utilizzati nel processo penale. L'obiettivo principale di tale indagine è quello dell'acquisizione "*garantita*" in grado di assicurare la non alterazione dell'ambiente originale e l'individuazione dell'autore del fatto. Tuttavia, il raggiungimento di tali obiettivi risulta spesso complesso, poiché le tracce informatiche possono essere facilmente distrutte, modificate o occultate oppure l'autore del fatto può risultare difficilmente

[103] Amato, G. *I reati informatici: nuova disciplina e tecniche processuali di accertamento*. cit. pp. 1-3

raggiungibile, rendendo quindi difficoltoso l'accertamento delle prove. Per tale ragione risulta indispensabile che le indagini siano svolte da personale altamente qualificato, dotato di specifiche competenze tecniche nel campo informatico, come ufficiali e agenti di polizia giudiziaria specializzati o gli appartenenti alla polizia postale e delle telecomunicazioni. Parimenti, è necessario disporre di adeguati mezzi in grado di consentire una corretta acquisizione della prova che, prima dell'attuazione della Convenzione di Budapest del 2001, risultavano inesistenti nell'ordinamento interno[104].

I mezzi di ricerca della prova previsti nel nostro ordinamento includono le ispezioni, le perquisizioni, i sequestri e le intercettazioni. L'ispezione, disposta con decreto motivato dall'autorità giudiziaria, ha una funzione conoscitiva e descrittiva finalizzata ad analizzare soggetti, luoghi o cose allo scopo di accertare le tracce e gli effetti materiali del reato. La legge 48/2008 ha apportato modifiche volte ad allargare le attività ispettive dell'art.244 c.p.p., stabilendo la possibilità di svolgere ispezione in riferimenti "*a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*»[105]. Tale nuova modalità di ispezione si riferisce alla necessità di adottare misure tecniche volte a soddisfare due esigenze fondamentali: da un lato il dovere di conservare inalterato il dato informatico originario per garantirne l'autenticità e la validità probatoria, e dall'altro il dovere di impedire una sua alterazione successiva.

Sullo stesso presupposto si basa la disciplina della perquisizione, prevista dall'art.247 comma 1-bis c.p.p., secondo cui *"quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"*[106]. La perquisizione consiste in un'attività ulteriore rispetto all'ispezione, finalizzata alla ricerca del corpo del reato e delle cose ad esso pertinenti le quali, in caso di ritrovamento, verranno sottoposte a sequestro. Le stesse cautele si applicano anche alle

[104] Ivi. p.33
[105] Codice di procedura penale. (1988). art. 244
[106] Ivi art. 247 c.1-bis c.p.p.

perquisizione di iniziativa della polizia giudiziaria come prevede il comma 1-bis dell'art. 352 c.p.p.[107].

Un ulteriore mezzo di ricerca della prova è rappresentato dal sequestro probatorio, disciplinato dall'art.253 c.p.p., che può essere disposto con decreto motivato dell'autorità giudiziaria nonché, in caso di urgenza, anche dalla polizia giudiziaria. Esso comporta lo spossessamento coattivo che determina l'indisponibilità di una cosa mobile o immobile, finalizzata ad assicurare un elemento probatorio utile per l'accertamento del reato.

Una distinzione rilevante tra la perquisizione e il sequestro si ricava dall'art.247 comma 1-bis secondo il quale la perquisizione deve avere ad oggetto l'originale del sistema, dei dati, dei programmi e delle informazioni e non la mera copia. Diversamente, per il sequestro di dati informatici avvenuto nei confronti di fornitori di servizi informatici, telematici e di telecomunicazione, disciplinato all'art.254-bis c.p.p., si prevede che l'acquisizione debba avvenire mediante copia idonea ad assicurare la riproduzione fedele e integrale dell'originale. Tale differenza si giustifica in quanto si ritiene che, presso un operatore professionale, i dati siano conservati in modo ordinato, rendendo il sequestro più agevole rispetto all'asportazione fisica del sistema. Ciò non esclude che il sequestro di copie, anziché degli originali, possa essere disposto in tutti gli altri casi.

L'attività di estrazione e duplicazione dei dati digitali è estremamente delicata a causa della natura delle informazioni che sono vulnerabili e soggette a possibili modifiche; per questo motivo deve essere garantire la non alterazione dei dati nelle attività di copia.

Sebbene l'art.247 comma 1-bis, faccia riferimento agli originali non sempre è possibile procedere al sequestro fisico di quest'ultimi, soprattutto quando ciò comporterebbe l'interruzione di attività pubbliche ed economiche. In tali circostanze, si ritiene legittimo il sequestro mediante copia, che consente di acquisire il contenuto informatico rilevante senza compromettere la funzionalità del sistema. Inoltre, anche se si potessero acquisire gli originali, non è sempre necessario procedere al sequestro

[107] Pietropaoli, S. (2025). *Informatica criminale: diritto e sicurezza nell'era digitale: aggiornata alla legge 90/2024 e alla direttiva NIS2* (Seconda edizione.). Giappichelli. p.89-102

dell'intera postazione di lavoro, specialmente laddove vi siano elementi che non ineriscono le indagini. Se infatti fosse consentito il sequestro indiscriminato di un intero sistema informatico, si produrrebbe un'eccessiva penalizzazione nei confronti dello stesso indagato, che potrebbe subire la perdita o l'alterazione di dati o programmi non pertinenti al reato. Per estendere il sequestro all'intero sistema informatico, è dunque necessario che sussista una stratta correlazione tra il bene sottoposto a sequestro e le esigenze probatorie da soddisfarsi. A titolo esemplificativo, il sequestro dell'intero *hardware* può ritenersi legittimo se un sistema nel suo complesso sia strumentale alla commissione del reato, come nel caso della produzione illecita di opere d'ingegno. Nella maggior parte dei casi, tuttavia, è più frequente il sequestro di un *hard disk* contenente le informazioni utili ai fini delle indagini.

Per quanto concerne le modalità di esecuzione della perquisizione e del sequestro, si applicano le disposizioni generali del codice di procedura penale. Anche in questa situazione, la polizia giudiziaria può procedere di iniziativa, nell'immediatezza del fatto e nei casi di urgenza, quando vi sia pericolo che le cose o tracce di reato vengano alterate, distrutte, occultate o lo stato dei luoghi venga mutato.

È inoltre ammesso il sequestro di un sito internet il quale può essere disposto a fini probatori o a fini preventivi quando si renda necessario interrompere l'attività criminosa in corso o per impedire che vengano protratte le condotte illecite. L'esecuzione avviene in modalità telematica, con strumenti idonei a colpire l'operatività del sito in rete.

Infine, l'art.254 c.p.p. prevede il sequestro di corrispondenza "*presso coloro che forniscono servizi postali, telegrafici, telematici e di telecomunicazione è consentito procedere al sequestro di lettere, pieghe, pacchi valori telegrammi e altri oggetti di corrispondenza, anche se inoltrate per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso per mezzo di persona diversa o che comunque possano avere relazioni con il reato*"[108]. Si tratta, dunque, di un sequestro eseguito presso i gestori di servizi postali, telematici e di telecomunicazioni non direttamente presso l'indagato. Il riferimento alle "*lettere inoltrate per via telematica*" è problematico in quanto potrebbe sembrare riferirsi alle e-mail. La dottrina prevalente ritiene, invece, che tale

[108]Codice di procedura penale. art. 254

espressione si riferisca alla "*posta tradizionale*" ma trasmessa con mezzi telematici e non alle comunicazioni telematiche vere e proprie. Infatti le email, in quanto comunicazioni telematiche, sono assoggettate per la loro captazione a procedure di intercettazione telematica definite dall'art. 266 e 266-bis c.p.p[109]. Operare una distinzione in tal senso è fondamentale, in quanto il sequestro è un mezzo di ricerca della prova che deve essere portato a conoscenza del soggetto interessato affinché questi possa esercitare i suoi diritti di difesa, mentre l'intercettazione è un'operazione che avviene in maniera segreta per garantire l'efficacia investigativa della stessa[110].

Altro mezzo di ricerca della prova rilevante nel contrasto ai crimini informatici consiste nell'intercettazione di comunicazione informatiche o telematiche. In tale ambito opera l'art.266-bis c.p.p., che estende la possibilità di disporre le intercettazioni telematiche non solo per i reati per cui si consentono le intercettazioni telefoniche (art.266 c.p.p.), ma anche per ogni reato commesso mediante l'utilizzo di strumenti informatici e telematici. Lo scopo di tali intercettazioni è quello di acquisire informazioni in transito da e verso il sistema informatico oggetto di indagine. Le modalità esecutive sono disciplinate dall'art. 268, comma 3-bis c.p.p. il quale dispone che "*quando si procede a intercettazione di comunicazioni informatiche o telematiche (266 bis), il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati*"[111] indipendentemente dalla sussistenza di ragioni di urgenza o di mancanza di impianti specifici presso la Procura della Repubblica. Allo scopo di preservare esigenze di riservatezza e correttezza, può risultare opportuno nominare un consulente tecnico con adeguate competenze.

Effettuando una specificazione più tecnica sulla materia, i moderni strumenti informatici consentono di acquisire i dati in transito attraverso la tecnica del "*sniffing*" che consiste nell'ascolto e nell'intercettazione dei flussi di dati scambiati tra due sistemi informatici, duplicandone poi le informazioni rilevanti. Tale tecnica, utilizzata in maniera illecita da *hacker* e *cracker*, può essere impiegata legittimamente dall'autorità giudiziaria ai fini investigativi collocando lo strumento di captazione nel

[109] Corona, *Reati informatici e investigazioni digitali: diffamazione via web, prove digitali, sex crimes, cyberstalking, cyberbullismo, reati privacy*, cit. p.31
[110] Pietropaoli, *Informatica criminale: diritto e sicurezza nell'era digitale,* cit., p. 34
[111]Codice di procedura penale. art.268 c.3-bis

punto di passaggio dei dati tra il dispositivo dell'indagato e il punto di connessione con la rete Internet.

Inoltre, non vi sono limiti ai dati che possono essere acquisiti: rientrano tra questi dati di transito, dati di navigazione nel web, email, chat. L'unico ostacolo operativo è rappresentato dai protocolli di sicurezza crittografici, quali HTTPS e SSL, che impediscono la decrittazione in tempo reale dei dati intercettati. Per tale motivo, in assenza del certificato con cui viene negoziato il protocollo sicuro, il contenuto della comunicazione resterà illeggibile e la decriptazione successiva risulterà molto complessa. Tuttavia, nonostante le difficoltà determinate dall'utilizzo di questi protocolli, la captazione permette comunque di identificare il punto di partenza del servizio, il server erogante e il servizio utilizzato. Inoltre il contenuto può comunque essere acquisito attraverso il sequestro del sistema informatico.

Le intercettazioni possono altresì essere effettuate direttamente sul *provider* al fine di individuare gli autori dell'illecito, tramite tecniche che consentono di filtrare solo le informazioni ritenute pertinenti ai fini dell'indagine. Tale metodologia è particolarmente utile per le indagini in materia di pedopornografica online, per le quali tra l'altro, la semplice connessione a siti contenenti materiale illecito già consisterebbe in consumazione del reato di cui all'art. 600 quarter c.p. La legge n. 547/1993 ha consentito di disporre intercettazione telematiche preventive in materia di criminalità organizzata; tale possibilità è stata successivamente estesa ai delitti con finalità di terrorismo con la legge n. 374/2001.

Infine, uno degli strumenti più discussi in questo contesto è quello del *Trojan horse*, un programma in grado di istallarsi in modo occulto su un dispositivo elettronico e di consentire l'acquisizione da remoto di dati, immagini e comunicazioni. L'utilizzo di tale strumento solleva dubbi circa la genuinità delle prove raccolte poiché il programma, modificando il sistema operativo, potrebbe potenzialmente alterare i dati oggetti d'indagine. Inoltre l'installazione da remoto potrebbe risultare complicata qualora il dispositivo sia dotato di un sistema *antivirus* o *firewall*, che ne rivelerebbero immediatamente la presenza. Nonostante tali criticità, il programma informatico risulta comunque utile per acquisire dati preesistenti nel dispositivo, consentendo di analizzare le attività pregresse dell'indagato, trattandosi di un'operazione che, a

differenza delle intercettazioni "*tradizionali*" rivolte a comunicazioni future o in corso, appare maggiormente assimilabile ad un'ispezione effettuata in via telematica. [112]

4.3 Coordinamento investigativo nazionale

Oltre alle novità introdotte con la legge del 2008, risulta necessario considerare gli interventi più recenti che hanno profondamente ridefinito l'architettura italiana della cybersicurezza. Un ruolo centrale è assunto dal decreto legge 14 giugno 2021, n.82 recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"* [113]. Tale normativa introduce per la prima volta la nozione di cybersicurezza nazionale all'art.1, c.1 lett.a definendola come *"l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico"*[114] [115].

Elemento di maggiore rilievo è l'istituzione della Agenzia per la Cybersicurezza Nazionale (ACN), ente di diritto pubblico dotato di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. Le funzioni attribuite all'Agenzia, ai sensi dell'art. 7 commi da 1 a 4, riguardano: il coordinamento dei soggetti pubblici coinvolti nella sicurezza informatica a livello nazionale, il supporto al Nucleo per la cybersicurezza, la predisposizione della strategia nazionale, la competenza in materia di accertamento delle violazioni e di irrogazioni delle relative sanzioni amministrative, l'esercizio del ruolo di autorità nazionale di certificazione, l' assunzione delle funzioni relative al perimetro di

---

[112] Amato. *I reati informatici: nuova disciplina e tecniche processuali di accertamento*. cit., pp. 146-151

[113] Decreto-Legge 14 giugno 2021, n. 82. *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.* Gazzetta Ufficiale n. 140 del 14 giugno 2021.

[114] Ivi. art.1, c.1, lett. a

[115] Rizzi, M. A., & Serini, F. (2024). *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*. Rivista Italiana di Informatica e Diritto, 6(2) p. 123

sicurezza nazionale cibernetica, lo sviluppo di capacità operative per la prevenzione, il monitoraggio, il rilevamento, l'analisi e la risposta agli incidenti di sicurezza informatica e agli attacchi informatici, anche attraverso il *Computer Security Incident Response Team – Italia*[116] ossia l'organo che si occupa di monitoraggio preventivo e di risposta agli incidenti informatici.

Il quadro normativo è stato ulteriormente arricchito dalla legge 28 giugno 2024, n.90 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"[117]. Essa rappresenta il punto di arrivo di un processo di adeguamento dell'ordinamento alle nuove vulnerabilità digitali e ai recenti standard europei. Tra i principiali argomenti si annoverano il perfezionamento della *governance* nazionale in materia di cybersicurezza tramite l'introduzione di obblighi più rigorosi a carico di enti pubblici e privati; l'introduzione di sanzioni specifiche volte a incentivare un'applicazione rigorosa delle disposizioni, la creazione della figura del referente per la cybersicurezza e la valorizzazione della crittografia come strumento fondamentale per la protezione dei dati[118].

Un aspetto particolarmente significativo della legge riguarda la possibilità di estendere ai più gravi delitti cibernetici l'applicabilità degli istituiti processuali tipici del nostro sistema antimafia quali l'inasprimento delle pene edittali, la possibilità di svolgere intercettazioni con regime semplificato, la semplificazione del regime delle indagini preliminari, nonché una più stretta cooperazione tra il pubblico ministero e ACN. Tale cooperazione è finalizzata a garantire il coordinato esercizio sia delle funzioni di resilienza, sia delle funzioni investigative volte alla raccolta delle prove digitali.

Proseguendo in questa direzione, in tema di coordinamento investigativo, la novità di maggiore rilievo riguarda quanto definito dal comma 4-bis dell'art 371-bis

---

[116] Servizio Bilancio dello Stato. (2021, luglio 14). *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale* (Atto Camera n. 3161). Camera dei Deputati – Dossier VQ3161.

[117] Legge 28 giugno 2024, n. 90: *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*. Gazzetta Ufficiale n. 153 del 2 luglio 2024.

[118] Calì, S., Capparelli, F., Hazan, M., Martini, F., & Razzante, R. (2025). *Cybersecurity: tra rischio e responsabilità: profili operativi in un settore in continua evoluzione*. Giuffrè Francis Lefebvre. pp.85-91

c.p.p. che, per effetto della legge 137/2023, ha attribuito al Procuratore Nazionale Antimafia e Antiterrorismo una funzione di impulso in materia di indagini sui reati informatici. In questo modo, il quadro normativo colloca la Direzione Nazionale Antimafia e Antiterrorismo (DNAA) al centro del sistema di contrasto ai crimini informatici.

Ciò che risulta decisivo per rendere realmente efficace la dimensione giudiziaria del contrasto agli attacchi malevoli nel cyberspazio è la collaborazione tra DNAA e ACN. È stato infatti compreso che limitarsi a una visione esclusivamente giudiziaria e procedurale dei reati informatici, trascurandone le specifiche caratteristiche tecniche e le dinamiche operative, risulta non funzionale alla loro repressione. Un'azione repressiva efficace impone un raccordo tra funzioni di sicurezza e funzioni di direzione delle indagini

In questo senso, il coordinamento tra Direzione nazionale antimafia, Procuratore nazionale antimafia e le procure distrettuali, ACN e gli altri attori istituzionali coinvolti, quali il servizio di polizia postale e il Ministero della giustizia, consente di perseguire simultaneamente obiettivi di accertamento dei fatti e delle responsabilità sul piano investigativo, e finalità di ripristino delle vulnerabilità create dagli attacchi cibernetici.

Si deve naturalmente tenere conto, in questa evoluzione prospettica, di alcune criticità strutturali del sistema nazionale: il mancato allineamento tecnologico rispetto alla rapidità evolutiva della criminalità informatica e la difficoltà di usufruire, nell'ambito internazionale, della cooperazione tanto di Paesi al di fuori dell'UE o di trattati vincolanti, quanto dei colossi mondiali delle tecnologie, restii alla pratica della "*voluntary disclosure*"[119].

[119] Melillo, G. (2024, March 22). *Audizione del Procuratore Nazionale Antimafia e Antiterrorismo Giovanni Melillo – In materia di rafforzamento della cybersicurezza nazionale e reati informatici* [Audizione, Riunione delle Commissioni Affari Costituzionali e Giustizia, Camera dei Deputati]. Camera dei Deputati WebTV.

Capitolo II.

Le operazioni sotto copertura nei reati informatici: evoluzione normativa e prassi applicativa

Sommario: 1. Natura e fondamento giuridico delle operazioni sotto copertura 1.1 Quadro giuridico italiano in materia di operazioni sotto copertura 1.2 Legge 137/2023: modifica in senso estensivo della L. n. 146/2006 1.3 Coordinamento a più livelli: l'architettura nazionale per la cybersicurezza e il coordinamento con ENISA 1.3.1 Coordinamento a più livelli: raccordo interistituzionale tra piano operativo-strategico e piano investigativo-giudiziario 2. La cooperazione di *law enforcement* per il contrasto di crimini extraterritoriali 2.1 Le forme di cooperazione internazionale nelle operazioni *undercover* 2.2 L'ordine europeo d'indagine e le operazioni sotto copertura 2.4 Le modalità di collaborazione e supporto investigativo transnazionale: il contributo di INTERPOL, Europol ed Eurojust 3. Tecniche investigative e strumenti applicativi nelle operazioni sotto copertura digitali 3.1 Operazioni transnazionali significative nel contrasto ai reati informatici

1. Natura e fondamento giuridico delle operazioni sotto copertura

La figura dell'agente sotto copertura non è una scoperta recente. Le sue origini risalgono al periodo storico dell'assolutismo francese del XVII secolo nel quale i delatori privati scoprivano così l'avversione politica dei cittadini[120]. Il fenomeno trovò ampio utilizzo anche negli Stati Uniti d'America dove le attività sotto copertura, in quanto non funzionali al controllo sociale e politico, si affermarono quale strumento di repressione prettamente criminale[121].

Le operazioni sotto copertura rientrano tra le cosiddette "*special investigation techniques*", vale a dire tecniche di indagine non convenzionali che hanno progressivamente ottenuto una regolamentazione prima nell'ordinamento statunitense, poi a livello internazionale ed europeo, e infine nell'ordinamento italiano. Tali normative risultano finalizzate a contrastare fenomeni criminosi su cui la pubblica opinione manifesta un progressivo allarme sociale rendendo necessaria l'esigenza di contrasto. Ci si riferisce in particolare alla repressione della criminalità organizzata,

[120] Curtotti, D. (2015). *Operazioni sotto copertura*. In B. Romano (a cura di), *Le associazioni di tipo mafioso*. UTET giuridica. p. 427.
[121] Melillo, G. (2003). *Le operazioni sotto copertura nelle indagini relative a delitti con finalità di terrorismo*. In G. Di Chiara (a cura di), *Il processo penale tra politiche di sicurezza e nuovi garantismi* Torino: Giappichelli. p. 34.

alla corruzione e alla pedopornografia[122]. Tali tecniche speciali si caratterizzano per un ambito di applicazione ridotto, strettamente correlato alla peculiare esigenza investigativa e per un elevato grado di invasività nei diritti fondamentali dei soggetti indagati[123].

Nonostante non ci sia una definizione normativa di operazioni sotto copertura la locuzione indica comunemente " *un complesso di attività investigative nelle quali una persona- un ufficiale di polizia giudiziaria o un privato cittadino- celando la propria identità, si infiltra all'interno di organizzazioni criminali allo scopo di scoprirne la struttura, sottrarle risorse essenziali , denunciare i partecipanti*"[124].

Lo strumento investigativo oggetto di studio è, per sua natura, anomalo e non esente da critiche; esso opera ai confini della liceità e per tale ragione è opportuno tracciare i limiti entro cui le condotte dell'agente sotto copertura possono ritenersi giustificate e valutare le correlate implicazioni sul piano processuale. Difatti, al di fuori del contesto in cui opera l'esimente, il soggetto incorrerebbe in responsabilità penali, e potrebbero determinarsi potenziali violazioni delle garanzie processuali dell'imputato.

Ulteriori aspetti problematici riguardano: l'individuazione del punto di equilibrio tra le esigenze di difesa e sicurezza nazionale e la tutela dei diritti dell'imputato, l'inserimento di questa disciplina come aspetto sostanziale o processuale e le difficoltà di inserire queste pratiche investigative in un quadro normativo specifico e determinato di comportamento e attività[125].

1.1 Quadro giuridico italiano in materia di operazioni sotto copertura

Per lungo tempo prive di una disciplina nell'ordinamento interno, le operazioni sotto copertura hanno fatto ingresso nella legislazione nazionale a partire dagli anni Novanta del secolo scorso. La disciplina è nata nell'ambito della legislazione speciale in attuazione di programmi anticrimine tesi ad inasprire la risposta dell'ordinamento a fenomeni criminosi che sollevavano particolare allarme sociale.

---

[122] Curtotti, D. *Operazioni sotto copertura*. cit. p. 428.
[123] Bronzo, P. (2025). *Le operazioni sotto copertura nel web*. In *Indagini e prove nella società digitale. Questioni attuali e prospettive future* (ISBN 979-12-235-0292-1) pp.173.
[124] Curtotti, D. *Operazioni sotto copertura*. cit. p. 429
[125] Ivi pp. 427-430

In ragione della peculiarità di queste tecniche investigative, necessarie ma da adottare con estrema cautela, si è delineato un quadro iniziale disorganico in materia[126]. Infatti, se inizialmente nella prassi investigativa si palesava da tempo la necessità di strumenti investigativi non convenzionali, quando le norme furono introdotte le stesse mancarono di disciplinare tutti i nodi problematici relativi alla dimensione processuale dell'attività sotto copertura. Si pensi alla questione della punibilità dell'agente provocatore o all'utilizzabilità processuale delle dichiarazioni raccolte nell'attività di investigazione[127].

Un primo passo verso una razionalizzazione e sistemazione organica della materia è rappresentato dalla legge 16 marzo 2006, n.146[128], attuativa della Convenzione di Palermo contro la criminalità organizzata transnazionale[129], successivamente modificata dalla legge n.136 del 2010[130]. La nuova disciplina assorbì le preesistenti disposizioni settoriali all'interno dell'art.9 per eliminare le profonde incertezze della materia che risultavano sia sul piano interpretativo che su quello applicativo. Tuttavia, l'obiettivo di porre fine ad una " stratificazione normativa" non fu del tutto raggiunto essendo sopravvissute le previsioni specifiche relative al personale dei servizi di informazione per la sicurezza e il settore dei giochi e quelle dettate per il contrasto dello sfruttamento sessuale dei minori[131].

La legge 146/2006, come modificata nel 2010, definisce tuttora la disciplina più compiuta in materia di operazioni sotto copertura. L'articolo 9 detta una particolare causa di giustificazione affermando che, fermo restando quanto disposto dall'art.51 c.p. "*non sono punibili gli ufficiali di polizia giudiziaria della Polizia di Stato, dell'Arma dei Carabinieri e del Corpo della guardia di finanza, appartenenti alle*

---

[126] Scalfati, A. (2019). *Operazioni digitali sotto copertura*. In *Le Indagini Atipiche /*. G. Giappichelli Editore. p. 623

[127] Melillo, G. *Le operazioni sotto copertura nelle indagini relative a delitti con finalità di terrorismo*. cit. p. 38

[128] Legge 16 marzo 2006, n. 146. *Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro la criminalità organizzata transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001.* Gazzetta Ufficiale n. 85 del 11 aprile 2006. art.9

[129] United Nations. (2000). *United Nations Convention against Transnational Organized Crime*.

[130] Legge 13 agosto 2010, n. 136. *Piano straordinario contro le mafie, nonché delega al Governo in materia di antimafia. Disposizioni sulla tracciabilità dei flussi finanziari.* Gazzetta Ufficiale n. 196 del 23 agosto 2010.

[131] Scalfati, A. *Operazioni digitali sotto copertura*. cit. p. 623-627

strutture specializzate o alla DIA, e anche gli ausiliari o loro interposte persone, quando danno rifugio, prestano assistenza agli associati, acquistano, ricevono, sostituiscono od occultano denaro, armi, documenti, sostanze stupefacenti o psicotrope, o altrimenti ostacolano l'individuazione della loro provenienza o ne consentono l'impiego o compiono attività prodromiche e strumentali"[132]. Tale esimente opera esclusivamente per determinate operazioni di polizia finalizzate all'acquisizione di prove per reati specificamente determinati nell'articolo e purché le attività, secondo lo schema elaborato precedentemente dal d.l. 374/2001, siano state disposte da organi di vertice previa comunicazione senza ritardo all'autorità giudiziaria competente dei soggetti coinvolti e delle modalità di impiego. In riferimento a quest'ultime l'agente *undercover* può utilizzare documenti, identità fittizie e avvalersi di beni mobili o immobili indispensabili ai fini dell'operazione[133].

Passando ad analizzare l'evoluzione delle operazioni sotto copertura nell' ambiente digitale, la stessa va di pari passo con quelle finora descritte. La figura del *cyber*-agente è comparsa per la prima volta in materia di contrasto alla prostituzione, pornografia e turismo sessuale in danno ai minori, primi ambiti nei quali si sono sfruttate le potenzialità del cyberspace per compiere reati. Infatti ai sensi dell'art.14 comma 2 della legge n.269/1998[134] si prevedeva che l'organo del Ministero dell'interno per la sicurezza e la regolarità delle telecomunicazioni, ossia la Polizia Postale, potesse eseguire, su richiesta dell'autorità giudiziaria, le attività sotto copertura occorrenti nell'ipotesi in cui i delitti siano commessi con l'impiego di sistemi informatici o mezzi di comunicazione telematica. Le attività sotto copertura potevano consistere in attivazione di siti nelle reti, nella realizzazione e gestione di aree di comunicazione e scambio, nella partecipazione a sistemi telematici, nell'acquisto di materiale pornografico e nella simulata partecipazione o intermediazione ad iniziative turistiche volte allo sfruttamento della prostituzione minorile[135].

Il riordino normativo operato dalla legge 146/2006 ha inciso anche sul piano digitale. Sebbene non abbia eliminato integralmente la disciplina preesistente di cui

[132] Curtotti, D. *Operazioni sotto copertura*. cit. pp. 436-437
[133] Ibidem
[134] Legge 3 agosto 1998, n. 269. *Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*. Gazzetta Ufficiale della Repubblica Italiana, n. 185 del 10 agosto 1998
[135] Scalfati, A. *Operazioni digitali sotto copertura*. cit. p. 624

alla legge 269 del 1998, la normativa ha esteso la possibilità di utilizzare documenti, identità e indicazioni sotto copertura anche ai fini dell'infiltrazione in reti di comunicazione, con obbligo di tempestiva informazione al pubblico ministero e comunque non oltre le quarantotto ore successive all'inizio dell'attività. Si è inoltre prevista la possibilità di attivare cosiddetti "siti civetta" e di realizzare e gestire comunicazioni e scambi nelle reti e nei sistemi informatici[136].

Si deve notare che se da un lato la disciplina della legge 146/2006 ha contribuito a legittimare tale mezzo di investigazione, dall'altro ne ha progressivamente attenuato la sua natura originaria di attività eccezionale e residuale. Invero viene sempre più adottato per la sua eccezionale efficacia più che per la sua necessità e questo lo si riscontra con particolare evidenza nelle successive estensioni normative quale, ad esempio, la l. 9 marzo del 2022 n.22 in tema di attività sotto copertura nei reati di traffico di beni culturali. La sua eccessiva diffusione ha però consentito l'affinamento e la modernizzazione delle tecniche di investigazione sotto copertura soprattutto nel contesto del cyberspace sempre più teatro e strumento di attività criminali[137].

1.2 Legge 137/2023: modifica in senso estensivo della L. n. 146/2006

È solo con la legge n.137/2023[138] che ha convertito il d.l. 105/2023, che si introducono rilevanti modifiche all'art.9 della l.n.146/2006 in tema in investigazioni digitali sotto copertura. Se ne enfatizza il ruolo sia con riferimento ai "*reati commessi con finalità di terrorismo o di eversione*" che per "*i reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale*"[139]. La normativa riconosce all'agente sotto copertura alcuni poteri

[136] Ivi p. 628
[137] Bronzo P. *Le operazioni sotto copertura nel web*. cit. pp.177-178
[138] Legge 9 ottobre 2023, n. 137: *Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 104, recante disposizioni urgenti a tutela degli utenti, in materia di attività economiche e finanziarie e investimenti strategici*. Gazzetta Ufficiale della Repubblica Italiana, n. 236, 9 ottobre 2023.
[139] Ciampi, S. (2024). *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*. Processo Penale e Giustizia: Rivista di dottrina e giurisprudenza, (3). p.726

operativi nel mondo digitale. Allo stesso è consentito di introdursi nel sistema informatico, di alternare o danneggiare il suo funzionamento nonché di cancellare dati e programmi in esso contenuti. È altresì ammessa l'attivazione di identità digitali fittizie, la creazione di domini o spazi informatici utilizzando dati simulati o dati reali ma appartenenti a terzi e il compimento di attività prodromiche e strumentali ai fini investigativi. Le operazioni devono essere disposte da organi di vertice "*al solo fine di acquisire elementi di prova in ordine ai delitti commessi*" e devono essere immediatamente e dettagliatamente comunicate al pubblico ministero competente per le indagini e, nei casi di cui agli art.51 c.3 bis e 3 quater e 371-bis comma 4-bis c.p.p., al Procuratore Nazionale Antimafia e Antiterrorismo[140].

L'analisi della normativa evidenzia come il legislatore abbia adottato una scriminante complessiva in relazioni a fattispecie tipiche di reati informatici. Essa copre le condotte lesive dei sistemi telematici o informatici come le condotte dannose dei loro contenuti, legittimando azioni demolitorie ma anche interventi volti ad acquisire in maniera occulta dati attraverso la copia e l'archiviazione degli stessi. Esula invece dall'ambito applicativo della disciplina l'attività di mero monitoraggio della rete nei casi in cui la stessa si risolva nelle osservazioni di contenuti visibili alla generalità di utenti, anche se finalizzata alla raccolta e analisi di informazioni[141].

Di fatto, attraverso tale legge si supera il modello dell'*undercover* basato esclusivamente sulla costruzione di identità fittizie da poter infiltrare in contesti criminali virtuali, prevedendosi attività proattive che consentono di effettuare veri e propri attacchi informatici con l'esclusiva finalità di acquisire elementi di prova[142].

A tal proposito, è stata realizzata un'intervista con il Prefetto Bruno Frattasi, Direttore Generale dell'Agenzia per la cybersicurezza nazionale che ha ribadito la centralità delle operazioni *undercover* nel contrasto alla criminalità informatica. Ad avviso di Frattasi questi strumenti consentono un approccio proattivo negli ambienti digitali nei quali le minacce vengono a formarsi e ad operare.

---

[140] Ivi. pp.767-729

[141] Ciampi, S. *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*. cit. p.730

[142] Gabrielli, I. (2025, 6 dicembre). Intervista condotta dall'autore. Intervista non pubblicata.

Tale fondamentale attività si realizza a livello tecnico nel cosiddetto *deep* e *dark web*, in forum chiusi, piattaforme di messaggistica cifrata e *marketplace* illeciti, nei quali l'anonimato e le tecniche di offuscamento rendono complesso l'impiego degli ordinari strumenti investigativi. Le tecniche *undercover* consentono invece, in ambiti così oscuri del cyberspazio, la raccolta di informazioni in tempo reale, favorendo la possibilità di anticipare gli effetti di azioni illecite e di individuare vulnerabilità contribuendo al rafforzamento delle capacità di prevenzione e di *early warning.*

Sotto il profilo strategico, le operazioni sotto copertura costituiscono un fondamentale meccanismo per l'identificazione e il perseguimento dei singoli responsabili e, al contempo, per la ricostruzione delle dinamiche operative e delle infrastrutture di comando e di controllo delle organizzazioni illegali transnazionali. Dall'analisi di questi due profili, ne deriva che le operazioni sotto copertura si differenziano dalle attività di *cyber-defence*, che sono prettamente tecniche e orientate alla protezione perimetrale, al monitoraggio e alla risposta agli incidenti. Le operazioni invece consentono un meccanismo di intervento a monte volto ad ottenere informazioni utili per indentificare le tecniche, tattiche e procedure utilizzate nel cyberspazio per commettere reati.

In questa prospettiva, il Prefetto Frattasi sostiene che tali strumenti investigativi speciali si inseriscono in un approccio di sicurezza cibernetica "*integrata*" che combina misure difensive, capacità investigative e strumenti di cooperazioni giudiziaria e di polizia a livello internazionale.

Ne consegue che le operazioni sotto copertura non si pongono in alternativa alle attività di difesa cibernetica ma si ritrovano con esse in un meccanismo che ne garantisce l'assoluta complementarietà e interdipendenza. Questo perché, nonostante la riconducibilità all'ambito repressivo e investigativo, le attività dell'agente *undercover* producono un patrimonio informativo che, nei limiti di condivisione consentiti dall'ordinamento, può rafforzare le capacità di prevenzione e risposta degli attori deputati alla sicurezza nazionale cibernetica[143].

[143]Frattasi, B. (2025, 6 dicembre). Intervista condotta dall'autore. Intervista non pubblicata.

1.3 Coordinamento a più livelli: l'architettura nazionale per la cybersicurezza e il coordinamento con ENISA

In un'ottica complessiva per comprendere lo sviluppo di un sistema integrato di protezione e sicurezza nazionale è necessario riferirsi ad una visione a più livelli volta al perseguimento di finalità comuni.

A tal fine, è stato svolto un approfondimento attraverso interviste al Procuratore Nazionale Antimafia e Antiterrorismo Giovanni Melillo, al Prefetto Bruno Frattasi, Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale e al Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica, Ivano Gabrielli.

Nella prospettiva multilivello si colloca l'architettura nazionale per la cybersicurezza, fondata su quattro pilastri tra loro interconnessi che concorrono unitariamente al perseguimento della sicurezza nazionale nello spazio cibernetico. L'architettura così delineata è particolarmente efficace perché consente di definire chiaramente i ruoli e le responsabilità dei diversi attori coinvolti.

Il primo pilastro riguarda la cybersicurezza e la resilienza di cui si occupa in via primaria l'ACN. Ad essa competono le funzioni di prevenzione, regolazione, supporto agli operatori pubblici e privati, gestione tecnica degli incidenti e rafforzamento della capacità di resistenza e recupero in conformità con gli obblighi derivanti dalla direttiva NIS2[144] e dalla Direttiva CER[145].

Il secondo pilastro relativo alla prevenzione e al contrasto della criminalità informatica è affidato alle Forze di Polizia, che operano per l'individuazione di autori dei reati e per il contrasto a forme di criminalità organizzata transnazionale che si insinuano nello spazio cibernetico.

Occorre evidenziare, in tale ambito, l'imprescindibile ruolo del Servizio di Polizia Postale e per la Sicurezza Cibernetica quale Autorità Nazionale di Pubblica Sicurezza nello spazio cibernetico e il tendenziale monopolio che ad essa viene riservato in materia di indagini sotto copertura nella rete.

---

[144] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, L 333, 1–116.

[145] European Union. (2022). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities*. Official Journal of the European Union, L 333, 164–201.

Il Servizio si articola in cinque divisioni. La Prima, affidata al Commissariato di P.S. online svolge funzioni strategiche di coordinamento operativo, definisce programmi formativi e funzioni di presidio. La Seconda Divisione opera attraverso il Centro Nazionale per il Contrasto della Pedopornografia Online (C.N.C.P.O.), destinato alla tutela dei minori e dei soggetti vulnerabili.

La Terza Divisione è affidata al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), introdotto con il d.l. 144/2005[146] che, ad oggi gestisce la minaccia cibernetica di matrice comune, organizzata e terroristica, coordinando la rete dei Nuclei Operative di Sicurezza Cibernetica (N.O.S.C.), presenti nei 18 Centri Operativi della Polizia Postale (C.O.S.C.)[147].

Le principali innovazione introdotte per la protezione delle infrastrutture critiche riguardano sia la realizzazione di una Sala operativa, disponibile 24/7, la quale costituisce un punto di contatto, a livello nazionale e internazionale, per gli attori coinvolti nella protezione delle infrastrutture critiche, sia la predisposizione di collegamenti telematici esclusivi e non accessibili tra il C.N.A.I.P.I.C. e le infrastrutture critiche, funzionali allo scambio di informazioni necessarie ai fini della prevenzione e repressione dei crimini informatici[148].

Infine, la Quarta Divisione è posta a presidio delle minacce economico-finanziarie, mentre la Quinta garantisce il supporto tecnico ai fini delle indagini[149].

Al terzo pilastro compete la difesa e la sicurezza militare dello Stato demandata al Ministero della Difesa. Ad esso è affidata la salvaguardia degli interessi nazionali nel dominio cibernetico divenuto, a tutti gli effetti, spazio tradizionale di potenziali attacchi ostili.

Il quadro e ultimo pilastro è gestito dagli Organismi di informazione e sicurezza e si concentra sull'analisi, ricerca ed elaborazione informativa che

[146] Decreto-legge 27 luglio 2005, n. 144*: Misure urgenti per il contrasto del terrorismo internazionale*. Convertito con modificazioni dalla Legge 31 luglio 2005, n. 155. Gazzetta Ufficiale della Repubblica Italiana, n. 176, 30 luglio 2005.

[147] Gabrielli, I. Intervista condotta dall'autore. Intervista non pubblicata.

[148] Commissariato di Polizia Postale e delle Comunicazioni. *Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC).*

[149] Polizia di Stato. (2025). *Report annuale 2025* per la tutela dei diritti. Servizio di Polizia Postale e per la Sicurezza Cibernetica.

consentono di comprendere le minacce e le intenzioni degli attori ostili supportando il decisore politico mediante valutazioni anticipatorie dei rischi.

