RIVISTA TRIMESTRALE

DELLA SCUOLA DI PERFEZIONAMENTO PER LE FORZE DI POLIZIA

Periodico trimestrale
di Dottrina, Legislazione e Giurisprudenza

Anno 2021, n. 4

RIVISTA TRIMESTRALE

DELLA SCUOLA DI PERFEZIONAMENTO PER LE FORZE DI POLIZIA

Periodico trimestrale
di Dottrina, Legislazione e Giurisprudenza

Anno 2021, n. 4

SOMMARIO

Editoriale

a cura del Gen. D. CC Giuseppe La Gala
Direttore della Scuola di Perfezionamento per le Forze di Polizia
e Direttore responsabile della Rivista trimestrale dell'Istituto

Il Gen. D. CC Giuseppe La Gala

In questo numero della Rivista trimestrale e dell'annesso Quaderno vengono pubblicati alcuni contributi scientifici realizzati dai frequentatori del 36° corso di Alta formazione (che si è concluso lo scorso mese di giugno), a testimoniare l'intensa attività di produzione scientifica della Scuola, sempre attenta a cogliere l'evoluzione del panorama normativo con riferimento a temi "caldi" nel dibattito pubblico e di primario interesse per le forze di polizia.

La prima parte di questo numero ("*Interventi*") è dedicata al contributo del Dirigente Aggiunto della Polizia penitenziaria Maria Luisa Tattoli, dal titolo "*La sfida della cybersecurity nel coordinamento interforze e nella cooperazione internazionale*". Il saggio verte sull'attualissimo tema della *cybersecurity*, il quale, data la crescente e sempre più significativa penetrazione delle tecnologie dell'informazione e delle comunicazioni in tutte le funzioni della società moderna, ha gradualmente acquisito un'importanza strategica ai fini della sicurezza nazionale e della crescita economica degli Stati. Il lavoro approfondisce le principali tematiche che riguardano la difesa e la sicurezza dello spazio cibernetico: le caratteristiche del dominio cibernetico e l'evoluzione della minaccia *cyber* nelle sue diverse tipologie; la normativa nazionale e internazionale e le strategie politiche in tema di *cybersecurity*; l'architettura istituzionale preposta alla protezione cibernetica nazionale, costituita dai soggetti e dai meccanismi di prevenzione dei rischi e di gestione di crisi cibernetiche, nonché gli organismi di *cyber investigation* delle forze di polizia e del settore Difesa, in un'ottica di coordinamento interforze e di cooperazione internazionale. Vengono infine trattati alcuni specifici ambiti particolarmente sensibili alla minaccia cibernetica, con particolare riferimento al processo di trasformazione digitale della pubblica amministrazione – obiettivo previsto come vincolo di progetto nel *Piano Nazionale di Ripresa e Resilienza* (PNRR) – e alla disciplina del c.d. *golden po-*

wer e l'ampliamento della sua applicazione alle reti 5G nell'assetto degli equilibri globali.

Nella Parte II (*Articoli e Saggi*) riportiamo il contributo del Vice Questore della Polizia di Stato Carmelo Alba, dal titolo "*Criticità tra la presentazione dell'istanza di ammonimento, ai sensi dell'art. 8 legge 38/2009 e dell'art. 3 legge 119/2013, e l'obbligo di trasmissione da parte della polizia giudiziaria all'autorità giudiziaria degli atti relativi ai fatti esposti dalla vittima previsto dall'art. 1 della legge 69/2019*", che tratta del rapporto tra procedimento amministrativo (per l'adozione del provvedimento di ammonimento questorile) e procedimento penale (a carico dell'ammonito). L'autore, dopo un articolato inquadramento normativo sulle funzioni affidate al Questore nel nostro ordinamento (specificamente in materia di misure di prevenzione), che incidendo sugli spazi di libertà del cittadino ne sostanziano il ruolo quale autorità di p.s., si sofferma sulla disciplina degli istituti degli ammonimenti questorili introdotti dai decreti-legge n. 11 del 2009 e n. 93 del 2013, circoscrivendone gli spazi di operatività rispetto all'azione penale esercitata dall'autorità giudiziaria. Il lavoro successivamente si concentra sulle novità legislative recate dalla legge n. 69/2019 (in materia di tutela delle vittime di violenza domestica e di genere) e dalle modifiche da essa introdotte nell'art. 347 c.p.p., con riferimento all'obbligo della polizia giudiziaria di immediata trasmissione all'a.g. – anche in forma orale – delle notizie di reato relative a taluni specifici delitti per i quali è ammesso il parallelo istituto preventivo dell'ammonimento questorile.

Nella Parte III (*Voci dall'Aula*) è stato inserito il lavoro redatto dal Colonnello dell'Arma dei Carabinieri Vincenzo Pascale, che ha approfondito il tema de "*Il traffico di stupefacenti e armi on-line: strumenti e metodologie di indagine nel darkweb. Le chat cifrate*". Il lavoro è incentrato su una partizione della rete Internet nota come *deep web* (un sottoinsieme non accessibile attraverso gli ordinari strumenti di navigazione che raccoglie materiale informatico "non indicizzabile" che, secondo alcune stime, ammonterebbe al 96% circa del totale delle informazioni nell'intera rete) e, in particolare, sulla parte più profonda di tale mondo sommerso – conosciuta come *dark web* – che ospita attività illegali di ogni genere, trai quali spiccano i c.d. *black markets*, veri e propri negozi *on-line* "virtuali" in cui si vendono droghe, armi e servizi illeciti di ogni tipo. Il fenomeno dei black markets ha oggi raggiunto livelli preoccupanti e costituisce una delle sfide investigative più complesse, in quanto l'attività di contrasto necessita di strumenti tecnologici all'avanguardia e di un'operatività svliluppata con un approccio globale a un fenomeno che non ha confini. Dopo un'ampia disamina di tipo tecnico sugli strumenti informatici

necessari per accedere ed operare nei market illegali in totale anonimato, l'autore concentra la propria analisi su alcuni dei principali strumenti investigativi in uso (la raccolta di informazioni tramite le fonti aperte e i connessi sistemi di analisi; il "web profiling" e la riproduzione *off-line* dei market; le operazioni speciali antidroga in rete quali l'infiltrazione e l'acquisto simulato; gli strumenti di cooperazione internazionale giudiziaria e di polizia) ed offre alcuni spunti di miglioramento delle tecniche investigative, nella consapevolezza che il fenomeno dei traffici in rete di droga e armi richiede l'adozione di strumenti di contrasto ulteriori rispetto a quelli disponibili, oltre che l'affinamento delle metodologie d'indagine.

Nella parte IV (*Documenti, Normativa e Giurisprudenza di interesse*) viene proposto il contributo del Vice Questore della Polizia di Stato Francesca Romana Capaldo, dal titolo "*Hate crime* e *hate speech*: *strategia di prevenzione e di contrasto del Dipartimento della Pubblica Sicurezza*". Il lavoro è incentrato sul tema degli *hate crimes* ("crimini d'odio"), nella loro dimensione internazionale ed unionale, nonchè attraverso la tutela apprestata dall'ordinamento italiano nel contrastarli, recependo convenzioni e direttive internazionali. Particolare attenzione è stata prestata nel tratteggiare i contorni dell'odio *on-line*, soffermandosi sulle peculiarità e caratteristiche dello stesso, nonché sulla necessità di un'azione di contrasto sinergica, multidisciplinare, ma soprattutto condivisa a livello sovranazionale. Parte centrale del lavoro riveste l'analisi della struttura e delle funzioni dell'Osservatorio per la Sicurezza Contro gli Atti Discriminatori (Oscad), istituito presso la Direzione centrale della polizia criminale, che rappresenta un *unicum* nel panorama europeo ed internazionale, ma soprattutto l'impegno del sistema di *law enforcement* italiano per poter sviluppare una cultura del rispetto e della non discriminazione. Altro importante capitolo del saggio è dedicato all'esperienza americana dei movimenti suprematisti di estrema destra (tra cui Proud Boy, Qanon, Boogaloo, ecc.), che nell'ultimo anno hanno avuto un'enorme diffusione *on-line* e sono passati all'azione in numerose occasioni, mettendo in pericolo la stabilità delle istituzioni democratiche.