L'integrazione funzionale della architettura così delineata è assicurata da meccanismi interistituzionali tra i quali il Nucleo per la cybersicurezza (NCS) che rappresenta il fulcro gestionale di politiche di prevenzione, preparazione e risposta alle minacce cibernetiche integrando la dimensione politico-strategico con quella tecnico-operativa. I compiti affidati al NCS attengono sia alla fase di prevenzione e di preparazione rispetto a possibili scenari di crisi, sia alla attivazione di procedure di allertamento e di coordinamento in caso di attacchi cibernetici significativi. In qualità di meccanismo di coordinamento, NCS garantisce un dialogo continuo e strutturato tra gli attori coinvolti, favorendo la condivisione di informazioni e valutazioni di rischio e sviluppando una partecipazione con tutti gli stakeholders privati e pubblici rilevanti.

Un ruolo centrale è svolto anche dall'Agenzia per la Cybersicurezza Nazionale che opera come punto di sintesi tra esigenze di sicurezza nazionale nello spazio cibernetico e sviluppo di un ecosistema digitale resiliente. L'ACN invero, non solo coordina la gestione degli incidenti cyber in sinergia con il CSIRT Italia, ma esercita una funzione di indirizzo nell'attuazione della Strategia nazionale per la cybersicurezza e del relativo piano di implementazione. A tal proposito definisce i requisiti di sicurezza, supervisiona i soggetti essenziali e supporta le amministrazioni pubbliche e gli operatori privati strategici. Tali funzioni risultano coerenti con il quadro normativo nazionale ed europeo che valorizza modelli di governance strutturati, accentrati e capaci di stabilire un'unitarietà di indirizzo e una rapidità decisionale necessaria nella gestione di crisi cibernetiche. Nei primi anni di operatività dell'ACN, si è compreso come la questione "cybersicurezza" non potesse essere considerata solo dal punto di vista della gestione tecnica, ma dovesse essere reputata una componente strutturale della sicurezza del Paese.

Dal punto di vista della *governance* europea, l'architettura nazionale si inserisce nei meccanismi delineati nella raccomandazione del Consiglio dell'Unione Europea denominato "Cyber Blueprint"[150], che delinea un quadro di riferimento per la gestione coordinata delle crisi cibernetiche definendo principi, fasi di intervento e

[150] Council of the European Union. (2025, June 6). *Recommendation on the Cyber Blueprint for coordinated response to major cross-border cyber crises*.

meccanismi di cooperazione tra i diversi livelli istituzionali. L'obiettivo principale è l'allineamento delle politiche degli Stati Membri per favorire una gestione della crisi cibernetica fondata su procedure condivise e su una logica di solidarietà e impegno comune. La struttura di coordinamento italiana risponde perfettamente a questa modello poiché vi è una struttura centrale identificata e rappresentata dall'ACN, in grado di coordinare gli attori nazionali coinvolti nella gestione della crisi.

Nell'attuazione delle politiche di cybersicurezza, riveste un ruolo imprescindibile il coordinamento con ENISA che rappresenta un punto di riferimento dell'Unione Europea con funzioni di supporto agli Stati membri, di produzione di analisi strategiche e di facilitazione della collaborazione operativa. Il coordinamento tra ACN ed ENISA consente di rafforzare l'interoperabilità tra le istituzioni e la coerenza nelle risposte nazionali attraverso l'adozione di politiche tecniche e scambi di conoscenze comuni. Inoltre, sempre nel contesto della raccomandazione "*Cyber Blueprint*", ENISA svolge la funzione di *hub* tecnico, favorendo la condivisione tempestiva di informazione e di *best practices* tra le autorità nazionali e i CSIRT. Di conseguenza il dialogo strutturato con ENISA rappresenta per l'ACN non solo un canale di supporto tecnico, ma anche uno strumento di allineamento strategico alle politiche europee e di rafforzamento della credibilità e dell'efficacia dell'azione nazionale[151].

1.3.1 Coordinamento a più livelli: raccordo interistituzionale tra piano operativo-strategico e piano investigativo- giudiziario

L'emersione di gravissimi illeciti correlati allo sfruttamento abusivo di banche dati strategiche ha reso necessaria il potenziamento delle capacità di analisi e di indirizzo unitario delle investigazioni. Per tale fondamentale ragione è stata attribuita al Procuratore Nazionale Antimafia e Antiterrorismo un ruolo di coordinamento delle indagini in materia di sicurezza cibernetica. Risulta infatti impensabile l'assenza un centro di coordinamento tra le procure volto a mettere in comune le conoscenze, posto che la distribuzione territoriale delle banche dati di interesse strategico, senza un raccordo informativo centralizzato, determinerebbe la dispersione di risorse investigative su reati e autori identici. Il nuovo ruolo del PNAA consente di mettere a

[151] Frattasi, B. (2025, 6 dicembre). Intervista condotta dall'autore. Intervista non pubblicata.

disposizione il valore aggiunto delle banca dati nazionali non solo per le acquisizioni investigative riferite a delitti di mafia e di terrorismo, ma anche per le indagini in materia di *cybercrime*, formando un patrimonio conoscitivo rilevante anche per fenomeni criminosi tradizionali.

Tale funzione di coordinamento acquisisce altresì rilievo anche dal punto di vista internazionale. Quando una minaccia colpisce diversi Paesi diventa fondamentale avviare forme di cooperazione fra Stati per comprendere la natura, le modalità e la portata degli attacchi. In questo contesto un coordinamento interno è imprescindibile, in quanto sarebbe inefficace che le Autorità giudiziarie nazionali si presentassero con richieste di cooperazione non coordinate. A tal proposito il Procuratore Nazionale Antimafia e Antiterrorismo afferma che "*non vi è nulla di peggio per le sorti della cooperazione internazionale del trasferimento sul piano del rapporto con gli altri Stati del peso di un insufficiente coordinamento interno*".

Per tali ragioni la funzione di coordinamento affidata alla Direzione Nazionale Antimafia e Antiterrorismo assume un'importanza strategica nella repressione di quei fenomeni criminosi caratterizzati da diffusività e transnazionalità per i quali il coordinamento non è solo utile ma anche indispensabile. Tali tendenze si presentano con ordini di priorità basati su tradizioni istituzionali diverse, anche in altri Stati: si pensi all'esperienza francese dove la tradizionale pluralità dei centri decisionali giudiziari è stata attenuata con l'inserimento di uffici di coordinamento nazionale dapprima in materia di terrorismo, successivamente in riferimento al *cybercrime* e da ultimo in materia di criminalità organizzata.

Le condotte criminali che colpiscono i sistemi informatici e le banche dati di interesse nevralgico pongono problematiche di varia natura. Innanzitutto occorre, in tempi estremamente rapidi, provvedere all'immediato ripristino delle funzioni informatiche interrotte, sempre più essenziali per la vita delle istituzioni e dei cittadini. Si deve altresì considerare l'aspetto prettamente investigativo poiché dall'analisi dei sistemi violati possono emergere elementi utili per il celere avvio delle indagini e l'identificazione dei responsabili ed anche per prevenire eventuali reiterazioni delle condotte criminose. Da ciò discende l'esigenza di un coordinamento tra attività di resilienza e quelle prettamente investigative, in modo tale da consentire la simultanea operatività, senza interferenze, dell'Agenzia per la cybersicurezza nazionale e della

polizia postale, sotto il coordinamento dalla procura competente[152]. A tal fine, quanto mai opportuno è stato l'inserimento del comma 4-bis nell'articolo 371-bis del c.p.p. che ha rafforzato il coordinamento istituzionale tra l'Autorità giudiziaria, in particolare la Direzione Nazionale Antimafia e Antiterrorismo, e l'Agenzia per la cybersicurezza nazionale.

La disposizione, infatti, estende le funzioni di impulso e coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo ai procedimenti relativi a delitti informatici e telematici quando gli stessi presentano profili di particolare gravità, serialità, organizzazione e impatto sistemico o risultano connessi a finalità di terrorismo, eversione o criminalità organizzata. Attraverso tale estensione si consente alla Direzione Nazionale Antimafia e Antiterrorismo di svolgere un ruolo di raccordo tra procure distrettuali e soggetti istituzionali competenti in materia di cybersicurezza, prima fra tutti l'ACN, realizzando così una sinergia strutturata tra livello operativo-strategico e livello investigativo-giudiziario funzionale a fornire una risposta efficace dell'ordinamento al fenomeno del *cybercrime*.

In questo ambito, la legge 90/2024[153] ha disciplinato i rapporti tra l'ACN, il Procuratore Nazionale Antimafia e Antiterrorismo, la Polizia giudiziaria e il pubblico ministero introducendo un sistema di flusso continuo di informazioni per consentire l'interoperabilità tra le istituzioni.

Dal punto di vista operativo, si prevede che l'ACN informi senza ritardo il Procuratore Nazionale Antimafia e Antiterrorismo di un attacco ai sistemi informatici o telematici di cui all'art.371-bis c.4 bis c.p.p. e, in ogni caso, qualora l'attacco sia indirizzato nei confronti di soggetti del perimetro di sicurezza nazionale cibernetica (PSNC), di operatori di servizi essenziali e fornitori di servizi digitali (Soggetti NIS) e di imprese che forniscono reti pubbliche o servizi di comunicazione elettronica accessibili al pubblico (soggetti TELCO).

La cooperazione si instaura anche mediante l'iniziativa del pubblico ministero che, quando acquisisce la notizia di reato relativa a gravi delitti informatici, deve darne tempestiva informazione all'ACN e assicurare il raccordo informativo con l'organo

[152] Melillo, G. (2025, 6 dicembre). Intervista condotta dall'autore. Intervista non pubblicata.
[153] Legge 28 giugno 2024, n. 90: *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*. Gazzetta Ufficiale della Repubblica Italiana, n. 153, 2 luglio 2024.

centrale del Ministero dell'Interno competente per la sicurezza e la regolarità dei servizi di telecomunicazioni. Inoltre il p.m. deve svolgere le indagini tenendo conto e garantendo le attività di ripristino svolte dall'Agenzia, eventualmente differendole per evitare un grave pregiudizio per il corso delle indagini; è altresì tenuto a informare l'ACN per consentire la sua partecipazione agli accertamenti tecnici irripetibili per i delitti cibernetici previsti dalla norma[154].

Si prevede inoltre la possibile partecipazione del Procuratore Nazionale Antimafia e Antiterrorismo alle riunioni del Comitato Interministeriale per la Sicurezza della Repubblica (CISR). Ciò a dimostrazione dell'innovativo sistema di condivisione che di fatto garantisce la sicurezza cibernetica a livello nazionale mediante il concorso dei soggetti sopramenzionati. Acquisisce inoltre rinnovata importanza l'art.118-bis c.p.p. intitolato "*Richiesta di copie di atti e di informazioni da parte del Presidente del Consiglio dei Ministri*"[155]. Tale norma prevede la possibilità che il Presidente del Consiglio dei Ministri, anche in deroga alle disposizioni concernenti il segreto di Stato, possa richiedere all'autorità giudiziaria competente il rilascio di copie di atti di procedimenti penali e informazioni sul loro contenuto per esigenze connesse al Sistema di informazioni per la sicurezza della Repubblica[156].

In conclusione, l' estensione delle funzioni della DNAA consente di interpretare tali fenomeni delittuosi cibernetici non come atti isolati ma come fattispecie complesse, strutturate e talvolta transnazionali che richiedono una risposta integrata in ossequio alle finalità perseguite dal quadro normativo nazionale ed europeo[157].

2. La cooperazione di *law enforcement* per il contrasto di crimini extraterritoriali

Il diritto internazionale, prevedendo il principio di sovranità statale, sancisce la giurisdizione territoriale degli Stati imponendo alle parti il divieto di esercitare, al di fuori del proprio territorio, funzioni giurisdizionali o funzioni riservate esclusivamente

[154] Frattasi, B. Intervista condotta dall'autore. Intervista non pubblicata.
[155] Codice di procedura penale. Gazzetta Ufficiale della Repubblica Italiana. art. 118-bis
[156] Gabrielli, I. Intervista condotta dall'autore. Intervista non pubblicata.
[157] Frattasi, B. Intervista condotta dall'autore. Intervista non pubblicata.

alle autorità dello Stato territorialmente competente[158]. Questo significa che, in assenza di norme definite dalla consuetudine o dalle convenzioni internazionali, uno Stato che esercita unilateralmente la giurisdizione extraterritoriale agisce in modo illecito[159]. Di conseguenza, qualora uno Stato sia tenuto a procedere a indagini per procurarsi prove necessarie ai fini dell'accertamento del reato e queste si possano rinvenire nel territorio di un altro Stato, si devono necessariamente attivare meccanismi di cooperazione internazionale. È bene specificare che non si tratta di un ipotesi di conflitto di legge per la quale bisogna stabilire la normativa applicabile, bensì, ai fini della cooperazione, lo Stato che ha giurisdizione la esercita come fonte di ausilio per le necessità procedurali di un altro Stato[160]. In questo senso il diritto penale transnazionale ha la funzione di stabilire norme generali per regolare le modalità con cui la cooperazione deve essere effettuata, stabilendo procedure formali, informali e forme di collaborazione spontanea.

Nella fase iniziale delle indagini, la cooperazione si instaura prevalentemente tra le forze di polizia. Questa forma di assistenza reciproca si differenzia da quella tradizionale in quanto consiste in comunicazioni dirette e spesso informali realizzate attraverso forum di polizia. Infatti nella prima fase investigativa la cooperazione giudiziaria reciproca può risultare meno efficace data la lentezza della procedura irrigidita da formalismi. La cooperazione di polizia presenta anche il vantaggio di avere una natura tecnica meno avvezza a eventuali condizionamenti di natura politica. Nonostante tali aspetti positivi, la cooperazione tra forze dell'ordine non è immune da talune criticità tecniche legate alle differenze linguistiche e ai differenti metodi investigativi. Basti pensare alla diversità dei poteri delle agenzie federali statunitensi che sono di gran lunga maggiori rispetto a quelli delle autorità di polizia di altri Stati. Occorre tuttavia rilevare che sovente l'ostacolo più rilevante all'efficace collaborazione tra le forze di polizia è costituito dalla mancanza di reciproca fiducia

[158] United Nations. (2000). *United Nations Convention against Transnational Organized Crime*, art. 4(2).
[159] Permanent Court of International Justice. (1927). *The Case of the S.S. "Lotus" (France v. Turkey), Judgment of 7 September 1927* (Ser. A, No. 10).
[160] Dubber M.D. (2006*). Criminal Law in Comparative Context.* 56 Journal of Legal Education. pp. 433-434.

tra le forze dell'ordine che limita la possibilità di un proficuo scambio delle più delicate e utili informazioni funzionali alle indagini[161].

2.1 Le forme di cooperazione internazionale nelle operazioni *undercover*

La grande maggioranza degli Stati fa ricorso a metodi investigativi speciali per acquisire informazioni necessarie alla prevenzione, individuazione e repressione di determinate tipologie di reato e, considerata la natura ormai transnazionale della criminalità contemporanea, è fondamentale che le autorità nazionali dispongano di adeguati meccanismi di cooperazione internazionale in materia.

Ciò nonostante, la cooperazione in tale ambito non trova ad oggi esplicito riconoscimento a livello internazionale. Pertanto, nella fase iniziale, per renderla giuridicamente attuabile si è fatto riferimento al principio di cooperazione tra Stati definito nella Carta delle Nazioni Unite agli articoli 1,11,13,55 e 56[162] e nel preambolo della Convenzione di Vienna sul diritto dei Trattati[163]. Tuttavia, sebbene manchi una base giuridica unitariamente riconosciuta, l'imprescindibilità di tale cooperazione si rinviene in alcuni trattati bilaterali e multilaterali in materia di contrasto alla criminalità e, soprattutto, nella prassi operativa consolidatasi tra gli Stati.

A tal proposito, ponendo l'attenzione sulle operazioni *undercover*, è possibile individuare varie forme di cooperazione internazionale. Una prima modalità consiste nello scambio di informazioni che può assumere carattere formale e informale. La procedura formale consiste nella trasmissione di informazioni necessarie all'instaurazione di un'operazione sotto copertura, richieste dalle autorità operative specificamente autorizzate di uno Stato verso quelle di un altro. Nell'ipotesi di un operazione già instaurata, le autorità di *law enforcement* competenti possono rilasciare

[161] Boister, N. (2018). *An introduction to transnational criminal law* (2nd ed.). Oxford University Press. pp. 280-284
[162] United Nations. (1945). *Charter of the United Nations.* 59 Stat. 1031, T.S. No. 993. art.1,11,13,55,56
[163] United Nations. (1969). *Vienna Convention on the Law of Treaties*. 1155 U.N.T.S. 331.

spontaneamente informazioni qualora ritengano le stesse necessarie ai fini delle indagini[164].

Dal punto di vista informale, lo scambio di informazioni può essere effettuato direttamente tra funzionari delle forze dell'ordine senza l'autorizzazione delle autorità centrali. Tale modalità si giustifica alla luce della complessità delle procedure formali che spesso non consentono uno scambio tempestivo di informazioni rilevanti.

La cooperazione si sostanzia anche nella condivisione di strumenti tecnici, apparecchiature forensi o altri mezzi materiali utilizzati durante l'attività di indagine. Tale condivisione comporta frequentemente l'ausilio di specialisti competenti nell'utilizzo delle apparecchiature provenienti dal paese che ne fornisce la disponibilità.

L'assistenza di specialisti stranieri può risultare utile anche ai fini dell'attività investigativa sotto copertura nei casi in cui sia necessario intercettare conversazioni di esponenti di gruppi criminali provenienti da uno Stato straniero che utilizzano un particolare gergo specifico per il quale non è sufficiente l'utilizzo del traduttore ovvero quando, ai fini dell'infiltrazione in gruppi criminali transnazionali, si renda indispensabile l'ausilio di agenti stranieri.

Il coinvolgimento di agenti sotto copertura provenienti da altri Stati può essere previsto nella normativa nazionale che disciplina specificamente tale forma di cooperazione. Si pensi al codice di procedura penale tedesco che all'art.110-a comma 2, oltre a dare una definizione di investigatori sotto copertura, consente la partecipazione di agenti esteri o alla legge belga e polacca che determinano le condizioni e i presupposti di tale collaborazione. Nonostante la differente formulazione delle discipline interne, le normative presentano caratteristiche comuni. In particolare esse prevedono che il coinvolgimento di uno specialista straniero avvenga generalmente su iniziativa dello Stato nel cui territorio le operazioni sono condotte. Qualora però le attività siano svolte ad iniziativa dello Stato estero, queste devono essere previamente concordate con le autorità competenti dello Stato territorialmente coinvolto. In questo caso gli agenti stranieri verranno considerati

[164] Cherniavskyi, S. S., Hribov, M. L., Nebytov, A. A., Kniaziev, S. M., & Telenyk, S. S. (2020). (2020) *The forms of international co-operation in the area of undercover investigations.* Journal of Legal, Ethical and Regulatory Issues, 23(1).

semplici partecipanti alle attività sotto copertura e non potranno organizzare l'infiltrazione senza il coordinamento con le forze dell'ordine locali. Infatti, solo attraverso l'intervento di quest'ultime, si può instaurare e organizzare adeguatamente ed efficacemente lo svolgimento della misura investigativa[165].

Una forma avanzata di cooperazione giudiziaria e investigativa transnazionale è costituita dalle *Joint Investigation Teams* (JITs). Esse sono state introdotte per la prima volta in ambito internazionale con la Convenzione contro il traffico di stupefacenti del 1988 la quale, all'art.9 (1) (c)[166], prevede che le parti debbano, nei casi opportuni e in conformità al proprio diritto interno, istituire squadre comuni tenendo conto delle esigenze di sicurezza delle operazioni e della tutela dei cittadini. Si precisa inoltre che i funzionari che prendono parte alle operazioni devono agire conformemente a quanto disposto nell'autorizzazione rilasciata dalle autorità competenti e devono garantire il rispetto della sovranità dello Stato nel cui territorio l'operazione deve avere luogo. In tale contesto un gruppo di esperti del "*United Nation Office on Drugs and Crime*" ha identificato due modelli di JITs. Il primo è quello delle "*parallel and coordinated investigation*" nel quale determinati Stati localizzati in diversi ambiti regionali cooperano perseguendo un obiettivo comune, senza poter agire unitamente nel medesimo territorio. Il secondo è il modello cosiddetto "*integrato*" che si instaura tra Stati confinanti i quali, salvo diversa disposizione interna, possono quindi operare in co-localizzazione[167].

Le squadre investigative comuni sono disciplinate, come già osservato in precedenza, anche a livello regionale dalla normativa dell'Unione Europea, in particolare, nell'art.13 della Convenzione relativa all'assistenza giudiziaria in materia penale[168] e nella decisione quadro 2002/495/GAI del Consiglio dell'Unione Europea

[165] Cherniavskyi, S. S., Hribov, M. L., Nebytov, A. A., Kniaziev, S. M., & Telenyk, S. S. *The forms of international co-operation in the area of undercover investigations*.
[166] United Nations. (Vienna, 20 December 1988). *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. United Nations Treaty Series, vol. 1582. art.9
[167] Boister, N. *An introduction to transnational criminal law* (2nd ed.). Oxford University Press. cit. pp.291-292
[168] European Union. (2000, May 29). *Convention on Mutual Assistance in Criminal Matters between Member States of the European Union* (2000/C 197/01). Official Journal of the European Communities. art. 13

relativa alle squadre investigative comuni[169]. Esse permettono la raccolta e lo scambio diretto di informazioni e prove senza che sia necessario ricorrere ai meccanismi tradizionali di assistenza giudiziaria e ammettono la partecipazione di funzionari stranieri alle varie attività sempre nel rispetto della legislazione nazionale dello Stato territoriale e delle istruzioni impartite dal responsabile del team investigativo.

Le squadre investigative comuni, secondo la disciplina europea, vengono costituite per agevolare lo svolgimento di indagini complesse che presentano collegamenti con altri Stati membri o per indagini che necessitano un'azione coordinata transnazionale. A tal fine, si tiene conto della complessità della rete criminale sottoposto alle indagini, delle misure investigative da realizzare e del livello di coordinamento necessario tra gli Stati interessati. Un ruolo funzionale viene attribuito a Europol e Eurojust che, oltre a fornire una prospettiva internazionale più completa, possono agevolare gli Stati interessati nella costituzione della squadra investigativa comune, valutandone l'opportunità e i diversi requisiti nazionali applicabili[170].

L'esigenza delle JITs risulta particolarmente accentuata nelle operazioni sotto copertura, nelle quali la cooperazione garantisce non solo uno scambio di competenze e *know-how* operativo evitando la sovrapposizione investigativa in più Stati, ma consente anche di fronteggiare al meglio imprevisti che richiederebbero una nuova linea investigativa da attuare tempestivamente[171].

Il Procuratore Nazionale Antimafia e Antiterrorismo Giovanni Melillo guarda con favore alla costituzione di JITs a carattere permanente, sostenendo che le stesse consentono di accelerare le attività investigative, evitando la procedura di nuova costituzione ogni volta che emergono nuove esigenze operative. Inoltre, la stabilità dello strumento facilita la mutua fiducia, la conoscenza di reciproci sistemi normativi, la condivisione di *best practices* investigative e degli avanzamenti tecnologici. Tale

[169] Council of the European Union. (2002). *Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams* (OJ L 162, 20.6.2002, pp. 1–3). Official Journal of the European Union.
[170] Consiglio dell'Unione Europea. (2017). *Squadre investigative comuni – Guida pratica* (Doc. 6128/1/17 REV 1). Eurojust. pp. 6,7
[171] Paulesu, P. P. (2018). *Operazioni sotto copertura e ordine europeo d'indagine penale*. Archivio Penale: Rivista Quadrimestrale Di Diritto, Procedura e Legislazione Penale Speciale, Europea e Comparata. pp. 39-40

strumento infatti è stato fortemente implementato dalla DNA sulla base di accordi bilaterali conclusi nell'ambito della Convenzione di Palermo[172].

2.2 Fonti internazionali in materia di *special investigation techniques*

Una prima normativa in materia di strumenti investigativi speciali a livello sovranazionale si rintraccia nell'art.11 della Convenzione delle Nazioni Unite contro il traffico illecito di stupefacenti e sostanze psicotrope[173]. L'articolo 11 disciplina la tecnica della consegna controllata con cui si consente il passaggio di merci o sostanze illecite tra più Stati sotto il controllo delle autorità competenti con l'obiettivo di identificare soggetti coinvolti nella commissione di reati[174].

Partendo da tale disciplina, emerge come la profonda trasformazione delle modalità operative della criminalità nell'era della globalizzazione impone un ripensamento delle tecniche di indagine ordinarie. In questo contesto si inserisce l'art.20 della Convenzione di Palermo che ha segnato un punto di svolta nella regolamentazione delle tecniche investigative speciali. Tale disposizione ha l'obiettivo di realizzare nuove forme di cooperazione giudiziaria con Paesi terzi per il contrasto dei reati aventi natura transnazionale e di delineare uno standard internazionale che rafforzi la funzionalità e le garanzie delle nuove tecniche investigative ormai profondamente influenzate dalla rivoluzione tecnologica[175].

Le tecniche investigative cosiddette "*speciali*" non sono definite tali per la loro eccezionalità in quanto molte di esse, come le intercettazioni, sono ormai divenute strumento tradizionale di indagine. Esse sono definite speciali perché il loro impiego risulta spesso costoso e complesso in quanto richiede particolari competenze tecniche avanzate e può sollevare problemi di compatibilità con i diritti fondamentali della persona. Per tali ragioni, il loro utilizzo dovrebbe essere limitato ai casi in cui non sia

---

[172] Melillo, G. (2025, 6 dicembre). Intervista condotta dall'autore. Intervista non pubblicata
[173] United Nations. (1988 December 20). *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. Vienna.
[174] United Nations. Economic and Social Council. (1998). *Commentary on the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988* (UN Doc. E/CN.7/590). United Nations.
[175] Mattarella, A. (2020). Cap 9 *Le tecniche investigative speciali e le loro potenzialità sul piano internazionale.* In *La Convenzione Di Palermo: il Futuro Della Lotta Alla Criminalità Organizzata Transnazionale /*. G. Giappichelli Editore, p. 289

disponibile un'alterativa efficace per ottenere informazioni e prove; nella prassi, tuttavia, esse consentono di conseguire un risultato insostituibile come attività di indagine di particolare natura[176].

Nello specifico, il primo paragrafo dell'art.20 della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale stabilisce che "*se consentito dai principi di base del proprio ordinamento giuridico interno, ciascuno Stato Parte, nelle sue possibilità e alle condizioni prescritte dalla propria legislazione nazionale, adotterà le misure necessarie per consentire l'uso appropriato di consegne controllate e, ove lo ritenga opportuno, per l'uso di altre tecniche investigative speciali, come la sorveglianza elettronica o altre forme di sorveglianza e le operazioni sotto copertura, da parte delle sue autorità competenti nel suo territorio allo scopo di combattere efficacemente la criminalità organizzata*"[177].

Da tale articolo si desume anzitutto la necessità che ciascun Paese adatti la propria normativa interna agli standard internazionali; emerge inoltre che un'applicazione realmente uniforme, pur in presenza di disposizioni volutamente generali, sia di fatto impossibile, poiché l'impiego delle tecniche speciali deve comunque rispettare i principi costituzionali e la disciplina processuale di ciascun ordinamento. Tale eterogeneità normativa riduce il livello di armonizzazione e può rendere più difficoltosa la cooperazione internazionale nelle indagini transnazionali.

L'art. 20 della Convenzione di Palermo cita espressamente 3 strumenti di investigazione speciale. Indica, in prima battuta, "*l'uso appropriato delle consegne controllate*" intendendo per tali il trasferimento monitorato di carichi illeciti o sospetti al fine di indagare su un reato e di identificare i soggetti coinvolti nella sua commissione. In secondo luogo, la Convenzione fa riferimento alla "*sorveglianza elettronica o altre forme di sorveglianza*": ci si riferisce in questa fattispecie agli spostamenti, alle comunicazioni o ogni altro comportamento dell'indagato rilevante ai fini delle indagini. In tal senso possono essere utilizzate sia le modalità tradizionali adottate dalla polizia come il pedinamento o l'osservazione, sia gli espedienti

[176] United Nations Office on Drugs and Crime. (2012). *Digesto di casi di criminalità organizzata / Digest of Organized Crime Cases*. pp.44-45

[177] United Nations. (2000). *United Nations Convention against Transnational Organized Crime*. Art. 20

elettronici avanzati per effettuare, ad esempio, intercettazione di messaggi di posta elettronica.

Infine, l'articolo contempla espressamente le "*operazioni sotto copertura*", definite come l'infiltrazione di un soggetto all'interno di gruppi criminali partecipando alle loro attività illecite al fine di acquisire e riferire informazioni sui reati commessi o pianificati, nonché sulla struttura, sulla conformazione e sugli appartenenti dell'organizzazione. [178]

Una disposizione analoga a quella dell'art.20, è contenuta nell'art. 50 della Convenzione di Merida contro la corruzione[179], che obbliga gli stati ad adottare tecniche speciali di investigazione. Tale articolo evidenzia come tali attività di indagine non siano limitate al contrasto della criminalità organizzata, ma possano trovare applicazione in ambiti diversi per esempio nella lotta alla criminalità amministrativa e ai reati corruttivi. La disposizione sopra richiamata assume inoltre un valore specifico poiché testimonia una convergenza internazionale su obiettivi, standard e *best practices* in tema di tecniche investigative speciali, ponendosi come parametro di orientamento per la regolamentazione nazionale.

Rispetto all'art. 20 della Convenzione di Palermo, l'art.50 sancisce l'impegno degli Stati all'adozione di misure necessarie per garantire l'ammissibilità della prova ottenuta tramite tali tecniche investigative. Tale disposizione assume un rilievo particolare per le attività dell'agente sotto copertura poiché consente di realizzare una connessione tra la fase investigativa e la formazione della prova nel dibattimento. Si tratta di un passaggio decisivo in quanto solo tramite l'utilizzabilità processuale del materiale raccolto, si conferisce reale efficacia all'attività di infiltrazione e si consente il perseguimento dei soggetti indagati.

Sul piano internazionale entrambe le disposizioni incentivano gli Stati a predisporre un quadro giuridico appropriato idoneo a consentire l'uso delle *special*

[178] United Nations Office on Drugs and Crime. *Digesto di casi di criminalità organizzata / Digest of Organized Crime Cases*.
[179] United Nations. (2004). *United Nations Convention against Corruption*. New York: United Nations. art. 50

investigation techniques tramite l'implementazione di accordi e intese bilaterali o multilaterali per promuovere la cooperazione in questo settore[180].

Risulta opportuno precisare che entrambi gli articoli esaminati rendono obbligatoria la previsione della consegna controllata, mentre non impongono, ma raccomandano fortemente, l'uso della sorveglianza elettronica e delle operazioni sotto copertura. Infatti queste ultime, in determinati procedimenti penali, rappresentano un approccio investigativo proattivo capace di produrre risultati che sarebbero impossibili se si adottassero tecniche meno sofisticate. Con specifico riferimento alle operazioni sotto copertura la loro rilevanza risulta evidente poiché consentono alle autorità competenti di entrare in contatto con autori di condotte illecite, di ricostruirne l'operato e agevolare dichiarazioni collaborative o ammissioni di colpevolezza da parte degli imputati, eliminando così inutili lungaggini del processo[181].

A completamento del quadro normativo internazionale, è necessario richiamare le disposizioni e le raccomandazioni del Consiglio d'Europa. In primo luogo, le tecniche speciali d'indagine sono state definite nell'art.23 della Convenzione del Consiglio d'Europa contro la corruzione[182], riconoscendo la necessità ai fini del rilevamento di tale forma di reato, di strumenti investigativi specializzati. Nonostante la norma non preveda un elenco delle tecniche ammesse, si ritiene che i redattori della Convenzione si riferissero in particolare all'uso di agenti infiltrati, intercettazioni telefoniche e installazioni di dispositivi per l'ascolto clandestino. Data la particolare preoccupazione concernente tali tecniche investigative, l'art. 23 consente agli Stati di poter scegliere quali tecniche ammettere nel proprio ordinamento interno e di stabilirne i limiti ai fini dell'utilizzo[183].

Ulteriore rilevante disposizione è prevista all'art.19 del Secondo Protocollo Addizionale alla Convenzione europea di assistenza giudiziaria in materia penale che disciplina la cooperazione nelle operazioni di infiltrazione transnazionale, stabilendo

---

[180] Mattarella, A. *Le tecniche investigative speciali e le loro potenzialità sul piano internazionale.* In *La Convenzione Di Palermo: il Futuro Della Lotta Alla Criminalità Organizzata Transnazionale* pp.290-292

[181] Ivi p.294

[182] Council of Europe. (1999). *Criminal Law Convention on Corruption* (ETS No. 173, art. 23). Concluded 27 January 1999, Strasbourg, entered into force 1 July 2002. Council of Europe Treaty Series. art. 23

[183] Council of Europe. (1999). *Explanatory Report to the Criminal Law Convention on Corruption* (European Treaty Series No. 173) Council of Europe pp. 22-23

la procedura per la richiesta di svolgimento di operazioni sotto copertura da parte di uno Stato nel territorio di un altro Stato, nel rispetto del diritto e delle procedure dello Stato nel cui territorio si svolge l'attività operativa[184].

Di fondamentale importanza, nel quadro delineato dal Consiglio d'Europa, è la Raccomandazione del 2017 che intende rafforzare il quadro normativo degli Stati membri in materia di strumenti speciali d'indagine, evidenziandone la rilevanza operativa per il contrasto di gravi reati e, al contempo, vuole stabilire garanzie e limiti connessi alla loro disciplina. Nelle "*operational guidelines*" della Raccomandazione, il Comitato dei Ministri del Consiglio d'Europa incoraggia gli Stati membri a fornire alle autorità competenti strumenti tecnologici, risorse umane e finanziarie necessarie al fine di facilitare l'uso di tali strumenti. Per ciò che attiene le indagini informatiche si precisa, inoltre, che gli Stati debbano facilitare l'uso appropriato dello *special investigation techniques* per prevenire, indagare e perseguire la commissione di attacchi informatici connessi a reati gravi, inclusi quelli di terrorismo. Il Capitolo III della raccomandazione prevede che le Parti facciano ricorso, nella misura più ampia possibile, agli strumenti di cooperazione giudiziaria e di polizia tanto sul piano interno quanto su quello internazionale, incoraggiandole, in questo ultimo caso, alla conclusione di convenzioni o accordi specifici in materia[185].

2.3 L'ordine europeo di indagine e le operazioni sotto copertura

Le operazioni sotto copertura, considerate strumento investigativo invasivo, versatile e concepito per contrastare i gravi delitti e per neutralizzare le organizzazione criminali, ha trovato riconoscimento esplicito nell'ambito dell'ordine europeo d'indagine disciplinato dalla Direttiva 2014/41/UE[186]. Tale approdo, successivo alla

[184] Council of Europe. (2001). *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters* (ETS No. 182). Concluded 8 November 2001, Strasbourg; entered into force 1 February 2004. Council of Europe Treaty Series. art.19

[185] Council of Europe. (2017, July 5). *Recommendation CM/Rec (2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism*. Council of Europe.

[186] European Union. (2014). *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.* Official Journal of the European Union, L 130/1, 1 May 2014.

disciplina dell'art.14 della Convenzione MAP[187] che si limitava a prevedere timidamente la possibilità per gli Stati di collaborare nello svolgimento di indagini mediante agenti sotto copertura[188], assume una funzione decisiva data la particolare efficacia che tale strumento investigativo speciale manifesta nel quadro della cooperazione giudiziaria tra organi di polizia di Paesi diversi[189].

Il d.lgs.108/2017, attuativo della Direttiva, disciplina sia la procedura cosiddetta "*passiva*", relativa al riconoscimento ed esecuzione di un ordine di indagine proveniente da altro Stato membro, sia la procedura "*attiva*" riferita all'emissione di un ordine d'indagine proveniente dall'autorità italiana.

Con riguardo alla procedura passiva, il riconoscimento e l'esecuzione dell'ordine d'indagine è affidato al procuratore distrettuale, che ha l'obbligo di informare il Procuratore Nazionale Antimafia e Antiterrorismo nei casi previsti dll'art.51, c.3-bis e 3-quater c.p.p. Il rifiuto del riconoscimento e dell'esecuzione può essere disposto esclusivamente quando le attività sotto copertura non risulterebbero ammissibili per un caso interno analogo, secondo i criteri dell'art.9. l. n. 146 del 2006, ovvero quando non sia possibile raggiungere un accordo con l'autorità richiedente in ordine al compimento di atti diversi, ma comunque idonei al raggiungimento dello scopo perseguito.

Qualora l'ordine europeo d'indagine non esponga le ragioni che rendono l'atto rilevante ai fini del procedimento straniero, il procuratore della Repubblica richiede informazioni utili all'autorità di emissione al fine di consentire una efficace e tempestiva collaborazione. Tuttavia, non si comprende cosa debba intendersi per "*rilevante*", specialmente con riferimento alle operazioni sotto copertura, la cui effettiva utilità investigativa è verificabile solo nella fase esecutiva. Inoltre, il procuratore non può sindacare le motivazioni dell'autorità straniera, non essendo legittimato ad effettuare valutazione approfondite sul procedimento in corso.

---

[187] European Union. (2000, May 29). *Convention on Mutual Assistance in Criminal Matters between Member States of the European Union* (2000/C 197/01). Official Journal of the European Communities. art.14

[188] Marchetti, M.-R., Selvaggi, E., & Barrocu, G. (2019). *La nuova cooperazione giudiziaria penale: dalle modifiche al Codice di procedura penale all'ordine europeo di indagine.* Wolters Kluwer. p.424

[189] Paulesu, P. P. *Operazioni sotto copertura e ordine europeo d'indagine penale*. cit. pp. 24-25

Con riferimento alla disposizione di cui all'art.9 della legge n. 146/2006 è fondamentale il passaggio relativo all'acquisizione degli elementi di prova. Nel sistema interno, viene previsto, come requisito di legittimazione delle operazioni *undercover*, la previa instaurazione di un procedimento penale con notizia di reato completa o comunque già acquisita ma non ancora iscritta nel registro di cui all'at.335 c.p.p.

Tale requisito, determinante ai fini dell'utilizzabilità probatoria delle risultanze ottenute tramite l'attività dell'agente sotto copertura, si ritiene applicabile anche con riferimento alla mutua assistenza tra Stati per la quale il riconoscimento e l'esecuzione dell'ordine europeo di indagine vada subordinato all'esistenza del procedimento penale interno. E ciò sembrerebbe trovare conferma nella disposizione che consente al procuratore di differire l'esecuzione e il riconoscimento dell'ordine se questo possa arrecare un pregiudizio alle indagini in corso.

Altro aspetto rilevante attiene al ruolo del pubblico ministero nelle indagini sotto copertura e la diversa declinazione che tale ruolo assume sul versante della cooperazione. Sul piano interno vige un'ambiguità normativa che sembra prospettare una posizione marginale dell'organo dell'accusa, attribuendo agli organi di vertice della polizia la valutazione circa l'opportunità dell'attivazione delle operazioni. Al p.m. è infatti data preventiva comunicazione dell'avvio delle indagini sotto copertura e delle successive modalità di svolgimento, senza che sia formalmente richiesta una sua autorizzazione, lasciando alla volontà discrezionale degli organi di polizia la decisione circa l'utilizzo di tale strumento investigativo. Tuttavia, tale lettura non appare sostenibile in quanto, sulla base di un'interpretazione costituzionalmente e convenzionalmente orientata, non si dovrebbe prescindere dall'autorizzazione del pubblico ministero per avviare indagini *undercover*. Ciò si può desumere proprio dal meccanismo di preventiva comunicazione da cui logicamente deriverebbe la possibilità per il P.M. di indirizzare e dirigere le indagini sotto copertura.

Sul piano della cooperazione investigativa, il pubblico ministero assume un ruolo centrale poiché l'autorità richiedente il compimento di attività sotto copertura non può sottrarsi al vaglio dell'organo dell'accusa circa il rispetto delle normative richieste ai fini del riconoscimento e dell'esecuzione dell'ordine di indagine.

Rileva inoltre la qualificazione giuridica che viene assegnata ai soggetti infiltrati provenienti dallo Stato di emissione dell'ordine europeo d'indagine. Tali soggetti sono considerati pubblici ufficiali ma non ufficiali di polizia giudiziaria e ciò implica che non possono agire autonomamente ma ogni iniziativa del funzionario straniero deve sottostare al controllo costante della polizia giudiziaria italiana. Al contempo, al funzionario straniero che opera quale agente infiltrato vengono applicate le cause di non punibilità dell'art.9 l.n. 146/2006.

Relativamente alla procedura attiva, la competenza circa l'emissione dell'ordine europeo d'indagine spetta al pubblico ministero o al giudice che procede. Anche in questa ipotesi, nei casi di cui all'art.51 comma 3-ter e 3-quater c.p.p., è prevista la comunicazione al Procuratore Nazionale Antimafia e Antiterrorismo.

In tal caso, resta ferma la possibilità di emettere l'ordine di indagine esclusivamente nei casi e con le modalità previste dall'art.9. l. n. 146/2006 e lo stesso viene trasmesso direttamente all'autorità di esecuzione straniera, con la quale devono essere concordate le modalità di svolgimento dell'operazione.

Qualora nel corso dell'attività investigativa emergano ulteriori fattispecie delittuose non previste nell'istanza di collaborazione emessa, trova applicazione l'art. 34 d.lgs. n. 108 del 2017 il quale consente di integrare o completare l'ordine investigativo previamente emanato.

Rimane invece aperta la questione relativa allo status dell'agente infiltrato italiano operante nel territorio straniero. Tale profilo si ritiene debba essere regolato negli accordi preventivi con l'autorità di esecuzione poiché costituisce un aspetto essenziale per chiarire previamente le attività che l'agente è legittimato a compiere e quelle che gli sono precluse[190].

2.4 Le modalità di collaborazione e supporto investigativo transnazionale: il contributo di INTERPOL, Europol ed Eurojust

Con il passaggio "*Reducing the global impact of cybercrime and protecting communities for a safer world*", si sintetizza il mandato prefissato da Interpol nella Global Cybercrime Stategy 2022-2025, orientata al perseguimento di quattro obiettivi

[190] Ivi. pp. 33–39.

principali tra loro integrati: la prevenzione, l'individuazione, l'investigazione e la neutralizzazione delle minacce informatiche[191]. Considerando, in via primaria, il versante investigativo, Interpol mira a prevenire il *cybercrime* attraverso la predisposizione di azioni coordinate e partnership tra forze dell'ordine, professionisti della cybersicurezza e settore privato. Tale approccio risulta essenziale poiché , a differenza dei reati tradizionali, i *cybercrimes* non presuppongono l'esistenza di prove fisiche o di testimoni da interrogare, ma coinvolgono vittime, attori e infrastrutture dislocati in Stati differenti, richiedendo dunque una risposta globale integrata di soggetti dotati di particolari competenze tecniche anche provenienti dal settore privato[192].

Un caso tipico di supporto investigativo fornito da Interpol è il progetto "*African Joint Operation against Cybercrime*" (AFJOC). La regione africana si trova in una fase di profonda evoluzione nel settore digitale che genera di conseguenza l'emersione di nuove minacce alla sicurezza informatica del continente attraverso la crescita esponenziale di fenomeni criminosi quali l'estorsione digitale, gli attacchi *ransomware*[193] e il *phishing*. Data l'assenza di solide infrastrutture di cybersicurezza, Interpol ha avviato l'iniziativa sopra menzionata con lo scopo di rafforzare le capacità interne delle forze dell'ordine locali.

Le attività previste comprendono, in primo luogo, il supporto analitico finalizzato a costituire un'attività di intelligence tempestiva e accurata tramite i *Cyber Activity Reports* i quali forniscono approfondimenti diretti sulle minacce verificatesi. In secondo luogo si organizzano attività per lo sviluppo di capacità e competenze interne nel contrasto alla criminalità digitale attraverso la partecipazione a piattaforme quali la *Cybercrime Collaborative Platform* che consente scambio di dati operativi in modo sicuro.

Ulteriori forme di collaborazione riguardano la definizione di un quadro operativo congiunto volto ad aumentare il dialogo con attori privati, forze dell'ordine e organizzazioni internazionali e intergovernative. In questo contesto si inserisce l'*African Cybercrime Operations Desk*, responsabile dell'attuazione dell'AFJOC e

[191] INTERPOL. (2022). *Global Cybercrime Strategy 2022–2025*.
[192] Interpol. (2024). *INTERPOL Global Cybercrime Conference 2023: Outcome Report*. p. 37
[193] ACN definisce il Ransomware come "*un Malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione*".

tenuto a instaurare un dialogo sinergico con l'unione africana e AFRIPOL. Interpol fornisce inoltre supporto investigativo per lo smantellamento delle reti criminali che si celano dietro il *cybercrime* e promuove la diffusione di *best practices* rivolte a cittadini e imprese[194].

Per una proficua ed efficace attività investigativa, è altresì necessario il contributo del settore privato, detentore di una parte essenziale delle infrastrutture e dei dati presi di mira dai cybercriminali. A tal fine è stato instituito nel 2019 il "*Project Gateway*" che definisce un quadro giuridico per la condivisione di informazione di *cyber threat intelligence* tra Interpol e partner selezionati, quali società di cybersicurezza, fornitori di servizi tecnologici e istituzioni finanziarie. Tale iniziativa consente l'accelerazione dello scambio di informazioni garantendo una maggiore rapidità nella neutralizzazione delle minacce e nell'identificazione dei soggetti responsabili. Inoltre, si permette agli analisti di esaminare i dati ricevuti, verificarne l'attendibilità e fornirli come patrimonio di conoscenza ai Paesi attaccati mentre gli attori privati contribuiscono a rendere proattiva la risposta globale alle cyberminacce. Tale progetto si è rivelato particolarmente utile sia per operazioni multinazionali, come l'operazione "*Seregenti 2.0*"[195], sia per la gestione della sicurezza cibernetica di grandi eventi internazionali ospitati in Paesi membri di Interpol, come il Vertice G20 del 2024 in Brasile[196].

Per favorire la condivisione di informazioni, Interpol ha creato il *Cybercrime Knowledge Exchange workspace* e la *Cybercrime Collaborative Platform-Operation.* Il *Cybercrime Knowledge Exchange workspace* permette lo scambio di conoscenze non operative tra forze dell'ordine, organizzazioni internazionali ed esperti nel settore in materia di *cybercrime*. In questo modo si crea una rete internazionale che favorisce la circolazione di competenze e informazioni sulle nuove frontiere della cybercriminalità e sui più aggiornati strumenti tecnologici per fronteggiarla.

La *Cybercrime Collaborative Platform-Operation* consente, d'altro canto, un coordinamento globale delle operazioni di *law enforcement* nel *cyberspace*. Su tale

[194] INTERPOL (2024-2025). *AFJOC – African Joint Operation against Cybercrime*. INTERPOL.
[195] INTERPOL. (2025, 22 agosto). *African authorities dismantle massive cybercrime and fraud networks, recover millions.* INTERPOL.
[196] INTERPOL. *Spotlight: Cybercrime outreach*. INTERPOL.

piattaforma l'accesso è riservato ai soli attori operativi per condividere informazioni di intelligence contribuendo così ad visione complessiva delle minacce con conseguente razionalizzazione e riduzione degli sforzi operativi[197].

Nell'ambito europeo, Europol svolge un ruolo fondamentale nella lotta alla criminalità informatica anche attraverso l'istituzione, nel 2013, dell'*European Cybercrime Centre* (EC3). Il mandato dell'EC3 si concentra su 3 principali tipologie di reati: i crimini cyber-dipendenti, lo sfruttamento sessuale dei minori e le frodi nei sistemi di pagamento spesso realizzate nel Dark Web o tramite piattaforme alternative.

L'EC3 fornisce supporto operativo, strategico e analitico attraverso la raccolta e lo scambio di informazioni e di intelligence, coordina le indagini degli Stati Membri favorendo la cooperazione con le *Law Enforcement Agencies* (LEAs) e altre istituzioni europee rilevanti nel settore della *cybersecurity* quali ENISA. In aggiunta, offre supporto operativo e tecnico 24/7 alle LEAs per reagire tempestivamente ad incidenti cyber urgenti, agevolando l'integrazione di conoscenze tra settore pubblico e privato e consentendo decisioni informate nella prevenzione e nel contrasto al *cybercrime*[198].

Da ultimo, l'EC3 ospita e facilita i lavori della *Joint Cybercrime Action Taskforce* (J-CAT), task force operativa permanente istituita nel 2014 che consente un'azione coordinata e congiunta sia tra Stati membri dell'Unione Europea sia con Paesi terzi. J-CAT coordina le azioni contro le principali minacce cyber, facilita l'avvio congiunto di indagini e operazioni transfrontaliere, dando priorità ai casi di "*alto profilo*". L'azione della task force si focalizzata su reati cyber-dipendenti quali gli attacchi *ransomware* e le intrusioni illecite nei sistemi informatici, nonché sulle frodi nei pagamenti transnazionali, sullo sfruttamento sessuale online di minori e sulle piattaforme criminali nel *Dark Web*.

J-CAT è composto da un team di ufficiali di collegamento specializzati in cybercrime, coordinati da un Board costituito dai rappresentanti senior delle forze dell'ordine anch'essi esperti nel settore. I membri provengono da tredici Stati membri dell'UE (Austria, Belgio, Repubblica Ceca, Danimarca, Finlandia, Francia, Germania, Italia, Paesi Bassi, Polonia, Romania, Svezia e Spagna) e sei Paesi non UE (Australia, Canada, Norvegia, Svizzera, Regno Unito e Stati Uniti) rappresentati all'interno della

[197] INTERPOL. (2020). *Cybercrime Collaboration Services*. INTERPOL
[198] Europol. *European Cybercrime Centre (EC3)*. Europol.

task force da quattro agenzie: il *Federal Bureau of Investigation*, il *Secret Service*, l'*Internal Revenue Service* e l'*Homeland Security Investigations*.

L'approccio operativo di J-CAT si struttura in quattro fasi, di cui la prima si riferisce ad una preliminare identificazione delle minacce cyber volta alla definizione delle priorità d'intervento sulla base della prontezza operativa e della disponibilità di dati condivisibili. Segue la fase preparatoria, nella quale si affrontano eventuali casi di sovrapposizioni investigative tra i vari Stati. La successiva e conclusiva fase definisce le attività strettamente operative e investigative e infine quelle giudiziarie[199].

Un esempio di supporto fornito da J-CAT nelle operazioni contro il *cybercrime* è l'Operazione "*Eastwood*", nella quale è stato realizzato un profondo coordinamento tra le autorità di polizia di dodici Paesi sia appartenenti all'UE che extra-UE, con il coinvolgimento di Europol, di Eurojust, di altre istituzioni europee quali Enisa, e di alcuni attori privati quali *ShadowServer* e *Abuse.ch.* Tale cooperazione ha portato tra il 14 e il 17 luglio 2025 allo smantellamento del network cybercriminale filo russo NoName057(16) attivo principalmente contro l'Ucraina e successivamente contro Paesi che la supportano nel conflitto. L'operazione ha reso possibile la neutralizzazione di una parte dell'infrastruttura di attacco, mettendo invece offline la parte restante, nonché l'esecuzione di due arresti, sette mandati d'arresto e numerose perquisizione domiciliari[200].

Nel quadro dell'operazione Eastwood, si inserisce altresì l'apporto della Polizia Postale Italiana attraverso il CNAIPIC, che ha operato sotto la direzione della Procura della Repubblica di Roma e in coordinamento con la DNAA. Le attività condotte dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche hanno portato all'individuazione di cinque soggetti responsabili degli attacchi informatici compiuti dal network filo-russo. In aggiunta, dalla sede della Polizia Postale Italiana sono stati diramati sia *alert* tecnici contenenti indicatori di compromissione determinati da malware sia aggiornamenti finalizzati a prevenire ulteriori iniziative di hackeraggio[201].

---

[199] Europol. Joint Cybercrime Action Taskforce (J-CAT). Europol.
[200] Europol. (2025, 16 luglio). *Global operation targets NoName057(16) pro-Russian cybercrime network*. Europol.
[201] Polizia di Stato. (2025). *Report Annuale 2025 per la tutala dei diritti.* Servizio Polizia Postale e per la Sicurezza Cibernetica. p.64

È risultato inoltre decisivo il coordinamento con Eurojust che ha assicurato la gestione delle attività giudiziarie successive attraverso l'esecuzione delle rogatorie internazionali (MLA) e dell' ordine europeo d'indagine[202].

La relazione Europol-Eurojust costituisce un elemento di sinergia indispensabile per una efficace e completa azione contro la criminalità informatica perché consente di integrare l'attività operativa e di intelligence, propria delle forze di polizia, con quella giudiziaria, integrazione necessaria per il riconoscimento e l'utilizzabilità probatoria delle risultanze acquisite.

Costituisce un esempio significativo di tale sinergia, la promozione e il sostegno di Eurojust alla costituzione e al funzionamento delle *Joint Investigations Teams* (JITs), sempre più affermatesi come strumenti efficaci nella lotto al crimine transfrontaliero e quali sedi adeguate allo scambio di informazioni operative tra diversi Paesi[203]. Invero, le squadre investigative comuni consentono di raggiungere risultati vantaggiosi nel contrasto al *cybercrime* perché permettono di ottenere risposte immediate che non si possono acquisire con mere attività di assistenza giudiziaria tradizionali. I principali benefici operativi consistono in primo luogo nella possibilità di condividere risorse, competenze ed expertise tecniche, consentendo anche lo svolgimento di attività investigative da parte di uno Stato Membro nel territorio di un altro che non disponga di adeguati strumenti tecnici. In aggiunta, le JITs garantiscono la conservazione e condivisione immediata di prove elettroniche, la possibilità di identificare una strategia investigativa comune e la più agevole partecipazione di attori privati e Stati terzi e, in definitiva, il conseguente ampliamento del patrimonio conoscitivo e investigativo[204].

In conclusione, a conferma dell'importanza delle azioni investigative coordinate, il Direttore del servizio Polizia Postale e delle Comunicazioni Ivano Gabrielli ha affermato che "*proprio la permanenza, ovvero il collegamento continuo tra rappresentanti accreditati, situazione che consente in tempo reale l'attivazione degli organi collaterali di Polizia, può essere la soluzione più rapida per le attività di*

[202] Europol. *Global operation targets NoName057(16) pro-Russian cybercrime network*.
[203] United Nations Office on Drugs and Crime. (2012). *The use of the Internet for terrorist purposes* (UNODC).
[204] Council of the European Union & Eurojust. (2019, November 5). *Conclusions of the 15th Annual Meeting of National Experts on Joint Investigation Teams (JITs) (Document 13752/19)*

preservazione e di acquisizione degli elementi utili alle indagini di crimini informatici"[205].

3. Tecniche investigative e strumenti applicativi nelle operazioni sotto copertura digitali

L'intervista con il Direttore del servizio di Polizia Postale e per la Sicurezza Cibernetica ha dato modo di comprendere l'impostazione operativa di un'operazione sotto copertura. A tal proposito, una volta autorizzata l'attività *undercover* da parte dell'autorità giudiziaria, si compie ad una fase di studio e approfondimento tecnico necessario all'individuazione delle metodologie più utili ed efficaci per acquisire gli elementi probatori prefissati. Imprescindibile è poi la fase di rendicontazione dell'attività sotto copertura, idonea a dimostrare la legittimità dell'attività e dei metodi seguiti[206].

Per analizzare i metodi investigativi e le attività sotto copertura utilizzate sulla rete occorre comprendere la particolarità dell'ambito di applicazione in cui si insinuano generalmente i *cybercrime*, ossia il Dark Web.

Il Dark Web, originariamente utilizzato dal U.S. Naval Resaerch Laboratory come mezzo di comunicazione criptato per non svelare la tracciabilità, costituisce ad oggi una rete globale di computer che, tramite un protocollo crittografico, generalmente The Onion Router (Tor), consente l'anonimato agli utenti sulla piattaforma. Tale tecnologia di occultamento dell'identità permette la non rintracciabilità dell'indirizzo IP dei server, attraverso l'instradamento casuale e criptato della comunicazione tra mittente e destinatario. Tale strumento era considerato talmente efficace da rendere difficoltosa qualsiasi attività investigativa evidenziando le molteplici lacune legali e tecnologiche che, in passato, limitavano la capacità delle forze di polizia di affrontare e rispondere alla criminalità informatica. In tal senso, l'attività investigativa volta a tracciare l'indirizzo IP del presunto autore del reato risulta complessa ma non impossibile[207].

---

[205] Gabrielli, I. Intervista condotta dall'autore. Intervista non pubblicata.
[206] Ibidem
[207] Davies, G. (2020). *Shining a light on policing of the dark web: An analysis of UK investigatory powers*. Journal of Criminal Law, 84*(5).* pp.407–426

Una delle tecniche di polizia più frequentemente utilizzate è l'Open Source Intelligence (OSint) una speciale attività di monitoraggio che consiste nell'acquisizione di informazioni disponibili e aperte al pubblico, specificamente processate per un dato fine informativo. Partendo da informazioni rilevabili da fonti diverse e apparentemente slegate, l'OSint, attraverso un'attenta analisi, le riconduce a un quadro coerente atto a ricavare spunti investigativi che non si paleserebbero attraverso una verifica isolata. Tale attività, in quanto circoscritta all'accesso a dati di pubblico dominio, non rientra nella fattispecie dell'attività sotto copertura anzi spesso si configura come fase preliminare all'attivazione della stessa[208]. Questo strumento investigativo gioca sulla vulnerabilità dei cybercriminali che devono trovare un punto di equilibrio tra il mascherare la propria identità e lasciare parte della stessa scoperta per attrarre potenziali clienti, mettendo in conto il rischio di attirare così anche le forze dell'ordine. Infatti, attraverso informazioni open source è stato smantellato il marketplace illegale Silk Road, pubblicizzato su un forum di Bitcoin tramite un indirizzo mail. Il suo tracciamento ha permesso l'arresto del suo titolare, Ross Ulbricht successivamente condannato in cinque procedimenti penali con diverse pene tra cui due ergastoli[209].

Più complesso e controverso appare lo strumento utilizzato dalle forze di polizia dell'accesso "*mascherato*". Si tratta di un'attività investigativa riconosciuta come lecita nel nostro ordinamento e quindi non rientrante nella fattispecie delle infiltrazioni sotto copertura, soggette ad autorizzazione dall'autorità giudiziaria, nel caso in cui si sostanzi nella creazione di identità virtuali utilizzando nomi di fantasia ai soli fini di attività di osservazione senza entrare in contatto con utenti della rete.

In tale ipotesi, infatti, le forze dell'ordine svolgono una mera attività di monitoraggio che, come già evidenziato, esula dal perimetro dell'investigazione sotto copertura poiché consiste nella sola analisi di contenuti pubblici, e, come tale, è un'attività liberamente esercitabile da chiunque.

Qualora invece l'ingresso nella rete sia subordinato ad un consenso ottenuto simulando la propria identità di agente di polizia ovvero mediante l'impiego di mezzi

---

[208] Troisi, P. (2022). *Investigazioni nella rete e attività sotto copertura* in *Le investigazioni digitali sotto copertura.* Bari: Cacucci Editore. pp.85-86

[209] Davies, G. *Shining a light on policing of the dark web: An analysis of UK investigatory powers.* cit. pp.407–426

di pagamento creati ad hoc, è evidente che si fuoriesce dall'area del monitoraggio per entrare nel perimetro dell'attività sotto copertura. In tal caso infatti, la condotta è volta a mascherare la propria identità e le proprie funzioni al fine di infiltrarsi e ottenere informazioni da altri soggetti. Invero, da un lato l'assunzione di identità virtuali per fingere di essere altri integra la fattispecie di sostituzione di persona e, dall'altro, utilizzare identità fittizie al solo scopo di introdursi in siti "chiusi" costituirebbe un'ingerenza illegittima nella sfera privata altrui. Tali condotte risultano scriminate se rientranti nella disciplina dell'agente sotto copertura altrimenti integrerebbero autonome fattispecie di reato[210].

In questo senso si possono distinguere le attività investigative "*discrete use*" ove le forze di polizia adottano l'anonimato per la ricerca e la conservazione di informazioni tratte da siti pubblici e le attività investigative "*covert use*" che sono maggiormente invasive in quanto comportano la creazione di un'identità digitale sotto copertura finalizzata a interagire con i soggetti[211].

Ulteriore tecnica investigativa consiste nell'acquisizione di contenuti illecite attraverso programmi di file-sharing quali le reti *peer to peer*. In tal caso è pacifica la legittimità dell'accesso a tali programmi senza che ciò costituisca, di per sé, esercizio di una tecnica investigativa speciale. Ciò che è fondamentale chiarire, invece, riguarda il compimento di atti delle forze di polizia riconducibili a fattispecie di reato quali il procurarsi e il detenere materiale pornografico. In tal caso, l'attività risulta scriminata e il risultato delle indagini utilizzabile processualmente soltanto se la condotta è riconducibile alla disciplina delle operazioni sotto copertura[212].

Strumento essenziale risulta, infine, l'hackeraggio di sistemi informatici utilizzato dalle autorità di *law enforcement*. Attraverso le attività investigative sopra menzionate, le autorità possono osservare utenti che compiono reati nel dark web ma non sempre possono identificarli. L'*hacking*, invece, consente di localizzare i presunti autori dei reati anche nel caso in cui questi utilizzino tecnologie di occultamento dell'identità. Dal punto di vista operativo, l'hackeraggio consente di accedere da

---

[210] Troisi, P. *Investigazioni nella rete e attività sotto copertura* in *Le investigazioni digitali sotto copertura.* cit. pp.88-90

[211] Shipley, T. G. (2013). *Investigating internet crimes: an introduction to solving crimes in cyberspace. Syngress.* p. 258

[212] Troisi, P. *Investigazioni nella rete e attività sotto copertura* in *Le investigazioni digitali sotto copertura.* cit. pp.92-94

remoto al dispositivo e di installare un malware all'interno del computer bersaglio. Una volta installato, si può forzare il sistema informatico a fare qualsiasi compito come caricare un file sul server o raccogliere foto e immagini. Data la sua evidente intrusività, lo strumento può essere disposto solo con la necessaria autorizzazione da parte dell'autorità giudiziaria. [213]. Tale sistema è disciplinato specificamente in varie ordinamenti ed anche in Italia dove, a seguito, della legge 137/2023, alle autorità competenti viene riconosciuta la possibilità di infiltrarsi nei sistemi informatici e alterarne o distruggerne funzionamento. Analogamente, nei Paesi Bassi il "*Dutch Computer Crime III Bill*" indica le funzionalità e le tecniche che le forze dell'ordine possono utilizzare al fine di perquisire da remoto un sistema informatico[214]. Negli Stati Uniti, l'FBI, durante l'indagine sul sito pedopornografico "*Playpen*", ha distribuito un malware che una volta aperto dall'utente rileva il suo indirizzo IP[215].

Le tecniche investigative utilizzate dalle forze dell'ordine in ambiente digitale sollevano rilevanti questioni in materia di tutela del diritto alla privacy e alla protezione dei dati personali. Dal punto di vista internazionale, la diversità di discipline interne può comportare ostacoli alla cooperazione internazionale che verranno analizzati successivamente, una volta trattati gli aspetti problematici delle operazioni sotto copertura.

3.1 Operazioni transnazionali significative nel contrasto ai reati informatici

Analizzando il profilo operativo della cooperazione internazionale con riferimento alle operazioni sotto copertura è necessario prendere in esame dei casi pratici nei quali l'utilizzo di strumenti investigativi speciali si è rivelato funzionale allo smantellamento di reti criminali nello spazio cibernetico.

Un esempio particolarmente significativo è rappresentato da due operazioni distinte: una statunitense condotta dal *Federal Bureau of Investigation* (FBI) insieme

[213] Davies, G. *Shining a light on policing of the dark web: An analysis of UK investigatory powers*
[214] European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs. (2017). *Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices* (Study No. PE 583.137 EN). European Parliament. pp.58-59
[215] Ivi. cit. p.126

alla *US Drug Enforcement Agency* (DEA) e una olandese gestita dalla Polizia Nazionale. Entrambe sono state coordinate e assistite da Europol e hanno portato allo smantellamento di due tra i principali *marketplace* illegali, ossia AlphaBay e Hansa.

AlphaBay veniva considerata la più grande piattaforma di scambio illecito presente nel Dark Web, con oltre 200000 utenti e 40000 venditori. Venivano commercializzati stupefacenti, sostanze chimiche tossiche, armi da fuoco, documenti d'identità illecitamente sottratti, merci contraffatte e strumenti di *hacking* quali malware. La stima del guadagno totale era pari ad almeno un miliardo di dollari[216].

Tale mercato è stato progettato per facilitare il commercio illecito attraverso l'anonimato, garantito dall'utilizzo del network "*The Onion Router*" (TOR) che consente di occultare il reale indirizzo IP degli utenti, e dall'impiego, ai fini delle transazioni, di criptovalute quali Bitcoin, Monero and Ethereum, che essendo prive di supporto fisico e utilizzabili esclusivamente online, assicuravano la riservatezza[217].

Hansa rappresentava invece il terzo *marketplace* criminale per dimensioni e presentava caratteristiche analoghe a AlphaBay quanto alla tipologia di beni e servizi illeciti scambiati. Decisivo è stato il ruolo delle indagini, condotte dalla Polizia Nazionale olandese con la collaborazione di Bitdefender, società di sicurezza informatica partner dell'*European Cybercrime Centre* (EC3) con il coordinamento di Europol.

Le indagini hanno consentito di localizzare l'infrastruttura del mercato illecito nei Paesi Bassi e di sequestrare server della stessa ubicati in Germania e in Lituania. Successivamente, grazie al coordinamento tra Europol e altre agenzie nazionali, la Polizia olandese ha assunto il controllo occulto di Hansa tramite un'operazione di infiltrazione che ha reso possibile l'effettuazione di attività di monitoraggio della piattaforma fino alla chiusura della stessa, avvenuta il 20 luglio del 2017. L'assunzione occulta del controllo di Hansa sotto l'autorizzazione giudiziaria olandese ha costituito l'elemento strategicamente determinante dell'operazione, rendendola uno dei più significativi successi della cooperazione investigativa europea.

---

[216] Europol. (2017, July 20). *Massive blow to criminal Dark Web activities after globally coordinated operation – Takedown of AlphaBay and Hansa will lead to hundreds of new investigations in Europe.* Europol.

[217] U.S. Department of Justice, Office of Public Affairs. (2017, July 19). *AlphaBay-Cazes forfeiture complaint and exhibits*

Occorre segnalare come sia decisiva la collaborazione internazionale oltreoceano anche per la peculiare coincidenza temporale con le operazioni statunitensi volte allo smantellamento di AlphaBay. Poiché, a seguito della chiusura della stessa, gli utenti si erano trasferiti su Hansa Market, determinando un incremento degli accessi pari ad oltre otto volte la media ordinaria, le autorità olandesi sono state poste in condizione di identificare anche gli utenti di AlphaBay[218].

L'operazione di infiltrazione ha sollevato rilevanti questioni che sono emerse in alcune sentenze, tra cui la pronuncia del tribunale distrettuale di Rotterdam in relazione a un procedimento per complicità nel traffico di stupefacenti sul Dark Web, riciclaggio di Bitcoin e possesso di armi da fuoco e munizioni. La difesa eccepiva la violazione del diritto al giusto processo causata dall'acquisizione, da parte delle forze di polizia, del marketplace Hansa, sostenendo che tale operazione sotto copertura non solo avesse facilitato il traffico illecito, ma che fosse stata condotta in assenza di presupposti normativi che legittimerebbero l'azione degli inquirenti. Secondo la difesa risulterebbe infatti impossibile verificare la legittimità dell'azione di polizia e il rispetto dei requisiti di proporzionalità e sussidiarietà necessari ai fini dell'infiltrazione.

Il tribunale ha tuttavia ritenuto legittima l'attività sotto copertura sostenendo che questa fosse conforme con quanto disposto dall'art.126h del codice di procedura penale olandese[219]. L'operazione era stata disposta nel giugno 2016 in attuazione del

---

[218] Europol. *Massive blow to criminal Dark Web activities after globally coordinated operation – Takedown of AlphaBay and Hansa will lead to hundreds of new investigations in Europe.*

[219] Netherlands. (2012). Code of Criminal Procedure: Incorporating amendments up to October 2012 (English non-official translation). United Nations Office on Drugs and Crime. Art. 126h: *In the case of suspicion of a serious offence as defined in section 67(1), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required in the interest of the investigation, order an investigating officer as referred to in section 141(b) to participate in or render assistance to a group of persons which may be reasonably suspected of planning or committing serious offences.*

2. In the execution of the warrant the investigating officer may not incite a person to commit criminal offences other than the criminal offences he already intended to commit.

3. The infiltration warrant shall be in writing and shall state:

a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect;

b. a description of the group of persons;

c. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met;

progetto "*26Gravesac*" del personale della High Tech Crime Unit olandese, sotto la responsabilità della Procura Nazionale di Rotterdam. Successivamente, il 20 giugno 2017, era stato emesso l'ordine di infiltrazione da parte del pubblico ministero. Tale ordine autorizzava il rilevamento occulto dell'infrastruttura senza modificarne il funzionamento, allo scopo di acquisire password, messaggi, ordini e informazioni relative ai Bitcoin in forma non crittografata per identificare venditori e acquirenti. Il team investigativo ha agito sotto forma di amministratore dell'infrastruttura illecita, rispondendo alle richieste degli utenti, partecipando alla messaggistica e mantenendo contatti con gli acquirenti. L'operazione è terminata il 20 luglio del 2017 con la chiusura del mercato illegale.

Il tribunale ha sancito la legittimità dell'azione di polizia visto che la relazione integrativa "*Gravesac*" forniva una descrizione accurata dell'operazione di infiltrazione e dei metodi di lavoro utilizzati dal team investigativo, dimostrando l'assoluta urgenza e necessità di tale strumento ai fini dell'indagine. L'infiltrazione ordinata, tenuto conto della natura e della gravità del traffico internazionale di stupefacenti online e dell'impossibilità di acquisire materiale probatorio relativo ai reati e agli attori operanti sul mercato illegale con mezzi meno invasivi, soddisfaceva i requisiti di proporzionalità e di sussidiarietà richiesti dalla norma.

Quanto all'ulteriore censura concernente una possibile ipotesi di istigazione al compimento del reato da parte delle autorità di polizia, il tribunale non ha ritenuto sussistente tale fattispecie in quanto l'operazione ha mantenuto invariata la situazione preesistente e non vi sono risultanze probatorie che integrassero la fattispecie di induzione alla commissione del reato o alla commissione di reati diversi rispetto a quelli che l'imputato aveva già intenzione di compiere. Pertanto, alla luce di tali argomentazioni, il giudice ha respinto le eccezioni della difesa sostenendo la piena legittimità e l'assenza di vizio procedurali dell'indagine sotto copertura[220].

Per quanto concerne l'operazione AlphaBay, Europol ha svolto un ruolo fondamentale di coordinamento, ospitando nei giorni precedenti al take down

---

d. the manner in which the warrant will be executed, including punishable acts, insofar as could be foreseen when the warrant was issued, and e. the term of validity of the warrant.

[220] Rechtbank Rotterdam. (2019, 3 luglio). ECLI:NL: RBROT: 2019:5339 (zaaknummer 10/960249-17). Raad voor de Rechtspraak.

dell'infrastruttura, un centro di comando con rappresentanti dell'FBI, della DEA e del Dipartimento di Giustizia statunitense. Tale struttura di comando è stata il nodo centrale dello scambio di informazioni e della cooperazione investigativa con le autorità degli Stati coinvolti. Successivamente Europol ha organizzato una *Cyberpatrol Action Week* internazionale con più di 40 investigatori provenienti da ben 22 Paesi, per permettere di costruire un quadro unitario dei fenomeni criminosi commessi nel Dark Net [221].

L'operazione AlphaBay ha consentito l'arresto del cittadino canadese Alexandre Cazes, alias Alpha02 e Admin, effettuato, per conto degli Stati Uniti, il 5 luglio 2017 in Thailandia, accusato di essere il creatore e l'amministratore del marketplace illecito. Cazes è stato imputato in un'*indictment*[222], depositato presso il Distretto Orientale della California contenente ben 16 capi di imputazione relativi ad associazione a delinquere finalizzata al racket, alla distribuzione di sostanze stupefacenti, al furto d'identità, alla frode informatica, al riciclaggio di denaro nonché per trasferimento illecito di documenti di identificazione falsi e traffico di strumenti di produzione di dispositivi. Inoltre è stato disposto dall'*U.S. Attorney's Office* del Distretto Orientale della California una *civil forfeiture complaint*[223] finalizzata a congelare e preservare i proventi illeciti delle attività realizzate nell'infrastruttura[224].

[221] Federal Bureau of Investigation. (2017, July 20). *AlphaBay takedown*. FBI.
[222] U.S. Department of Justice, Office of Public Affairs. (2017, July 20). *Indictment, United States v. Alexandre Cazes* (Case No. 1:17-CR-00144-LJO). U.S. Department of Justice.
[223] U.S. Department of Justice, Office of Public Affairs. (2017, July 19). *AlphaBay-Cazes forfeiture complaint and exhibits.* U.S. Department of Justice.
[224] U.S. Department of Justice, Office of Public Affairs. (2017, July 20). *AlphaBay, the largest online "dark market," shut down.*

Capitolo III.

Le criticità delle operazioni sotto copertura nei reati informatici

Sommario: 1. La finalità probatoria e la prassi "preventiva" 1.1 Limiti giuridici dell'uso di agenti sotto copertura e prevenzione dell'entrapment 1.2 Utilizzabilità delle prove acquisite: la testimonianza anonima e le operazioni sotto copertura illegittime 2. Differenze normative tra ordinamenti nazionali come ostacolo alla cooperazione internazionale 2.1 Criticità degli strumenti di cooperazione tradizionali e innovativi 2.2 *Law enforcement*, privacy e protezione dei dati personali 3. Rafforzamento della cybersicurezza nazionale ed europea 3.1 Strumenti tecnici e investigativi innovativi: l'avvento dell'AI 3.2 Prospettive nell'ipotesi di non cooperazione 3.3 Convenzione delle Nazioni Unite sul *cybercrime*: aspetti controversi

1. La finalità probatoria e la prassi "preventiva"

Avendo trattato fin qui degli aspetti prevalentemente positivi dell'evoluzione delle operazioni sotto copertura, specie in una prospettiva di cooperazione e di coordinamento nel contesto interno ed internazionale, risulta ora opportuno soffermarsi sugli aspetti più problematici della disciplina in esame che si rivelano ancora più critici quando il terreno operativo è il cyberspazio.

Un primo elemento problematico si riferisce alla fase in cui le operazioni sotto copertura possono essere attivate. Fin dalla loro prima disciplina normativa, le *covert actions* sono state concepite "*al solo fine di acquisire elementi di prova*" [225]. Di conseguenza, l'interpretazione prevalente le ha qualificate al pari di mezzi di ricerca della prova che presuppongono la già avvenuta commissione di un reato e la sussistenza di un procedimento penale, dovendosi quindi escludere l'interpretazione di un loro impiego per meri fini di prevenzione criminale[226].

Non sempre però la notizia di reato, attraverso cui si instaura un procedimento penale, risulta essere dettagliatamente delineata. In alcune ipotesi essa si presenta come lacunosa e imprecisa per via del tipologia di reato che presenta caratteristiche

[225] Troisi, P. *Investigazioni nella rete e attività sotto copertura* in *Le investigazioni digitali sotto copertura.* cit. pp.95-96

[226] Melillo, G. *Le operazioni sotto copertura nelle indagini relative a delitti con finalità di terrorismo*. cit. p. 49

esecutive difficilmente tracciabili o per la tipologia di reato che consiste in un reato permanente non ancora concluso oppure, infine, perché si tratta di un reato che muta nel corso delle indagini[227]. In tali ipotesi, i confini tra prevenzione e repressione appaiono sfumati e assottigliati.

Ciò avviene principalmente con riferimento ai fenomeni criminosi complessi quali ad esempio i reati associativi nei quali l'organizzazione criminosa è finalizzata programmaticamente alla commissione di ulteriori reati. In questi casi le attività sotto copertura possono tendere non tanto ad acquisire elementi probatori quanto a ricercare la *notitia criminis*. Si è infatti diffusa la prassi per cui la tecnica investigativa, essendo finalizzata a smantellare l'organizzazione criminale, può partire dai livelli più bassi della struttura organizzativa per poi allargarsi fino all'individuazione delle posizioni apicali, ampliandone di fatto l'ambito applicativo[228].

Lo stesso ragionamento vale per le operazione di intelligence criminale che si collocano, per loro natura, in una fase precedente rispetto all'indagine penale e sono finalizzate a " *raccogliere, elaborare e analizzare informazioni su reati o attività criminali al fine di stabilire se sono stati commessi o possono essere commessi in futuro atti criminali concreti*"[229].

In tema di *cybercrime*, i problemi finora delineati si amplificano in conseguenza non tanto della natura dei reati ma del terreno su cui essi operano: lo spazio cibernetico. Quest'ultimo, consentendo maggiore libertà di movimento, offuscando la differenza tra lecito e illecito e permettendo operazioni particolarmente invasive, rischia di trasformare l'operazione sotto copertura in una sollecitazione a commettere ulteriori reati o in un meccanismo di prevenzione più che di ricerca di prova.

Non appare sufficiente a ricondurre tale strumento nella sfera della repressione l'autorizzazione del pubblico ministero. Infatti si è portati a ritenere che, essendoci un coinvolgimento del magistrato che viene informato dei progressi operativi delle forze

---

[227] Curtotti, D. *Operazioni sotto copertura*. cit. p. 437

[228] Troisi, P. *Investigazioni nella rete e attività sotto copertura* in *Le investigazioni digitali sotto copertura.* cit. p.96

[229] Council of the European Union. (2006, December 18). *Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union* (OJ L 386, 29.12.2006, pp. 89–100). art. 2 c.1 lett.c

di polizia, si entri automaticamente nell'area delle indagini preliminari. Tuttavia, spesso l'intervento del p.m. è visto più come un mero requisito procedurale per garantire la non punibilità dell'agente piuttosto che come meccanismo per limitare la discrezionalità operativa degli organi di polizia. Inoltre non è infrequente l'attrazione del magistrato requirente nella fase in cui una notizia di reato non è ancora compiutamente formata e in cui i confini tra le funzioni di polizia giudiziaria e di polizia di prevenzione generale risultano difficilmente distinguibili.

Inoltre, anche se si volesse escludere la necessità di un procedimento già instaurato, rimarrebbe come presupposto per il ricorso a tale strumento speciale d'indagine la finalità probatoria volta a ricercare elementi utili a ricostruire condotte già esaurite o in via di commissione. Ciò richiederebbe almeno la parvenza di un sospetto che, pur non determinando una *notitia criminis*, sia idoneo almeno a imprimere la necessità di accertare fatti suscettibili di integrare ipotesi di reato. Pertanto, resterebbero in ogni caso escluse dalla disciplina in esame le attività investigative destinate a rinvenire notizie di reato o ad agevolare e creare situazioni favorevoli alla commissione dell'illecito.

Nonostante l'orientamento interpretativo prevalente sia orientato verso la necessaria esistenza di una notizia di reato e di un procedimento, la disciplina non definisce in modo puntuale i confini delle operazioni *undercover*. Ne consegue che, sul piano applicativo, il loro impiego ai fini preventivi o proattivi non sia infrequente. Si pensi alla prassi adottata nel contrasto alla pedopornografia. Sulla base di un'interpretazione sistematica dell'art. 14 della legge 269/1998, l'attività sotto copertura così delineata dovrebbe essere adoperata ai solo fini di acquisizione di elementi probatori. Tuttavia, le modalità operative quali l'attivazione di siti civetta, la possibilità di realizzare aree di scambio o partecipare a *chatbot* sembrano più che altro orientate a stimolare la commissione di un reato, dimostrando che la notizia di reato viene vista sempre più come un obiettivo piuttosto che una premessa[230].