Annesso al presente numero della Rivista trimestrale viene pubblicato anche il Quaderno II/2021. I "Quaderni", tipicamente, ospitano monografie di ampie dimensioni che non trovano spazio in una delle parti che compongono la Rivista e, in questa edizione, si è deciso di inserire il lavoro redatto dal Colonnello della Guardia di finanza Ugo Liberatore, che ha approfondito il tema de "*Il ruolo della cooperazione transnazionale di polizia in europa nel settore della tutela degli interessi economico-finanziari dell'Unione*". Lo specifico argomento riveste particolare interesse in quanto è incentrato sulla necessità

inderogabile di un'armonizzazione tra i diversi sistemi giuridici presenti nei Paesi membri, al fine di evitare che lacune normative possano offrire al crimine organizzato l'opportunità di prosperare attraverso la commissione di gravi reati quali il traffico di droga, il riciclaggio di denaro e le diverse forme di frode e corruzione ai danni delle comuni risorse economiche. Il lavoro, in particolare, si concentra su uno degli obiettivi primari dell'Unione europea, ovvero la tutela degli interessi finanziari dell'Unione stessa contro le minacce al benessere sociale dei cittadini rappresentate dalla criminalità transnazionale. Dopo un'analisi preliminare delle politiche europee di spesa, l'autore approfondisce i fondamenti giuridici in materia di protezione degli interessi economico-finanziari comunitari e di lotta antifrode (sia a livello di Trattati istitutivi che di cooperazione intergovernativa), concentrando la propria attenzione sui vigenti strumenti di "cooperazione diretta" di polizia ed amministrativa ed evidenziando l'importante ruolo svolto dai principali organismi dell'Unione quali Europol, OLAF e gli *Anti Fraud Coordination Services* (AFCOS), di recente istituzione. Conclude il lavoro una puntuale analisi delle difformità delle azioni antifrode poste in essere dagli Stati membri e una ragionata previsione dei possibili scenari futuri – specie nei settori penale e della cooperazione amministrativa – proprio nell'ottica della necessaria (e non più procrastinabile) omogeneizzazione di tali azioni.

Parte I

Interventi

La sfida della *cybersecurity* nel coordinamento interforze e nella cooperazione internazionale

di Maria Luisa Tattoli*

Abstract

La pandemia Covid-19, intervenuta nel mese di febbraio del 2020 con la sua portata dirompente e planetaria, si è rivelata, nella sua drammatica incidenza nella nostra vita e in tutte le sue sfaccettature (lavorative, affettive, relazionali), un acceleratore di dinamiche e fenomeni latenti dinnanzi al quale gli attori pubblici, quelli privati e i cittadini si sono trovati completamente impreparati.

La prima pandemia dell'era digitale ha colpito le nostre "nuove" vulnerabilità, esponendoci, accanto ai primari rischi di natura sanitaria, alla minaccia cibernetica e a quella derivante dalla manipolazione delle informazioni, con rilevanti ricadute geopolitiche, economiche, giuridiche e soprattutto esistenziali. Ciò è accaduto simultaneamente in molti Paesi, rivelando fragilità a livello globale quanto a livello nazionale. L'emergenza sanitaria ha reso il panorama della minaccia più ampio, fluido e complesso.

In questo contesto, il tema della cybersecurity, a causa della crescente e sempre più significativa penetrazione delle tecnologie dell'informazione e delle comunicazioni in tutte le funzioni della società moderna, ha gradualmente acquisito un'importanza strategica, ai fini della sicurezza nazionale e della crescita economica degli Stati. Il dominio cibernetico, per la sua intrinseca vulnerabilità, per la sua pervasività, per l'impunità ch'esso concede, si è confermato un terreno d'elezione per attività criminali e a vario titolo ostili, con effetti che vanno ben oltre il dominio dal quale promanano e finiscono per avere un diretto impatto sulla sicurezza nazionale.

Anzitutto, il confine impostoci dal Covid-19 ha accresciuto la superficie d'attacco che esponiamo ad attori ostili: per continuare a lavorare ci colleghiamo di più alla rete, scambiamo più dati, e siamo dunque più esposti ai crimini informatici e alla penetrazione dei nostri sistemi da parte di altri attori malevoli. Siamo stati molto meno negli uffici, per le strade e nei negozi, e pro-

(*) Dirigente Aggiunto della Polizia penitenziaria, già frequentatrice del XXXVI corso di Alta formazione presso la Scuola di perfezionamento per le forze di polizia.

prio per questo siamo sempre connessi, ed è quindi su internet che ci vengono a colpire.

In secondo luogo, ci affidiamo sempre di più al dominio cibernetico per la nostra resilienza economica (lo smart working, l'e-commerce, ecc.) e sociale (social networks, insegnamento a distanza, ginnastica on-line, contatti interpersonali, ecc.). Eventuali interruzioni di servizio dunque "costano", a noi personalmente ed alla nostra società complessivamente, più caro, come dimostrano gli attacchi cibernetici ai danni degli ospedali, e, per converso, gli attacchi cibernetici divengono potenzialmente più vantaggiosi ed efficaci per chi li attua.

Infine, il dominio cibernetico ha ancora una volta dimostrato la sua intrinseca capacità di intervenire sui nostri processi cognitivi, di modellare la nostra comprensione del mondo, di consentire un'efficace manipolazione delle narrative e dunque di influenzare le nostre opinioni. Ecco perché le sfide legate alla dimensione cibernetica assumeranno una risoluta rilevanza geopolitica e geostrategica, determinata dalla sua peculiare trasversalità, in quanto potenziale canale di propagazione e amplificazione degli altri tipi di minaccia.

La dimensione cibernetica dei conflitti si è aggiunta, infatti, a quella tradizionale, rendendola maggiormente pericolosa ed estendendola anche al dominio cognitivo. In particolare, la celerità di sviluppo e diffusione di tecnologie innovative, sempre più pervasive, oltre alla possibilità di provocare il collasso dei sistemi e dei servizi essenziali, ha evidenziato le potenzialità destabilizzanti e di condizionamento delle opinioni pubbliche attraverso il "controllo" delle reti e dei dati. La capacità di gestione della grande mole di dati sarà uno dei parametri fondamentali per determinare il peso di ciascun attore in ambito economico e politico. L'importanza dei flussi di dati è tale che si parla di sovranità digitale ovvero della possibilità che soggetti, anche privati, in grado di intercettarli e renderli fruibili, possano riscrivere gli equilibri geostrategici ed imporre nuove regole.