Accogliere l'impostazione che permetterebbe di collocare la tecnica investigativa coperta nell'ambito delle attività pre-procedimentali compiute dalla polizia comporterebbe rilevanti criticità anche alla luce dei diritti costituzionali. Infatti

[230] Troisi, P. (2022) *Induzione al reato e giusto processo* in *Le investigazioni digitali sotto copertura.* Bari: Cacucci Editore. pp.96-107

taluna dottrina sostiene che "*in una fase esterna del procedimento penale, non fondata né sul pericolo di futura commissione di un reato, né ancora sulla notizia di reato già commesso, può farsi uso solo di mezzi che non intacchino il patrimonio giuridico di diritti e libertà oggetti di esplicita tutela (...) della Costituzione*"[231]. Pertanto, le indagini *undercover* non possono essere adoperate preventivamente senza incidere sulla posizione processuale di chi le subisce e sui i diritti di cui il soggetto dispone quali il diritto all'informazione, il contraddittorio, le garanzie del giusto processo[232].

Il dubbio tra prevenzione e repressione appena delineato è il frutto di una disciplina processuale incompleta e poco coordinata. Infatti, il legislatore italiano nel disciplinare le operazioni *undercover*, ha preferito concentrarsi sugli aspetti sostanziali dell'istituto quali sono i confini della condotta scriminante tralasciando però gli aspetti processuali che, invero, rappresentano la caratterizzazione principale dell'istituto.

Per tale ragione, un miglioramento della disciplina processuale consentirebbe di limitare maggiormente i rischi di abusi investigativi e attenuerebbe questioni interpretative controverse come quella sopra menzionata[233].

1.1 Limiti giuridici dell'uso di agenti sotto copertura e prevenzioni dell'*entrapment*

Una delle questioni più discusse in materia di operazioni sotto copertura concerne i margini di responsabilità penale dell'agente *undercover*. Anzitutto, è opportuno sottolineare il divieto di interpretazione analogica dei presupposti definiti dall'art.9 della l. 146/2006. Ne consegue che incorrerà in responsabilità penale l'agente sotto copertura che opera per l'accertamento di reati diversi da quelli definiti dalla norma[234].

Occorre, invece, analizzare il discrimine tra condotte lecite e illecite dell'agente sotto copertura. In tal senso si configura come condotta lecita quella dell'agente infiltrato, ossia del soggetto che si inserisce nelle strutture criminose,

[231] Zappulla, A. (2012). *La formazione della notizia di reato: Condizioni, poteri ed effetti.* Giappichelli. p.249
[232] Curtotti, D. *Operazioni sotto copertura*. cit. pp. 448-450
[233] Ivi pp.431-432
[234] Ivi p. 440

studiandone il funzionamento, senza mai assumere un ruolo attivo nella determinazione al reato, divenendo al più provocato alla commissione dello stesso per celare al meglio la propria identità. L'infiltrato, sulla base di una attività investigativa ufficiale, si limita ad osservare e contenere le attività illecite che, con estrema probabilità, siano già in fase di preparazione o di commissione del reato.

Diversamente è qualificabile come illecita l'attività dell'agente "*provocatore*" il quale, appartenente o meno alle forze dell'ordine, induce taluno a commettere un reato allo scopo di denunciare o cogliere in flagranza il soggetto provocato, ponendo in essere una condotta attiva senza la quale il reato non si sarebbe verificato[235].

Tale distinzione è stata elaborata dalla Corte europea dei diritti dell'uomo che sostiene che la provocazione da parte di agenti delle forze dell'ordine possa pregiudicare l'equità del processo comportando quindi una violazione dell'articolo 6 della Convenzione Europea dei Diritti dell'Uomo (CEDU) [236].

L'evoluzione giurisprudenziale che ha portato a tale affermazione parte dal *leading case Teixeira de Castro c. Portogallo*[237] nel quale la Corte ha qualificato come istigazione al reato l'acquisto simulato di sostanze stupefacenti effettuato da parte di due agenti della polizia portoghese. Quest'ultimi, operando in borghese, si erano introdotti in luoghi frequentati da tossicodipendenti per acquistare una certa quantità di eroina dal ricorrente, senza che l'operazione fosse stata previamente autorizzata dall'autorità giudiziaria e in assenza di indizi tali da far presumere che il soggetto fosse un narcotrafficante. In aggiunta la condanna era stata pronunciata facendo riferimento prevalentemente alle dichiarazioni dei due agenti di polizia.

La corte ritenne che l'attività investigativa, per come posta in essere, integrasse una violazione del principio del "giusto processo" in quanto, eccedendo i limiti della mera infiltrazione, aveva provocato il soggetto alla commissione del reato che non si sarebbe verificato in assenza di tale condotta[238]. Nel pronunciare la sentenza, la Corte

---

[235] Genovese, A. (2024). Capitolo XII. *Dall'agente sotto copertura all'agente provocatore. Limiti di applicazione della fattispecie.* In I *reati in materia di stupefacenti: iter legislativi e percorsi giurisprudenziali*. Giappichelli. pp. 293-312

[236] Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms* (Council of Europe Treaty Series No. 5). Council of Europe. art.6

[237] European Court of Human Rights. (1998, June 9). *Teixeira de Castro v. Portugal* (Application No. 25829/94). HUDOC.

[238] Bortolin, C. (2008). *Operazioni sotto copertura e «giusto processo».* In *giurisprudenza europea e processo penale italiano*. pp. 396–397

ha riconosciuto la tendenziale prevalenza del diritto ad una corretta amministrazione della giustizia rispetto a esigenze investigative finalizzate alla lotta contro il traffico di stupefacenti, stabilendo che "*While the rise in organised crime undoubtedly requires that appropriate measures be taken, the right to a fair administration of justice nevertheless holds such a prominent place (...) that it cannot be sacrificed for the sake of expedience. The general requirements of fairness embodied in Article 6 apply to proceedings concerning all types of criminal offence, from the most straightforward to the most complex. The public interest cannot justify the use of evidence obtained as a result of police incitement*"[239]. Ne deriva che nel caso in cui il reato sia stato determinato dall'intervento dell'agente delle forze dell'ordine che ha influito sulla sua commissione, tale condotta illecita si ripercuote sul piano processuale nel senso di escludere che una sentenza di condanna possa basarsi su prove create artificiosamente. Ciò è di fondamentale importanza, perché emerge una profonda e continua interazione tra profili processuali e sostanziali che impone al sistema processuale di non poter prescindere da una coerenza con i principi che disciplinano il rapporto cittadino-autorità pubblica[240].

A conferma di questa interazione, La Corte di Strasburgo ha elaborato un vero e proprio test di accertamento dell' "*entrapment*", via via perfezionato nelle successive pronunce su casi analoghi[241].

Il primo passo riguarda la dimensione sostanziale dell'operato dell'agente che viene appurata tramite il "*substantive test of incitement*". Si vuole accertare se l'agente sotto copertura sia un membro delle forze dell'ordine o un privato che opera sotto loro istruzione e se la condotta sia essenzialmente passiva o se, al fine di conseguire la prova, l'agente abbia influenzato altri alla commissione di un reato che altrimenti non avrebbero commesso. Per vagliare ciò, bisogna inizialmente verificare le ragioni che rendono necessario l'utilizzo di tale strumento atipico. Sotto questo profilo, la Corte ha stabilito che necessitano "*good reasons*" per poter procedere ad un'operazione sotto copertura, vale a dire che devono ricorrere obiettivi e concreti sospetti che rendano

[239] European Court of Human Rights. *Teixeira de Castro v. Portugal*. cit. par.36
[240] Bortolin, C. *Operazioni sotto copertura e «giusto processo».* cit. pp. 399-400
[241] Cfr. tra le altre: Ramanauskas c. Lituania (5 febbraio 2008); Bannikova c. Russia (4 novembre 2010); Matanovic c. Croazia (4 luglio 2017)

evidente il coinvolgimento dell'imputato in attività criminali o la sua predisposizione verso la commissione del reato.

Vi sono tuttavia casi in cui tale valutazione risulta problematica. Ad esempio la Corte ha ammesso che i presupposti per l'utilizzo di tale strumento investigativo si possano ricavare anche da informatori purché siano verificabili. Qualora, però, l'informatore agisca in collaborazione con la polizia, la condotta si riterrà lecita, e dunque non si parlerà di *entrapment*, se il reato era già in itinere. Più problematica è l'ipotesi di manovre coperte poste in essere in assenza di sospetti individualizzati, ma finalizzate a ricercare i membri di un'organizzazione criminale. In tal caso, la Corte ha affermato che debbano ricorrere elementi identificativi di condotte illecite preesistenti, quali la conoscenza dei prezzi delle droghe o la possibilità di poterle recuperare in poco tempo.

In secondo luogo, bisognerà verificare la condotta delle forze dell'ordine, per la quale la Corte ha escluso un atteggiamento passivo, e di conseguenza lecito, nell'ipotesi in cui le stesse prendano l'iniziativa di contattare l'indagato, formulino nuove richieste di contatto a seguito di alcune già rifiutate o, in generale, insistano per instaurare un contatto con il soggetto attenzionato. È stato, inoltre, stabilito che la prassi più adeguata a limitare i casi di provocazione si rinviene nell'esistenza di procedure autorizzative e di controllo da parte del giudice o, con determinate garanzie, da parte del pubblico ministero nonché nella sussistenza di un'adeguata documentazione delle attività investigative[242]. In aggiunte la Corte ha precisato che l'onere di provare l'assenza di condotte rientranti nella fattispecie della provocazione è in capo alla parte pubblica[243].

Sul piano processuale, la Corte europea dei diritti dell'uomo ha elaborato una verifica ulteriore tramite il cosiddetto "*procedural test of incitement*" volto a verificare se sia stato possibile per l'imputato sollevare il "*plea of incitement*" ossia far valere l'istigazione subita, se i giudici abbiano effettuato le idonee verifiche e laddove, rilevata la sussistenza della provocazione, ne abbiano rimosso gli effetti. In caso di esito negativo, si configurerebbe una violazione dell'art 6 della CEDU, determinando

[242] Troisi, P. *Investigazioni nella rete e attività sotto copertura* in *Le investigazioni digitali sotto copertura.* cit. pp.243-247
[243] Curtotti, D. *Operazioni sotto copertura*. cit. p. 446

quindi una iniquità del processo. In un primo momento, la Corte ha ritenuto di procedere alle verifiche procedurale solo nel caso in cui il test sostanziale non producesse esiti definitivi a causa di mancanze di elementi valutativi o per la non chiara ricostruzione degli eventi. Invero, recenti pronunce rendono necessario il vaglio procedurale, anche nel caso in cui sia già stato accertato *l'incitement*.

Il confine tra condotta lecita e illecita è ancora più labile nel caso di operazioni sotto copertura digitali che spesso presentano una tendenza provocatoria. Si pensi alle innovazioni stabilite dalla legge 137/2023, che ha previsto strumenti investigativi quali la possibilità di assumere il controllo dell'altrui dominio e di alterarne e modificarne le caratteristiche. In tali ipotesi, risulta opportuno precisare che la presenza di una disciplina normativa non vale come meccanismo di legittimità delle condotte istigatorie, al contrario, rende ancora più evidente come vi sia un problema strutturale alla base[244].

L'unico antidoto che limiterebbe le pratiche illecite è la costante controllabilità delle stesse. Sarebbe auspicabile, in tal senso, un controllo del giudice per le indagini preliminari sulla condotta dell'agente e sulla sua eventuale antigiuridicità. Si renderebbe inoltre necessaria una descrizione più puntuale delle attività che è consentito compiere sotto copertura sia per delimitare maggiormente l'area in cui opera la scriminante, sia per evitare violazioni del giusto processo nei confronti dell'indagato. Tale obiettivo, di maggiore tipizzazione risulta ancora più difficile da raggiungere nel contesto digitale, rendendo possibili maggiori condotte illecite [245].

1.2 Utilizzabilità delle prove acquisite: la testimonianza anonima e le operazioni sotto copertura illegittime

Sul piano delle implicazioni processuali, una delle maggiori problematiche consiste nella spendibilità dei risultati delle indagini *undercover* nel processo penale. Le risultanze probatorie acquisite nell'ambito di tali operazioni non si limitano, come accade frequentemente, a disporre arresti, sequestri di prove reali o del corpo del reato,

[244] Ciampi, S. *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*. cit. p. 734

[245] Bronzo, P. (2023, 19 ottobre). *Le indagini undercover nel mondo digitale*. Penale Diritto e Procedura. p. 7-8

ma consistono, principalmente, in dichiarazioni di informazioni raccolte dall'agente infiltrato[246]. La testimonianza dell'agente sotto copertura riveste un ruolo fondamentale nel procedimento, sia ai fini accusatori, sia per corroborare la posizione della difesa perché l'agente potrebbe fornire informazioni che escludano o limitino la responsabilità di determinati soggetti, a maggior ragione quando si metta in dubbio l'attività dell'agente come provocatore[247].

Tuttavia, l'esame degli agenti che hanno preso parte all'operazione avviene generalmente in forma anonima poiché questi, ai sensi dell'art.497 c.2-bis c.p.p., nel momento in cui sono invitati a fornire le proprie generalità, indicano quelle di copertura utilizzate nel corso dell'indagine. Solo il pubblico ministero potrà richiedere di conoscere l'identità reale dell'agente come previsto dall'art.9 c.4 della l.146/2006[248], determinando uno squilibrio di poteri tra accusa e difesa.

La testimonianza anonima qui discussa può determinare un pregiudizio nei confronti dell'imputato, al quale viene limitato di fatto il controesame dell'agente infiltrato comportando quindi una lesione del diritto di difesa, della presunzione di non colpevolezza e del principio del contradditorio. Su tale aspetto problematico si è concentrata ancora una volta la Corte di Strasburgo, che ha delineato le ipotesi in cui l'istituto della testimonianza anonima, posta a protezione dell'agente *undercover*, determinerebbe una violazione del diritto al controesame stabilito dell'art. 6 par.3 lett. d) della CEDU, traducendosi quindi in un effettivo pregiudizio per l'imputato e in una iniquità del procedimento.

Ai fini dell'accertamento di tale violazione, la Corte ha stabilito che vada verificata, in primo luogo, la sussistenza di "*buone ragioni*" idonee a giustificare l'anonimato dell'agente: esse sono ravvisabili nelle esigenze di protezione del soggetto e della sua famiglia ovvero nella possibilità di effettuare ulteriori future indagini. Nell'ordinamento interno, tuttavia, si è consentito sovente l'impiego della testimonianza anonima senza accertare la presenza di presupposti che la rendessero necessaria. Un esempio sono le operazioni sotto copertura nel contesto digitale dove l'agente non opera svelando il proprio ruolo ai cybercriminali, ma agisce per mezzo di

[246] Bronzo P. *Le operazioni sotto copertura nel web.* cit. p. 183
[247] Biral, M. (2023). *La testimonianza anonima degli agenti sotto copertura*. Wolters Kluwer. p.210
[248] Bronzo P. *Le operazioni sotto copertura nel web.* cit. p. 183

identità fittizie, operando perciò come mero gestore virtuale schermato dal mezzo tecnologico. In questo caso il pregiudizio arrecato all'imputato risulterebbe ancor meno giustificabile.

In secondo luogo, occorre verificare la valenza probatoria degli elementi raccolti, accertando se questi siano esclusivi e decisivi ai fini della decisione oppure se siano avvalorati da elementi esterni diversi dalla testimonianza anonima, così da non comportare una iniquità del processo.

Occorrerà inoltre appurare se siano state assicurate "*strong procedural safeguards*" per consentire al giudice di valutare l'affidabilità delle dichiarazioni e alla difesa di contestarle. Solo una volta accertati questi tre presupposti, si può confermare se si è in presenza di un'effettiva violazione del diritto al contradditorio. Ne consegue che, nonostante la testimonianza anonima, si può ancora assicurare l'equità del procedimento[249].

I limiti finora esposti attengono prevalentemente alla tutela del contraddittorio nei confronti dell'imputato. Tuttavia un ulteriore profilo problematico, messo in rilievo dal Direttore del servizio di Polizia Postale e per la Sicurezza Cibernetica Ivano Gabrielli, attiene alla necessità di salvaguardare il *know-how* tecnologico dell'attività investigativa. In particolare, il riferimento è all'art.329 c.p.p. che disciplina la segretezza delle indagini sino al momento in cui l'imputato possa averne conoscenza e, comunque, non oltre la chiusura delle indagini preliminari. Tale disposizione comporta, nell'ambito delle investigazioni sotto copertura, la rivelazione delle tecniche e delle tecnologie innovative utilizzate ai fini delle indagini. Tuttavia, rendendo pubbliche tali informazioni, si rischierebbe di compromettere l'utilizzo del *know-how* tecnologico, finora acquisito, per le indagini successive, rendendole così inefficaci.

A tal proposito Gabrielli ritiene necessario un intervento normativo che, fermo restando il rispetto del contraddittorio come presupposto del giusto processo, tenga in considerazione la necessaria esigenza di mantenere la riservatezza delle informazioni circa le tecnologie utilizzate nel corso dell'attività *undercover*[250].

[249] Troisi, P. (2022). *Provocazione per la prova e garanzie difensive* in *Le investigazioni digitali sotto copertura.* Bari: Cacucci Editore pp.329-333
[250] Gabrielli, I. Intervista condotta dall'autore. Intervista non pubblicata.

Ancora più controverse sono, invece, le questioni legate all'utilizzabilità processuale dei risultati di operazioni sotto copertura poste in violazione delle norme regolatrici. Anche in questo caso l'origine del problema viene rinvenuto nella mancanza di adeguati dettami processuali in materia. Il legislatore, invero, si è preoccupato di stabilire i limiti della non punibilità dell'agente sotto copertura, tralasciando però di dettare disposizioni in merito alle sorti processuali del materiale probatorio acquisito a seguito di un'operazione *contra legem*. A tal proposito, dottrina e giurisprudenza hanno analizzato il problema proponendo quattro diversi scenari possibili.

Il primo si riferisce alla possibilità di determinare l'inutilizzabilità della prova ai sensi dell'art.191 c.p.p., riconducendo la violazione delle norme penali dettate per le operazioni sotto copertura allo schema della "*prova illecita*" prevista dalla disposizione. Tuttavia, è difficilmente plausibile determinare tale sanzione processuale sulla base di una violazione di norme sostanziali.

Un'altra ricostruzione ammette l'inutilizzabilità sulla base di violazioni di norme costituzionali o convenzionali, facendo riferimento al principio del giusto processo. Questa impostazione potrebbe essere accolta esclusivamente per l'ipotesi dell'*entrapment* che, come già analizzato, determinerebbe una iniquità nel processo. Difficilmente, infatti, tale conclusione può essere accettata nelle altre ipotesi di violazioni di legge come nel caso di operazioni disposte per reati diversi da quelli tassativamente indicati oppure indagini effettuate in assenza di autorizzazione da parte dell'autorità giudiziaria. In queste ipotesi, si potrebbe configurare un'ingerenza nella vita privata che non sempre si traduce in una violazione del diritto ad un processo equo.

Una terza interpretazione si riferisce alla normativa *undercover* come una disciplina non solo sostanziale ma anche processuale perché stabilisce i procedimenti per i quali la tecnica è consentita e determina la necessità di un'autorizzazione dall'autorità giudiziaria. Da ciò deriverebbe, nel caso di violazione della normativa *undercover*, un divieto probatorio di cui all'art. 191 c.p.p. di tipo "*indiretto*". Anche questa impostazione purtroppo non convince perché l'art.191 c.p.p. determina l'inutilizzabilità solo per le prove vietate ossia per quelle prove che non rispettano i requisiti di ammissibilità. Perciò la violazione delle modalità di acquisizione di una prova in sé ammissibile determinerebbe una mera irregolarità per la quale non potrebbe

operare la sanzione processuale, salvo che la norma stessa preveda la nullità o l'inutilizzabilità, ipotesi che non ricorre nel caso di specie.

L'ultima alternativa è quella che nega la rilevanza processuale delle violazioni per cui la normativa delle operazioni sotto copertura sarebbe esclusivamente finalizzata a delimitare l'area della non punibilità, senza incidere sul piano processuale. Ovviamente ammettendo tale impostazione sarebbero alti i rischi di abusi investigativi e di violazioni di diritti dell'imputato nel processo[251].

2. Differenze normative tra ordinamenti nazionali come ostacolo alla cooperazione internazionale

Dato la natura ormai transnazionale di alcune tipologie di reato perpetrate da le organizzazioni criminali e reti terroristiche in ambito *cybercrime*, si è reso indispensabile adottare forme di cooperazione internazionale che permettano di coordinare efficacemente le attività di *law enforcement*. Tale esigenza emerge specialmente con riferimento ad uno degli strumenti investigativi ritenuti più efficaci nel contrasto a tali fenomeni, ossia le operazioni sotto copertura. A tal fine si necessita un sempre maggiore allineamento tra ordinamenti giuridici differenti, obiettivo questo non sempre facilmente raggiungibile.

Vari, infatti, sono gli ostacoli ad una efficace cooperazione transnazionale in materia di operazioni sotto copertura. In primis, la tendenza dei sistemi di polizia nazionale a rispondere in via prioritaria alle esigenze del proprio ordinamento interno, piuttosto che alle necessità degli attori stranieri.

In secondo luogo, il fondamentale impedimento ad una cooperazione efficace si sostanzia nella eterogeneità degli ordinamenti giuridici interni, i quali concepiscono e regolano le operazioni *undercover*, già controverse per loro stessa natura, in maniera tendenzialmente diversa[252]. Un esempio emblematico di pluralità di approcci normativi è rappresentato dalla diversa concezione dell'*entrapment defense*, ossia la difesa che l'imputato può sollevare in merito all'ipotesi in cui "*a government agent*

[251] Bronzo P. *Le operazioni sotto copertura nel web.* cit. p. 183-193
[252] Ross, J. E. (2004). *Impediments to Transnational Cooperation in Undercover Policing: A Comparative Study of the United States and Italy.* The American Journal of Comparative Law., 52(3), pp. 570-574

induc[es] a person to commit an offense that the person would otherwise have been unlikely to commit"[253].

Soprattutto sul piano digitale, le operazioni sotto copertura, pur essendo fondamentali per combattere la criminalità informatica, sollevano questioni in merito alla possibile istigazione al reato. Si pensi al rischio di provocazione che potrebbe insinuarsi nel caso di utenti che operano nei *marketplace* del *dark web* gestiti e controllati dalle forze dell'ordine le quali hanno l'obiettivo di instaurare rapporti di fiducia con i cybercriminali. In tale ambito, l'assenza di una disciplina normativa comune in materia di *entrapment* può rappresentare un ostacolo alla cooperazione internazionale tra forze dell'ordine. Infatti, come afferma Giulio Calcara, studioso di diritto penale transnazionale, "*police services might decide to desist on activating cooperation processes if differences in substantive criminal law are significant. In general, police cooperation is firmly grounded on the premise of an equivalent criminalization of specific acts or omissions*"[254].

Tra i sistemi giuridici nazionali che prevedono l'*entrapment defense*, è necessario menzionare il sistema statunitense, nel quale l'istituto ha avuto origine nel XX secolo. I tribunali federali americani ammettono due tipi di modello di *entrapment*. Il primo, di tipo soggettivo, si concentra sulla predisposizione dell'imputato a commettere il crimine più che sulla condotta delle forze dell'ordine. In tal caso, se il soggetto era già intenzionato a commettere il reato, la difesa della provocazione non viene accolta. Il secondo modello è invece oggettivo poiché analizza la condotta delle forze dell'ordine verificando se la stessa sarebbe stata idonea ad istigare alla commissione del reato una persona ragionevole e rispettosa della legge. Se ciò viene accertato l'eccezione dell'*entrapment* è accolta, senza che rilevi la predisposizione del soggetto a commettere il crimine[255]. Il sistema statunitense, tuttavia, ammette un impiego particolarmente esteso delle operazioni sotto copertura, prevedendo una disciplina generale che non ne limita l'applicazione a determinate fattispecie di reato e non prevede sanzioni penali nei confronti dell'agente provocatore.

---

[253] *Entrapment*, (nov. 12, 2010), IBJ crim. defence wiki

[254] Calcara. G. (2019). *Rethinking Legal Research on Matters of International Police Cooperation: Issues, Methods and Raison d'Être,* 40 LIVERPOOL L. REV. pp. 95-96

[255] Girard, R. N. (2023). *The honeypot stings back: Entrapment in the age of cybercrime and a proposed pathway forward*. Chicago Journal of International Law, 24(1), pp. 189–197.

Questo si differenzia profondamente da ciò che avviene in Italia che, oltre ad avere una disciplina che permette l'utilizzo di tale strumento investigativo solo in casi tassativi, è maggiormente orientata per la tutela dello Stato di diritto. Questo, infatti, verrebbe a corrodersi se si consentisse agli agenti sotto copertura di partecipare ai reati senza subire conseguenze e quindi senza far rispettare il principio per cui il diritto penale si applica a tutti[256]. Inoltre, il richiamo alle libertà civili è stato delineato anche, come già visto, dalla Corte europea dei diritti dell'uomo che ha interpretato la CEDU nel senso di stabilire una tutela per il giusto processo degli imputati le cui condanne si fondano su prove ottenute tramite operazioni sotto copertura caratterizzate da condotte di provocazione.

Sempre nel contesto europeo, molti ordinamenti nazionali, interpretando l'articolo 8 della CEDU posto a garanzia della vita privata e familiare, hanno predisposto un quadro normativo che subordina le investigazioni sotto copertura ad autorizzazione e vigilanza continuativa da parte dell'autorità giudiziaria, limitandone l'impiego per reati gravi tassativamente indicati per i quali strumenti meno invasivi risulterebbero inefficaci. In questo modo, in favore di una maggiore tutela delle libertà sociale, si delimita il loro ambito di applicazione, sia in senso soggettivo stabilendo quali soggetti sono autorizzati ad infiltrarsi, sia in senso oggettivo definendo specifiche categorie di reati e determinando le tecniche che possono essere impiegate. Tale assetto normativo è necessario anche in ragione del fatto che molti sistemi nazionali prevedono la responsabilità penale degli agenti che operano al di fuori dei suddetti limiti. La disciplina garantista europea, per contro, non trova cittadinanza negli Stati Uniti dove gli strumenti *undercover* non necessitano di alcune procedura autorizzativa e possono essere attivati anche in assenza di prove o sospetti circa la commissione di un reato[257]. Inoltre, mentre in Europa esse sono strettamente legate agli apparati di polizia e al potere pubblico, negli Stati Uniti tali tecniche sono comuni anche al di fuori dell'ambito governativo, potendo essere utilizzate anche in settori privati[258].

[256] Ross, J. E. *Impediments to Transnational Cooperation in Undercover Policing: A Comparative Study of the United States and Italy.* cit. pp.577-581
[257] Ross, J. E. (2014). *Undercover Policing and the Varieties of Regulatory Approaches in the United States*. *American Journal of Comparative Law, 62*(Suppl. 1) pp. 675-676
[258] Ross, J. E. (2015). *Anti-terror stings and human subjects research: The implications of the analogy for notions of entrapment and for the pursuit of strategic deterrence. New York University Journal of International Law and Politics, 47*(2), p. 390.

Quanto finora osservato dimostra come, nel sistema statunitense, la disciplina delle investigazioni sotto copertura sia molto più permissiva e solo in minima parte regolamentata. Ciò emerge sia nella fase preventiva, connotata da un quadro normativo scarno e dall'assenza della garanzia dell'autorità giudiziaria, sia sul piano processuale, dove l'*entrapment defense* è ammessa ma la si riconosce in casi eccezionali nei quali l'influenza governativa sia talmente grave da comportare una totale distorsione della volontà del soggetto imputato[259].

Differenti approcci emergono anche con rifermento alla dimensione operativa delle investigazioni, potendo distinguere tra "*reactive investigations*" ossia indagini che intervengono in presenza di un reato già consumato e "*proactive investigations*" cioè indagini che si attivano prima o durante la commissione dello stesso[260]. Il sistema statunitense tende ad adottare un approccio proattivo alle operazioni sotto copertura. A tal proposito, taluna dottrina le qualifica come " *a proactive investigative tactic that allows police officers and informants to infiltrate criminal organizations or to test the criminal resolve of suspected offenders, by disguising their true identities and orchestrating criminal opportunities*"[261]. Al contrario, in Italia l'interpretazione prevalente, come previamente analizzato, tende verso un modello di indagine reattivo, seppur la prassi non sia sempre di tale avviso.

Concentrandosi sui modelli legislativi che prevedono l'*entrapment* è da menzionare il Canada che si è spinto, seppure in materia limitata, verso una più attenta protezione dello Stato di diritto e del diritto ad un equo processo, prendendo esempio dalla giurisprudenza della Corte EDU. Il Canada ha definito in via giurisprudenziale i limiti all'approccio proattivo nelle indagini, definendo i casi in cui si stia creando un'opportunità criminale da quelli in cui vi è una condotta di provocazione inammissibile. Tuttavia, la disciplina è peculiare in quanto i giudici, una volta ravvisato l'*entrapment*, sono tenuti a sospendere il procedimento per abuso del

[259] Ross, J. E. *Undercover Policing and the Varieties of Regulatory Approaches in the United States*. cit. 683.
[260] Shipley, T. G. (2013). *Investigating internet crimes: an introduction to solving crimes in cyberspace* /. Syngress,.
[261] Ross, J. E. *Undercover Policing and the Varieties of Regulatory Approaches in the United States*. cit.p.673

processo ma tale rimedio interviene solo dopo che la colpevolezza sia stata accertata[262].

Esistono invece ordinamenti nei quali la tutela della posizione dell'imputato da condotte di provocazione instaurate delle forze di polizia risulta essere particolarmente debole. A titolo esemplificativo, il sistema di Singapore riconosce generalmente l'*entrapment* come una condotta lecita consentendo, al più, la mitigazione della pena o l'inutilizzabilità probatoria nel caso in cui il danno arrecato all'imputato sia superiore rispetto all'utilità della prova nel procedimento.

L'Australia, invece, ha optato per la possibile (e rara) esclusione della prova, rimessa alla discrezionalità del giudice, quando le azioni delle forze di polizia siano talmente gravi da dover dare prevalenza alla tutela dell'ordine pubblico piuttosto che alla condanna del soggetto.

In Cina, l'*entrapment* non viene considerata una condotta illecita. Il tribunale, anziché escludere la prova, potrà, in rare ipotesi, ridurre la pena qualora accerti l'induzione al reato. Il governo cinese, infatti, qualifica le operazioni sotto copertura come un "*test di virtù*" volto a saggiare la predisposizione criminale di determinati soggetti. Tale impostazione riflette la concezione dello Stato particolarmente improntato alla sorveglianza e poco attento alle libertà sociali dei cittadini.

Da quanto finora analizzato, emerge una profonda differenziazione tra le diverse concezioni di *entrapment*, sia per i Paesi che la riconoscono, sia per quelli che la escludono o la limitano fortemente. Questa eterogeneità compromette la cooperazione internazionale in materia di *cybercrime*, il quale, essendo il reato transnazionale per eccellenza, è probabile che coinvolga una pluralità di Stati che difficilmente possono cooperare efficacemente in presenza di significative differenze normative[263].

2.1 Criticità degli strumenti di cooperazione tradizionali e innovativi

[262] Bronitt, S. (2004). *The law in undercover policing: A comparative study of entrapment and covert interviewing in Australia, Canada and Europe*. Common Law World Review, 33 (1). p.78

[263] Girard, R. N. *The honeypot stings back: Entrapment in the age of cybercrime and a proposed pathway forward*. pp. 202-205

Il principio di territorialità, che attribuisce agli Stati la giurisdizione sui reati commessi nel proprio territorio, viene progressivamente intaccato dal fenomeno del *cybercrime*. Ciò accade perché i cybercriminali, potendo operare da qualsiasi luogo connesso a Internet, estendono generalmente la loro attività oltre le barriere giurisdizionali tradizionali. In tale contesto, uno dei principali obiettivi a livello internazionale è quello di evitare che gli autori dei reati informatici non siano perseguibili a causa dell'impossibilità di attivare alcuna giurisdizione nei loro confronti. Per tale ragione numerose convenzioni e sistemi nazionali adottano un approccio estensivo della propria giurisdizione. A titolo esemplificativo, l'art.22 della Convenzione di Budapest[264] stabilisce che uno Stato può esercitare la propria giurisdizione in relazione ai reati in essa disciplinati se gli stessi siano commessi nel suo territorio, a bordo di una nave battente bandiera dello Stato, a bordo di un aeromobile immatricolato secondo le sue leggi ovvero da un suo cittadino, se il reato è punibile secondo il diritto penale del luogo in cui è commesso o se il reato è stato commesso al di fuori della giurisdizione territoriale di qualsiasi Stato[265].

Tuttavia, se da una parte tale estensione consente di perseguire i cybercriminali che hanno commesso reati in più ordinamenti, dall'altra può determinare una espansione eccessiva della giurisdizione comportando conflitti tra Stati.

Si pensi ad un criminale informatico che operando da un Paese A, magari dotato di un'attività di law enforcement inadeguata, violi dei server nello Stato B causando danni finanziari a vittime dello Stato C[266]. In tal caso, si potrebbe determinare un conflitto positivo di giurisdizioni, ossia una situazione in cui più Stati rivendicano la propria giurisdizione su quella condotta e nei confronti dello stesso autore del reato[267], non sempre attivando meccanismi di coordinamento investigativo.

La questione di giurisdizione non rileva ai soli fini procedurali ma anche ai fini operativi, in particolare compromettendo l'efficacia operativa delle indagini in materia

---

[264] Council of Europe. *Convention on Cybercrime*. cit. art.22

[265] Khalifa, A. M. M. (2020). *Overcoming the conflict of jurisdiction in cybercrime* (Master's thesis, The American University in Cairo). AUC Knowledge Fountain. pp. 41-42

[266] Coupland, H. (2025). *Investigating cybercrime: The key jurisdictional and technical challenges faced by law enforcement and ways to address them* (Vol. 6). *York Law Review*. University of York. pp.7-9

[267] Brenner Susan W. (2006) '*Cybercrime Jurisdiction'* in *Cybercrime: The Transformation of Crime in the Information Age*. Polity. p. 197

di reati informatici[268]. Data la natura transnazionale del *cybercrime* e la pluralità di giurisdizioni coinvolte, le autorità di *law enfocement* sono tenute ad attivare i tradizionali strumenti di cooperazione quali le Mutual Legal Assistance (MLA). Tuttavia, i rigidi requisiti formali che ne presuppongono l'attivazione possono provocare ritardi procedurali significativi, risultando spesso inefficaci per le esigenze investigative in materia di reati informatici. Se il cybercriminale impiega pochi minuti per compiere il reato, l'attività investigativa effettuata tramite gli strumenti di cooperazione internazionale può richiedere mesi prima di produrre dei risultati concreti. In questo senso, le inutili lungaggini procedurali non fanno che rendere ineffettiva la risposta globale al *cybercrime* che dovrebbe essere, in verità, rapida e immediata.

In aggiunta, sovente i meccanismi di cooperazione non vengono neppure attivati perché gli Stati non sono a conoscenza delle indagini effettuate in altri paesi sulle stesse condotte. Per ovviare a ciò, Europol e Eurojust hanno previsto, in via prioritaria, la "*deconfliction*" che consiste nell'evitare che gli Stati membri indaghino sugli stessi autori e sullo stesso reato senza previamente instaurare un meccanismo di coordinamento, rendendo così le indagini incomplete e prive di utilità[269].

Al fine di superare gli inutili rallentamenti che caratterizzato le procedure tradizionali sono state predisposte, come visto in precedenza, le *Joint Investigation Teams* (JITs). Nonostante siano considerate strumento investigativo d'eccellenza, anche queste presentano varie criticità rilevate nel sistema europeo. Anche per tale meccanismo investigativo, è stato evidenziato come le differenti legislazioni nazionali relative alla sua attivazione possano rallentare l'istituzione di una squadra investigativa comune, compromettendo le indagini sul *cybercrime*. Per questo è stato ideato da Eurojust un modello standard di accordo JITs per i cyber-attacchi, volto ad evitare ritardi significativi per questioni procedurali. Ulteriori problematiche sono connesse al numero dei Paesi che partecipano alle indagini. Per ovviarvi, si è prevista la possibilità di ricorrere a forme di cooperazione aggiuntive quali le *task-force* di cui un esempio è J-CAT. Altre criticità riguardano la finalità della JITs che deve essere

[268] Coupland, H. *Investigating cybercrime: The key jurisdictional and technical challenges faced by law enforcement and ways to address them*. cit. p.8
[269] Europol. (2024). *Common challenges in cybercrime 2024*. p.20

previamente determinata ma che potrebbe subire modifiche nel corso delle indagini, determinando così l'esigenza di nuove autorizzazione. Inoltre, si è riconosciuta anche una generale carenza di conoscenze ed esperienza in materia di cybercrime che certamente limita l'efficacia investigativa[270].

In tema di strumenti innovativi volti a facilitare la cooperazione, la Convenzione di Budapest del 2001 ha introdotto il network 24/7, un meccanismo di cooperazione che consente la conservazione dei dati elettronici e lo scambio tempestivo di informazioni investigative sui crimini informatici. Nonostante tale preziosa utilità, non tutti i paesi che hanno ratificato la Convenzione hanno predisposto un punto di contatto 24/7[271], con la conseguenza che lo strumento risulta scarsamente utilizzato. Secondo i dati disponibili, risulta che solo il 3% dei casi di criminalità informatica transnazionale è stato risolto con l'impiego di tale strumento di cooperazione.

Con riferimento agli strumenti di cooperazione, un'ulteriore limite è rappresentato dalla disparità di risorse tra gli Stati. Tale divario è in larga misura riconducibile all'assenza di un quadro giuridico globale uniforme, dal momento che il *cybercrime* è disciplinato prevalentemente da strumenti bilaterali e multilaterali. Ne consegue che, mentre alcuni Stati sono dotati di meccanismi idonei a fronteggiare il crimine informatico, altri Paesi, non avendo a disposizione gli stessi mezzi finanziari o lo stesso grado di conoscenza in materia, risultano strutturalmente incapaci di affrontare tale minaccia di portata globale[272].

In conclusione, l'assenza di uniformità internazionale e la presenza di un quadro giuridico frammentato, minano l'utilizzo di forme di cooperazione formali ed informali e permettono ai criminali informatici di sfruttare tali carenze per perpetrare reati in ordinamenti distinti[273].

---

[270]Council of the European Union. (2019, 5 November). *Conclusions of the 15th Annual Meeting of National Experts on Joint Investigation Teams (JITs): JITs in cybercrime cases: challenges and opportunities* (Document 13752/19). Eurojust. p.7-8

[271]Council of Europe. (2008). *The effectiveness of international co-operation against cybercrime: Examples of good practice* (T-CY/DOC-567study4-Version7). p. 15

[272] United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime* (E/CN.15/2013/CRP.4). pp.24-26

[273] Coupland, H. *Investigating cybercrime: The key jurisdictional and technical challenges faced by law enforcement and ways to address them*. cit. p.9

2.2 *Law enforcement*, privacy e protezione dei dati personali

Le indagini sui reati informatici possono ledere diversi diritti fondamentali, tra i quali assume rilievo il diritto al rispetto della vita privata e familiare definito in ambito internazionale dall'art.8 della CEDU[274] e dall'art.17 del Patto internazionale sui diritti civili e politici[275].Tale diritto garantisce la tutela della riservatezza nelle comunicazioni telematiche e la protezione del soggetto da ingerenze indebite del potere statale[276]. Esso, tuttavia, non ha carattere assoluto e può essere soggetto a limitazioni determinate, nel caso di specie, da esigenze di prevenzione e repressione dei reati. A tal fine, il diritto internazionale dei diritti umani prevede che qualsiasi restrizione di un diritto debba essere prevista dalla legge e debba rispettare i requisiti di necessità e proporzionalità.

Il principio di legalità stabilisce che ogni restrizione ai diritti dell'individuo sia specificamente prevista nella legislazione nazionale, che tale disciplina sia accessibile a tutti e che si prevedano idonee garanzie volte a prevenire applicazioni arbitrarie da parte del potere pubblico. Il principio di necessità impone la presenza di un fine legittimo che giustifichi la limitazione del diritto. La CEDU in tal senso ha riconosciuto, al comma 2 dell'art.8, che le restrizioni all'esercizio dei diritti possono essere giustificate da esigenze di sicurezza nazionale, di pubblica sicurezza, di protezione dei diritti di libertà o di prevenzione di disordini o reati. Inoltre, le misure restrittive devono avere durata limitata ed essere circoscritte a quanto strettamente necessario per il raggiungimento della finalità perseguita, limitandone dunque un impiego eccessivamente penetrante. Il principio di proporzionalità prevede che qualsiasi misura limitativa dei diritti deve essere proporzionata al fine legittimo perseguito. Ciò richiede di verificare l'inesistenza di misure meno invasive e di garantire che la restrizione non sia arbitraria e discriminatoria[277].

---

[274] Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms* (Council of Europe Treaty Series No. 5). Council of Europe. art.8

[275]United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) [Treaty Series, vol. 999, p. 171]. United Nations.

[276] Organization for Security and Co-operation in Europe. (2023). *Ensuring human rights compliance in cybercrime investigations: OSCE training guide for criminal justice practitioners* (ISBN 978-92-9271-245-7). OSCE Secretariat, Transnational Threats Department.p.15

[277] Ivi p.18

Si desume quindi la necessità di un adeguato bilanciamento tra le esigenze investigative e il rispetto del diritto alla privacy. Tale punto di equilibrio, in materia di operazioni sotto copertura, si riferisce innanzitutto alla predisposizione di una durata limitata di tali attività estremamente invasive, sottolineato anche dalla giurisprudenza della Corte di Strasburgo[278]. Le operazioni *undercover*, anche qualora risultino giustificate da esigenze di repressione dei reati, se predisposte in assenza di delimitazione temporale, rischierebbero di trasformarsi in forme di sorveglianza segreta e continuativa, sproporzionate rispetto ai fini stabiliti dal mezzo investigativo.

Tuttavia, la fissazione di limiti temporali per uno strumento di indagine che dipende in larga parte dalle risultanze ottenute è particolarmente complessa, soprattutto se l'indagine viene svolta nel contesto digitale. Si pensi alla normativa francese che non prevede alcuna limitazione temporale alle infiltrazioni cibernetiche.

In secondo luogo, le operazioni sotto copertura devono essere previamente autorizzate da un'autorità giudiziaria quale il pubblico ministero o il giudice.

Tuttavia, non sempre la preventiva autorizzazione è prevista dalla disciplina interna degli Stati. Ad esempio in Francia gli agenti sotto copertura nell'ambiente digitale possono operare anche in assenza di previa autorizzazione se le esigenze investigative lo giustifichino. Se, da un lato, ciò consente una maggiore flessibilità operativa, dall'altro, solleva dubbi circa la conformità della disciplina interna alla giurisprudenza della Corte EDU. Quest'ultima, ha ritenuto che le operazioni sotto copertura debbano essere eseguite sotto il controllo di un organo indipendente, anche non necessariamente giudiziario[279], riconoscendo peraltro che il pubblico ministero non sempre soddisfi tali requisiti[280].

La Corte EDU ha altresì riconosciuto la possibilità che l'infiltrazione sia attivata, in casi urgenti, senza autorizzazione preventiva se ciò non determini una discrezionalità illimitata per gli organi di polizia[281]. In tal senso, la Corte riconosce anche la particolare funzione dell'autorizzazione che consente di delimitare l'attività

[278] ECtHR. (2016) Szabó and Vissy v. Hungary. 37138/14.
[279] ECtHR. (2006) Weber and Saravia v. Germany. 54934/00; (2016) Szabó and Vissy v. Hungary. 37138/14.
[280] ECtHR. (2010) Moulin v. France. 37104/06.
[281] ECtHR. (2015) Roman Zakharov v. Russia. 47143/06.

di indagine sotto copertura soprattutto con riferimento alla durata la cui limitazione non è sempre prevista dalla legge[282].

Un ulteriore aspetto fondamentale del diritto alla privacy attiene alla protezione dei dati personali riconosciuta in vari strumenti internazionali tra i quali la Convenzione del Consiglio d'Europa per la protezione delle persone rispetto al trattamento automatizzato dei dati del 28 gennaio 1981, il Regolamento dell'UE 2016/679 (GDPR) riferito alla protezione delle persone fisiche con riguardo al trattamento di dati personali e alla loro libera circolazione, la Direttiva UE 2016/680 che disciplina il trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali.

La Corte di Strasburgo ha individuato diverse misure di polizia che possono comportare una limitazione al diritto ad una adeguata conservazione, trattamento e utilizzo di dati personali. Tra queste rientrano, ad esempio, l'uso della sorveglianza tramite GPS nelle indagini penali[283], la comunicazione di dati identificativi alle autorità di polizia da parte dei fornitori di servizi[284] e la conservazione a tempo indeterminato di impronte digitali o altri dati relativo all'indagato dopo la conclusione del procedimento penale nei suoi confronti[285].

La Corte EDU ha ritenuto la protezione dei dati personali di fondamentale importanza per il pieno godimento del diritto al rispetto della vita privata e familiare sancito dall'art.8 CEDU. In tal senso, la Corte ha stabilito che devono essere predisposte garanzie adeguate al trattamento dei dati personali il cui utilizzo deve essere pertinente e necessario ai fini delle indagini. I dati devono essere conservati al fine dell'identificazione del soggetto interessato per un periodo non superiore a quello per cui la limitazione risulta indispensabile e devono essere garantite misure di protezione contro l'uso improprio dei dati conservati[286] [287].

---

[282] Lannier, S. (2024). *Infiltrating virtual worlds: The regulation of undercover agents through fundamental rights*. Revista Brasileira de Direito Processual Penal, 10(3), e1066. pp.17-19
[283] ECtHR (2010) Uzun v. Germany. No. 35623/05
[284] ECtHR (2018) Benedik v. Slovenia. No. 62357/14.
[285] ECtHR (2008) S. and Marper v. The United Kingdom [GC]. No. 30562/04 and 30566/04.
[286] Ibidem
[287] Organization for Security and Co-operation in Europe. Ensuring human rights compliance in cybercrime investigations: OSCE training guide for criminal justice practitioners. cit. p.28-29

Nel contesto delle indagini transfrontaliere, la tutela della privacy trova applicazione anche con riferimento alle attività d'indagine richieste da un'autorità straniera. Di conseguenza, qualora la stessa ecceda i limiti riconosciuti dall'ordinamento dello Stato territoriale a tutela dei diritti fondamentali, la richiesta di cooperazione può essere respinta. Sebbene molti Stati abbiano predisposto garanzie a tutela del diritto alla privacy, permangono differenze normative spesso ampie e difficilmente conciliabili nel momento in cui viene disposta un'indagine transfrontaliera, determinando così conflitti di leggi e vuoti di giurisdizione. Sarebbe infatti auspicabile che le leggi nazionali riflettessero principi comuni di tutela dei diritti fondamentali applicabili alle indagini delle forze dell'ordine. In tal senso un corretto punto di partenza è rappresentato dalla giurisprudenza della Corte europea dei diritti umani, una delle poche Corti internazionali ad aver determinato un bilanciamento tra diritti ed esigenze investigative[288].

3. Rafforzamento della cybersicurezza nazionale ed europea

La gestione degli attacchi informatici non è un tema che riguarda esclusivamente l'aspetto tecnologico ma si inserisce in un quadro più ampio determinando sfide di geopolitica, sovranità nazionale e sicurezza economica. In tale contesto è fondamentale una risposta globale e accentrata a livello nazionale e internazionale.

A livello interno, L'agenzia per la Cybersicurezza Nazionale svolge un costante lavoro di rafforzamento della resilienza del Paese che, data la sempre maggiore interconnessione tra sistemi digitali e la maggiore ampiezza del danno causato dalla minaccia *cyber*, costituisce il fattore centrale della sicurezza cibernetica nazionale. La resilienza consente a un dato sistema di adattarsi e resistere rispetto agli eventi che possono comportare una turbativa al suo funzionamento, in modo tale da garantire la continuità dei servizi erogati e una rapida capacità di recupero nel caso di attacchi cibernetici. La garanzia della resilienza è complessa e richiede la collaborazione di attori istituzionali, delle imprese e delle associazioni di categoria che, insieme, costruiscono un ecosistema digitale sicuro, accessibile e responsabile.

[288] United Nations Office on Drugs and Crime. Comprehensive study on cybercrime. cit. pp. 140-141

La sicurezza cibernetica costituisce un fondamentale presupposto per garantire la sicurezza nazionale, in particolare rispetto a forme di offesa estranee alle categorie belliche tradizionali. Si pensi al fenomeno della "*guerra ibrida*" configurabile come una forma di conflitto moderno non inquadrabile all'interno dei confini tradizionali della guerra poiché utilizza armi non convenzionali finalizzate a destabilizzare, indebolire o influenzare l'avversario. La peculiarità di tale modalità di conflitto consiste nella capacità di evitare uno scontro militare diretto su larga scala, poiché la guerra ibrida si colloca in una "*zona grigia*" del conflitto che generalmente non genera una risposta militare convenzionale. Si tratta di una strategia particolarmente efficace, che rende indeterminabile la linea di confine tra guerra e pace e che combina diversi tipi di strumenti e tattiche, tra cui quelle informatiche, per raggiungere gli obiettivi strategici[289]. Tale modalità di conflitto invisibile rende evidente l'imprescindibile necessità di proteggere la popolazione e gli *asset* critici, civili e militari da attacchi intangibili. Un esempio significativo di tecnica d'attacco è il cosiddetto *jamming* che consiste nell'interferenza intenzionale di frequenze, comunicazioni radio e segnali elettronici. Tale pratica è divenuta assai nota anche a seguito del presunto attacco elettronico al GPS dell'aereo con a bordo Ursula von der Leyen, Presidente della Commissione Europea. Episodi di questo tipo rendono ancora più evidente l'esigenza di rafforzare la sovranità digitale nazionale ed europea per far fronte a nuovi fenomeni di conflitto[290] e la necessaria trasformazione della dimensione bellica ormai sempre più spostata dal campo di battaglia alla dimensione cibernetica.

La sicurezza nazionale nello spazio cibernetico, di cui uno dei punti fermi è la resilienza, è presupposto della sovranità digitale nazionale, europea ed euro-atlantica che l'Italia sta via via costruendo.

In tema di cooperazione internazionale, l'azione dell'Agenzia per la Cybersicurezza Nazionale si è incentrata principalmente su tre macro-aree che rappresentano i principali poli globali della cybersicurezza. La prima si è indirizzata verso le aree del Mediterraneo e dei Balcani, di prioritaria importanza per la collaborazione internazionale. In secondo luogo, ci si è avvicinati ai Paesi del corridoio

[289] Frattasi, B. Intervista condotta dall'autore. Intervista non pubblicata.
[290] Affaritaliani.it. (2025, 2 settembre). *Von der Leyen, il gps dell'aereo va in tilt. Benigni (Elt Group): "Rafforzare l'autonomia strategica e la sovranità tecnologica italiana e dell'UE"*. Affaritaliani.it.

IMEC (*India-Middle East Economic Corridor*) per consentire una collaborazione con l'India, passando per i Paesi del Golfo e del Mediterraneo. Infine, la terza direttrice riguarda le Agenzie e i Centri di Responsabilità per la cybersicurezza dei Paesi del G7 con i quali si condividono interessi fondamentali in materia di protezione dello spazio cibernetico e delle infrastrutture critiche. A tal fine, il 16 maggio 2024, durante la Presidenza italiana, è stato istituito il Gruppo di lavoro G7 sulla cybersicurezza, nel quale l'Italia ha potuto affermare la sua importanza internazionale anche in ambito *cyber*[291].

All'interno del gruppo di lavoro G7 è stata affrontata, tra le varie tematiche, la questione dell'interdipendenza tra cybersicurezza e intelligenza artificiale. Se l'uso malevolo dell'intelligenza artificiale è ormai una certezza, ciò che è interessante è la prospettiva futura legata al suo impiego per monitorare le minacce, abbattere i rischi ad essa connessi e comprendere le opportunità di tale tecnologia nel settore della cybersicurezza e del cyberspazio.

Ulteriori temi trattati hanno riguardato l'importanza della cooperazione volta a rafforzare la sicurezza informatica delle infrastrutture in settori critici quali quello energetico, discutendo su come garantire la sicurezza dell'intera catena di approvvigionamento per ridurre rischi connessi alla possibilità, per determinate componenti tecnologiche, di diventare strumento per il passaggio di attacchi informatici. Un coordinamento efficace tra più Stati richiede continuità operativa e il coinvolgimento, non solo del settore pubblico, ma anche delle imprese private o partecipate e del settore della ricerca[292]. L'obiettivo di *governance* globale è stato poi ribadito nel successivo vertice tenuto a Ottawa il 23 novembre 2025, a dimostrazione che "*la più stretta solidarietà tra le democrazie occidentali è il più grande strumento per fronteggiare ogni sviluppo distopico della dimensione digitale*"[293].

Nel quadro europeo, la sovranità digitale non è ancora un traguardo consolidato o già raggiunto ma è una prospettiva verso cui tendere[294]. Essa costituisce un obiettivo politico più che giuridico per consentire all'Unione Europea di inserirsi

[291] Frattasi, B. Intervista condotta dall'autore. Intervista non pubblicata.
[292] Agenzia per la Cybersicurezza Nazionale. (2024, 16 maggio). *Gruppo di lavoro G7 sulla cybersicurezza*. ACN.
[293] Frattasi, B. Intervista condotta dall'autore. Intervista non pubblicata.
[294] Finocchiaro, G. (2024). Intelligenza artificiale: quali regole? Il Mulino. p. 109

in un quadro internazionale ormai dominato da grandi potenze tecnologiche. Ciò non implica che la dimensione nazionale venga trascurata. Infatti la sicurezza europea parte da quella nazionale che, se inserita in un quadro unitario, viene rafforzata.

Questo è l'obiettivo delineato nella "*Declaration for European Digital Sovereignty*", che definisce la sovranità digitale europea come la capacità dell'Unione di agire in modo autonomo nel mondo digitale. Ciò non comporta l'adozione di un modello protezionistico o isolazionista, bensì permette all'Unione Europea di decidere autonomamente le scelte da compiere nell'ambito tecnologico, senza dipendere da fonti esterne, ma mantenendo sempre un'ottica di cooperazione internazionale con altri Paesi. Per raggiungere tale obiettivo occorrono investimenti, chiarezza normativa e garanzie per la competitività. Vengono identificate, inoltre, alcune aree tecnologiche particolarmente interessanti in una visione di lungo periodo, quali il calcolo ad alte prestazioni, le reti di comunicazione di nuova generazione, le infrastrutture satellitari, le tecnologie quantistiche, i *cloud*, l'intelligenza artificiale e, naturalmente, la cybersicurezza.

In tema di chiarezza normativa, è vero che ogni Stato definisce un proprio approccio alla cybersicurezza ma per evitare che sterili nazionalismi limitino la gestione accentrata della minaccia *cyber* a livello europeo, il quadro normativo deve essere armonizzato. In tale prospettiva si è inserita, come ricordato precedentemente, la Direttiva NIS2, recepita con il decreto legislativo 4 settembre 2024, n. 138, che comporta un'ulteriore rafforzamento della cybersicurezza, coprendo ben 18 settori critici e altamente critici.

Le attuali tensioni geopolitiche hanno spostato l'attenzione europea verso l'obiettivo finale della costruzione di una difesa comune unionale nel campo cibernetico idonea a confrontarsi con le più grandi potenze avanzate nel settore. Si tratta di un cambio di prospettiva di significativa rilevanza che segna un'evoluzione rispetto agli obiettivi di riferimento precedenti orientati alla tutela del mercato e alla prioritaria posizione del consumatore nell'evoluzione digitale. Si assiste così a un crescente avvicinamento tra il mercato unico, fondato su un principio sovranazionale, e il settore della difesa tradizionalmente di competenza nazionale ed estraneo all'integrazione europea.

Un primo passo in tale direzione è rappresentato dal rafforzamento della solidarietà digitale per fronteggiare minacce informatiche che passano da uno Stato membro ad un altro o da uno stato terzo all'Unione. In tal senso è stato predisposto il *Cyber Solidarity Act*[295] che introduce il cosiddetto "*scudo europeo per la cybersicurezza*", ossia un sistema di allerta composto da centri operativi di sicurezza (SOC) nazionali e transfrontalieri, che utilizzeranno tecniche avanzate di intelligenza artificiale per fronteggiare gli attacchi cibernetici così da garantire un alto livello di sicurezza e reattività. Il Regolamento si fonda su tre pilastri.

Il primo si riferisce al cosiddetto "*European Cyber Shield*" ossia un sistema di allerta sulla cybersicurezza che consiste in una rete di poli informatici per sviluppare e potenziare capacità coordinate di rilevamento e di conoscenza situazionale. Tutto parte dai *National Cyber Hub* che, per mezzo di tecnologie avanzate, rilevano tempestivamente le minacce informatiche e condividono le informazioni in modo coordinato con gli Stati Membri, migliorando la capacità di risposta.

Il secondo pilastro è costituito da un meccanismo per le emergenze informatiche, finalizzato a rafforzare la preparazione dell'Unione contro gli incidenti *cyber*. Esso prevede: un'attività di preparazione agli incidenti attraverso test e valutazioni nei settori maggiormente critici quali quello della sanità, energia e finanza; la creazione di una riserva europea di risposta rapida agli incidenti anche attraverso l'impiego, su richiesta di Stati e istituzioni comunitarie, di fornitori privati affidabili e specializzati; la cooperazione tra stati diretta e rapida in caso di attacchi informatici.

Il terzo pilastro, attinente il meccanismo di revisione degli incidenti di cybersicurezza, consente di analizzare le cause che hanno generato a un dato incidente permettendo di definire raccomandazioni operative per migliorare la capacità di risposta dell'Unione. Può essere attivato su richiesta della Commissione Europea o dalle Autorità Nazionali competenti, ed è gestito dall'Agenzia europea per la cybersicurezza (ENISA).

Il *Cyber Solidarity Act* ha, inoltre, istituito la Riserva di Cybersicurezza volta a rafforzare e potenziare le capacità di risposta agli incidenti, fornendo ben 45 servizi

[295] European Union. 2025. *Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act).* Official Journal of the European Union, L38.

di cybersicurezza affidabili, di cui 6 italiani, per assistere, su richiesta, gli Stati membri, le istituzioni, gli organi e le agenzie dell'Unione Europea nonché i Paesi terzi che fanno parte del Programma Digitale Europeo.

Nel quadro europeo così delineato, ACN svolge un importante funzione di raccordo tra l'ordinamento interno e quello europeo. Nella sua veste di Autorità nazionale NIS, l'agenzia partecipa al gruppo di Cooperazione NIS e alla Rete degli CSIRT nazionali, strumenti finalizzati ad assicurare una cooperazione rapida ed efficiente tra gli Stati membri. Essa è inoltre parte della Rete europea CyCLONe che, prioritariamente, dovrà garantire la gestione coordinata degli incidenti e delle crisi informatiche su larga scala. Attraverso tali meccanismi, viene messa in atto una *governance* multilivello, nazionale ed europea, che esalta aspetti di armonizzazione e di cooperazione sul piano nazionale e sovranazionale.

Un ulteriore aspetto fondamentale, di cui tenere conto in vista di un rafforzamento della cybersicurezza, è il fattore della consapevolezza e formazione per lo sviluppo di una cultura *cyber*. Il fattore H, cioè il fattore umano, rimane ancora una dei principali punti di debolezza nella difesa informatica rappresentando, di conseguenza, un *vulnus* per le nostre libertà nello spazio digitale.

La cultura della cybersicurezza parte dal riconoscimento della sua rilevanza quale strumento di protezione dello Stato, posto sullo stesso piano degli altri sistemi di sicurezza; anzi, proprio in ragione del suo carattere trasversale, essa costituisce il presupposto per garantire la sicurezza in altri ambiti, sia nazionali che europei.

La cultura è un fattore determinante che deve essere comune a tutti i cittadini, non solo perché diversamente avremmo un problema di *digital divide*, ossia di esclusione sociale incompatibile con i principi di uno Stato democratico, ma anche per fare in modo che lo strumento informatico venga considerato un alleato dell'uomo più che uno strumento in grado di assoggettarlo.

In tal senso, la Strategia nazionale per la sicurezza informatica del Paese considera la crescita della sensibilità collettiva verso il digitale un ingrediente essenziale per la sua attuazione. L'ACN nell'ambito di questa finalità, ha instaurato una seria di rapporti con Università e mondo accademico volti a implementare e promuovere una cultura cibernetica avanzata nel Paese. A titolo esemplificativo, l'Agenzia ha elargito borse di dottorato nel settore della cybersicurezza in più di 200

università, privilegiando studi nei settori di *quantum computing* e di intelligenza artificiale, utilizzabile, quest'ultima, come risorsa indispensabile anche nell'ambito della difesa. Ancora, ACN contribuisce alla campagna di sensibilizzazione "*I Navigati*" promossa dalle istituzioni di tutela del mercato bancario e finanziario, volte a proteggere i consumatori dal rischio di *phishing* insegnando a riconoscerne i tratti distintivi. Obiettivo ancora più ambizioso è quello di promuovere la cultura *cyber* nei vari cicli scolastici sia per stimolare l'interesse del cittadino, sia per fornirgli una formazione progressiva. Questo è l'obiettivo dalla collaborazione posta in essere tra il Ministero dell'Istruzione e del Merito e l'Agenzia per la Cybersicurezza Nazionale.

In conclusione, lo sviluppo delle competenze digitali acquista un rilievo straordinariamente importante nel panorama attuale e, soprattutto, in prospettiva degli scenari futuri, che richiederanno sempre più una solida risposta delle istituzioni statuali all'evoluzione della minaccia cibernetica.

3.1 Strumenti tecnici e investigativi innovativi: L'avvento dell'AI

Il dominio digitale ha ormai cessato di essere una mera estensione della realtà fisica, divenendo progressivamente un ecosistema a sé stante nel quale la realtà criminale si è adattata e, anzi, ha progressivamente ampliato il suo raggio d'azione, sfruttando le nuove tecnologie emergenti che consentono un maggiore livello di anonimato e una maggiore entrata di profitti.

Tra queste, l'Intelligenza Artificiale sta modificando e trasformando le metodologie criminali adottate nel web. Oggi infatti vi sono attaccanti automatizzati che sono in grado di sfruttare le vulnerabilità sistemiche, consentendo l'uso dell'AI in attività ostili, quali la generazione di *malware* o il *phishing* automatizzato. Si pensi, a tal proposito, all'affermazione e all'utilità che i cybercriminali possono trarre dall'uso dell'intelligenza artificiale cosiddetta "*agentica*", che si sostanzia in macchine robotiche che affiancano l'uomo nelle più disparate attività, sollevandolo da compiti faticosi e ripetitivi.

Allo stato attuale, la trasformazione non è ancora definitiva ma risulta ancora più evidente la necessità di forme di collaborazione, di formazione, consapevolezza e *governance* globale per fronteggiare o comunque adeguarsi a tali realtà innovative.

Con l'avvento di tali tecnologie, inoltre, è maggiormente prevedibile che il rischio tecnologico divenga presto rischio sistemico poiché gli effetti di un attacco malevolo potrebbero essere incrementati attraverso l'uso dell'IA. In tale prospettiva è stato approvato il Regolamento europeo sull'intelligenza artificiale, l'*AI Act*[296], da cui emerge che solo attraverso un quadro normativo complessivo e coeso è possibile garantire un'adeguata protezione dello spazio digitale anche nei confronti di tentativi di infiltrazione da parte delle organizzazione criminali, che operando ormai in modo assiduo nel *cyberspace*, sfruttano le nuove tecnologie per occultare i loro traffici transnazionali.

Con l'avvento dell'intelligenza artificiale e dei nuovi modi per sfruttarla, intervengono però anche tematiche etiche e scientifiche che insistono sia sulla formazione di competenze avanzate, sia sull'importanza dello sviluppo di una cultura cibernetica. Infatti una delle sfide più complesse è quella di educare ad un uso consapevole e corretto dell'intelligenza artificiale anche per proteggersi da rischi di un'incauta cessione di patrimonio informativo in modelli *open source* che possono arrivare fino a piattaforme *cloud* sottratte al controllo e alla giurisdizione dello Stato[297].

Sul piano strettamente investigativo, l'ordinamento italiano, con la legge 137/2023, ha previsto l'*undercover* informatico per le indagini in materia di cybercrime e terrorismo in rete, aprendo la strada verso gli ancora inesplorati terreni dell'utilizzo dell'intelligenza artificiale come strumento investigativo, nei casi in cui la commissione dei reati avvenga proprio mediate tali tecnologie.

L'IA costituisce un formidabile strumento per la commissione di reati. Si pensi che con l'abbinamento tra IA e computistica quantistica, entro pochi anni non ci saranno *password* o crittografie così forti da non poter essere violate.

Per tale ragione, la nuova sfida investigativa è proprio l'intelligenza artificiale. Con essa, infatti, si potranno agevolare attività come il controllo di sicurezza dei sistemi informatici, l'individuazione di indici di *cyber*-spionaggio, l'analisi e la decriptazione di attacchi malevoli nonché il controllo di enormi quantità di dati ai fini

[296] European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
[297] Frattasi, B. Intervista condotta dall'autore. Intervista non pubblicata.

investigativi. In questa prospettiva, non è sufficiente dotarsi di un quadro normativo interno ma risulta necessario un sistema uniforme a livello sovranazionale che ne regoli l'impiego, la valenza probatoria delle risultanze ottenute e il possibile riconoscimento tra diversi ordinamenti. Sarà inoltre fondamentale dotarsi di sistemi proprietari di IA investigativa che dovranno essere adeguatamente istruiti e particolarmente affidabili.

Ciononostante, si registrano anche istanze di arretramento per gli strumenti investigativi già disciplinati dalla legge. Ci si riferisce in particolare all'introduzione del nuovo articolo 254-ter c.p.p. che prevede una procedura particolarmente complessa in materia di sequestri di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi e comunicazioni. L'inserimento di questa disposizione produce una forte limitazione all'utilizzo di tali dati ai fini probatori sia per i reati informatici sia per qualsiasi altro tipo di reato.

Accanto all'esigenza di evitare pericolosi arretramenti, emerge anche la necessità di prevedere nuove fattispecie incriminatrici quali, ad esempio, l'introduzione di un delitto che si potrebbe definire come "*traffico organizzato di dati personali*". Una tale disposizione consentirebbe sia di acquisire informazioni sulla complessità delle reti criminali orientate verso l'acquisizione abusiva di dati personali sia di comprenderne il loro sfruttamento illecito volto a produrre un indebito condizionamento degli scenari economici e politici attuali. Questa esigenza nasce dalle risultanze investigative che già chiariscono la necessità di un intervento normativo in tal senso.

Ritornando all'impiego di strumenti di intelligenza artificiale nell'ambito investigativo, è opportuno sottolineare come la necessità di un quadro normativo innovativo non è una sfida futura ma è una considerazione attuale su cui discutere se si vuole evitare che le strutture criminali avanzino, lasciando indietro l'azione repressiva dello Stato[298].

3.2 Prospettive nell'ipotesi di non cooperazione

[298] Melillo, G. Intervista condotta dall'autore. Intervista non pubblicata.

Come sostenuto dal Procuratore Nazionale Antimafia e Antiterrorismo, il regime attuale dell'*undercover* informatico consente di operare anche al di fuori dei confini nazionali esclusivamente nell'ambito della cooperazione giudiziaria e di polizia, ossia previa informazione e previo consenso dello Stato estero nel cui territorio si attiva il mezzo investigativo in esame.

Non sempre, tuttavia, risulta possibile realizzare l'auspicabile cooperazione specie qualora si sia in presenza di Stati non collaborativi o addirittura ostili. In tale ipotesi, i principi internazionali sovraordinati che riconoscono l'inviolabilità della sovranità statale, costituiscono un limite invalicabile che è presidiato, nel nostro ordinamento, dell'art. 10 della Costituzione. Ciò naturalmente costituisce un impedimento all'efficace repressione del crimine informatico specie quando i cybercriminali trovino riparo in Stati non collaborativi o nel caso in cui siano agenti riconducibili a Stati ostili.

Per tale fondamentale ragione, il Procuratore Giovanni Melillo sostiene che sia indispensabile perseguire l'obiettivo di un più ampio e resistente tessuto internazionale penale e di una sempre più coesa e uniforme cooperazione giudiziaria e di polizia[299].

L'interpretazione prospettata dal Direttore del servizio di Polizia Postale e per la Sicurezza Cibernetica Ivano Gabrielli, appare particolarmente innovativa. Partendo dalla considerazione che l'indagine cibernetica si muove, per la natura stessa del crimine informatico, in un terreno senza barriere, si potrebbe prospettare una visione del *web* come un dominio dai confini dinamici. Già ad oggi, un sistema informatico nazionale viene considerato tale anche con riferimento ai suoi ambienti *cloud*, ancorché ubicati all'estero. Sempre ad avviso di Gabrielli sarebbe teoricamente concepibile una sorta di canale di comunicazione tra il sistema attaccante e il sistema attaccato come fosse un'unica entità tecnica abilitata ancorché creata per scopi criminosi. In tale prospettiva, l'attività investigativa sotto copertura, muovendosi dal sistema nazionale vittima dell'attacco fino alla risorsa attaccante, potrebbe considerarsi legittima, proprio in virtù della relazione tecnica che lega le due entità determinando la nascita di un'unica struttura telematica[300].

[299] Ibidem
[300] Gabrielli, I. Intervista condotta dall'autore. Intervista non pubblicata.

3.3 Convenzione delle Nazioni Unite sul *cybercrime*: aspetti controversi

L'Assemblea generale delle Nazioni Unite ha adottato, il 24 dicembre 2024 ,la Convezione ONU sul cybercrime (UNCC)[301], la quale, prevedendo norme comuni a livello mondiale, è destinata ad avere un impatto significativo sulla lotta al crimine informatico[302]. Il percorso, attivato con la risoluzione 74/247 del 2019, ha evidenziato l'urgente necessità di una forte e coesa cooperazione internazionale per prevenire e contrastare la criminalità informatica, ormai concepita come minaccia globale idonea ad incidere su aspetti economici, sociali e giuridici. La Convezione, forte della convinzione di una impellente necessità di politiche globali di giustizia penale, idonee a creare un quadro convenzionale di legislazione, poteri procedurali e cooperazione internazionale, stabilisce procedure di rafforzamento del coordinamento tra Stati e agevola i Paesi in via di sviluppo nell'implementazione di idonee misure di prevenzione e repressione dei crimini informatici[303].

Tuttavia, fin dall'inizio dei lavori preparatori, il progetto di Convenzione ha sollevato forti dubbi e numerosi dibattiti e ha generato un diffuso scetticismo da parte di numerosi Stati e ONG. Innanzitutto, il periodo storico nel quale tale Trattato è stato predisposto non è certamente dei più felici caratterizzato com'è da forti tensioni geopolitiche, tanto da essere stato definito, da alcuni osservatori, come "*era glaciale del multilateralismo*". Tale instabilità si è riflessa, tra le altre cose, anche sul numero di Stati contrari alla Convenzione che sono 60 mentre 33 sono gli astenuti.

Inoltre, la circostanza che il processo negoziale sia stato avviato dalla Russia con il benestare della Cina ha sollevato numerosi interrogativi, in quanto ambedue gli Stati sono stati spesso accusati di tollerare o, addirittura, di fornire protezione ad *hacker* e cybercriminali.

---

[301] United Nations. (2024). *United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes* (adopted 24 December 2024, Resolution A/RES/79/243)

[302] Consiglio dell'Unione Europea. (2025, 13 ottobre). Lotta alla criminalità informatica: l'UE firmerà la Convenzione delle Nazioni Unite contro la criminalità informatica [Comunicati stampa]. Consilium

[303] Abdelkarim, Y. A. (2025). *UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age*. *Journal of Digital Technologies and Law, 3*(4). p. 553

Forti dubbi sono emersi, in particolare, dagli Stati parte della Convenzione di Budapest, i quali hanno manifestato riserve circa il rischio che una nuova Convenzione potesse determinare un quadro normativo internazionale frammentato. Inoltre, la posizione della Russia che aveva visto con sfavore la Convenzione del 2001 ha alimentato il sospetto che tale iniziativa mirasse ad indebolire il quadro giuridico che si era precedentemente affermato[304].

Un secondo profilo di criticità, ha riguardato l'individuazione delle fattispecie di reato da includere all'interno della Convenzione. La Russia con l'adesione di altri Stati propendevano per una Convenzione dall'ampio raggio d'azione, non confinata ai soli reati "*cyber dependent*" ossia ai reati che non possono essere commessi se non tramite le tecnologie dell'informazione e della comunicazione. Per contro, gli Stati occidentali ritenevano che le condotte di reato dovessero essere rigorosamente definite e limitarsi ai soli reati informatici in senso stretto, anche per garantire una coerenza sistematica con le condotte definite dalla Convenzione di Budapest.

La discussione, infatti, si è incentrata sui reati "*cyber enabled*" che possono essere commessi anche al di fuori dell'ambito digitale ma che, con l'impiego di tecnologie ICT, aumentano notevolmente l'impatto e la diffusività. La maggior parte di queste fattispecie è stata, infine, esclusa dal testo della Convenzione sia perché riprendeva fenomeni criminosi già tutelati in altre Convenzione, sia per evitare che l'eccessiva ampiezza dei reati da criminalizzare comportasse un eccessivo ambito di estensione dell'azione repressiva statale e finisse così per ledere le libertà fondamentali. Su quest'ultimo punto si è fortemente contestata la posizione di Stati quali Russia, Cina, India e Iran di voler introdurre alcuni reati "*content-related*" altamente controversi, quali l'incitamento ad attività sovversive o l'uso di internet per diffondere informazioni dannose.

Nonostante molte fattispecie controverse siano state escluse dalla Convenzione queste potrebbero riproposto visto che il Trattato prevede la possibilità di adottare protocolli aggiuntivi. Per quest'ultimi, gli art. 61 e 62 prevedono che la proposta deve essere presentata da almeno 60 Stati e deve essere adottata per consenso. In assenza di

[304] Bannelier-Christakis, K. (2025). *Risks and Opportunities of the UN Cybercrime Convention for the UNDOC & the Fight Against Transnational Organised Crime: A First Assessment.* Transnational Criminal Law Review., 4(1). pp.145-147

consenso, protocolli possono essere adottati con la maggioranza dei due terzi degli Stati presenti e votanti alla riunione della Conferenza delle Parti. Tale procedura consentirebbe, di conseguenza, a Stati autoritari di integrare fattispecie di reato particolarmente controverse come i reati di contenuto. È vero che l'eventuale integrazione vincolerebbe solo gli Stati che decidessero di aderirvi, ma ciò produrrebbe un segnale di instabilità dell'integrità del diritto internazionale , incidendo negativamente sulla credibilità delle Nazioni Unite[305].

Un terzo aspetto controverso riguarda le misure di *law enforcement* e gli strumenti di cooperazione internazionale.

Con riferimento alle prime, Il Trattato prevede misure particolarmente invasive quali ad esempio, l'intercettazione dei dati di contenuto(art.30), la raccolta in tempo reale dei dati di traffico(art.29), la perquisizione e il sequestro di dati elettronici conservati (art.28). In tale ambito, la questione discussa riguarda l'eccessiva ampiezza dei reati per i quali queste misure possono essere disposte. Infatti, l'art.23, che disciplina l'applicazione delle misure procedurali, prevede che i reati interessati non si limitino a quelli espressamente previsti dalla Convenzione in esame, ma che le misure di law enforcement possano applicarsi anche per altri reati commessi avvalendosi delle tecnologie di informazione e di comunicazione e per qualsiasi tipologia di reato le cui risultanze probatorie possano essere reperite in formato elettronico. Inoltre, l'applicazione di tali misure invasive dipende fortemente dal sistema nazionale poiché è solo il diritto interno che può stabilire cosa costituisce reato, comportando rilevanti implicazioni in tema di diritti fondamentali. A titolo esemplificativo, qualora uno Stato qualifichi l'omosessualità come reato, le misure procedurali previste dalla Convenzione potrebbero essere utilizzate per avviare un'indagine su tale condotta.

Le disposizioni finora analizzate, in realtà, non differiscono tanto da quelle previste nella Convenzione del Consiglio d'Europa, la quale prevede l'applicazione di strumenti di law enforcement per le stesse tipologie di reato. Tuttavia, ciò che è differente è il sistema di diritto complessivo nel quale essa si inserisce. Infatti, la Convenzione di Budapest è stata elaborata dal Consiglio d'Europa, sotto l'influenza

[305] Ivi. pp. 147-151

determinante della Convenzione europea dei diritti dell'uomo che, come tale garantisce, un quadro giuridico strutturato e vincolante in tema di diritti fondamentali.

Quanto all'ambito della cooperazione internazionale, la UNCC prevede la predisposizione di una rete operativa 24/7 (art.41), la possibilità di richiedere o imporre agli stati la conservazione rapida dei dati elettronici conservati (art.42), di richiederne l'accesso (art.44) e di raccogliere in tempo reale dati di traffico(art.45). L'art.47 disciplina altresì la cooperazione tra le autorità di *law enforcement* finalizzata a rafforzare o istituire canali di comunicazione con autorità, agenzie e servizi competenti per facilitare lo scambio sicuro e rapido di informazioni. Inoltre, lo stesso articolo incentiva la cooperazione nello svolgimento di indagini, sia consentendo alle autorità lo scambio reciproco di informazioni in merito agli elementi investigativi, sia permettendo la facilitazione del coordinamento, eventualmente anche tramite la designazione, subordinata ad accordi bilaterali o multilaterali, di un ufficiale di coordinamento.

Anche in tema di cooperazione, emergono criticità legate a eventuali limitazioni alle libertà fondamentali e alla protezione dei dati personali[306]. In tal senso, gli Stati possono rifiutare richieste di mutua assistenza giudiziaria qualora le stesse siano contrarie rispetto alle proprie politiche nazionali in tema di diritti fondamentali e alla protezione dati personali venendo comunque riconosciuta la possibilità di invocare il principio di doppia incriminazione. Tuttavia, tali garanzie possono risultare insufficienti e inadeguate rispetto alle misure procedurali particolarmente invasive della Convenzione. Si pensi all'art. 24 che prevede che l'applicazione delle misure procedurali debba essere conforme alle garanzie e agli obblighi stabiliti dal proprio diritto interno, in conformità con gli obblighi internazionali in materia di diritti umani. Tale disposizione, pur dando valore al rispetto delle libertà fondamentali, è stata considerata di per sé insufficiente in quanto rilega tali garanzie ancora una volta alla disciplina degli ordinamenti nazionali, i quali non condividono lo stesso standard di tutela in materia di diritti umani, lasciando la materia alla discrezionalità degli Stati.

Inoltre, pur essendo espressamente richiamato il principio di proporzionalità nell'applicazione delle misure invasive, non viene previsto alcun controllo giurisdizionale né alcun rimedio effettivo in caso di lesione sproporzionata dei diritti

[306] Ivi. pp. 151-152

dell'individuo. Da ciò si evince che, pur essendo previste disposizioni a tutela dei diritti umani, le stesse risultano scarne e insufficienti, lasciando allo Stato un eccessivo margine di apprezzamento statale che rischia di compromettere la tutela dello Stato di diritto[307].