Il cyberspace diventerà la futura arena della competitività dove verranno riscritte le nuove dinamiche e regole delle relazioni internazionali con equilibri che saranno ridefiniti secondo parametri nuovi. Ne consegue che la sicurezza cyber costituirà un settore strategico nevralgico per la protezione delle infrastrutture critiche istituzionali di un Paese, in cui il crescente livello della minaccia cibernetica impone di proseguire ed implementare un programma di potenziamento dei livelli di sicurezza.

Così come questa crisi sta facendo crescere un po' ovunque il tasso di digitalizzazione del Paese, matura inoltre la comune consapevolezza di quanto la nostra prosperità, libertà e stabilità siano intimamente connesse

alla sicurezza delle nostre reti. E siamo indotti forse a riconsiderare in chiave evolutiva la sempre più anacronistica antinomia "privacy contro sicurezza". Ad ogni emergenza nazionale, sia essa idro-geologica, sanitaria o cibernetica, vediamo chiaramente come la sicurezza sia il bene propedeutico al godimento di ogni libertà. L'attuale crisi pandemica ha dunque rinforzato il ruolo dello Stato, evidenziando la necessità di ripartire proprio dal concetto di sicurezza, intesa sia come "sicurezza partecipata", sia come "cultura della sicurezza". Questa più matura e diffusa consapevolezza è condizione necessaria per poter in futuro meglio mitigare e rispondere agli shock sistemici, ai "cigni neri" quale indubbiamente è questa pandemia. Ne va della tutela e della promozione dell'interesse nazionale, e, in definitiva, anche della nostra privacy individuale.

Infine, soffermandosi sul contesto internazionale in cui questa pandemia interviene, la crisi Covid-19 è un acceleratore anche della Great power competition in corso. L'ambiente securitario diviene più volatile ed il confronto, anche nelle narrative nazionali, è sempre più aspro. Lo vediamo anche nel dibattito internazionale e nei fenomeni globali che stanno emergendo. E ciò proprio mentre crescono le interdipendenze complesse e il nostro orizzonte strategico diviene più imprevedibile, anche per via della progressiva erosione dei tradizionali strumenti multilaterali, tra cui quelli per il controllo degli armamenti.

La cybersecurity, la gestione del rischio cyber, è questione primariamente culturale. È dunque necessario innestare un processo di conoscenza, di apprendimento, di formazione continua estesa a tutta la società civile, di progetti comuni, anche infrastrutturali – si pensi al 5G – partendo dalle comunità di valori e dall'Alleanza a cui apparteniamo. Pertanto, indipendentemente dal livello di profondità che si intende dare al termine cybersecurity, le variabili da prendere in considerazione non possono prescindere da tecnologia, organizzazione, processi, vigilanza e, soprattutto, formazione. Occorre sviluppare e poi trasmettere alla società approcci realmente condivisi, rifuggendo da visioni meramente transattive della nostra sicurezza.

* * *

The Covid-19 pandemic, which outbroke with disruptive force at global level in February 2020, has seriously affected all the aspects of our life (our work, families, friends, relations), and triggered some underlying dynamics and reactions which are difficult to be faced by public and private actors as well as by common people, who were unprepared to manage that kind of situation.

The first pandemic in the digital age affected our "new" weaknesses and exposed ouselves to the health risks as well as to the cyber threat and to the manipulation of information, with serious consequences at geopolitical, economic, legal level but, above all, at personal level. This situation arose at the same time in many countries, thus revealing a lot of weaknesses at global and national level. The health emergency brought about a more comprehensive, complex and wide-ranging threat scenario.

In this framework, the topic of cybersecurity has gradually acquired a strategic importance for domestic security as well as for the economic growth of the States, due to the increasing, fast and wide spreading of information and communication technologies in every fields of modern society. Cyberspace resulted to be a valuable tool for criminal groups as well as for hostile actors, because of its vulnerability, increasing pervasiveness and since it allows a large degree of anonymity. The relevant consequences overcome the cyber domain and directly affect domestic security.

First of all, the limitations imposed by Covid-19 pandemic contributed to increase the possibilities to be the attacked by hostile actors: in order to go on working we have to connect to the network on several occasions, we exchange more data and we are more exposed to cybercrimes as well as to the possibility that our servers could be hacked by other hostile actors. We have been far from our offices, shops and streets and just for this reason we have been often connected to internet where the hackers use to operate.

Moreover, we are increasingly connected to the cyber domain for economic reasons (smart working, e-commerce) as well as for social reasons (social networks, distance learning, on-line gym classes, interpersonal relations etc). Then, every possible network service outages seriously affect people and the whole society, as it is demonstrated by the cyber-attacks perpetrated against hospitals, although they are potentially profitable for their perpetrators.

Finally, cyberspace has showed, once again, its peculiarity which consists in affecting our cognitive processes, influencing our knowledge of reality, facilitating an efficient manipulation of information and then in shaping our opinions. This is why the challenges deriving from cyberspace will acquire a considerable geopolitical and geostrategical importance, affecting all the fields of society, since the cyber domain is a potential channel for the spreading and expansion of other types of threats.

As a matter of fact, in addition to the traditional clashes, cyberspace is characterized by a lot of conflicts and has become more dangerous, thus affecting also the cognitive domain. In particular, the rapid development and

spreading of innovative technologies, which are growingly pervasive, have underlined their power to destabilize and influence public opinion by means of the "control" over networks and data as well as their ability to cause the breakdown of essential systems and services. The skill to manage the huge amount of data will be one of the main issues to be analyzed in order to understand the impornance of any single actor in the economic and political fields. The importance of data flows is to be underlined, since it is related to the concept of digital sovereignty, that is to say the possibilty for actors, also private actors, to be able to hack computer systems, influence the geostrategical stability and impose new rules.

Cyberspace will become the future scenario in which conflicts take place, and it will be characterized by new dynamics and rules of international relations based on different criteria and guidelines. As a consequence, cybersecurity will represent a strategic sector for the protection of the main institutional infrastructures of every country, which will be obliged to develop and implement enhanced security plans due to the increasing level of cyber threat.

It is to be pointed out that the current critical situation brings about an increase in level of digitalization in our country, and for this reason we are aware that our welfare, freedom and stability are strictly associated with the security of our networks. Perhaps, we will be obliged to change our viewpoint on the anthitesis between "privacy and security" which nowadays seems to be anacronistic. When we have to face an emergency at national level, such as a hydrogeological, health or cyber emergency, we realize that security is fundamental to guarantee any form of freedom. The current pandemic has surely strenghtened the role of the State, stressing the need to focus our attention on the concept of security, which must be considered both as "multi-level and shared security" and as "culture of security". This increased awareness is fundamental to more appropriately reduce and manage in the future the critical situations and the emergencies represented, for example, by this pandemic. The national security must be protected and promoted together with our personal privacy.

Finally, taking into account the international context in which this pandemic has spread, the Covid -19 health emergency represents also a trigger for the ongoing Great power competition. There is a major risk posed to security and the discussions, also at national level, are more animated. This is evident also taking into account the international debates as well as the phenomena emerging at global level. At the same time, we have to manage more complex interconnections and our strategies are out of focus, also becuase of

the progressive elimination of the traditional multilateral tools, such as for example the ones used for the weapons control.

Cybersecurity and the management of cyber risk are to be dealt with from a cultural perspective. Therefore, it is necessary to enhance knowledge and to undertake learning and training activities to be delivered to the whole civil society, as well as to formulate common plans, including infrastructural projects such as the 5G, starting from our common values and from the Alliance we have joined. Therefore, regardless of the scope given to the definition of cybersecurity, the different aspects to be taken into account are: technology, organization, procedures, surveillance and, above all, training. It is necessary to develop and provide civil society with really shared projects aimed at strenghtening our security.

* * *

Introduzione

La *minaccia cibernetica*, nelle sue molteplici manifestazioni e forme, è notevolmente cresciuta a causa della maggiore interconnessione dei sistemi e della disponibilità di nuove tecnologie. Queste ultime, pur fornendo soluzioni in grado di proteggere in modo incisivo dati e comunicazioni, pongono nuovi e delicati problemi sul fronte della sicurezza nazionale, con particolare riferimento alla minaccia ibrida. Parliamo, cioè, di quell'utilizzo coordinato e mirato di attività ostili da parte di attori statuali e non solo, caratterizzato da un alto livello di opacità e negabilità, atto a sfruttare le vulnerabilità sistemiche del Paese target, attraverso strumenti di varia natura, tra cui *cyber-spionaggio*, *cyber-sabotaggio* e campagne di disinformazione, anche attraverso piattaforme *on-line*.

Tale minaccia si accentua, a tutti i livelli, in periodi connotati da un forte incremento dell'utilizzo del *web*, quale quello che si sta vivendo a causa della pandemia *Covid-19*.

Tra l'altro, e rapidamente, l'iperconnessione ha progressivamente riguardato non solo le persone, ma anche le cose, con una dipendenza funzionale sempre più stretta e automatica tra piattaforme di gestione di dati e servizi pubblici o comunque di interesse pubblico, nonché tra servizi, persone e oggetti, come nel caso dell'"*internet of things*", vale a dire l'estensione di *internet* al mondo degli oggetti e dei luoghi fisici identificata concettualmente oltre 20 anni fa. Si è passati da un'era analogica a quella digitale, e la prossima frontiera sarà quella quantistica, il mondo della crittografia.

Il *web* ha quindi assunto le sembianze di un vero e proprio *organismo*

vivente, globale, dalle articolazioni non sempre identificabili e dalle connessioni sempre più remote. Un organismo le cui regole comportamentali non sono univoche, ma cambiano in base a parametri territoriali che spesso nulla hanno a che fare con l'effettiva "vita" dell'organismo; regole che sono nella maggior parte dei casi assolutamente sconosciute alle persone che sfruttano ed al tempo stesso alimentano l'organismo con i loro dati, con il loro quotidiano comunicare.

Nel suo evolversi, l'"*organismo web*" ha contratto molteplici patologie dagli uomini che lo (mal)manipolano a livello planetario e molte ne ha immesse o inoculate nella vita "reale". Prevenzione e cura di tali patologie hanno assunto negli anni la consistenza di una vera e propria disciplina: la *cybersicurezza*, intesa come l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche. Missione della *cybersicurezza* è la protezione dalla patologia della "*minaccia informatica*", intesa come qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone. Questa attività avviene utilizzando i poteri che ha a disposizione uno Stato: diplomatico, informativo, militare, economico, finanziario, intelligence e *law enforcement*.

Negli ultimi tre anni è stato avviato un processo di progressivo adeguamento normativo volto a potenziare la resilienza del Paese. In questo senso, con la *legge sul perimetro*, l'Italia si è posta all'avanguardia in Europa, prevedendo oltre all'applicazione della Direttiva *Network and Information Security* (NIS), anche una normativa che tutela gli *asset* digitalizzati che riguardano la sicurezza nazionale, in quanto impiegati per assicurare l'esercizio di funzioni e servizi essenziali dello Stato. La legge ha stabilito, rispetto alla Direttiva NIS, più stringenti criteri di notifica degli incidenti allo CSIRT, in aggiunta a mirate misure di *cybersecurity* e di *screening* tecnologico, volte ad alzare anche l'asticella della sicurezza dell'approvvigionamento tecnologico (c.d. *procurement* ICT).

Il presente lavoro si propone di approfondire le principali tematiche che riguardano la difesa e la sicurezza dello spazio cibernetico e la normativa europea e nazionale in tema di *cybersecurity*, con un *focus* sulle novità normative e sulle strategie politiche che la sfida della cybersicurezza comporterà nel prossimo futuro, in ambito nazionale ed internazionale.

La prima parte del lavoro è, pertanto, dedicata all'analisi delle caratteristiche del dominio cibernetico e all'evoluzione della minaccia *cyber* nelle sue diverse tipologie malevole.

Nel secondo capitolo viene illustrato il *framework* internazionale e nazionale della sicurezza cibernetica. Sulla base dell'analisi della normativa vigente si riporta l'architettura istituzionale preposta alla protezione cibernetica nazionale, analizzando ruoli e competenze dei soggetti incaricati, nonché i meccanismi per la prevenzione dei rischi e per la gestione di crisi cibernetiche. Sono, inoltre, richiamate le principali disposizioni di contrasto della criminalità informatica e vengono presentati gli organismi di *cyber investigation* delle forze di polizia e del settore Difesa, in un'ottica di coordinamento interforze e di cooperazione internazionale.

Lo sviluppo successivo è dedicato alle politiche nazionali ed europee volte a innalzare le capacità di protezione, reazione e risposta nei confronti della minaccia cibernetica in taluni ambiti strutturalmente interessati. Dal punto di vista nazionale, si analizza il processo di trasformazione digitale della pubblica amministrazione, obiettivo previsto come vincolo di progetto nel *Piano Nazionale di Ripresa e Resilienza* (PNRR). Viene inoltre approfondita la disciplina del c.d. *golden power* e l'ampliamento della sua applicazione alle reti 5G nell'assetto degli equilibri globali.

Si è dunque acquisita la consapevolezza che la tutela da minacce informatiche non potesse più essere limitata ai meri aspetti contrattuali "utente/fornitore di servizi e apparecchiature *web*", involgendo il funzionamento stesso di istituzioni e comunità e determinando l'esigenza di affrontare la questione della *cybersicurezza* in termini di legislazione più ampia, anzi, considerandone il carattere transnazionale, tramite lo sviluppo di un quadro normativo sempre più articolato e complesso, nazionale ed europeo, in grado di offrire ai clienti/cittadini la protezione più uniforme e affidabile possibile.

Se fino ad oggi tutto ciò che attiene alla *cybersicurezza* è stato patrimonio esclusivo dei tecnici, nel prossimo decennio questa materia diventerà una disciplina organizzata, con regole chiare accessibili ad un mondo di utenti sempre più esteso. In tal senso, l'attuale situazione emergenziale provocata dalla pandemia di *Covid-19* ci ha reso consapevoli della sfida della *cybersicurezza*, conferendogli connotati di indifferibilità, in termini sia di accelerazione del progetto già avviato, sia di un suo perfezionamento, con un innalzamento dei livelli di garanzia e di tutela.

1. *Cyber spazio* e minaccia cibernetica

1.1. L'esperienza umana digitalizzata: nuovi spazi esperienziali verso la digitalizzazione

Le *information and communication technology* (ICT[1]), sono oramai pervasive e stanno penetrando trasversalmente in tutti i settori produttivi e nei sistemi, che regolano le dinamiche sociali: servizi pubblici, conoscenza, convergenza dei *media*, reti sociali, gestione ambientale, problemi energetici, agricoltura e mondo lavorativo. Le società organizzate, dunque, si stanno evolvendo verso un modello di interazione abilitato da I.C.T. *anytime*, *anywhere*, *for anybody.* È necessario rapportarsi con l'entità della popolazione internauta, per comprendere meglio questo scenario fortemente digitalizzato.