In conclusione, la UNCC determinerà indubbiamente un rafforzamento dei poteri delle forze dell'ordine e dei meccanismi di cooperazione internazionale nel contrasto al fenomeno del *cybercrime*. Tuttavia, taluna dottrina sostiene che "*Broadly scoped investigative powers should not transform this instrument into a general-purpose vehicle for digital evidence gathering. Any cross-border investigative powers, in particular, should be carefully and narrowly crafted and remain closely linked to investigations of a specific, precisely worded criminal conduct*"[308].

[307] Ivi pp.153-154

[308] Rodriguez Katitza & Gullo Karen. mar. 3, 2022. Negotiations Over U.N. Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights, ELEC. FRONTIER FOUND.

CONCLUSIONI

L'analisi svolta ha consentito di indagare le forme di cooperazione internazionale attuate per contrastare il crimine informatico. Da quanto emerso rileva che il fenomeno del *cybercrime* si distingue dalle fattispecie tradizionali di reato perché non costituisce una minaccia isolata e settoriale facilmente inquadrabile, bensì è capace di incidere contemporaneamente su molteplici ambiti e su ordinamenti statuali differenti.

Ciò implica che il contrasto al crimine informatico non comprende solo la dimensione della cooperazione interstatuale ma anche il coordinamento multisettoriale nel quale tutti gli attori coinvolti possano fornire il proprio *know-how* per realizzare una collaborazione su più fronti, avendo presente un quadro d'insieme e non solo i singoli ambiti. In tal senso il Prefetto Bruno Frattasi afferma che "*Solo con il contributo di tutti si può fronteggiare, infatti, una minaccia così penetrante, quale quella cyber, divenuta sempre più sofisticata e in grado di coinvolgere porzioni crescenti della popolazione, a partire dai più indifesi e dai più esposti"*[309].

Un esempio significativo in tale direzione è il coordinamento a livello nazionale istituito tra le strutture investigative e giudiziarie e quelle prettamente tecniche e istituzionali, ossia tra la Direzione Nazionale Antimafia e Antiterrorismo, le procure distrettuali, la Polizia Postale e l'ACN. Attraverso la definizione di un coordinamento sistematico e trasversale si delinea una prospettiva interna uniforme che rafforza dapprima il quadro europeo e, successivamente, quello globale.

Sul versante investigativo, emerge chiaramente l'efficacia dello strumento delle operazioni digitali sotto copertura quale strumento peculiare e innovativo di individuazione dei cybercriminali in grado di consentire un'adeguata prevenzione e repressione del crimine informatico. Tuttavia, l'analisi mette in luce anche l'insufficienza della regolamentazione interna e internazionale che genera dubbi interpretativi e disomogeneità normative tra Stati diversi, certamente non funzionali all'ottimale coordinamento investigativo. Per queste ragioni si evidenzia l'opportunità di un intervento normativo per il quale risulta indispensabile identificare con precisione le modifiche da apportare. In ambito interno e internazionale, ci si è, infatti,

[309] Frattasi, B. Intervista condotta dall'autore. Intervista non pubblicata.

concentrati per lo più sulla disciplina sostanziale dell'agente sotto copertura, dando rilievo alle condotte per le quali opera la scriminante e alla disciplina dell'*entrapment*, attribuendo minore rilevanza alla normativa processuale. Invero, assumono un'importanza imprescindibile anche in tema di tutela del giusto processo dell'imputato le questioni relative alle risultanze processuali, il momento in cui si può attivare l'infiltrazione e la legittimità dell'intero iter operativo dell'operazione *undercover*. Tali aspetti controversi dovrebbero essere trattati anche sul piano normativo e non solo su quello giurisprudenziale come avvenuto con talune pronunce della Corte di Strasburgo, in modo tale da bilanciare adeguatamente l'esigenza di attivare le operazioni sotto copertura, efficace strumento di contrasto alla minaccia cibernetica, con la garanzia di assicurare il rispetto delle libertà fondamentali su cui tali tecniche possono incidere.

In ambito internazionale, l'occasione opportuna poteva essere la Convenzione delle Nazioni Unite del 2024 che, tuttavia, ha generato numerose problematiche in tema di diritti fondamentali impedendo la definizione di una disciplina delle operazioni sotto copertura.

Taluna dottrina sostiene che le modifiche in tema di *undercover* digitale andrebbero apportate nel contesto della Convenzione di Budapest del 2001, più che nel quadro delle Nazioni Unite. Ciò consentirebbe di raggiungere, con maggiore probabilità, un ampio consenso su una più uniforme disciplina dell'operazioni sotto copertura, anche in materia di *entrapment*. Ciò perché gli Stati membri del Consiglio d'Europa condividono valori comuni e predispongono numerose garanzie in materia di libertà fondamentali essendo parti della Convezione europea dei diritti dell'uomo[310]. Tale comunanza viene meno nel contesto delle Nazioni Unite, caratterizzato da tradizioni giuridiche e tendenze normative profondamente divergenti. In tal senso, un'eventuale emendamento alla Convenzione sopra richiamata costituirebbe di per sé un significato passo in avanti verso l'adozione di una disciplina uniforme, ma non risolverebbe la questione della mancanza di omogeneità normativa. Infatti la cooperazione investigativa è efficace se viene eseguita globalmente, quindi anche al

[310] Girard, R. N. *The honeypot stings back: Entrapment in the age of cybercrime and a proposed pathway forward*. cit. pp. 212-213

di fuori di contesti regionali. Di conseguenza, sarebbe auspicabile una normativa universale più che regionale che consenta un'idonea regolamentazione della materia, tenendo conto delle prospettive e dei limiti da apporre alle operazioni sotto copertura.

Un'altra scuola di pensiero sostiene la necessità che per un più proficuo coordinamento investigativo occorra predisporre un doppio standard normativo che differenzi le operazioni sotto copertura interne da quelle per il contrasto ai crimini transnazionali, così da consentire, nel quadro internazionale, una disciplina più flessibile e idonea ad adeguarsi alle richieste di Stati stranieri. Tuttavia, anche se tale soluzione genererebbe una maggiore efficienza investigativa, essa rischierebbe di accentuare le questioni controverse relative alle operazioni di infiltrazione aumentando i rischi relativi all'*entrapment* e creando una disciplina di operazioni transnazionali in deroga al diritto vigente. Inoltre, le operazioni *undercover* disposte per i crimini transnazionali finirebbero inevitabilmente per influenzare la normativa in tema di infiltrazioni nazionale, generando, in ultima istanza, un quadro giuridico maggiormente permissivo per tutte le operazioni[311].

Dalle prospettive appena delineate emerge, in ogni caso, l'esigenza di un quadro comune in materia di operazioni digitali sotto copertura che faciliti la cooperazione, permettendo di agevolare il sistema di contrasto al crimine informatico. In tal senso si auspica un intervento che tenga in considerazione il valore investigativo dell'*undercover* digitale senza tralasciare le questioni delicate relative alla loro disciplina.

In conclusione, è certamente auspicabile un intervento normativo che funga da punto di partenza nell'ambito investigativo del contrasto al *cybercrime*. Tuttavia, come già sostenuto, la cooperazione necessita di una visione complessiva di ambiti tra loro molto diversi e non sempre facilmente sovrapponibili. Solo attraverso un approccio sistemico, un quadro normativo coerente sia a livello nazionale che internazionale e una cooperazione fortemente strutturata, si possono ottenere vantaggi effettivi sul crimine informatico.

[311] Ross, J. E. *Impediments to Transnational Cooperation in Undercover Policing: A Comparative Study of the United States and Italy.* cit. 612-616

BIBLIOGRAFIA

ABDELKARIM, Y. A. 2025. *UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age*. *Journal of Digital Technologies and Law, 3*(4). pp. 543 – 569.

AITALA, R., & SEVERINO, P. 2021. *Diritto internazionale penale*. Le Monnier.

AMATO, G. 2010. *I reati informatici: nuova disciplina e tecniche processuali di accertamento*. Padova: CEDAM.

BANNELIER-CHRISTAKIS, K. 2025. *Risks and Opportunities of the UN Cybercrime Convention for the UNDOC & the Fight Against Transnational Organised Crime: A First Assessment.* Transnational Criminal Law Review., 4(1). pp.140-155.

BASSIOUNI, M. C. 2005. *La cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo.* Giuffrè.

BIRAL, M. 2023. *La testimonianza anonima degli agenti sotto copertura*. Wolters Kluwer.

BOISTER, N. 2018. *An introduction to transnational criminal law* (2nd ed.). Oxford University Press.

BORTOLIN, C. 2008. *Operazioni sotto copertura e «giusto processo».* In *Giurisprudenza europea e processo penale italiano*.

BRENNER Susan W. 2006. '*Cybercrime Jurisdiction'* in *Cybercrime: The Transformation of Crime in the Information Age*. Polity.

BRONITT, S. 2004. *The law in undercover policing: A comparative study of entrapment and covert interviewing in Australia, Canada and Europe*. Common Law World Review, 33 **(**1). pp.35-80.

BRONZO, P. (2023, 19 ottobre). *Le indagini undercover nel mondo digitale*. Penale Diritto e Procedura. pp.1-11.

BRONZO, P. 2025. *Le operazioni sotto copertura nel web*. In *Indagini e prove nella società digitale. Questioni attuali e prospettive future* (ISBN 979-12-235-0292-1).

BUÇAJ, E., & THAQI, A. 2025. *Global Regulation of Cybercrime through International Law and Cyberconventions.* Kriminologie - Das Online-Journal, no. 7. pp.155-170

BUCCARELLA M. 28 gennaio 2023. *Il Secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione internazionale in*

ambito digitale: Quali rischi per la protezione dei dati personali nell'Unione europea? in I Post di AISDUE, V, n. 8, AISDUE pp.184-203

CADOPPI, A. 2023. Cybercrime (2. edizione.). UTET Giuridica.

CALCARA. G. 2019. *Rethinking Legal Research on Matters of International Police Cooperation: Issues, Methods and Raison d'Être,* 40 LIVERPOOL L. REV. pp. 95-111

CALÌ, S., CAPPARELLI, F., HAZAN, M., MARTINI, F., & RAZZANTE, R. 2025. *Cybersecurity: tra rischio e responsabilità: profili operativi in un settore in continua evoluzione*. Giuffrè Francis Lefebvre.

CAMALDO, L. 2014, 27 maggio. *La Direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*. DIRITTO PENALE CONTEMPORANEO.

CHERNIAVSKYI, S. S., HRIBOV, M. L., NEBYTOV, A. A., KNIAZIEV, S. M., & TELENYK, S. S. 2020. *The forms of international co-operation in the area of undercover investigations.* Journal of Legal, Ethical and Regulatory Issues, 23(1). pp.1-9.

CIAMPI, S. 2024. *Legge n. 137/2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*. Processo Penale e Giustizia: Rivista di dottrina e giurisprudenza, (3). pp. 723-742.

CLOUGH, J. 2012. *The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World.* Crime Law Forum 23, pp.363–391.

COLOMBO E., 2009. *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in Ciberspazio e Diritto 2009, n. 3-4. pp. 285-304.

CONSIGLIO DELL'UNIONE EUROPEA. 2017. *Squadre investigative comuni – Guida pratica* (Doc. 6128/1/17 REV 1). Eurojust.

CONSIGLIO DELL'UNIONE EUROPEA. 2017. *Squadre investigative comuni – Guida pratica* (Doc. 6128/1/17 REV 1). Eurojust.

CONSIGLIO DELL'UNIONE EUROPEA. 2025, 13 ottobre. Lotta alla criminalità informatica: l'UE firmerà la Convenzione delle Nazioni Unite contro la criminalità informatica [Comunicati stampa]. Consilium.

COUNCIL OF EUROPE. 1959. *Explanatory Report to the European Convention on Mutual Assistance in Criminal Matters* (CETS No. 30)

COUNCIL OF EUROPE. 1999. *Explanatory Report to the Criminal Law Convention on Corruption* (European Treaty Series No. 173) Council of Europe.

COUNCIL OF EUROPE. 2001, November 8. *Explanatory Report to the Convention on Cybercrime* (ETS No. 185).

COUNCIL OF EUROPE. 2013. *Mutual Legal Assistance Manual*. Belgrado: Council of Europe.

COUNCIL OF EUROPE. 2008. *The effectiveness of international co-operation against cybercrime: Examples of good practice* (T-CY/DOC-567study4-Version7).

COUNCIL OF THE EUROPEAN UNION. 2019, 5 November. *Conclusions of the 15th Annual Meeting of National Experts on Joint Investigation Teams (JITs): JITs in cybercrime cases: challenges and opportunities* (Document 13752/19). Eurojust.

CORONA, F. 2021. *Reati informatici e investigazioni digitali: diffamazione via web, prove digitali, sex crimes, cyberstalking, cyberbullismo, reati privacy*. Pacini giuridica.

COUPLAND, H. 2025. *Investigating cybercrime: The key jurisdictional and technical challenges faced by law enforcement and ways to address them* (Vol. 6). *York Law Review*. University of York.

CRYER, R., ROBINSON, D., & VASILIEV, S. 2019. *State Cooperation with Respect to National Proceedings.* In *an Introduction to International Criminal Law and Procedure* chapter, Cambridge: Cambridge University Press.

CURTOTTI, D. 2015. *Operazioni sotto copertura*. In B. Romano (a cura di), *Le associazioni di tipo mafioso*. UTET giuridica.

DAVIES, G. 2020. *Shining a light on policing of the dark web: An analysis of UK investigatory powers*. Journal of Criminal Law, 84*(5).* pp.407–426

DUBBER M.D. 2006. *Criminal Law in Comparative Context.* 56 Journal of Legal Education. pp. 433-443.

EUROPEAN PARLIAMENT, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS. 2017. *Legal frameworks for hacking by law enforcement: Identification, evaluation and comparison of practices* (Study No. PE 583.137 EN). European Parliament.

EUROPOL. 2024. *Common challenges in cybercrime 2024*.

EUROPOL. *European Cybercrime Centre (EC3)*. Europol.

EUROPOL. Joint Cybercrime Action Taskforce (J-CAT). Europol.

FINOCCHIARO, G. 2024. Intelligenza artificiale: quali regole? Il Mulino.

GENOVESE, A. 2024. Capitolo XII. *Dall'agente sotto copertura all'agente provocatore. Limiti di applicazione della fattispecie.* In I *reati in materia di stupefacenti: iter legislativi e percorsi giurisprudenziali*. Giappichelli.

GILLESPIE, A. 2026. *Cybercrime: key issues and debates* (3. ed.). Routledge, Taylor & Francis Group.

GIRARD, R. N. 2023. *The honeypot stings back: Entrapment in the age of cybercrime and a proposed pathway forward*. Chicago Journal of International Law, 24(1), pp. 187–221.

GROTIUS, H. 1625. *De jure belli ac pacis libri tres*. Parisiis: Nicolaum Buon.

HUFNAGEL, S., MCCARTNEY, C., HUFNAGEL, S.; MCCARTNEY, C. (2017). *Trust in International Police and Justice Cooperation* (1st ed.). Hart Publishing. p. 3

ILARDA, G., MARULLO, G., & Osservatorio permanente sulla criminalità organizzata. 2004. *Cybercrime: conferenza internazionale: la Convenzione del Consiglio d'Europa sulla criminalità informatica.* Giuffrè.

INTERPOL 2024-2025. *AFJOC – African Joint Operation against Cybercrime*. INTERPOL.

INTERPOL. 2020. *Cybercrime Collaboration Services*. INTERPOL.

INTERPOL. 2022. *Global Cybercrime Strategy 2022–2025*. INTERPOL.

INTERPOL. 2024. *INTERPOL Global Cybercrime Conference 2023: Outcome Report*. INTERPOL

KARSAI, K. 2019. *Locus/forum regit actum - A dual principle in transnational criminal matters.* Hungarian Journal of Legal Studies, 60(2) pp. 155–172.

KHALIFA, A. M. M. 2020. *Overcoming the conflict of jurisdiction in cybercrime* (Master's thesis, The American University in Cairo). AUC Knowledge Fountain.

KOSKENNIEMI, M., & KARI, V. (2020). *Sovereign Equality*. In J. E. Viñuales (Ed.), *The UN Friendly Relations Declaration at 50: An Assessment of the Fundamental Principles of International Law*. Cambridge: Cambridge University Press.

KOSTORIS, R. E. 2017. *Manuale di procedura penale europea* (5ª ed.). Milano: Giuffrè Editore

LANNIER, S. 2024. *Infiltrating virtual worlds: The regulation of undercover agents through fundamental rights*. Revista Brasileira de Direito Processual Penal, 10(3), e1066. pp.1-38

MARCHETTI, M.-R., SELVAGGI, E., & BARROCU, G. 2019. *La nuova cooperazione giudiziaria penale: dalle modifiche al Codice di procedura penale all'ordine europeo di indagine.* Wolters Kluwer.

MARCHETTI, R., & MULAS, R. 2017. *La governance internazionale della sicurezza cibernetica: L'Unione Europea*. In *Cyber security: hacker, terroristi, spie e le nuove minacce del web.* LUISS University Press.

MARCHETTI, R., & MULAS, R. 2017. *La Minaccia cibernetica*. In *Cyber security: hacker, terroristi, spie e le nuove minacce del web.* LUISS University Press.

MATTARELLA, A. 2020. Cap 9 *Le tecniche investigative speciali e le loro potenzialità sul piano internazionale.* In *La Convenzione Di Palermo: il Futuro Della Lotta Alla Criminalità Organizzata Transnazionale /.* G Giappichelli Editore.

MATTARELLA, A. *Le tecniche investigative speciali e le loro potenzialità sul piano internazionale.* In *La Convenzione Di Palermo: il Futuro Della Lotta Alla Criminalità Organizzata Transnazionale /.* G Giappichelli Editore.

MELILLO, G. 2003. *Le operazioni sotto copertura nelle indagini relative a delitti con finalità di terrorismo*. In G. Di Chiara (a cura di), *Il processo penale tra politiche di sicurezza e nuovi garantismi* Torino: Giappichelli.

MULA, D.; CONTALDO, A. 2020. *Cybersecurity Law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche* Pacini Editore.

NICASTRO, G. 2006. *Eurojust* in *Diritto penale europeo e ordinamento italiano*. Giuffrè Editore.

OĞURLU, E. 2023. *International Law in Cyberspace: An Evaluation of the Tallinn Manuals*. Annales de la Faculté de Droit d'Istanbul, (73). pp.327-344.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. 1986. *Computer-related crime: Analysis of legal policy.* Paris: OECD.

ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE. 2023. *Ensuring human rights compliance in cybercrime investigations: OSCE training guide for criminal justice practitioners* (ISBN 978-92-9271-245-7). OSCE Secretariat, Transnational Threats Department.

ONUF, N. G. 1994. *Civitas Maxima: Wolff, Vattel and the Fate of Republicanism. The American Journal of International Law*, 88(2), pp. 280–303.

PAULESU, P. P. 2018. *Operazioni sotto copertura e ordine europeo d'indagine penale*. Archivio Penale: Rivista Quadrimestrale Di Diritto, Procedura e Legislazione Penale Speciale, Europea e Comparata. pp. 25-46.

PERDUCA, A., & CHIAVARIO, M. 2022. *Cooperazione giudiziaria internazionale in materia penale*. Giappichelli.

PICOTTI, L. 2023. Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme. in Cybercrime (2. edizione.). UTET Giuridica.

PIETROPAOLI, S. 2025. *Informatica criminale: diritto e sicurezza nell'era digitale: aggiornata alla legge 90/2024 e alla direttiva NIS2* (Seconda edizione.). Giappichelli.

POLYZOIDOU, V. 2021. *Combatting the cybercrime: Thoughts based on the second additional protocol (draft) to the Budapest Convention on Cybercrime*. In T.-E. Synodinou, P. Jougleux, C. Markou, & T. Prastitou (Eds.), *EU Internet law in the digital single market*. Springer International Publishing.

POLIZIA DI STATO. 2025. *Report Annuale 2025 per la tutala dei diritti.* Servizio Polizia Postale e per la Sicurezza Cibernetica.

POLIZIA DI STATO. 2025. *Report annuale 2025* per la tutela dei diritti. Servizio di Polizia Postale e per la Sicurezza Cibernetica.

RIZZI, M. A., & SERINI, F. 2024. *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*. Rivista Italiana di Informatica e Diritto, 6(2) pp. 116-136.

ROSS, J. E. 2004. *Impediments to Transnational Cooperation in Undercover Policing: A Comparative Study of the United States and Italy.* The American Journal of Comparative Law., 52(3), pp. 569-623.

ROSS, J. E. 2014. *Undercover Policing and the Varieties of Regulatory Approaches in the United States*. *American Journal of Comparative Law, 62*(Suppl. 1) pp. 673-683.

ROSS, J. E. 2015. *Anti-terror stings and human subjects research: The implications of the analogy for notions of entrapment and for the pursuit of strategic deterrence*. *New York University Journal of International Law and Politics, 47*(2), pp. 379-407.

SCALFATI, A. 2019. *Operazioni digitali sotto copertura*. In *Le Indagini Atipiche /*. G. Giappichelli Editore.

SHIPLEY, T. G. 2013. *Investigating internet crimes: an introduction to solving crimes in cyberspace* /. Syngress.

TROISI, P. 2022. *Investigazioni nella rete e attività sotto copertura* in *Le investigazioni digitali sotto copertura.* Bari: Cacucci Editore.

TROISI, P. 2022. *Induzione al reato e giusto processo* in *Le investigazioni digitali sotto copertura.* Bari: Cacucci Editore.

TROISI, P. 2022. *Provocazione per la prova e garanzie difensive* in *Le investigazioni digitali sotto copertura.* Bari: Cacucci Editore.

UNITED NATIONS. ECONOMIC AND SOCIAL COUNCIL. 1998. *Commentary on the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988* (UN Doc. E/CN.7/590). United Nations.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. 2012. *Digesto di casi di criminalità organizzata / Digest of Organized Crime Cases*.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. 2012. *Manual on mutual legal assistance and extradition.* United Nations.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. 2012. *The use of the Internet for terrorist purposes* (UNODC).

UNITED NATIONS OFFICE ON DRUGS AND CRIME. 2013. *Comprehensive study on cybercrime* (E/CN.15/2013/CRP.4).

WIENER, N. (1970). Introduzione alla cibernetica. L'uso umano degli esseri umani. Bompiani.

ZAPPULLA, A. 2012. *La formazione della notizia di reato: Condizioni, poteri ed effetti.* Giappichelli.

SITOGRAFIA

AFFARITALIANI.IT. 2025, 2 settembre. *Von der Leyen, il gps dell'aereo va in tilt. Benigni (Elt Group): "Rafforzare l'autonomia strategica e la sovranità tecnologica italiana e dell'UE"*. Affaritaliani.it.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE. 2024, 16 maggio. *Gruppo di lavoro G7 sulla cybersicurezza*. ACN.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE. 2024. Portale NIS

COMMISSARIATO DI POLIZIA POSTALE E DELLE COMUNICAZIONI. *Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC*

EUROPOL. 2017, July 20. *Massive blow to criminal Dark Web activities after globally coordinated operation – Takedown of AlphaBay and Hansa will lead to hundreds of new investigations in Europe.* Europol.

EUROPOL. 2025, 16 luglio. *Global operation targets NoName057(16) pro-Russian cybercrime network*. Europol.

FEDERAL BUREAU OF INVESTIGATION. 2017, July 20. *AlphaBay takedown*. FBI.

INTERPOL. 2025, 22 agosto. *African authorities dismantle massive cybercrime and fraud networks, recover millions.* INTERPOL.

INTERPOL. *Spotlight: Cybercrime outreach*. INTERPOL.

MELILLO, G. 2024, March 22. *Audizione del Procuratore Nazionale Antimafia e Antiterrorismo Giovanni Melillo – In materia di rafforzamento della cybersicurezza nazionale e reati informatici* [Audizione, Riunione delle Commissioni Affari Costituzionali e Giustizia, Camera dei Deputati]. Camera dei Deputati WebTV.

NATO Cooperative Cyber Defence Centre of Excellence, istituito il 14 maggio 2008.

RODRIGUEZ Katitza & GULLO Karen. March 3, 2022. *Negotiations Over U.N. Cybercrime Treaty Under Way in New York, With EFF and Partners Urging Focus on Human Rights*, ELEC. FRONTIER FOUND.

U.S. DEPARTMENT OF JUSTICE, Office of Public Affairs. 2017, July 20. *AlphaBay, the largest online "dark market," shut down.*

ATTI NORMATIVI E GIURISPRUDENZA

Council of Europe. 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms* (Council of Europe Treaty Series No. 5). Council of Europe.

Council of Europe. 1959. *European Convention on Mutual Assistance in Criminal Matters* (CETS No. 30).

Council of Europe. 1999. *Criminal Law Convention on Corruption* (ETS No. 173, art. 23). Concluded 27 January 1999, Strasbourg, entered into force 1 July 2002. Council of Europe Treaty Series.

Council of Europe. 2001, November 23. *Convention on Cybercrime* (ETS No. 185). Budapest: Council of Europe.

Council of Europe. 2001. *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters* (ETS No. 182). Concluded 8 November 2001, Strasbourg; entered into force 1 February 2004. Council of Europe Treaty Series.

Council of Europe. 2017, July 5. *Recommendation CM/Rec (2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism*. Council of Europe.

Council of Europe. 2003, January 28. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189).* Strasbourg: Council of Europe.

Council of Europe. 2022, May 12. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224). Strasbourg: Council of Europe

Council of the European Union. 2002. *Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States*. Official Journal of the European Union, L 190, 1–20.

Council of the European Union. 2002. *Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams* (OJ L 162, 20.6.2002, pp. 1–3). Official Journal of the European Union.

Council of the European Union. 2006, December 18. *Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union* (OJ L 386, 29.12.2006, pp. 89–100).

Council of the European Union. 2025, June 6. *Recommendation on the Cyber Blueprint for coordinated response to major cross-border cyber crises*.

Decreto-Legge 14 giugno 2021, n. 82. *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.* Gazzetta Ufficiale n. 140 del 14 giugno 2021.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. 2013, 7 febbraio. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Bruxelles.

European Union. 1992, February 7. *Treaty on European Union* (Maastricht Treaty). Official Journal of the European Communities, C 191.
European Union. 1997, October 2. *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts*. Official Journal of the European Communities, C 340.

European Union. 2000, May 29. *Convention on Mutual Assistance in Criminal Matters between Member States of the European Union* (2000/C 197/01). Official Journal of the European Communities.

European Union. 2002. *Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams*. Official Journal of the European Union, L162, 1–3.

European Union. 2007, December 13. *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*. Official Journal of the European Union, C 306.

European Union. 2012. *Treaty on the Functioning of the European Union*. *Official Journal of the European Union*, C 326.

European Union. 2014. *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.* Official Journal of the European Union, L 130/1.

European Union. 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Official Journal of the European Union, L194, 1–30.

European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Official Journal of the European Union, L119, 1–88.

European Union. 2019. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Official Journal of the European Union, L 151, 15–69.

European Union. 2022. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).* Official Journal of the European Union, L 333, 80–152.

European Union. 2022. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union*. Official Journal of the European Union, L 333, 1–116.

European Union. 2022. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities*. Official Journal of the European Union, L 333, 164–201.

European Union. 2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.

European Union. 2025. *Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act).* Official Journal of the European Union, L38.

International Criminal Police Organization – INTERPOL. (1956). *Constitution of the ICPO–INTERPOL*.

Codice di procedura penale. 1988. Gazzetta Ufficiale della Repubblica Italiana.

Legge 23 dicembre 1993, n. 547. *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*. (Gazzetta Ufficiale della Repubblica Italiana, n. 305, 2008).

Legge 3 agosto 1998, n. 269*. Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*. Gazzetta Ufficiale della Repubblica Italiana, n. 185 del 10 agosto 1998

Decreto-legge 27 luglio 2005, n. 144*: Misure urgenti per il contrasto del terrorismo internazionale*. Convertito con modificazioni dalla Legge 31 luglio 2005, n. 155. Gazzetta Ufficiale della Repubblica Italiana, n. 176, 30 luglio 2005.

Legge 16 marzo 2006, n. 146. *Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro la criminalità organizzata transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001.* Gazzetta Ufficiale n. 85 del 11 aprile 2006. art.9

Legge 18 marzo 2008, n. 48 *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme*

di adeguamento dell'ordinamento interno. Gazzetta Ufficiale della Repubblica Italiana, n. 80.

Legge 13 agosto 2010, n. 136. *Piano straordinario contro le mafie, nonché delega al Governo in materia di antimafia. Disposizioni sulla tracciabilità dei flussi finanziari.* Gazzetta Ufficiale n. 196 del 23 agosto 2010.

Legge 9 ottobre 2023, n. 137*: Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 104, recante disposizioni urgenti a tutela degli utenti, in materia di attività economiche e finanziarie e investimenti strategici*. Gazzetta Ufficiale della Repubblica Italiana, n. 236, 9 ottobre 2023.

Legge 28 giugno 2024, n. 90: *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*. Gazzetta Ufficiale della Repubblica Italiana, n. 153, 2 luglio 2024.

Servizio Bilancio dello Stato. 2021, luglio 14. *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale* (Atto Camera n. 3161). Camera dei Deputati – Dossier VQ3161.

Netherlands. 2012. Code of Criminal Procedure: Incorporating amendments up to October 2012 (English non-official translation). United Nations Office on Drugs and Crime.

United Nations. 1945. *Charter of the United Nations.* 59 Stat. 1031, T.S. No. 993.

United Nations. 1969. *Vienna Convention on the Law of Treaties*. 1155 U.N.T.S. 331.
United Nations. 1988 December 20. *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. Vienna.

United Nations. 1998. *Rome Statute of the International Criminal Court*, July 17, 1998, 2187 U.N.T.S. 3 (entered into force July 1, 2002).

United Nations. 2000. *United Nations Convention against Transnational Organized Crime and the Protocols Thereto*. New York: United Nations.

United Nations. 2004. *United Nations Convention against Corruption*. New York: United Nations.

United Nations. 2024. *United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes* (adopted 24 December 2024, Resolution A/RES/79/243)

United Nations. Vienna, 20 December 1988. *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. United Nations Treaty Series, vol. 1582.

European Court of Human Rights. 1998, June 9. *Teixeira de Castro v. Portugal* (Application No. 25829/94). HUDOC.

European Court of Human Rights. 2008. S. and Marper v. The United Kingdom [GC]. No. 30562/04 and 30566/04.

European Court of Human Rights. 2008, February 5. Ramanauskas v. Lithuania. No. 74420/01.

European Court of Human Rights. 2010. Uzun v. Germany. No. 35623/05

European Court of Human Rights. 2010, November 4. Bannikova v. Russia. No. 24694/07.

European Court of Human Rights. 2018. Benedik v. Slovenia. No. 62357/14.

European Court of Human Rights. 2006. Weber and Saravia v. Germany. 54934/00; 2016 Szabó and Vissy v. Hungary. 37138/14.

European Court of Human Rights. 2010. Moulin v. France. 37104/06.

European Court of Human Rights. 2015. Roman Zakharov v. Russia. 47143/06.

European Court of Human Rights. 2016. Szabó and Vissy v. Hungary. 37138/14.

European Court of Human Rights. (2017, July 4). Matanović v. Croatia. No. 55700/12.

Permanent Court of International Justice. 1927. *The Case of the S.S. "Lotus" (France v. Turkey), Judgment of 7 September 1927* (Ser. A, No. 10).

Rechtbank Rotterdam. 2019, 3 luglio. ECLI:NL: RBROT: 2019:5339 (zaaknummer 10/960249-17). Raad voor de Rechtspraak.

U.S. Department of Justice, Office of Public Affairs. 2017, July 20. *Indictment, United States v. Alexandre Cazes* (Case No. 1:17-CR-00144-LJO). U.S. Department of Justice.

U.S. Department of justice, Office of Public Affairs. 2017, July 19. *AlphaBay-Cazes forfeiture complaint and exhibits.* U.S. Department of Justice.

U.S. Department of Justice, Office of Public Affairs. (2017, July 19). *AlphaBay-Cazes forfeiture complaint and exhibits*

United Nations General Assembly. 1966. *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) [Treaty Series, vol. 999, p. 171]. United Nations.

APPENDICE

1. Intervista al Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, il Prefetto Bruno Frattasi

1) Come valuterebbe l'esperienza maturata dall'ACN in questi primi anni di operatività e l'efficacia della nuova architettura nazionale per la cybersicurezza? In questo quadro, quale ruolo assume il coordinamento con ENISA?

L'ACN nei primi anni di piena operatività ha visto il progressivo consolidamento del proprio ruolo di perno dell'architettura nazionale per la cybersicurezza, operando come punto di sintesi tra esigenze di sicurezza nazionale nello spazio cibernetico e sviluppo di un ecosistema digitale resiliente. Come indicato, tra l'altro, nella Relazione annuale 2024 dell'Agenzia, l'ACN agisce all'interno di un'architettura istituzionale ormai solida, composta da più attori con distinte competenze e funzioni. La stessa si fonda su quattro pilastri complementari e tra loro interconnessi, che concorrono in modo unitario alla tutela degli interessi strategici nazionali nel dominio cibernetico.

Il primo pilastro è rappresentato dalla cybersicurezza e dalla resilienza, affidate in via primaria all'ACN, nel cui ambito rientrano le funzioni di prevenzione, regolazione, supporto agli operatori pubblici e privati, gestione tecnica degli incidenti e rafforzamento della capacità di resistenza e di recupero del sistema Paese, in coerenza con il quadro normativo nazionale ed europeo e con gli obblighi derivanti dalla Direttiva NIS2 e dalla Direttiva CER.

Il secondo pilastro riguarda la prevenzione e il contrasto della criminalità informatica, demandati alle Forze di polizia, che operano per l'individuazione degli autori degli attacchi, la repressione dei reati cibernetici e il contrasto alle forme di criminalità organizzata e transnazionale che utilizzano il cyberspazio come dominio operativo.

Il terzo pilastro attiene alla difesa e alla sicurezza militare dello Stato, affidate al Ministero della Difesa, con riferimento alla protezione delle reti e dei sistemi militari, e alla salvaguardia degli interessi nazionali nel dominio cyber quale nuovo spazio operativo, integrato con gli altri domini tradizionali della difesa.

Il quarto pilastro è costituito dalla ricerca, analisi ed elaborazione informativa, svolte dagli Organismi di informazione per la sicurezza, che contribuiscono alla comprensione delle minacce, delle intenzioni e delle capacità degli attori ostili, supportando il decisore politico-strategico attraverso attività di intelligence e di valutazione anticipatoria dei rischi.

L'integrazione funzionale della delineata architettura è assicurata dai meccanismi di coordinamento interistituzionale e, in particolare, dal Nucleo per la cybersicurezza, che rappresenta il fulcro istituzionale per la gestione unitaria delle politiche di prevenzione, preparazione e risposta alle minacce cibernetiche di rilievo nazionale, assicurando il raccordo tra indirizzo politico-strategico e dimensione tecnico-operativa. In tale contesto, l'NCS svolge un ruolo centrale sia nella fase di prevenzione e preparedness rispetto a potenziali scenari di crisi, sia nell'attivazione delle procedure di allertamento e di coordinamento in caso di eventi cibernetici significativi o di crisi su vasta scala. Attraverso la partecipazione delle Amministrazioni competenti e delle strutture istituzionali interessate, il Nucleo garantisce uno scambio informativo strutturato e continuo, favorendo la condivisione tempestiva di informazioni, valutazioni e indicatori di rischio. Tale funzione di raccordo si estende, secondo le necessità, anche ad altri stakeholder pubblici e privati rilevanti, in un'ottica di sicurezza nazionale integrata e di approccio whole-of-government e whole-of-society.

La sopra compendiata architettura nazionale cyber vede l'ACN in una posizione centrale per le funzioni di coordinamento e di raccordo che le vengono assegnate, e, soprattutto, per il ruolo di indirizzo e monitoraggio nell'attuazione della Strategia nazionale per la cybersicurezza e del suo Piano di implementazione. L'impegno profuso dall'Agenzia, le consente di dialogare e collaborare con le Istituzioni, le Pubbliche Amministrazioni – centrali e locali – con il mondo dell'Accademia e le imprese. In una parola, di rivolgersi all'intera Comunità nazionale. Solo con il contributo di tutti si può fronteggiare, infatti, una minaccia così penetrante, quale quella cyber, divenuta sempre più sofisticata e in grado di coinvolgere porzioni crescenti della popolazione, a partire dai più indifesi e dai più esposti. La maturazione, nelle varie componenti sociali, di una più forte coscienza del rischio digitale è una condizione ineludibile per dare fondamenta più robuste alla resilienza del Paese. Come

lo è, altresì, curare la crescita delle competenze digitali. Consapevolezza e formazione, del resto, rientrano pienamente nel concetto di cultura cibernetica perché entrambe considerano il fattore umano come un terreno di impegno, sia pure dedicandovi strumenti e modalità di intervento diversi.

Dal punto di vista dell'efficacia della nuova architettura nazionale, il principale valore aggiunto risiede nella chiarezza dei ruoli e delle responsabilità. L'ACN, anche in qualità di Autorità nazionale competente per la cybersicurezza ai sensi dell'art. 7 del DL n. 82 del 2021, è chiamata a svolgere un ruolo centrale non solo nella gestione degli incidenti cibernetici e nel coordinamento del CSIRT Italia, ma anche nella definizione di requisiti di sicurezza, nella supervisione dei soggetti essenziali e importanti e nel supporto alle amministrazioni pubbliche e agli operatori privati strategici. Tale impostazione risulta coerente con l'evoluzione del quadro normativo nazionale ed europeo, che tende a valorizzare modelli di governance accentrati e capaci di garantire rapidità decisionale, uniformità di indirizzo e capacità di escalation nei contesti di crisi.

In questo quadro, l'esperienza nei primi anni di operatività dell'ACN mostra come la cybersicurezza non possa essere considerata esclusivamente una questione tecnica, ma debba essere inquadrata come una componente strutturale della sicurezza del Paese. A tal fine l'ACN ha progressivamente rafforzato le attività di prevenzione, analisi delle minacce e supporto agli enti colpiti, promuovendo un approccio orientato all'innalzamento della postura di sicurezza complessiva del sistema Paese, in linea con gli obiettivi della NIS2 e con le più recenti strategie europee in materia di resilienza cibernetica.

L'architettura nazionale delineata, tra l'altro, si innesta in ambito unionale nei meccanismi delineati dal Cyber Blueprint (Raccomandazione del Consiglio del 6 giugno 2025 relativa a un programma dell'UE per la gestione delle crisi informatiche). Il Cyber Blueprint, difatti, fornisce un quadro di riferimento operativo per la gestione coordinata delle crisi cibernetiche su vasta scala, definendo principi, fasi di intervento, meccanismi di cooperazione e modalità di coinvolgimento dei diversi livelli istituzionali, inclusi quelli politici e costituisce uno strumento essenziale di indirizzo e armonizzazione, che invita gli Stati membri ad allineare i propri modelli nazionali di

gestione delle crisi cibernetiche a procedure condivise, testate attraverso esercitazioni congiunte e fondate su una logica di solidarietà e mutuo supporto.

In tale contesto, l'architettura italiana appare sostanzialmente coerente con le indicazioni della succitata Raccomandazione europea, nella misura in cui individua un'autorità nazionale chiaramente identificata, capace di coordinare gli attori tecnici, istituzionali e politici in caso di incidenti di particolare gravità o impatto sistemico.

Nell'attuazione delle politiche di cybersicurezza, un ruolo centrale riveste, altresì, il coordinamento con ENISA, principale punto di riferimento tecnico e metodologico a livello dell'Unione, con funzioni di supporto agli Stati membri, di produzione di analisi strategiche e di facilitazione della cooperazione operativa. La collaborazione tra ACN ed ENISA consente di valorizzare strumenti comuni, come le analisi del panorama delle minacce, le linee guida tecniche, i framework di maturità e le esercitazioni europee, contribuendo a rafforzare l'interoperabilità e la coerenza delle risposte nazionali. In particolare, nel contesto delineato dal Cyber Blueprint, ENISA svolge una funzione di raccordo e di hub tecnico, favorendo la condivisione tempestiva di informazioni, indicatori di compromissione e buone pratiche tra le autorità nazionali e i CSIRT. Per l'ACN, dunque, il dialogo strutturato con ENISA rappresenta quindi non solo un canale di supporto tecnico, ma anche uno strumento di allineamento strategico alle politiche europee e di rafforzamento della credibilità e dell'efficacia dell'azione nazionale.