Secondo il report *Global Digital 2020* di *We Are Social*[2], su 7,6 miliardi di abitanti nel pianeta, gli utenti connessi a Internet sono 4 miliardi (il 53% della popolazione mondiale), e di questi, 3,2 miliardi (il 42%) sono attivi sui *social media.* Lo stesso report dimostra come l'Italia si confermi un Paese maturo, connesso, *social* e con un *trend* di adozione in crescita per quanto riguarda sia Internet in senso ampio, sia le piattaforme *social*, sia le nuove tecnologie. Sono infatti quasi 50 milioni le persone on-line in Italia su base regolare, e 35 milioni quelle presenti ed attive sui canali social, con un aumento rispetto alle rilevazioni del 2019[3].

In particolare, per i giovani l'esposizione al digitale supera di gran lunga quella della frequentazione scolastica e, addirittura, quella dedicata al riposo notturno, anche a causa dell'uso costante dello *smartphone*, per cui i *media* si possono tramutare in "armi di distrazione di massa", con evidenti ripercussioni sulla preparazione scolastica, sui rapporti sociali e anche sulla psiche[4]. Lo *smartphone* è diventato infatti un prolungamento del nostro corpo, lo strumen-

---

1) Le tecnologie dell'informazione e della comunicazione (in acronimo TIC o ICT, dall'inglese *information and communications technology*) sono l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese).

2) *Wearesocial.com* è una "*socially-led creative agency*" fondata con l'obiettivo di creare connessioni rilevanti tra brand e persone, attraverso l'analisi del *social thinking.*

3) Secondo il report *Global Digital 2020* di *We Are Social*, non è solamente la quantità di persone presenti ed attive a crescere, ma anche il tempo che decidiamo di passare on-line: spendiamo 6 ore connessi ad internet ogni giorno, 1 ora e 57 minuti sui *social*, in aumento rispetto al dato rilevato nel 2019, che si era fermato a 1 ora e 51 minuti.

4) A. Teti, *Cyber espionage e cybercounterintelligence. Spionaggio e controspionaggio cibernetico*, Rubbettino, Soveria Mannelli, 2018. Risulta interessante la considerazione di Teti, secondo il quale "*nell'ecosistema digitale l'individuo viene messo nelle condizioni di poter dare libero sfogo alle pulsioni più represse, ad esempio esprimendo le critiche più dure e violente sugli estranei, oppure scagliandosi senza alcun timore in discussioni animate e inutilmente durature*". Il *cyberspace* può, pertanto, considerarsi un amplificatore di sentimenti negativi.

to che soddisfa l'irrefrenabile bisogno di sentirsi costantemente on-line. Basti considerare che solo in Italia abbiamo circa 80 milioni di connessioni basate su dispositivi mobili. I cellulari sono il principale strumento che consente di svolgere tutte le attività legate alla sfera personale, professionale, formative e lavorative[5].

L'avanzamento tecnologico ha reso disponibili a una moltitudine di soggetti mezzi, che ampliano enormemente il ventaglio delle potenzialità dell'essere umano, ma senza i necessari adeguamenti al quadro etico e normativo. Nel contesto delineatosi la crescita esponenziale delle tecnologie informatiche, non bilanciata da una adeguata regolamentazione giuridica, ha generato uno spazio grigio, dove è possibile agire impunemente per fini antisociali, che vanno dal *cybercrime* alla *cyberwar*[6].

All'evoluzione digitale dovrebbe, pertanto, corrispondere un'evoluzione etico-normativa, atta a rendere la rivoluzione informatica fruibile in sicurezza. Il *cyberindividuo* dovrebbe farsi carico consapevolmente del compito di con-

---

5) A. Teti, lezione dal titolo "*Deep web: istruzioni per l'uso. Virtual Humint Intelligence*" nel corso del Master in *intelligence* dell'Università della Calabria; F. De Vincentis, *Tra fake e realtà*, 21/03/2021, su *https://formiche.net*. Secondo Teti, la predilezione dell'utilizzo dei social è riferibile soprattutto alle due maggiori peculiarità che possiedono: semplicità e rapidità di utilizzo. L'autore osserva come non sia certamente un caso se le prime quattro applicazioni maggiormente utilizzate in Italia nel 2020 siano state YouTube, WhatsApp, Facebook e Instagram. È stato calcolato, per esempio, che in soli sessanta secondi vengono creati 701.389 login su Facebook; 69.444 ore di video guardati su Netflix; 150 milioni di email inviate; 1389 corse prenotate su Uber; 527.760 foto condivise su Snapchat; 2,78 milioni di video visualizzati su YouTube; 347.222 nuovi tweet e 38.194 post su Instagram. Le figure maggiormente richieste per svolgere queste attività di ricerca, acquisizione e raffinazione delle informazioni siano i *data scientist*, ovvero quegli 'scienziati dei dati' in grado di valorizzare le informazioni presenti nel *mare magnum* di internet, trasformandole in un prodotto di intelligence.

6) Le norme nazionali e internazionali che disciplinano i mezzi di comunicazione tradizionali (radio, stampa, televisione, editoria) risultano, a fronte della nuova dimensione dello spazio cibernetico, profondamente inadeguate, in quanto sono state congegnate pensando a uno spazio territoriale e, chiaramente, risulta complesso estenderle fino a ricomprendervi anche le operazioni effettuate attraverso la Rete poiché, quest'ultima, crea uno spazio virtuale costituito da siti e pagine web, che non si trovano in un determinato luogo fisico. Il rapporto diritto-*cyberspace* produce, dunque, una serie di rilevanti profili problematici, tra cui quelli relativi all'individuazione dell'azione criminosa e alla localizzazione dell'autore del crimine informatico. L'incessante evoluzione, ma anche le nuove esigente di globalizzazione, nonché la nascita di nuovi beni giuridici, finora sconosciuti, con le conseguenti nuove minacce ai medesimi costituiscono fattori di rapido invecchiamento delle norme e pongono al giurista il problema di una costante ricerca di regole nuove che meglio contemperino i diversi interessi.

trollo dell'avanzamento tecnologico, dirigendolo verso un auspicato miglioramento delle proprie e altrui condizioni di vita, fornendo una cornice normativa adeguata allo scopo. Si tratta di un compito di non facile realizzazione, poiché comporta un controllo cosciente ed etico della tecnologia in oggetto e delle sue evoluzioni.

In tale contesto, insegnare ai giovani l'educazione ai *media* e al digitale diventa una scelta sulla quale le politiche pubbliche saranno chiamate a rispondere. Le nuove modalità di apprendimento imposte dal *Covid* esigono un chiaro indirizzo delle istituzioni e della politica per interventi radicalmente diversi dalla "resa" all'eccesso di potere delle piattaforme digitali. Mai come oggi l'acquisizione e il possesso dei codici comunicativi e tecnologici rappresenta un allargamento della conoscenza; ma se ci si arriva dalla scuola e non dal *fai da te*, scatta una straordinaria possibilità di potenziamento della formazione[7].

1.1.1. Il *cyber* spazio

Oggi la vita quotidiana scorra su migliaia e migliaia di chilometri di cavi e di fibre ottiche che in un'intricatissima, fitta e capillare rete collegano i nodi più remoti del globo. Dati, informazioni, immagini e disposizioni economiche corrono fulminei nella dimensione intangibile, immateriale e senza tempo dello *spazio cibernetico*: una sorta di "non-luogo", in cui si muove e alimenta tutto il sistema sociale, economico, politico e militare dell'intero pianeta. Ma la rete muove anche gioie, dolori, sentimenti, pezzi di vita che gli utenti trasmettono, talvolta improvvidamente, a destinatari più o meno ampi.

La globalizzazione ha prodotto la nascita di un ecosistema informativo globale, in cui si annidano informazioni e dati che possono essere acquisiti rapidamente e in tempo reale, con tecniche e metodologie impensabili fino a pochi anni fa[8]. L'informazione è potere e la preziosità dei dati viene definita in

---

7) M. Morcellini, *Oltre la sudditanza digitale*, Lo specchio, Rivista *Formiche.net*, marzo 2021.

8) F. De Vincentis, *La lezione di Teti sul mondo virtuale e l'intelligence "Deep web: istruzioni per l'uso. Virtual Humint Intelligence. Tra fake e realtà"*, nel corso del Master in *intelligence* dell'Università della Calabria, 21/03/2021, su *https://formiche.net*. Secondo Teti è necessario "*essere consapevoli del valore di ogni singola e apparentemente insignificante informazione che inseriamo all'interno del web, poiché rimarrà per sempre nella Rete, anche in contrasto con le normative internazionali che tendono a garantire la tutela della privacy o il cosiddetto diritto all'oblio*".

funzione della capacità di saperle 'raffinare' e 'fonderle'. Noi tutti immettiamo quotidianamente, spesso senza rendercene conto, informazioni di ogni genere, finanche riservate, all'interno del mondo virtuale. Sono informazioni che possono rivelare molto di noi, delle nostre pulsioni, dei nostri comportamenti, dei nostri pensieri e perfino dei nostri più intimi desideri. Persino le *emoticon* che inseriamo nei post possono essere analizzate da applicazioni in grado di valutare il *sentiment* dell'individuo. Non è più possibile pensare che sussista ancora una linea netta di demarcazione tra il modo reale e quello virtuale. Tutto ciò che produciamo nel mondo virtuale ha delle conseguenze su quello reale e ci identifica viceversa.

Il termine *cyber spazio*[9], apparentemente futuristico, racchiude in realtà in modo succinto, ma efficace, un universo nuovo e complesso, attrattivo e pericoloso, virtuale e al contempo drammaticamente concreto, sul quale scorre gran parte della vitalità del mondo moderno. Tale nuova dimensione "*aspaziale*"[10] si presenta, per sua stessa natura, come "deterritorializzata", "decentralizzata" e contraddistinta dalla simultaneità, dall'anonimato, dalla "spersonalizzazione" e dalla "detemporalizzazione" delle attività[11].

Prima di porre l'attenzione sulle caratteristiche dello spazio cibernetico occorre, anzitutto, darne una definizione, che si trova nel *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, secondo cui lo spazio cibernetico è "*l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati e utenti, nonché delle relazioni logiche,*

9) Il termine "*cyberspace*" è stato coniato dallo scrittore W. GIBSON nel racconto *Burning Chrome* del 1982 per indicare una realtà virtuale. Il significato della parola si è poi ampliato, per riferirsi al "mondo di internet" in senso generale (cfr. voce *Cyberspazio* su *Wikipedia*); così pure, il termine "*cybercrime*" ha ormai assunto una portata ampia, in quanto indica "*any criminal act dealing with computers and networks*" (così, voce *Cyber Crime* su *Webopedia*).

10) Fonte: Comitato parlamentare per la sicurezza della Repubblica, *Relazione sulle procedure la normativa per la produzione ed utilizzazione di sistemi informatici per l'intercettazione di dati e comunicazioni*, XVII legislatura, Doc. XXXIV, n. 7. Da un punto di vista ambientale lo spazio cibernetico si presenta come un ambiente virtuale, privo di confini fisici nel senso tradizionale del termine, uno spazio indefinito nel cui ambito non esiste divisione tra pubblico e privato, tra la sfera militare e civile.

11) In merito all'importanza riconosciuta al fenomeno in esame, si può menzionare il pensiero di Michael Heim, definito il filosofo del *cyberspace* il quale, nell'ambito della sua "teoria della trasformazione", ritiene che la rivoluzione informatica sia da considerare tanto grande quanto il passaggio dall'oralità alla scrittura. Per un'interpretazione in chiave ontologica della nostra realtà alla luce del virtuale e del *cyberspace* si rimanda a M. Heim, *Metafisica della realtà virtuale*, ed. it. a cura di D. ROSSI, Guida, Napoli, 2015.

comunque stabilite, tra di essi, che *comprende Internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete.* [...]. *Esso costituisce un dominio virtuale di importanza strategica per lo sviluppo economico, sociale e culturale delle nazioni*"[12].

La dimensione cibernetica è pertanto generata dalla ramificatissima rete di infrastrutture materiali di collegamento e di comunicazione[13] che, attraverso la tecnologia informatica, mettono in contatto tra loro un crescente numero di esseri umani e permettono loro di attivare e controllare da ubicazioni remote macchine e apparati in tutto il mondo.

Si tratta di un ecosistema complesso, nel cui ambito gli esperti della materia sono soliti distinguere i seguenti tre livelli essenziali:

– il livello fisico infrastrutturale, rappresentato dalle macchine (le architetture delle reti, i *computer*, i *router*);

– il livello logico informativo rappresentato dal volume dei dati gestiti dalle macchine (*database*, *file*, ma anche *software* gestiti dalle macchine);

– il livello sociale cognitivo, ovvero l'insieme delle relazioni umane e delle caratteristiche socio-cognitive che possono costituire le identità virtuali (l'indirizzo *e-mail*, il profilo nei *social network*, gli indirizzi IP[14] delle macchine).

Essendo un dominio creato dall'uomo, lo spazio cibernetico è, inoltre, in continua evoluzione e implementazione, in connessione con la rapida ed ininterrotta evoluzione delle tecnologie dell'informazione e della comunicazione *(information and communication technology*, ICT) grazie alle quali vengono erogati in misura crescente servizi essenziali per la collettività e strategici per il Paese.

In quanto dominio artificiale, il dominio cibernetico presenta delle "vulnerabilità" ovvero dei punti di debolezza attraverso i quali è possibile acquisire illegalmente dati e informazioni che "transitano" nello spazio cibernetico ov-

---

12) Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, dicembre 2013, p. 10.

13) Grazie ai progressi delle tecnologie di comunicazione e l'impiego diffuso di dispositivi elettronici e di monitoraggio si intrecciano quotidianamente nello spazio cibernetico miliardi di interconnessioni, si scambiano conoscenze a livello globale e viene raccolto un gigantesco numero di dati e di informazioni compresi quelli di natura personale e sensibile (c.d. *big data*).

14) L'*Internet Protocol Address* o indirizzo IP è un codice numerico usato da tutti i dispositivi (computer, server web, stampanti, modem) per navigare in Internet e per comunicare in una rete locale.

vero compromettere in tutto o in parte il funzionamento di servizi e sistemi digitali.

Le vulnerabilità del dominio cibernetico rappresentano pertanto il rovescio della medaglia del progresso tecnologico ed informatico. Tali "fratture" del sistema informatico, di difficile individuazione e classificazione, possono dipendere sia da fattori tecnici congeniti al *software* applicativo, sia dal mancato o non corretto funzionamento dei sistemi di protezione[15]: da qui l'esigenza di disporre di materiali tecnologicamente certificati più facilmente controllabili e monitorabili, con particolare riferimento alla fornitura di materiale militare[16].