2) Dal punto di vista tecnico e strategico, qual è il ruolo delle operazioni undercover nel contrasto alla criminalità informatica? Ritiene tali strumenti utili e complementari alle tradizionali attività di cyber-defence?

Le operazioni undercover rappresentano uno strumento di crescente rilevanza nel contrasto alla criminalità informatica, in quanto consentono di agire in modo proattivo negli stessi ambienti digitali in cui le minacce vengono concepite, organizzate e talvolta commercializzate. A differenza delle tradizionali attività di cyber-defence, prevalentemente orientate alla protezione perimetrale, al monitoraggio delle infrastrutture e alla risposta agli incidenti, le operazioni sotto copertura

permettono di intervenire a monte del ciclo della minaccia, acquisendo informazioni preziose sui modelli organizzativi dei gruppi criminali, sulle tecniche, tattiche e procedure (TTP) utilizzate, nonché sui mercati illegali in cui vengono scambiati strumenti di attacco, credenziali e dati sottratti.

Sotto il profilo tecnico, tali operazioni si sviluppano prevalentemente negli spazi del cosiddetto deep e dark web, in forum chiusi, piattaforme di messaggistica cifrata e marketplace illeciti, dove l'anonimato e l'uso di strumenti di offuscamento rendono particolarmente complessa l'azione investigativa tradizionale. L'infiltrazione controllata di questi contesti consente invece di raccogliere informazioni in tempo reale, di anticipare campagne malevole e di individuare vulnerabilità sfruttate o in fase di sfruttamento, contribuendo così in modo diretto al rafforzamento delle capacità di prevenzione e di early warning.

Dal punto di vista strategico, il valore delle operazioni sotto copertura risiede nella loro capacità di incidere sull'ecosistema criminale digitale, non solo attraverso l'identificazione e il perseguimento dei singoli responsabili, ma anche favorendo la ricostruzione delle dinamiche operative delle reti illecite, individuando le infrastrutture di comando e controllo e mappando le filiere illegali transnazionali. In questo senso, tali operazioni si inseriscono pienamente in un approccio di sicurezza cibernetica "integrata", che combina misure difensive, capacità investigative e strumenti di cooperazione giudiziaria e di polizia a livello internazionale.

Sotto il profilo normativo, l'utilizzo di strumenti undercover nel dominio cibernetico trova fondamento, a livello internazionale ed europeo, nei principi sanciti dalla Convenzione di Budapest sul *cybercrime* del 2001, che promuove l'adozione di tecniche investigative efficaci e proporzionate per il contrasto dei reati informatici, nel rispetto dei diritti fondamentali. A livello dell'Unione europea, il quadro è ulteriormente rafforzato dalle direttive in materia di cooperazione giudiziaria e di contrasto alla criminalità organizzata e transfrontaliera, nonché dal ruolo di Europol e del suo *European Cybercrime Centre* (EC3), che coordina e supporta operazioni sotto copertura e attività di intelligence criminale nel cyberspazio.

Nel contesto nazionale la legge n. 137 del 2023 ha previsto che non siano punibili gli ufficiali di polizia giudiziaria appartenenti agli organismi investigativi della Polizia di Stato e dell'Arma dei carabinieri specializzati nell'attività di contrasto

al terrorismo e all'eversione e del Corpo della guardia di finanza competenti nelle attività di contrasto al finanziamento del terrorismo, i quali, nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova in ordine ai delitti commessi con finalità di terrorismo o di eversione, anche per interposta persona, compiano attività illegali [indicate nella lett. a) del comma 1 dell'art. 9 della legge n. 146/2006] ovvero - con la novella legislativa del 2023 - si introducano all'interno di un sistema informatico o telematico, danneggino, deteriorino, cancellino, alterino o comunque intervengano su un sistema informatico o telematico ovvero su informazioni, dati e programmi in esso contenuti, attivano identità, anche digitali, domini e spazi informatici comunque denominati, anche attraverso il trattamento di dati personali di terzi, ovvero assumano il controllo o comunque si avvalgano dell'altrui dominio e spazio informatico comunque denominato o compiano attività prodromiche o strumentali[312].

Una previsione ampia, minuziosa e analitica invero, legittima l'introduzione per gli ufficiali undercover all'interno di un sistema informatico o telematico, ove presupposto implicito è che l'introduzione avvenga clandestinamente, abusivamente, cioè violando limiti o protezioni concepiti per consentire solo accessi selezionati, in forza di uno ius admittendi aut prohibendi.

Si coglie, in ogni caso, in modo piuttosto limpido, l'intento del legislatore: scriminare o, comunque, escludere la punibilità dell'agente undercover che commetta fatti tipici ai sensi della menzionata norma incriminatrice o di altre che possano assumersi violate a fronte, ora di un accesso abusivo a un sistema informatico o telematico protetto da misure di sicurezza, ora della permanenza all'interno dello stesso contro la volontà del titolare dello ius excludendi[313]. Per converso, esula dal perimetro in discorso l'attività di mero monitoraggio della rete, che la polizia giudiziaria può compiere senza incontrare particolari ostacoli, ove si risolva nella

[312] Magi R., "*Sicurezza delle infrastrutture digitali e potenziamento del contrasto alla criminalità informatica. Fra nuovi poteri e difficili equilibri di sistema*" in Questione Giustizia 2024.
[313] Ciampi S. "*Legge n. 137 del 2023 e investigazioni (digitali) sotto copertura: la cedevolezza del "modello sostanzialista", l'assenza di uno statuto processuale, la necessità di una rivoluzione copernicana nell'approccio alla materia*" in Processo penale e giustizia, fasc. 3, 2024.

osservazione di contenuti visibili alla generalità dei naviganti, ancorché sfoci in attività di raccolta e analisi di informazioni provenienti da fonti 'aperte.

Le operazioni undercover si pone in ottica di assoluta complementarietà e interdipendenza funzionale con la cyber-defence. Al riguardo, le attività sotto copertura, tipicamente riconducibili all'ambito repressivo e investigativo, producono un patrimonio informativo che, se opportunamente valorizzato e condiviso nei limiti consentiti dall'ordinamento, può rafforzare le capacità di prevenzione e risposta degli attori deputati alla sicurezza cibernetica nazionale. In tal senso, esse non si pongono in alternativa alle funzioni di difesa cibernetica, ma ne costituiscono un naturale completamento, contribuendo a una visione integrata della sicurezza che tenga insieme dimensione tecnica, investigativa e strategica.

3) Quali sono, allo stato attuale, le forme operative di coordinamento tra DNA e ACN a seguito dell'estensione delle funzioni di impulso del Procuratore nazionale antimafia e antiterrorismo determinata dall'inserimento del comma 4-bis nell'art. 371-bis c.p.p.?

L'inserimento del comma 4-bis nell'articolo 371-bis del codice di procedura penale segna un passaggio di particolare rilievo nel rafforzamento del coordinamento istituzionale tra l'Autorità giudiziaria, e in particolare la Direzione nazionale antimafia e antiterrorismo, e l'Agenzia per la cybersicurezza nazionale.

La disposizione estende infatti le funzioni di impulso e coordinamento del Procuratore nazionale antimafia e antiterrorismo anche ai procedimenti relativi ai delitti informatici e ai reati commessi mediante l'uso di strumenti informatici o telematici, quando presentino profili di particolare gravità, serialità, organizzazione o impatto sistemico, ovvero risultino connessi a finalità di terrorismo, eversione o criminalità organizzata.

Dal punto di vista operativo, tale estensione normativa consente alla DNA di svolgere un ruolo di raccordo strategico tra le procure distrettuali e i soggetti istituzionali titolari di competenze tecniche in materia di cybersicurezza, primo fra tutti l'ACN. Il coordinamento non si traduce in una sovrapposizione di funzioni, ma in una

sinergia strutturata tra il livello investigativo-giudiziario e quello tecnico-preventivo e di risposta agli incidenti.

In questo quadro, la legge n. 90/2024, nel disciplinare i rapporti tra l'Agenzia, il Procuratore nazionale antimafia e antiterrorismo, la Polizia giudiziaria e il Pubblico ministero, ha introdotto un sistema di reciproca informazione volto a contemperare le esigenze dell'accertamento giudiziario con quelle, altrettanto importanti, di resilienza operativa dei sistemi e dei servizi impattati, per una loro più immediata ripresa funzionale. Al riguardo, il legislatore ha normato una prassi collaborativa già in essere tra i soggetti citati che si è dimostrata vincente anche rispetto a specifici casi giudiziari. Si prevede, in particolare, che l'ACN informi senza ritardo il Procuratore nazionale antimafia e antiterrorismo nei casi in cui ha notizia di un attacco ai sistemi informatici o telematici di cui all'art. 371-bis, co. 4-bis, del Codice di procedura penale e, in ogni caso, quando risultino interessati soggetti inclusi nel PSNC, operatori di servizi essenziali e fornitori di servizi digitali (soggetti NIS), imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (soggetti TELCO). Corrispondentemente, il Pubblico ministero – quando acquisisce la notizia dei citati gravi delitti informatici – deve darne tempestiva informazione all'Agenzia, assicurando anche il raccordo informativo con l'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione. Il Pubblico ministero, in ogni caso, ricevuta la notizia di reato e assunta la direzione delle indagini, è chiamato a impartire le disposizioni necessarie ad assicurare che gli accertamenti urgenti si svolgano tenendo conto delle attività di ripristino svolte dall'Agenzia e può eventualmente disporre il differimento di una o più attività per evitare un grave pregiudizio per il corso delle indagini. Viene, infine, introdotta la possibilità per l'ACN di partecipare agli accertamenti tecnici irripetibili per i delitti richiamati. Per garantire il miglior allineamento informativo tra l'Agenzia, la Direzione nazionale antimafia e antiterrorismo e la Polizia di Stato, è stato siglato un protocollo finalizzato proprio a strutturare il flusso delle informazioni, necessario per consentire a ognuna delle parti di esercitare le funzioni attribuite dalla legge.

L'estensione delle funzioni della DNA consente, altresì, di superare una visione frammentata dei reati informatici, spesso trattati come episodi isolati, e di ricondurli invece a fenomeni complessi e strutturati, talvolta transnazionali, che

richiedono una risposta integrata. In questo senso, la collaborazione con l'ACN favorisce una lettura sistemica delle minacce cibernetiche, coerente con il quadro delineato dalla normativa europea e nazionale in materia di cybersicurezza, inclusa la direttiva NIS2 e la legislazione nazionale di attuazione, che valorizzano la cooperazione tra autorità competenti e la condivisione delle informazioni rilevanti.

Infine, l'interazione tra DNA e ACN assume rilievo anche nella gestione delle crisi cibernetiche di particolare gravità, in cui il profilo penale si intreccia con esigenze di sicurezza nazionale e di continuità dei servizi essenziali. In tali contesti, il ruolo di impulso del Procuratore nazionale antimafia e antiterrorismo, rafforzato dal comma 4-bis dell'art. 371-bis c.p.p., consente di garantire un coordinamento tempestivo delle iniziative giudiziarie, evitando frammentazioni e favorendo una risposta coerente con le azioni di mitigazione tecnica e di gestione dell'incidente condotte dall'ACN.

4) Quali ritiene essere le principali difficoltà nella cooperazione internazionale per la gestione degli attacchi cyber e come crede si possano fronteggiare?

La cooperazione internazionale nella gestione degli attacchi informatici è un tema molto complesso, poiché le sfide in gioco non riguardano solo la tecnologia, ma anche la geopolitica, la sovranità nazionale e la sicurezza economica. La dimensione globale della minaccia – in cui tanto gli attacchi quanto le soluzioni non conoscono confini – esige, infatti, una risposta altrettanto globale, concertata e condivisa a livello internazionale.

L'attuale scenario geopolitico, in costante evoluzione, determina continue sfide per la cybersicurezza, rispetto alle quali ACN svolge un costante lavoro volto a rafforzare la resilienza sistemica del Paese, assicurando adeguati livelli di protezione, risposta e sviluppo della superficie digitale. In uno spazio cibernetico, definito ormai come un dominio globale all'interno del quale operano sistemi interdipendenti e interconnessi che utilizzano le tecnologie delle informazioni e delle comunicazioni[314] , si annida una minaccia sistemica crescente e incrementale rispetto alla quale occorre

[314] D.T. Kuehl, *From Cyberspace to Cyber-power: Defining the Problem*, in *Cyberpower and National Security*, ed. by F.D. Kramer, S. Starr, L.K. Wentz, National Defense University Press, Washington (D.C.) 2009

rispondere rafforzando ulteriormente la resilienza, altrettanto sistemica, del nostro Paese.

La resilienza, infatti, applicata alla dimensione cibernetica, esprime la capacità di un dato sistema di adattarsi alle condizioni d'uso e di resistere agli eventi in modo tale da garantire la funzionalità e la continuità dei servizi erogati, nonché la capacità di recupero e una rapida ricostruzione di fronte a un attacco cyber.

Si tratta di un impegno articolato e condiviso tra i diversi attori istituzionali, le imprese, le associazioni di categoria, chiamati a contribuire, insieme, alla realizzazione di una trasformazione digitale sicura, accessibile e responsabile.

Si tratta di un impegno articolato e vasto, in cui si compendiano gli elementi che in diverso modo concorrono a garantire la resilienza dell'ecosistema digitale nazionale.

Dinanzi a tale minaccia, è essenziale che il sistema Paese oltreché resistente agli attacchi informatici, si dimostri resiliente, quindi in grado di dare prova di elevata e diffusa sostenibilità digitale, cardine di quella sovranità digitale nazionale, europea ed euro-atlantica che stiamo costruendo. Una difesa della sovranità digitale che passa, necessariamente, dalla capacità di garantire la sicurezza nazionale impedendo forme di ingerenza che possano condurre alla perdita di controllo dei dati o di asset strategici.

La difesa della pace, della libertà e della sicurezza nazionale e internazionale diventano una priorità strategica anche dinanzi al diffondersi di meccanismi di offesa estranei alle categorie belliche tradizionali.

Si pensi, a tal proposito, alla c.d. "guerra ibrida". Essa è una forma di conflitto moderna e complessa che sfuma i confini tradizionali della guerra, utilizzando "armi non convenzionali" per raggiungere obiettivi strategici, spesso evitando lo scontro militare diretto su larga scala. L'obiettivo, infatti, è spesso quello di destabilizzare, indebolire, influenzare o coercire l'avversario senza necessariamente superare la soglia che scatenerebbe una risposta militare convenzionale, operando, dunque, nella cosiddetta "zona grigia". Spesso le azioni sono condotte in modo da rendere difficile l'attribuzione chiara a uno Stato specifico, mantenendo una "negabilità plausibile".

Si opera deliberatamente per confondere le linee tra guerra e pace, tra combattenti e civili, tra attori statali e non statali. Si tratta, quindi, di una strategia che combina diversi tipi di strumenti e tattiche – convenzionali, cibernetiche, informative,

economiche e politiche – in modo coordinato e sincronizzato per raggiungere obiettivi strategici. Inoltre, i più recenti sviluppi denotano come l'evoluzione del conflitto è costantemente aggiornata dall'utilizzo sul campo di nuove tecnologie, ad esempio droni e altre apparecchiature robotiche, in grado spesso di condizionare anche il corso degli eventi, riducendo, se non azzerando del tutto, l'esposizione umana. Tale modalità di conflitto "invisibile", sottosoglia ma comunque letale, comporta l'imprescindibile necessità di proteggere la popolazione e gli asset critici, civili e militari, anche da attacchi intangibili, quali sono quelli elettromagnetici e cyber[315] . In particolare, si pensi a tecniche di attacco, tanto insidiose quanto silenziose, come il jamming, una tecnica di disturbo di frequenze, comunicazioni radio o segnali elettronici, come il GPS, tramite l'emissione di interferenze[316] .

La conflittualità, dunque, si è spostata dal vecchio campo di battaglia alla dimensione cibernetica, alle covert actions, alle false flag operations, alla guerra dell'informazione e della disinformazione, alla guerra economica, alla lotta per la supremazia nello spazio, nel cyberspazio e nella dimensione subacquea

Nello spazio virtuale che ormai caratterizza il nostro vivere quotidiano, la sicurezza nazionale si presenta – intanto ed in primis – come un predicato della sovranità digitale nazionale.

Senonché abbiamo a che fare, e già da qualche tempo, con un'altra forma di sovranità digitale, quella europea, espressione "immaginifica e di grande forza evocativa"[317] che risale al discorso tenuto dalla Presidente Von der Leyen sullo stato dell'Unione nel 2020.

Come è stato rilevato in dottrina[318], tale espressione - la sovranità digitale europea - contiene un'affermazione politica e non giuridica, indica un obiettivo cui tendere e non descrive uno stato di fatto già acquisito e consolidato. Soprattutto essa si iscrive in una logica di competizione e di confronto tra potenze globali in cui la

[315]https://www.affaritaliani.it/economia/von-der-leyen-il-gps-dell-aereo-va-in-tilt-benigni-elt-group-rafforzare-l-autonomia-strategica-e-la-sovranita-tecnologica-italiana-e-dell-ue-982975.html?refresh_ce.

[316] P. MAURI, *Due vie per mandare l'elettronica in tilt. E anche i voli civili ora sono sotto tiro*, in "il Giornale", 02/09/2025. Un'altra tecnica di attacco "ibrido" è rappresentata dallo *spoofing*[316], che ha ad oggetto l'invio di un falso segnale, dalle caratteristiche di quello vero, per "ingannare" i sistemi di navigazione di bordo e quindi mandare fuori rotta l'aeromobile.

[317] G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, Bologna, il Mulino, 2024, p. 109.

[318] Ibidem

dimensione nazionale viene inevitabilmente trascesa, sovrastata, ma niente affatto eclissata; sicché anche in questa sua forma, quella sovranazionale europea, la sovranità digitale rimane ancora legata alla sicurezza nazionale, pur acquisendo una ricchezza e una forza ulteriori rispetto alla sola dimensione domestica.

È dalla prospettiva appena illustrata che si deve osservare la recente iniziativa adottata in ambito unionale, che ha visto la sottoscrizione, da parte dei rappresentanti degli Stati membri dell'Unione europea, della "Declaration for European Digital Sovereignty" (Dichiarazione per la Sovranità Digitale Europea).

La Dichiarazione, infatti, definisce la sovranità digitale come la capacità dell'Unione europea di agire in modo autonomo nel mondo digitale, regolando infrastrutture, dati e tecnologie secondo le proprie leggi, i propri valori e interessi di sicurezza, senza indebite dipendenze da attori esterni, ma restando comunque aperti alla cooperazione con i partner internazionali che condividono i principi europei.

Il documento, infatti, chiarisce che la sovranità digitale non identifica una forma di protezionismo o isolamento, ma un approccio comune europeo che rafforza la capacità di fare liberamente le proprie scelte tecnologiche. Ciò passa attraverso un clima favorevole agli investimenti, un quadro regolatorio chiaro e prevedibile e una forte attenzione alla competitività. Seppure al suo interno grande attenzione venga dedicata alla sovranità sui dati, considerati un asset strategico per l'Europa, vengono individuate anche alcune aree tecnologiche strategiche su cui concentrare una visione di lungo periodo e gli investimenti, come il calcolo ad alte prestazioni (HPC) e semiconduttori, reti di comunicazione di nuova generazione e infrastrutture satellitari, tecnologie quantistiche e cybersicurezza, cloud e intelligenza artificiale.

Naturalmente, ogni Paese ha un proprio quadro normativo e definisce un approccio nazionale alla cybersicurezza. Tuttavia, al fine di superare i "personalismi nazionali" che potrebbero determinare difficoltà nella prevenzione e gestione della minaccia cyber, i singoli Stati sono chiamati ad adottare un approccio comune che garantisca i più elevati standard di cybersicurezza.

È proprio questa la ratio della direttiva NIS2, volta a garantire un livello comune elevato di cybersicurezza nell'UE - recepita nell'ordinamento nazionale con il decreto legislativo 4 settembre 2024, n. 138[319] - che copre ben 18 settori distinti tra

[319] Pubblicato in G.U. n. 230 del 1 ottobre 2024 ed entrato in vigore il 16 ottobre 2024

critici e altamente critici - richiedendo un ulteriore rafforzamento della postura di cybersicurezza. La disciplina dettata dalla NIS 2 determina, come dico spesso, un cambio di registro di portata enorme rispetto alla grande questione della sicurezza informatica, la quale non ha una valenza solo tecnica e non "dialoga" solo con i professionisti dell'informatica e con gli addetti ai lavori. Con l'entrata in vigore, il 16 ottobre 2024, del D.lgs. n. 138/2024 (c.d. decreto NIS2), l'Italia è stata tra i primi Stati membri a completare l'iter legislativo di recepimento nei tempi previsti dall'UE, all'esito di un percorso concertato e condiviso con gli attori pubblici coinvolti e con i soggetti privati impattati dalla nuova disciplina.

Soffermandomi sui temi della cooperazione internazionale, l'ACN, in linea con le politiche del Governo e d'intesa con il Ministero degli Affari Esteri e della Cooperazione internazionale, ha promosso l'interesse nazionale nei diversi ambiti in cui si svolge la cooperazione cyber. Innanzitutto, ha continuato ad attribuire la consueta priorità alla collaborazione in sede di Unione europea, che costituisce una componente fondante della strategia di cybersicurezza del Paese, tanto a livello di policy quanto sul piano operativo.

L'azione dell'Agenzia si è sviluppata secondo tre macro-direttrici, orientate verso Paesi o aree di grande importanza sotto il profilo della cybersicurezza. Si è rivolta alle Agenzie e ai Centri di responsabilità per la cybersicurezza dei Paesi del G7, con i quali si condividono interessi fondamentali in tema di sicurezza dello spazio cibernetico e di protezione degli asset critici. Si è indirizzata, inoltre, verso le aree del Mediterraneo allargato e dei Balcani, da sempre prioritarie per la proiezione internazionale del Paese. Infine, si è orientata verso i Paesi che si collocano nel c.d. corridoio IMEC (India-Middle East Economic Corridor), che avvicina l'India all'Europa attraverso i Paesi compresi tra il Golfo e il Mediterraneo.

L'azione lungo queste tre direttrici ha beneficiato dell'importante iniziativa di politica internazionale assunta dall'Agenzia con la costituzione del Gruppo di lavoro G7 sulla cybersicurezza durante la Presidenza italiana del 2024.

In quell'occasione, il nostro Paese ha potuto affermare, anche in ambito cyber, la sua importante statura internazionale, venendo così a creare uno spazio di cooperazione continuativa tra le Agenzie e i Centri cyber dei Paesi like-minded, unico nel suo genere.

Lo scopo di promuovere una così utile strategia di governance globale ha determinato un modus operandi condiviso anche nel corso della successiva presidenza canadese, e potrà offrire ulteriori spunti per una comune riflessione su temi cruciali per la cybersicurezza che nell'attuale scenario geopolitico sembrano richiedere la più stretta solidarietà tra le grandi democrazie occidentali che, ritornando alla domanda posta, è il più grande strumento per fronteggiare ogni sviluppo distopico della dimensione digitale.

La cooperazione del Gruppo di lavoro G7 sulla cybersicurezza si è concentrata sulla sicurezza delle catene di approvvigionamento delle infrastrutture critiche, con un focus specifico sul settore energetico, e sulla cybersicurezza dell'intelligenza artificiale. Con l'obiettivo di armonizzare i meccanismi nazionali a presidio della sicurezza delle infrastrutture critiche, il Gruppo ha svolto una ricognizione della normativa e degli standard internazionali e nazionali di cybersicurezza, trovando punti di convergenza tra gli approcci e le misure adottate in ciascun Paese G7 per salvaguardare la supply chain di beni e servizi ICT nel settore energetico.

Sul tema del rapporto tra cybersicurezza e intelligenza artificiale, d'altro canto, il Gruppo ha voluto mettere a fattor comune le competenze e capacità dei partner al fine di comprendere meglio sia le minacce derivanti dall'uso malevolo di sistemi di IA, che le condizioni di sicurezza necessarie per beneficiare delle grandi potenzialità derivanti dall'impiego di questa tecnologia.

5) Una delle problematiche maggiormente rilevanti riguarda il disallineamento tra le capacità degli organi statali di prevenire e contrastare il fenomeno dei reati informatici e la rapidità con cui questi possono provocare danni, soprattutto alle infrastrutture critiche. Dal suo punto di vista, come può essere colmato questo divario affinché lo Stato italiano possa avere un vantaggio operativo nel contrasto al cybercrime? E, più in generale, quali strumenti e quali forme di cooperazione internazionale ritiene siano necessari per consentire al sistema internazionale di stare al passo con l'evoluzione delle minacce cibernetiche?

La tecnologia evolve rapidamente e con essa crescono anche i rischi informatici che minacciano i cittadini, le istituzioni, le imprese e l'intera società civile. L'Agenzia

per la cybersicurezza nazionale è la risposta dello Stato per contrastare i pericoli che si annidano all'interno di questo mondo sempre più radicato in ogni aspetto della nostra vita.

La minaccia cibernetica è, infatti, globale e incrementale, e lo è nel senso sia quantitativo che qualitativo anche in funzione dell'espansione della superficie digitale esposta. Con la crescente digitalizzazione gli stessi sistemi fisici sono diventati sempre più interconnessi e vulnerabili agli attacchi informatici. Questo ha portato alla necessità di adottare un approccio olistico alla sicurezza che consideri sia le minacce fisiche che quelle informatiche.

In questo senso, occorre rilevare come – sebbene le infrastrutture critiche siano esposte a varie tipologie di minacce, che variano in base al luogo in cui si trovi il bersaglio e al servizio colpito – l'unica che incombe equamente su tutte le infrastrutture – a prescindere dal luogo, dalla forma, dalla dimensione, o dal servizio fornito – è la minaccia cibernetica.

Minacce come *ransomware* e *phishing* possono compromettere la continuità operativa di un servizio e causare danni economici e reputazionali significativi. In particolare, il ransomware costituisce la tipologia di minaccia con l'impatto più elevato, sia in termini di interruzione dei servizi essenziali, nonché di perdita di disponibilità e integrità dei dati. Con il termine in questione ci si riferisce ad una tipologia di attacco cibernetico che ha lo scopo di cifrare i beni del target informatico, in modo da comprometterne la disponibilità, l'integrità e la riservatezza. L'impatto di questi attacchi può essere economico, operativo e reputazionale. Le strategie di attacco sono spesso meglio comprese attraverso lo studio della cyber kill chain, un modello che rappresenta le fasi sequenziali di un attacco informatico, consentendo un'analisi sistemica e strutturata delle metodologie operative adottate dagli attori criminali.

L'evoluzione della minaccia *ransomware* ha comportato una rimodulazione dell'ecosistema criminale, sostenuta dalla progressiva specializzazione degli attaccanti e da una loro riorganizzazione in *ransomware* gang.

Alcuni gruppi criminali hanno iniziato a offrire la propria infrastruttura anche ad utenti esterni, spesso in cambio di una percentuale sul riscatto richiesto. Questo modello criminale prende il nome di Ransomware as a Service e permette l'incremento dei profitti da parte degli attaccanti.

La minaccia rappresentata dal ransomware risulta duplicemente insidiosa, in quanto compromette gravemente la stabilità di due dei pilastri sui quali poggia la sicurezza nazionale: la sicurezza dei dati, la cui esfiltrazione e crittazione è funzionale al ricatto estorsivo, e la sicurezza economica, che viene incrinata in misura notevole.

Con lo scopo di contrastare tale fenomeno, la Legge n. 90/2024 ha introdotto nell'ordinamento un'apposita fattispecie penale denominata "estorsione informatica", con la quale s'intende reagire alla gravità e alla frequenza dei ricatti realizzati attraverso la minaccia o l'attuazione di attacchi informatici[320].

La diffusione mondiale della minaccia e il suo inasprirsi hanno portato, altresì, alla costituzione di una vasta alleanza internazionale, la Counter Ransomware Initiative, il cui obiettivo consiste nel definire un piano d'azione condiviso, capace di contrapporsi in maniera coesa al fenomeno, senza che alcun punto di permeabilità o di inefficace resistenza possa favorire la catena criminale. Questa iniziativa, che vede cooperare più di sessanta Paesi, tra i quali l'Italia, è seguita con grande attenzione dall'Agenzia per la cybersicurezza nazionale e rappresenta, accanto alla costante partecipazione ai Tavoli e ai gruppi di lavoro di Bruxelles, una parte significativa quanto rilevante della sua azione a livello internazionale. In questa, come in altre forme di cooperazione multilaterale sembra affacciarsi, anche sulla scena dello spazio virtuale, il principio solidaristico di sicurezza collettiva, posto a mutua garanzia dell'integrità e dell'indipendenza dei Paesi che liberamente aderiscono ad un vincolo di alleanza.

Ulteriori tecniche in grado di influenzare il panorama della minaccia ransomware riguardano l'utilizzo di strumenti basati sull'Intelligenza Artificiale (IA) e su Large Language Models (LLMs) per fini criminali. Simili strumenti possono essere usati per automatizzare lo sviluppo di malware, permettendo di condurre attacchi sofisticati. Strumenti basati su tali linguaggi e sviluppati per fini criminali sono già diffusi e utilizzati prevalentemente per lo sviluppo di e-mail di phishing credibili e specifiche per la vittima in questione.

[320] Disciplinata dall'art. 629, comma 3 c.p., la nuova ipotesi di reato punisce l'estorsione attuata mediante la commissione di taluni reati informatici, ovvero mediante la minaccia di compierli.

Rimanendo sul profilo delle forme di cooperazione necessarie a stare al passo con l'evoluzione delle minacce cibernetiche, è ragionevole affermare che le attuali tensioni geopolitiche hanno determinato lo spostamento del baricentro europeo dalla tutela del mercato alla difesa comune unionale.

Ci troviamo di fronte a un fatto trasformativo di grandissima rilevanza, che segna un'evoluzione degli stessi obiettivi di riferimento che l'Europa ha seguito quando ha scelto di porre al centro della disciplina della digitalizzazione gli interessi del consumatore, affinché il mercato potesse offrire a tutti i consumatori europei, ovunque fossero, la possibilità di utilizzare prodotti digitali performanti e a basso prezzo.

Oggi, però, siamo chiamati a tutelare un ventaglio di esigenze più ampio che ha determinato lo spostamento del baricentro degli interessi unionali.

Si assiste a un'ibridazione tra il mercato unico fondato su un principio sovranazionale e il profilo della difesa, che è un tema securitario nazionale, intergovernativo, dove non c'è mai stata una sovrapposizione dell'Europa rispetto alla dimensione nazionale. Tuttavia, questi due grandi filoni si stanno pian piano avvicinando e incrociando.

I crescenti rischi di cybersicurezza e un panorama di minacce globalmente complesso, con il chiaro pericolo di rapida propagazione di incidenti da uno Stato membro all'altro e da un paese terzo all'Unione, richiedono il rafforzamento della solidarietà digitale per migliorare il rilevamento delle minacce e degli incidenti informatici, nonché la preparazione e la risposta agli stessi.

È questa la ratio del Cyber Solidarity Act, entrato in vigore il 4 febbraio scorso e volto a rendere l'Europa più resiliente e reattiva di fronte alle minacce informatiche, rafforzando al contempo il meccanismo di cooperazione esistente.

Il Regolamento introduce il c.d. "scudo europeo per la cybersicurezza". Si tratta di un sistema europeo di allerta per la cybersicurezza composto da centri operativi di sicurezza (SOC) nazionali e transfrontalieri in tutta l'UE, che utilizzeranno tecnologie avanzate come l'intelligenza artificiale (IA) e l'analisi dei dati per rilevare e condividere avvisi sulle minacce.

Il Regolamento rappresenta un passaggio strategico nella costruzione di una difesa cibernetica comune, poiché introduce strumenti innovativi volti a garantire un alto livello di sicurezza e reattività nell'intero spazio digitale europeo.

Il Cyber Solidarity Act si fonda su tre pilastri principali:

1) Sistema europeo di allerta sulla cybersicurezza[321]: una rete paneuropea di poli informatici per sviluppare e potenziare capacità coordinate in materia di rilevamento e capacità comuni in materia di conoscenza situazionale. Questi centri nazionali di poli informatici (National Cyber Hub, indicati nella fase iniziale del negoziato come SOC Nazionali) sono collegati tra loro e impiegano tecnologie avanzate, come l'intelligenza artificiale e l'analisi dei dati, per rilevare tempestivamente le minacce informatiche e condividere informazioni in modo coordinato tra gli Stati membri, migliorando la capacità di risposta collettiva.

2) Meccanismo per le emergenze informatiche, volto a rafforzare la preparazione e la reattività dell'UE davanti agli incidenti di cybersicurezza. Questo meccanismo si articola in tre azioni principali:

- il supporto alle attività di preparazione attraverso test e valutazioni nei settori più critici come finanza, energia e sanità;
- la creazione di una riserva europea di risposta rapida costituita da fornitori privati affidabili specializzati, pronti a intervenire in caso di crisi su richiesta degli Stati o delle istituzioni comunitarie;
- l'organizzazione dell'assistenza reciproca tra Stati membri, facilitando la cooperazione diretta in caso di attacchi informatici.

3) Meccanismo europeo di riesame degli incidenti di cybersicurezza, istituito per analizzare in modo retrospettivo gli incidenti più rilevanti. Su richiesta della Commissione europea o delle Autorità nazionali competenti, l'Agenzia europea per la cybersicurezza (ENISA) conduce un'analisi approfondita degli eventi, identificando le cause sistemiche e formulando raccomandazioni operative e politiche per migliorare la capacità di risposta futura dell'Unione[322].

Riserva Cyber

[321] Si tratta del cd. Cyber Shield Europeo, definito dalla Cybersecurity Strategy Europea del 2021.

[322] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

Il Cyber Solidarity Act prevede un meccanismo di emergenza per la cybersicurezza volto a rafforzare la preparazione e a potenziare le capacità di risposta agli incidenti all'interno dell'Unione europea. Per questo motivo è stata istituita una Riserva di Cybersicurezza per assistere, su richiesta, Stati membri, istituzioni, organi e agenzie dell'UE e, se applicabile, paesi terzi associati al Programma Digitale Europeo (Digital Europe Programme). La Riserva dell'UE ha l'obiettivo di fornire servizi di cybersicurezza affidabili per supportare le entità dell'UE nella risposta e nel recupero da gravi incidenti informatici.

All'interno dell'elenco dei fornitori di servizi di cybersicurezza affidabili, selezionati tramite procedura di gara da ENISA, 6 (dei complessivi 45) sono italiani.

Sempre nell'ambito delle forme di cooperazione necessarie a prevenire e contrastare la minaccia cibernetica, non possiamo trascurare il ruolo dell'Agenzia per la cybersicurezza nazionale quale Autorità di gestione delle crisi e punto di contatto unico in coerenza, per entrambi i profili, con l'intero quadro ordinamentale interno ed europeo. La conoscenza della minaccia cyber resta un punto fondamentale anche all'interno del disegno fornito dalla già richiamata direttiva NIS 2. La notifica degli incidenti cibernetici avvenuti ai danni dei soggetti essenziali e importanti costituisce, infatti, il punto di emersione di questa esigenza conoscitiva, a cui attende CSIRT Italia, componente tecnico-operativa dell'Agenzia, che ricopre il ruolo di hub nazionale per la gestione delle notifiche obbligatorie e volontarie relative agli incidenti cibernetici cui fanno riferimento le normative di settore, quali sono, in sequenza cronologica, il Perimetro di Sicurezza Nazionale Cibernetica (Decreto legge 21settembre 2019, n. 105, convertito nella legge n. 133/2019), la Legge 28 giugno 2024, n. 90 e la Direttiva NIS 2 (D. Lgs. n. 138/2024).

Nella sua veste di Autorità nazionale competente NIS, l'Agenzia partecipa, inoltre, al gruppo di Cooperazione NIS e alla Rete degli CSIRT nazionali, strutture deputate alla cooperazione operativa rapida ed efficace tra gli Stati membri, nonché alla Rete europea che prioritariamente dovrà garantire il sostegno alla gestione coordinata degli incidenti e delle crisi su vasta scala (CyCLONe). La messa in esercizio della NIS implica, dunque, l'attuazione di un complesso modello di coordinamento, sia nazionale che europeo, ponendo così le basi di una governance

multilivello, tendente ad esaltare gli aspetti di armonizzazione e di cooperazione su un duplice piano ordinamentale.

6) Guardando al futuro, quali sviluppi si aspetta nell'evoluzione della criminalità informatica? E come dovrebbe strutturarsi la cooperazione nazionale e internazionale per prevenire e contrastare tali eventuali scenari?

La digitalizzazione imperante ha amplificato vulnerabilità sistemiche, rendendo la sicurezza informatica una questione non solo tecnica, ma anche sociale, economica e geopolitica, un presidio necessario anche per la prevenzione e il contrasto della criminalità.

Il dominio digitale ha, infatti, cessato di essere una semplice estensione della realtà fisica, trasformandosi in un ecosistema autonomo nel quale la criminalità, lungi dall'essere ancorata a logiche tradizionali, ha dimostrato una incisiva capacità di adattamento, sfruttando le tecnologie emergenti per ampliare il proprio raggio d'azione, aumentare l'anonimato operativo e moltiplicare i profitti illeciti[323].

Il web, e in particolare il dark web, funge da mercato, infrastruttura logistica, ambiente relazionale per le organizzazioni criminali. Tale contesto permette di operare con elevati livelli di anonimato, riducendo la necessità di interazioni fisiche e complicando la tracciabilità delle operazioni.

Le tecnologie emergenti e, tra queste, l'intelligenza artificiale stanno progressivamente incidendo sulla trasformazione delle stesse metodologie criminali. Oggi si osservano attaccanti automatizzati in grado di sfruttare vulnerabilità sistemiche, difese AI-driven che apprendono e reagiscono in tempo reale e modelli adattivi che evolvono con l'ambiente operativo.

Analisi su dati reali mostrano evidenze di uso dell'AI in attività ostili, come la ricognizione, la generazione di malware, il phishing personalizzato e l'elusione dei sistemi di sicurezza.

[323] Audizione del Procuratore nazionale antimafia e antiterrorismo dott. Giovanni Melillo presso la Commissione antimafia, svoltasi il 21.06.2023. "Oggi le organizzazioni criminali vivono nel cyberspace e lo piegano ai fini più diversi".

Ci si trova a un bivio: l'AI sta trasformando profondamente l'economia degli attacchi informatici, moltiplicandone la portata, ma non rivoluzionandola ancora del tutto.

C'è una finestra temporale in cui è ancora possibile agire: servono collaborazione, formazione, consapevolezza e una governance globale in grado di tradurre l'inarrestabile sviluppo tecnologico in progresso e benessere per la collettività[324].

Il rischio tecnologico, dunque, può diventare fonte di rischio sistemico i cui effetti sarebbero amplificati da un eventuale utilizzo malevolo delle emergenti tecnologie, tra cui l'intelligenza artificiale, al fine di incrementare la portata offensiva della minaccia cyber. E' questa una delle ragioni principali poste alla base del Regolamento europeo sull'intelligenza artificiale, l'AI ACT e della recente legge italiana n. 132, pubblicata in G.U. n. del 25 settembre scorso, da cui emerge la consapevolezza che solo attraverso regole comuni e condivise è possibile innalzare il livello di sicurezza e resilienza nello spazio cibernetico, garantendo un'adeguata protezione della superficie digitale anche nei confronti dei tentativi di infiltrazione nell'economia legale da parte di quelle organizzazioni criminali che hanno ormai cambiato "codice" cercando di sfruttare le nuove tecnologie per occultare i loro traffici illeciti.

Le attività criminali quindi, si stanno spostando sempre più nello spazio digitale.