1.1.2. L'intelligenza artificiale

L'intelligenza artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività. Tale abilità permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico. Il computer riceve i dati (già preparati o raccolti tramite sensori, come una videocamera), li processa e risponde. I sistemi di IA sono capaci di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia.

L'interesse che oggi si concentra intorno a questa disciplina si dispiega sia nel calcolo computazionale (basti pensare a sistemi *hardware* molto potenti, di ridotte dimensioni e con bassi consumi energetici), sia nella capacità di analisi in real-time ed in tempi brevi di enormi quantità di dati e di qualsiasi forma.

L'intelligenza artificiale potrà trasformare praticamente quasi tutti gli aspetti della vita quotidiana e dell'economia[17]. Nella vita di tutti i giorni vi sono tante applicazioni che utilizzano l'intelligenza artificiale, senza che ce ne

---

15) Cfr. Commissione difesa della Camera dei Deputati, seduta del 9 febbraio 2016, audizione del Prof. Baldoni, cit. Nel documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, condotta dalla Commissione difesa della Camera dei Deputati nella XVII legislatura, si analizzano le cause delle diverse vulnerabilità.

16) A.M. Balsano - L. Del Monte, *Il diritto internazionale di fronte al cyberspace*, in Osservatorio per la sicurezza nazionale (a cura di), *Cyberworld. Capire, proteggersi e capire gli attacchi in rete*, Hoepli, Milano, 2013, p. 219.

17) In particolare, nel campo della lotta alla disinformazione le applicazioni di intelligenza artificiale sono in grado di individuare *fake news* e disinformazione, analizzando i contenuti dei *social media* e identificando le parole e le espressioni sospette, perché sensa-

accorgiamo[18]. I sistemi di intelligenza artificiale possono inoltre aiutare a riconoscere e combattere gli attacchi e le minacce informatiche. Lo fanno imparando dal continuo flusso di dati, riconoscendo tendenze e ricostruendo come sono avvenuti gli attacchi precedenti.

1.1.3. Le infrastrutture critiche e la loro protezione

La protezione delle infrastrutture critiche dalle minacce *cyber* è un tema di sicurezza nazionale impostosi ormai da tempo, affrontato in sede legislativa anche in Europa.

Secondo la definizione del Dipartimento per la sicurezza interna degli Stati Uniti (DHS), "*Le infrastrutture critiche della Nazione forniscono i servizi essenziali che sono alla base della società statunitense e servono da spina dorsale dell'economia, della sicurezza e della salute della nostra Nazione*". Il DHS elenca 16 settori "*così vitali per gli Stati Uniti che il loro malfunzionamento o distruzione avrebbe un effetto debilitante sulla sicurezza, l'economia nazionale, la salute o la sicurezza pubblica nazionale, o qualsiasi combinazione di questi elementi*".

A livello europeo manca ancora una definizione con questo livello di chiarezza, probabilmente per la maggiore diversificazione degli Stati Uniti e

---

zionalistiche o allarmanti. Possono così aiutare a capire quali fonti possono essere considerate autorevoli. Nel campo della salute alcuni ricercatori stanno studiando come usare l'intelligenza artificiale per analizzare grandi quantità di dati medici e scoprire corrispondenze e modelli per migliorare le diagnosi e la prevenzione. Si sta sviluppando inoltre un programma per rispondere alle chiamate di emergenza che riconosce più velocemente un arresto cardiaco rispetto a un operatore umano. Nel settore dei trasporti l'intelligenza artificiale potrebbe migliorare la sicurezza, la velocità e l'efficienza del traffico ferroviario, anche grazie all'uso della guida autonoma. Nel campo della filiera agricola e alimentare l'IA può essere usata per costruire un sistema alimentare sostenibile, minimizzando l'uso di fertilizzanti, pesticidi e irrigazione, aiutando la produttività e riducendo l'impatto ambientale, l'intelligenza artificiale può aiutare a produrre cibo più sano. Nell'Amministrazione pubblica e nei servizi, usando i dati per elaborare modelli, l'IA può fornire un sistema di allerta per i disastri naturali, riconoscendone i primi segni sulla base di esperienze passate.

18) I principali ambiti in cui l'intelligenza artificiale viene utilizzata sono i seguenti:
– shopping in rete e pubblicità: l'intelligenza artificiale è largamente usata per fornire suggerimenti basati, ad esempio, su acquisti precedenti, su ricerche e su altri comportamenti registrati *on-line*. L'intelligenza artificiale è anche molto usata nel commercio al dettaglio, per ottimizzare gli inventari e organizzare i rifornimenti e la logistica;
– ricerche *on-line*: i motori di ricerca imparano da un grande numero di dati, forniti dagli utenti, per offrire i risultati di ricerca pertinenti;

perché sono ancora in fase di completamento gli adempimenti della Direttiva sulla sicurezza dei sistemi informativi di rete (NIS[19]), promulgata dal Parlamento europeo e dal Consiglio il 6 luglio 2016 e adottata da tutti gli stati membri il 9 maggio 2018.

La Direttiva NIS chiarisce che gli Operatori di Servizi Essenziali (OSE) – il nome che l'Unione europea ha scelto di adottare per le infrastrutture critiche – sono "*quei soggetti che forniscono un servizio essenziale per il mantenimento di attività sociali e/o economiche critiche*", che questo servizio dipende inoltre dalla rete e dai sistemi informativi e che un incidente avrebbe effetti di disturbo significativi sulla fornitura del servizio; chiede quindi agli stati membri di creare un proprio elenco di servizi basato su 7 settori principali e 7 sottosettori.

Da un punto di vista pratico, le infrastrutture critiche nei Paesi occidentali, e in Europa in particolare, non sono però entità autonome, ma piuttosto un complesso sistema di *asset* e reti con diverse tipologie di componenti tecnologiche, di provenienza mondiale, che sono state generalmente progettate per operazioni a sistema chiuso. In questo contesto, quando gli *asset* e le reti hanno iniziato ad essere interconnessi, e poi spesso aperti a internet, le vulnerabilità, trascurabili in un ambiente chiuso, sono diventate improvvisamente molto rilevanti.

– assistenti digitali personali: i telefoni cellulari usano l'intelligenza artificiale per offrire un prodotto più personalizzato possibile. Gli assistenti virtuali rispondono alle domande, forniscono suggerimenti e aiutano a organizzare l'agenda di tantissimi possessori di *smartphone*;

– traduzione automatica: i *software* di traduzione automatica, basati su testi audio o scritti, usano l'intelligenza artificiale per fornire e migliorare le traduzioni. Un altro uso sono i sottotitoli automatici dei video;

– case, città e infrastrutture intelligenti: i termostati intelligenti imparano i nostri comportamenti per ottimizzare energia. L'intelligenza artificiale può servire nelle città per migliorare la viabilità e ridurre gli ingorghi;

– veicoli: anche se le auto a guida autonoma solo ancora rare, le automobili che guidiamo hanno già alcune funzioni di sicurezza che usano l'intelligenza artificiale. L'Unione europea ha ad esempio contribuito a finanziare VI-DAS, i sensori che individuano possibili situazioni pericolose e incidenti.