Questo nuovo scenario include non solo il riciclaggio di denaro e le varie tecniche di estorsione, ma si estende anche al rischio di manipolazione di gare d'appalto, all'infiltrazione nel settore dell'energia e a tante altre attività. È una realtà connessa alla dimensione sempre più ibrida della criminalità organizzata, capace di adattarsi alle mutevoli situazioni spazio-temporali del mondo contemporaneo[325].

La crescente globalizzazione indica che le imprese italiane sono sempre più coinvolte in una rete economica globale, partecipando attivamente a transazioni

[324] UC Berkeley AI Law Institute 2025, Session 12 **"**AI & Cybersecurity" with Mikel Rodriguez, https://executive.law.berkeley.edu/programs/berkeley-law-ai-institute/

[325] A. Nicaso, M. Danesi (2023), The Dark Mafia. Organized Crime in the Age of the Internet, Routledge, London - New York.

internazionali, collaborazioni commerciali e altre attività che coinvolgono partner e mercati in tutto il mondo. Questo aumento della connettività e dell'interdipendenza economica è favorito dalle tecnologie dell'informazione, che agiscono come propulsore di crescita economica e benessere. Tale tendenza, come rilevato da molteplici operazioni su scala internazionale, è quella che hanno avuto anche le organizzazioni criminali.

Investire in misure efficaci di sicurezza informatica non è, dunque, un costo, ma una leva di competitività per le Pubbliche amministrazioni, le imprese e l'intero sistema Paese. Ciò implica la necessità di adottare pratiche avanzate di protezione dati, sviluppare protocolli di risposta agli incidenti informatici e promuovere la formazione e la consapevolezza in ordine alla sicurezza informatica. Solo preservando un ambiente digitale sicuro l'Italia può mantenere la sua competitività economica e prosperare nella sempre più interconnessa economia globale.

È pertanto necessario un impegno articolato e condiviso tra i diversi portatori di interesse: attori istituzionali, imprese, associazioni di categoria; tutti chiamati a contribuire, insieme, alla realizzazione di una trasformazione digitale sicura, accessibile e responsabile.

In questa direzione, ACN dialoga e collabora costantemente con le Istituzioni, le Pubbliche Amministrazioni – centrali e locali –, la Magistratura, le Forze di Polizia, l'Intelligence e la difesa, con il mondo dell'Accademia e delle Imprese, rivolgendosi all'intera Comunità nazionale.

Lo scenario evolutivo e le nuove sfide poste dall'innovazione tecnologica hanno, altresì, richiesto un'articolata revisione del quadro normativo in materia di cybersicurezza, sia a livello nazionale che in ambito unionale. Passaggi significativi e importanti sono stati, come già indicato, la legge 90/2024; il recepimento nazionale della Direttiva NIS2; la legge 132/2025 di recente approvazione inerente all'intelligenza artificiale; le funzioni attribuite ad ACN in materia di crittografia quantistica e post-quantistica alla luce dell'introduzione nella struttura operativa dell'Agenzia del Centro nazionale di crittografia.

Soffermandoci brevemente sulla Legge 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, si è particolarmente insistito sulla necessità di affinare e rafforzare gli aspetti collaborativi

sollecitando gli attori destinatari della disciplina ad aggiornare, ove esistenti, i piani di risposta e di gestione degli incidenti e, in caso di impatto, a prestare agli operatori dell'ACN la massima cooperazione perché il ripristino della piena funzionalità della parte digitale eventualmente compromessa avvenga nel più breve tempo possibile.

Si tratta di interventi che segnano un importante passo verso un ulteriore consolidamento della sicurezza cibernetica del Paese, rafforzando la capacità di prevenire e mitigare i rischi delle infrastrutture digitali.

Con la legge n. 90/2024 sono stati perseguiti vari obiettivi. Da un lato, il rafforzamento del quadro di sicurezza cibernetica mediante l'introduzione di obblighi di notifica e misure preventive, per garantire la protezione dei soggetti interessati e anticipare gli attacchi cibernetici. Dall'altro, la definizione di procedure di coordinamento tra gli attori coinvolti al fine di garantire un bilanciamento tra le esigenze di resilienza, quelle investigative e quelle di difesa militare e di intelligence, alle quali si aggiunge un generale aggiornamento del quadro penalistico in materia cyber.

Esigenze, queste ultime, che hanno messo in luce le già richiamate funzioni sulle quali si basa l'architettura nazionale di cybersicurezza: la resilienza sistemica, garantita, per l'appunto, da ACN; la prevenzione e il contrasto della criminalità informatica, garantita dalla Magistratura, dalla Polizia Postale e dalle Forze di Polizia competenti; la difesa e la sicurezza militare dello Stato, garantita dalle Forze armate; la ricerca e l'elaborazione informativa, garantita dall'intelligence.

La legge 90 ha ulteriormente rafforzato il profilo della collaborazione interistituzionale, mediante una modifica dell'articolo 8 del decreto-legge n. 82 del 2021, con l'introduzione di un nuovo comma 4.1 ai sensi del quale, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia, il Nucleo per la cybersicurezza può essere convocato nella composizione ristretta, di volta in volta estesa alla partecipazione di un rappresentante: della Direzione nazionale antimafia e antiterrorismo; della Banca d'Italia; di uno o più operatori di cui all'articolo 1, comma 2-bis, del decreto-legge n. 105 del 2019 (si fa riferimento ai soggetti iscritti nel Perimetro di sicurezza nazionale cibernetica); nonché di eventuali altri soggetti interessati alle stesse questioni.

La legge 90 rafforza, dunque, i rapporti tra i diversi soggetti istituzionali interessati, introducendo un sistema di reciproca informazione volto a contemperare le esigenze dell'accertamento giudiziario con quelle, altrettanto importanti, di resilienza operativa dei sistemi e dei servizi impattati, per una loro più immediata ripresa funzionale.

Conclusioni: Formazione e Consapevolezza per lo sviluppo di una cultura della cybersicurezza

La progressiva e incessante informatizzazione delle strumentazioni digitali che fanno capo ad istituzioni e amministrazioni pubbliche e ad operatori privati, ed anche la dimensione che ha assunto, a livello mondiale, la connettività ad Internet, fanno sì che la sicurezza informatica abbia il connotato di sicurezza trasversale, una sicurezza che assomma e ingloba anche le altre forme di sicurezza che da essa dipendono in una qualche misura.

Questa considerazione porta a ritenere che le strutture concettuali della sicurezza che applichiamo alla protezione dell'incolumità dei cittadini e alla integrità dei loro possessi, siano esattamente replicabili nel campo della sicurezza informatica e valgano in questo ambito con lo stesso grado di perentorietà. L'assenza o un grave deficit di sicurezza informatica è un vulnus per le nostre libertà, in quanto, come abbiamo compreso da tempo, sicurezza e libertà sono complementari, e non vi è pienezza dell'una se l'altra manca o è gravemente trascurata.

La cultura della sicurezza cibernetica inizia da qui, dal considerare questa forma di sicurezza non meno rilevante delle altre; anzi, per quel suo carattere di trasversalità orizzontale e per le dipendenze che ne discendono, possiamo ritenerla la "chiave" delle altre sicurezze, di quelle sociali come di quelle individuali.

Come ogni altra forma di cultura anche quella della sicurezza digitale deve poter raggiungere la comunità nazionale nella sua complessità e nella sua unità: cittadini, operatori del pubblico e del privato, donne e uomini -, con il massimo grado di espansione e diffusione; diversamente avremmo un serio problema di digital divide, cioè di esclusione o di marginalità sociale che non è accettabile in una visione compiutamente democratica di sicurezza.

Fare cultura della sicurezza informatica significa anche far emergere nel discorso pubblico la necessità che il digitale venga trasformato in un alleato dell'uomo. La cultura così recupera il suo significato radicale di liberazione da una forma di soggezione, di sottomissione al totem tecnologico. Una condizione umana complessa che, al cospetto delle tecnologie innovative e dell'intelligenza artificiale, può altrettanto essere riferita al rapporto uomo-macchina.

La Strategia nazionale per la sicurezza informatica del Paese considera la crescita della sensibilità collettiva verso il digitale e i suoi rischi un fattore abilitante, un ingrediente indispensabile per la sua stessa piena e compiuta attuazione. L'Agenzia – che è al centro di questo processo attuativo – ha diretto i suoi sforzi ad incoraggiare e promuovere l'affermazione di una cultura cibernetica più avanzata intessendo una rete di vivaci e strutturati rapporti con le Università e il mondo accademico in generale. Uno sforzo che serve a stimolare la nascita di corsi curriculari e post-curriculari, di master e percorsi formativi che abbiano il loro fuoco anche nello studio di sistemi difensivi avanzati della superficie digitale esposta.

La cultura, per questo aspetto, si pone in relazione alla crescita di una nuova leva informatica nazionale, cioè di una forza in grado di esprimere capacità e competenze pregiate nella sicurezza informatica.

Allo stesso tempo, l'attenzione va rivolta ad un altro documento di valenza strategica, l'Agenda di ricerca e innovazione per la cybersicurezza, che stiamo aggiornando proprio in questi giorni, insieme al Ministero dell'Università e della Ricerca. Vi deve essere, infatti, un circuito che metta in connessione gli obiettivi di avanzamento tecnologico, perseguiti in una direzione volta a cogliere margini sempre più ampi e consistenti di autonomia strategica, con i contenuti e le finalità delle proposte formative, in modo che l'intero ciclo di questo processo, che combina formazione e lavoro, risponda a una coerenza sistemica, rispettando insieme l'indipendenza della ricerca e le complesse esigenze del mercato e della produzione.

Alla luce di questo criterio che guarda al merito in una prospettiva positivamente fattuale, il finanziamento di borse di dottorato nel settore della cybersicurezza, promosso dall'Agenzia attraverso bandi annuali che hanno interessato più di 200 Università e istituti universitari, ha privilegiato gli studi più interessanti nel settore del quantum computing e dell'Intelligenza Artificiale; e ciò non per un vieto

omaggio alla crescente attenzione che da qualche tempo si è formata attorno a quest'ultima tecnologia. Sappiamo come essa rappresenti un'arma potente non solo di offesa ma anche di difesa dalla minaccia cibernetica: è il suo profilo blu, che si oppone al profilo red, quello rosso con cui identifichiamo gli aggressori informatici.

Il fattore H, il fattore umano – ed è questo elemento a riportarci alla centralità della questione della cultura della sicurezza – rimane ancora uno dei principali punti di debolezza nella difesa informatica.

L'appello ad un uso dei mezzi digitali responsabilmente attento, avveduto e non superficiale, si rivolge innanzitutto ad un vasto pubblico in una logica necessariamente generalista. Ne è un esempio, tra i più felici, la campagna di sensibilizzazione "I Navigati", promossa dalle istituzioni di tutela del mercato bancario e finanziario, a cui ACN ha dato, e continuerà a dare, un fattivo contributo. Il messaggio, efficacemente veicolato attraverso una serie di short-stories, è indirizzato non solo ad ammonire i consumatori dal rischio del phishing, la pratica fraudolenta più comune, ma anche a riconoscerne i suoi principali tratti distintivi, con riguardo soprattutto alle modalità di aggiramento della vittima.

Ancora più significativa, per le sue notevoli potenzialità penetrative in un'ampia parte del tessuto sociale, quella più vulnerabile, potrà rivelarsi l'iniziativa intesa a promuovere nei vari cicli scolastici un'attività didattica per l'educazione alla sicurezza digitale come nuova espressione del principio di formazione, partecipativa e responsabile, del cittadino. Credo sia importante sottolineare come la collaborazione sancita a dicembre scorso tra il Ministero dell'istruzione e del merito e l'Agenzia pe la cybersicurezza nazionale non guardi a possibili sbocchi occupazionali o professionali, prefiggendosi un compito forse più alto e ambizioso. Nel rivolgersi a un cittadino in formazione, intende infatti stimolarne un interesse propositivo verso il digitale, una curiosità conoscitiva aperta e dinamica, che aiuti il giovane anche a comprendere i rischi dell'isolamento autoriflesso e della sostituzione dei rapporti reali con quelli virtuali.

La formazione delle competenze digitali acquista un rilievo straordinariamente importante nel panorama attuale e negli scenari futuri che già si distinguono chiaramente. La natura incrementale ed evolutiva della minaccia richiede che i gangli vitali del Paese rispondano adeguatamente alla crescente domanda di sicurezza

informatica. Il dominio digitale per sua stessa natura presenta rischi di propagazione sistemica degli attacchi più severi, provenienti da attori criminali assai temibili per il livello di sofisticata capacità raggiunta.

Accanto alla necessità di una educazione al digitale capillare, riversata nei vari strati sociali, convive e si afferma in maniera prepotente l'esigenza che i settori sensibili e più esposti del Paese migliorino in fretta il loro grado di resilienza.

L'avvento della questione della sicurezza cibernetica, a livello europeo e globale, porta con sé problemi non facilmente affrontabili di skilling e di reskilling del capitale umano, nelle infrastrutture critiche e nei diversi settori produttivi, e anche nella stessa pubblica amministrazione. L'impatto riguarda i soggetti primari di questo vasto universo e tutte le altre realtà della lunga filiera dei fornitori di prodotti e servizi digitali, per il necessario prolungamento alla supply chain degli standard più elevati di sicurezza informatica.

La sfida ora più urgente è educare all'uso razionale e corretto degli strumenti di intelligenza artificiale, anche per proteggerci dal rischio di un'incauta cessione del nostro patrimonio informativo, visto che i dati che immettiamo nei modelli linguistici open source possono migrare verso piattaforme cloud sottratte al nostro controllo e alla nostra giurisdizione. Il recente intervento di promozione della sicurezza informatica nelle pubbliche amministrazioni italiane, frutto di un'iniziativa della Presidenza del Consiglio, condivisa dall'Agenzia con i Dipartimenti della Funzione Pubblica e dell'Editoria, guarda anche ai pericoli connessi all'utilizzo irriflessivo o eccessivamente disinvolto degli strumenti di intelligenza artificiale, proponendo a migliaia di operatori e dirigenti del settore pubblico un vademecum di buone pratiche cibernetiche, semplici e comprensibili.

Ci avviamo a ritmi sostenuti verso l'affermazione dell'intelligenza artificiale agentica. Macchine robotiche che affiancano l'uomo nelle più disparate attività, sollevandolo da compiti faticosi e ripetitivi. Si apre una nuova frontiera che implica, come accennavo all'inizio, un inedito e complesso tema, di tipo etico e scientifico, nella formazione delle competenze, destinato a giocare un ruolo fondamentale nella cultura cibernetica all'interno del rapporto con la post-modernità.

2. Intervista al Procuratore Nazionale Antimafia e Antiterrorismo Giovanni Melillo

1) Come si è evoluto il suo ruolo alla luce della progressiva digitalizzazione delle attività terroristiche e della criminalità organizzata? E quali sono le principali modalità operative di con cui tali fenomeni si manifestano nel contesto cyber?

Obiettivamente, l'attribuzione al PNA del ruolo di coordinamento delle indagini in materia di sicurezza cibernetica è avvenuta alla luce dell'emersione di gravissimi illeciti, correlati allo sfruttamento abusivo di banche dati strategiche, che rivelavano la necessità di potenziare le capacità di analisi e di coerente indirizzo delle investigazioni. Del resto, la stessa distribuzione delle banche dati di interesse strategico sul territorio nazionale fa sì che spesso diversi uffici giudiziari si trovino ad indagare su condotte di reato assimilabili e attribuibili agli stessi autori. Sarebbe inimmaginabile, se non a costo di una insostenibile dispersione di mezzi investigativi e della frustrazione di ogni possibile sforzo, che le diverse Procure coinvolte nelle indagini operino senza mettere in comune conoscenze e metodi investigativi. Da questo punto di vista, il nuovo ruolo del PNA consente di mettere a disposizione degli uffici giudiziari anche il valore aggiunto di una banca dati nazionale alimentata, oltre che dalle acquisizioni investigative riferite a delitti di mafia e di terrorismo, dalle indagini in materia di cybercrime, integrandosi per tale un patrimonio informativo rilevante anche per la lettura dei più tradizionali fenomeni criminosi.

Allo stesso modo, deve rilevarsi che la funzione di coordinamento investigativo nazionale sostiene i bisogni di estensione e rafforzamento dell'effettività della cooperazione giudiziaria internazionale. Quando una minaccia informatica colpisce diversi Paesi diventa fondamentale avviare forme di cooperazione fra Stati essenziali alla ricostruzione della natura, delle modalità e della portata degli attacchi e, anche in questo contesto, sarebbe defatigante d'inutile che le Procure italiane interessate si presentassero in ordina sparso e avanzando richieste di cooperazione non coordinate. In generale, non vi è nulla di peggio per le sorti della cooperazione internazionale del trasferimento sul piano del rapporto con gli altri Stati del peso di un insufficiente

coordinamento interno. Diventa allora centrale il ruolo di un ufficio nazionale che abbia funzione di raccordo e coordinamento, favorendo la scambio di informazioni e la collaborazione. In questo ruolo specifico l'esperienza ultra trentennale della DNA, che proprio questo compito svolge strutturalmente, diventa strategica. È quindi il carattere diffusivo e transnazionale di queste forme di criminalità ad aver favorito una evoluzione del ruolo della DNA, rendendo l'attività di coordinamento quintessenziale rispetto a quasi tutte le indagini in questa materia. Si tratta di tendenze che vanno affermandosi, con gli opportuni adattamenti, anche in altri Stati, come in Francia, ad esempio, dove la tradizionale pluralità dei centri decisionali giudiziari è stata attenuata dall'istituzione di uffici di coordinamento nazionale in materia di terrorismo dapprima e poi di cybercrime e, da ultimo, di criminalità organizzata, secondo un ordine di priorità temperale che naturalmente riflette la diversità di quell'esperienza.

2) Quali sono, allo stato attuale, le forme operative di coordinamento tra DNA e ACN a seguito dell'estensione delle funzioni di impulso del Procuratore Nazionale Antimafia e Antiterrorismo, determinata dall'inserimento del comma 4-bis nell'art.371-bis c.p.p.?

Le condotte criminali che colpiscono i sistemi informatici e le banche dati di interesse nevralgico pongono simultaneamente problemi di pressoché immediato ripristino delle funzioni informatiche interrotte, talvolta addirittura vitali per le istituzioni ed i cittadini e, al contempo problemi di tipo investigativo, atteso che l'analisi forense dei sistemi violati può rivelare elementi preziosi per l'avvio delle indagini e per l'identificazione dei responsabili. Ciò rende fondamentale il coordinamento delle attività di resilienza con quelle propriamente investigative. Era importante, quindi, stabilire protocolli condivisi che consentissero, senza interferenza reciproca, la simultanea operatività sullo stesso "teatro del crimine" di ACN, deputata alla resilienza, e della polizia postale, coordinata dalle Procure competenti. Per questo è stato redatto e sottoscritto, il 7 agosto 2024, un accordo tra DNA, ACN e Polizia Postale che struttura un flusso informativo continuo tra queste tre istituzioni, proprio per consentire una virtuosa interoperatività nello stesso ambiente informatico colpito

dall'azione criminale. Da quando l'accordo è stato definito gli scambi informativi sono pressoché quotidiani, perché molti sono i contesti colpiti dalle cyber minacce, e le operazioni sul campo si svolgono con maggiore efficienza e più proficui risultati. In generale, in questa materia, il bisogno di rafforzamento della cooperazione istituzionale diviene centrale, sia nella prospettiva della prevenzione che in quella del contenimento degli effetti degli attacchi cyber. Lo dimostra anche la scelta di aprire, quando ritenuto necessario e opportuno, l'attività del Comitato Interministeriale per la sicurezza della Repubblica alla partecipazione di ACN, della Banca d'Italia e della DNA.

3) Ritiene che gli strumenti tipici del contrasto alla criminalità organizzata siano efficaci e adeguatamente trasferibili al cybercrime o pensa che siano necessari nuovi strumenti investigativi ad hoc? Nel caso, quali innovazioni riterrebbe prioritarie?

Gli strumenti di contrasto si stanno evolvendo velocemente per tenere il passo dell'incessante incremento delle competenze cibernetica dei soggetti e dei gruppi criminali. Ma, naturalmente, su questo terreno il rischio di rapida consunzione degli strumenti normativi è assai più concreto ed evidente. Un passaggio importante si è avuto con la recente introduzione, con la L. 9 ottobre 2023, n. 137, dell'undercover informatico per le indagini in materia di cybercrime e terrorismo in rete, ciò che di per sé consente di affacciarsi sugli ancora largamente inesplorati territori dell'utilizzo dell'IA in indagini che hanno riguardo a delitti per la commissione dei quali il ricorso a tecniche di IA è ormai la regola. Tuttavia, affinché gli strumenti investigativi siano veramente efficaci è necessario che siano adottati dai legislatori nazionali nella cornice di norme e trattati internazionali, per far sì che i Paesi chiamati a collaborare nel contrasto ai fenomeni più pericolosi e dilaganti siano dotati di strumenti omogenei e disciplinati in modo conformate. Infatti, è sempre più frequente lo svolgimento di parte delle attività di indagine all'estero ed avvalendosi della cooperazione giudiziarie e di polizia. Solo una disciplina omogenea può, quindi, consentire, di svolgere questi atti all'estero con un sicuro valore probatorio nel sistema penale nazionale ove dovranno spiegare i loro effetti in sede di giudizio. Purtroppo, assistiamo però anche a contro spinte e istanze di arretramento degli strumenti investigativi già disciplinati dal nostro

codice. È quanto sta avvenendo attraverso l'introduzione di un nuovo articolo 254-ter del c.p.p., oggetto di ampio dibattito in Parlamento. Questa riforma renderebbe estremamente complicato e farraginoso acquisire, con valenza di prova, i contenuti comunicativi rinvenibili nei server e nei dispositivi informatici. Non è necessario spiegare come questi contenuti siano di vitale importanza per fornire la prova in giudizio delle responsabilità penali, non solo per i reati cyber ma pressoché per tutti i reati. Conseguentemente, una forte limitazione del loro utilizzo, che si prospetta nei lavori parlamentari, produrrebbe un arretramento nell'efficacia delle indagini e del contrasto. Ma non è importante soltanto evitare pericolosi arretramenti dell'efficacia degli strumenti investigativi. L'esperienza dimostra anche la necessità di integrare i modelli di incriminazione disponibili, attraverso nuove fattispecie. Mi riferisco, in particolare, alla necessità di introdurre un delitto che potremmo definire di "traffico organizzato di dati personali", essenziale per cogliere la complessità di reti criminali dalla struttura eterogenea, ma rette dalla consapevole convergenza verso obiettivi comuni, quali l'acquisizione abusiva di dati personali e lo sfruttamento illecito della loro conoscenza e pratica disponibilità, per finalità di illecito condizionamento della vita economica e delle istituzioni democratiche. Si tratta di scenari che le indagini restituiscono già con chiarezza sufficiente a dimostrare l'urgenza dell'adeguamento della trama normativa.

4) L'ordinamento italiano, con la legge n.137 del 2023, ha esteso l'impiego delle operazioni sotto copertura ai reati informatici. Considera tale estensione sufficiente oppure, alla luce del particolare ambito di applicazione, ritiene necessario un ulteriore intervento normativo che introduca modalità operative apposite per il cyberspazio?

L'undercover informatico è lo strumento più innovativo sino ad ora introdotto. Le Procure Distrettuali ne stanno sperimentando l'utilizzo e la DNA ne sta analizzando, alla luce dell'esperienza del coordinamento investigativo, anche le complesse implicazioni tecnico-giuridiche. Come anticipavo già è di fronte a noi la prossima sfida. L'IA costituisce un formidabile strumento utilizzato ampiamente dalle

organizzazioni criminali. Si calcola che, grazie all'abbinamento tra IA e computistica quantistica, entro pochi anni non ci sarà una password o un sistema di crittografia che, per quanto complessi, non potranno essere violati da azioni criminali dotate delle adeguate competenze. Fortunatamente, l'AI è suscettibile anche di impieghi sul fronte delle indagini e del contrasto. Effettuare il controllo di sicurezza dei sistemi informatici, individuare immediatamente gli indici di compromissione rivelatori di sistemi di cyber spionaggio, analizzare e decrittare i programmi malevoli, processare rapidamente masse enorme di dati per selezionare quelli di rilievo investigativo, sono tutte attività che potranno essere agevolate dall'IA utilizzata dagli investigatori. Anche in questo ambito, tuttavia, è necessario dotarsi di una base normativa nazionale e sovranazionale che ne regoli coerentemente l'impiego, conferendo ad esso pieno valore di prova e realisticamente praticabili possibilità di reciproco riconoscimento fra i diversi ordinamenti. Allo stesso modo, sarà importante, sul piano tecnico, dotarsi di sistemi di IA investigativa proprietari e istruiti in modo opportuno ed affidabile. Non sono cose lontane nel tempo, sono temi urgenti già ora se non vogliamo farci sopravanzare dalle competenze di strutture criminali sempre più sofisticate e complesse, anche perché capaci di agire nel teatro dei conflitti ibridi.

5) Sul piano internazionale è fondamentale la cooperazione tra Stati per contrastare efficacemente i reati informatici, data la loro particolare pervasività e la difficoltà di identificare gli autori. Come immagina possano funzionare le operazioni undercover nel caso di mancata cooperazione, in particolare quando gli attacchi informatici provengono da paesi "ostili" o non collaborativi?

Il regime attuale dell'undercover informatico consente di operare anche fuori dalla giurisdizione nazionale ma soltanto nell'ambito di procedure di cooperazione giudiziaria. Cioè mediante la previa informazione e cooperazione dello Stato estero nell'ambito del quale l'undercover andrà ad operare. Questo è un limite al suo utilizzo rispetto a quei Paesi non collaborativo o, addirittura ostili. Rispetto ad essi i sovra ordinati principi internazionali, che riconoscono l'inviolabilità della sovranità degli Stati, pongono un limite invalicabile se si vogliono rispettare gli impegni internazionali

assunti dall'Italia la cui doverosa osservanza è presidiata dall'art. 10 della Costituzione. Possiamo dire quindi che attualmente il contrasto al crimine informatico e soprattutto alle minacce che provengono dall'estero diventa ineffettivo quando gli attori criminali trovano riparo in Stati non collaborativi o sono agenti di Stati ostili. Per questo è indispensabile non deflettere nello sforzo, da esercitare a livello internazionale da parte delle autorità di Governo e Eurounitarie, finalizzato a rendere sempre più ampio e resistente il tessuto del diritto internazionale penale e della cooperazione giudiziario che esso consente di realizzare.

6) Una delle problematiche maggiormente rilevanti riguarda il disallineamento tra la capacità degli organi statali di prevenire e contrastare il fenomeno dei reati informatici e la rapidità con cui questi possono provocare danni, soprattutto alle infrastrutture critiche. Dal suo punto di vista come può essere colmato questo divario affinché lo Stato italiano possa avere un vantaggio operativo nel contrasto al cybercrime? E, più in generale, quali strumenti e forme di cooperazione internazionale ritiene siano necessari per consentire al sistema internazionali di stare al passo con l'evoluzione delle minacce cibernetiche?

Come ho già sottolineato, la cooperazione internazionale, giudiziaria e di polizia, è lo strumento più efficace per contrastare le minacce cibernetiche ed insieme tenere in piedi la stessa tenuta dello Stato di diritto e delle garanzie, affiancandosi, nel rispetto dei ruoli e delle diverse finalità istituzionali, all'azione di tutela della Sicurezza della Repubblica propria degli organismi chiamati in causa dalla frequente proiezione degli attacchi cibernetici verso gli interessi strategici del Paese. La cooperazione giudiziaria richiede, tuttavia, in questa materia, una continua immissione di dosi aggiuntive di efficacia e tempestività dell'azione del pubblico ministero, ma anche di capacità di operare, con lungimiranza ed essenziale rigore metodologico, in scenari sempre più complessi e delicati. In tale direzione si muove certamente la costituzione di squadre investigative comuni a carattere permanente. Lo strumento è stato, anche di recente, fortemente implementato dalla DNA attraverso la sottoscrizione di numerosi accordi bilaterali nella cornice della Convenzione di Palermo per il contrasto al crimine

organizzato. La costituzione di squadre investigative permanenti consente di accelerare le procedure di cooperazione bypassando la fase, spesso lunga ed onerosa, necessaria per attivarne la costituzione per la singola specifica indagine. Inoltre, la stabilità dello strumento facilita la mutua fiducia, la conoscenza dei reciproci sistemi normativi, la continua condivisione delle best practices investigative e degli avanzamenti tecnologici. Certamente l'affermazione di tali strumenti per il contrasto al cyber crime potrà costituire la base per un salto in avanti nel contrasto a questo fenomeno come già sta avvenendo nel settore del narcotraffico globale.

3. Intervista al Direttore del servizio Polizia Postale e per la Sicurezza Cibernetica Ivano Gabrielli.

1) Come descriverebbe l'esperienza finora maturata dalla Polizia Postale nella prevenzione e nel contrasto dei reati informatici anche alla luce delle novità introdotte della L. 90/2024? Inoltre, come si instaura il coordinamento tra Forze dell'ordine, Magistratura, Presidenza del Consiglio e ACN nel fronteggiare le minacce cibernetiche?

La Polizia Postale, di fatto dal 1998, individuata quale Organo del Ministero dell'Interno per la sicurezza e la regolarità delle comunicazioni, svolge le funzioni dell'Autorità Nazionale di Pubblica Sicurezza proiettata nel dominio cibernetico.

A tali funzioni di prevenzione si sono associate quelle specifiche di contrasto alla minaccia criminale cibernetica di matrice comune, organizzata e terroristica affidatale dal D.L.144/2005 che, in sede di conversione, all'Art.7 bis ha reso tale missione possibile: all'epoca con l'istituzione del CNAIPIC che oggi coordina la rete dei Nuclei Operativi di Sicurezza Cibernetica – N.O.S.C. presenti nei 18 Centri Operativi della Polizia Postale – C.O.S.C.

I successivi interventi normativi, quale il D.Lgs. 18 maggio 2018 n. 65 – Attuazione Direttiva NIS, il D.L. n. 105/2019 sul Perimetro di Sicurezza Nazionale Cibernetica, il D.L. 82/ 2021, istitutivo dell'Agenzia per la Cybersicurezza Nazionale-ACN e infine il D. Legs. 138/2024 (attuazione della Direttiva NIS 2) riconoscono alla Polizia Postale un ruolo centrale nella complessa Architettura Nazionale di Sicurezza

Cibernetica, delineata nel tempo in virtù anche di diversi DPCM (DPCM 24 gennaio 2013 – Decreto Monti e DPCM 17 febbraio 2017 – Decreto Gentiloni), che di volta in volta hanno completato la normativa di rango primario.

Per sostenere il necessario sforzo organizzativo richiesto da tale ruolo centrale nell'Architettura Nazionale di Sicurezza Cibernetica, la Polizia Postale ha dovuto riorganizzare i propri assetti centrali e territoriali, avviando quindi politiche specifiche di formazione del personale e di aggiornamento delle dotazioni tecnologiche.

La legge 90/2024 ha di fatto completato tale percorso evolutivo costruendo il raccordo inter-istituzionale tra ACN, Polizia Postale - Organo del Ministero dell'Interno per la sicurezza e la regolarità delle comunicazioni e Autorità Giudiziaria, quest'ultimo reso possibile dall'attività di coordinamento e di impulso attribuito dalla L. 137/2023 alla Procura Nazionale Antimafia e Antiterrorismo. L'attuale sistema delinea il flusso informativo tra ACN, DNAA e Servizio Polizia Postale anche in senso ascendente, prevedendo un ruolo attivo delle Procure territoriali che, in caso di attacco informatico, tenuto conto delle esigenze di intervento a garanzia della resilienza dei sistemi critici, devono informare ACN e garantire altresì il raccordo informativo con l'Organo del Ministero dell'Interno per la sicurezza delle comunicazioni.

A tale innovativo sistema di condivisione, che di fatto definisce il concorso dei tre soggetti sopra citati nel garantire la sicurezza nazionale cibernetica (è prevista la partecipazione del Procuratore Nazionale Antimafia Antiterrorismo alle riunioni del Comitato Interministeriale per la sicurezza della Repubblica – CISR) deve necessariamente aggiungersi quanto previsto dall'articolo 118 bis del C.P.P. "Richiesta di copie di atti e di informazioni da parte del Presidente del Consiglio dei ministri" il quale, proprio in materia di sicurezza cibernetica, ritrova rinnovata importanza e frequente utilizzo.

2) L'ordinamento italiano, con la legge n.137 del 2023, ha esteso l'impiego delle operazioni sotto copertura ai reati informatici. Considera tale estensione sufficiente oppure, alla luce del particolare ambito di applicazione, ritiene necessario un ulteriore intervento normativo che introduca modalità operative apposite per il cyberspazio?

La Legge nr. 137 del 2023 ha modificato l'art. 9 della Legge nr. 146 del 2006, andando ad introdurre alla lettera b) del primo comma il nuovo paragrafo b-ter) che disciplina le attività undercover previste per gli Ufficiali di Polizia Giudiziaria della Polizia Postale.

La norma estende quanto già in precedenza previsto, in materia di contrasto alla pedopornografia online ed in materia di contrasto agli attacchi contro le infrastrutture critiche informatizzate del Paese, superando il modello dell'undercover basato sulla costruzione di un'identità fittizia da poter infiltrare all'interno di contesti criminali virtuali, prevedendosi attività proattive quali, l'introduzione in un sistema informatico, il danneggiamento ovvero l'alterazione, sino a prevedere l'assunzione del controllo del sistema stesso.

Si tratta, in buona sostanza, della possibilità di svolgere veri e propri attacchi informatici con l'esclusiva finalità di acquisire elementi di prova. Tale importante innovazione tuttavia trova un limite sia nella possibilità di svolgere attività su sistemi allocati all'estero, sia con riferimento all'art. 329 del c.p.p. in virtù del quale con la messa a disposizione delle risultanze tecniche necessariamente si finisce nel dover rivelare quali siano state le tecnologie impiegate per l'attività undercover, quindi rendendo pubbliche informazioni a scapito del possibile successivo utilizzo di tale prezioso know how tecnologico.

Pertanto, potrebbe essere utile riflettere su un intervento normativo che, tenuto conto del bilanciamento dei diritti, possa garantire il contradditorio tra le parti e, allo stesso tempo, la riservatezza delle informazioni circa le tecnologie utilizzate nel corso delle attività undercover

3) Dal punto di vista operativo, come si struttura un'operazione sotto copertura in ambiente digitale e quali sono le principali criticità che emergono quando si agisce nel cyberspazio?

Dal punto di vista operativo, una volta autorizzata l'attività undercover, viene avviata una fase di studio e approfondimento tecnico necessario all'individuazione delle metodologie utili all'acquisizione degli elementi probatori prefissati.

L'attività tecnica avviata deve necessariamente essere rendicontata, per tale motivo è assolutamente necessario individuare metodologie utili alla migliore rappresentazione delle attività tecniche complesse.

Diverse sono le criticità, tra le quali l'esecuzione dell'attività sotto copertura su sistemi informatici dei quali si conosce poco, anche con riferimento alla loro collocazione geografica. Tale ultima considerazione diventa assume carattere primario, considerati i limiti giurisdizionali.

Altro aspetto di non poco conto è la necessità di tutelare le tecnologie e il know how tecnico a fronte di obblighi di pubblicità. A tal proposito sarebbe utile una norma che in qualche modo, rispettando i principi del giusto processo, preveda momenti di riservatezza a tutela di tecnologie e soluzioni che altrimenti sarebb88ero non più utilizzabili per l'attività investigativa.

4) Sul piano internazionale, risulta fondamentale la cooperazione tra Stati per contrastare efficacemente i reati informatici, data la loro particolare pervasività e difficoltà nell'indentificare gli autori. Come ritiene che le operazioni undercover possano operare nel caso di mancata cooperazione, in particolare quando gli attacchi informatici provengono da paesi "ostili" o non collaborativi?

Il paradosso dell'indagine cibernetica risiede nel fatto che l'attività investigativa si muove su un fronte che vede la totale mancanza di confini, utili per il miglior presidio dei diritti: i crimini informatici possono essere espletati direttamente da attori ostili, anonimi, che sfruttano risorse distribuite.

A fronte, ad esempio, di un attacco informatico verso infrastrutture critiche informatizzate potremmo trovarci di fronte a una interazione con una risorsa ostile che, mentre attiva un canale diretto per sottrarre materiale informatico, non può essere a sua volta attinta per comprenderne la portata dell'attività malevola ed eventualmente individuarne i responsabili. Meglio ragionando però si potrebbe cominciare a considerare il web come un dominio dai confini dinamici.

Di fatto, già oggi, un sistema informatico nazionale viene considerato tale anche con riferimento agli ambenti cloud nella propria disponibilità, ancorché ubicati all'estero.

Di tal guisa potrebbe essere concepibile considerare il sistema attaccante e il sistema attaccato come un'unica entità legata da un canale di comunicazione, un collegamento abilitato benché per scopi criminale. Potersi muovere quindi a partire dal sistema nazionale target, per arrivare alla risorsa da cui ha origine l'attacco, potrebbe considerarsi quindi legittimo proprio in virtù del fatto che la relazione tecnica che lega le due identità ne determina una derivata unica struttura telematica, pertanto legittimamente esplorabile nel corso di un'attività sotto copertura.

5) Ritiene che le task force internazionali, come Europol EC3 o la J-CAT, risultino proficue per un contrasto efficace e celere al cybercrime oppure è auspicabile un ulteriore rafforzamento della cooperazione internazionale per affrontare il fenomeno?

La Cooperazione Internazionale è fondamentale per il contrasto alla criminalità informatica, ma sconta un limite temporale che può essere ridotto mediante agili forme di cooperazione giudiziaria.

Esistono tuttavia interessanti modelli di cooperazione Internazionale come Europol, EC3 e lo J-Cat che si avvantaggiano della permanente presenza di canali di cooperazione.

Proprio la permanenza, ovvero il collegamento continuo tra rappresentanti accreditati, situazione che consente in tempo reale l'attivazione degli organi collaterali di Polizia, può essere la soluzione più rapida per le attività di preservazione e di acquisizione degli elementi utili alle indagini di crimini informatici.

6) Una delle problematiche maggiormente rilevanti riguarda il disallineamento tra la capacità degli organi statali di prevenire e contrastare il fenomeno dei reati informatici e la rapidità con cui questi possono provocare danni, soprattutto alle infrastrutture critiche. Dal suo punto di vista come può essere colmato questo divario affinché lo Stato italiano possa avere un vantaggio operativo nel contrasto al cybercrime? E, più in generale, quali strumenti e quali forme di cooperazione internazionale ritiene siano necessari per consentire al sistema internazionali di stare al passo con l'evoluzione delle minacce cibernetiche?

La minaccia cibernetica può essere considerata il prototipo della minaccia ibrida fortemente connotata dagli elementi di asimmetria.

Ciò significa che permane un'ontologica differenza del livello dello sforzo di chi è chiamato a presidiare i sistemi informatici rispetto a chi è tenuto a difenderli.

Per tale motivo, l'impegno statuale in termini di prevenzione e contrasto a tale tipologia di reati non può prescindere da significativi momenti di partenariato, meglio di corresponsabilità, tra strutture pubbliche e private di sicurezza cibernetica.

Difatti tale postura, a bene vedere, è richiamata da tutte le normative di settore nazionali ed internazionali. Si tratta infatti più che della privatizzazione delle funzioni di Pubblica Sicurezza, della riconosciuta funzione Pubblica dei presidi di sicurezza che doverosamente le infrastrutture critiche più sensibili debbono organizzare al loro interno, con precisi momenti di responsabilità in capo alle figure apicali dirigenziali.

Le normative nazionali debbono favorire tale processo di integrazione tra le funzioni di sicurezza Pubblica e privata: solo in questo modo è possibile attuare il più ampio presidio del perimetro di sicurezza cibernetica, attraverso l'organizzazione di una attività di prevenzione e risposta più rapida ai fenomeni criminali.