19) La direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi), approvata dal Parlamento europeo nel 2016, è stata recepita nel nostro ordinamento attraverso il decreto legislativo 18 maggio 2018, n. 65 (anche detto "decreto legislativo NIS"), in vigore dal 24 giugno 2018. La direttiva ha imposto ai cosiddetti Operatori di servizi essenziali di dotarsi di un'efficace gestione del rischio *cyber* tramite l'adozione di misure tecniche e organizzative adeguate al rischio, atte a prevenire e minimizzare l'impatto degli incidenti.

Ciò comporta la necessità, ormai avvertita con una forte consapevolezza, di innalzare il livello di protezione delle infrastrutture critiche.

Il vero obiettivo per le infrastrutture critiche dovrebbe essere, dunque, non solo la protezione informatica, ma piuttosto *la resilienza informatica*: per i servizi essenziali è infatti più importante garantire la continuità del servizio, magari in uno stato parzialmente degradato, ma controllato, che cercare di creare barriere a qualsiasi tipo di minacce e possibili attacchi, implementando, in tal modo, quello che viene definito nella dottrina militare deterrenza per negazione[20] (*deterrence by denial*).

Le infrastrutture critiche sono interconnesse oltre i confini nazionali, a volte attraversando aree geografiche "sensibili"[21] e quindi la resilienza non può essere semplicemente imposta, ma deve essere costruita attraverso accordi tra Stati, attraverso contratti commerciali e attraverso il riconoscimento dei benefici reciproci. Ancora una volta la condivisione delle informazioni è ne-

---

20) Secondo gli approcci e le metodologie attuali, questo obiettivo è raggiungibile attraverso una chiara disciplina in fase di progettazione e costruzione, utilizzando molte tecniche diverse, conosciute collettivamente come *security-by-design* e *resilience-by-design*. Purtroppo il raggiungimento di una situazione in cui gli operatori di servizi essenziali sono abbastanza resilienti da mitigare ad un livello accettabile i rischi derivanti da eventi informatici (indipendentemente dalla loro attribuzione da parte di hacktivisti, terroristi, atti di guerra, sabotaggio o altri iniziatori) deve tenere conto di alcune criticità sostanziali. In primo luogo, le tecniche di resilienza per progettazione possono essere applicate a sistemi di nuova progettazione, ma le infrastrutture critiche sono normalmente abbastanza vecchie o sono la sovrapposizione di molti sistemi con tecnologie diverse di epoche diverse; una situazione che rende difficile identificare tecniche generalizzate per creare resilienza: ogni caso deve essere analizzato singolarmente. Questo richiederà una forte cooperazione per allineare standard e tecniche e, cosa più importante, per scambiare quelle che potrebbero essere informazioni sensibili sui sistemi, protocolli e tecnologie sottostanti utilizzati dai vari fornitori di tecnologia. Poiché gli operatori di servizi essenziali sono strettamente interconnessi e richiedono almeno alcuni servizi da parte di altre infrastrutture critiche, come le telecomunicazioni, l'energia, il gas, l'acqua, i trasporti, ecc., o si progettano sottosistemi ridondanti multipli per qualsiasi infrastruttura critica o si deve trovare un modo per garantire un livello accettabile di prestazioni di tutte le infrastrutture critiche interconnesse. Ciò porta ancora una volta alla necessità di condivisione delle informazioni, ma aumenta nuovamente il livello di complessità, poiché si avrà bisogno di scambiare informazioni tra molti altri soggetti, non solo i fornitori di tecnologia, ma anche tra le infrastrutture critiche stesse, che a volte potrebbero essere parzialmente in concorrenza su determinati settori o mercati. Gli attori politici cercano in generale di consentire questo scambio attraverso la mediazione realizzata da enti indipendenti come i CSIRT (*Computer Security Incident Response Team*).

21) Si pensi ad esempio ai gasdotti, ai tubi del petrolio o ai cavi di *internet*.

cessaria e la complessità è di nuovo maggiore, dato che si parla di condivisione delle informazioni al di là dei confini nazionali e questo deve essere fatto, ovviamente, senza pregiudicare la sicurezza nazionale[22].

Le interconnessioni delle infrastrutture critiche transnazionali rendono inoltre difficile affrontare una risposta univoca ai rischi legati agli eventi cibernetici: iniziative congiunte o di coalizione aiuteranno in questo senso, ma dovrebbero essere stipulati trattati internazionali, perché se un'infrastruttura critica è messa a rischio da un evento che si verifica in una regione geografica diversa, le regole su come affrontare questa situazione dovranno essere chiaramente conosciute in anticipo per evitare il rischio di interpretazioni errate e di escalation.

Gli operatori di servizi essenziali sono generalmente aziende private, a scopo di lucro, e quindi i costi necessari per costruire la sicurezza e la resilienza devono essere riconosciuti come parte della *mission* della società, integrati nella sua *governance* – ad esempio come parte degli interessi degli stakeholder nella loro visione di responsabilità sociale d'impresa – ma necessariamente contribuendo anche al conto economico e al bilancio della società[23].

Purtroppo, la struttura complessa che supporta il nostro modo di vivere è stata costruita negli ultimi 70 anni; tuttavia, si ha a disposizione altrettanto tempo per districare tutti i collegamenti costruiti sinora e decidere come affrontare la resilienza dell'intero sistema.

1.2. Il fenomeno del *cybercrime*

La pervasività delle tecnologie dell'informazione e della comunicazione nelle società moderne, se da un lato ha contribuito a migliorare le prestazioni dei sistemi economici e civili, dall'altro ha esposto le democrazie a un tipo di

22) Vedasi articolo 7.3 della Direttiva NIS.

23) Qualsiasi scelta diversa metterebbe a repentaglio la posizione competitiva dell'azienda e, nel lungo periodo, potrebbe creare più danni alla resilienza complessiva del sistema che non un'incapacità di riconoscere e affrontare adeguatamente questa necessità. In breve, la sicurezza e la resilienza hanno un costo e si deve decidere collettivamente come questo costo deve essere sostenuto. La protezione e la resistenza cibernetiche delle infrastrutture critiche hanno una chiara dimensione tecnologica che può essere affrontata e gestita dai principali attori del settore della difesa e della sicurezza, ma la tecnologia non sarà sufficiente a fornire un contesto in cui la continuità delle operazioni delle infrastrutture critiche può essere garantita se le criticità sopra richiamate non sono affrontati dai responsabili politici, dalle organizzazioni sovranazionali e dagli *stakeholder*. Questi devono riconoscere che il quadro molto complesso delle tecnologie e delle interazioni dei servizi su cui si basa la nostra società richiede un'azione almeno altrettanto complessa per garantirne la sicurezza.

criminalità relativamente nuova, che negli ultimi anni ha colpito aziende, pubbliche amministrazioni, infrastrutture critiche e utenti privati, cagionando danni di grande entità. Tale nuova forma criminale è nata, cresciuta e radicata contestualmente allo sviluppo della Rete.

Si definisce crimine informatico un reato caratterizzato dall'utilizzo di tecnologie informatiche e di elaboratori informatici. Affinché si possa configurare un reato del tipo in questione, è necessario l'impiego di un elaboratore informatico, il c.d. *computer*; pertanto quest'ultimo assume sia la veste di strumento per la commissione del fatto illecito, sia di oggetto su cui cade la condotta criminosa; in sintesi, il *computer crime* è un reato commesso per il tramite o ai danni di un *computer*.

I reati informatici[24] (*computers crimes*) presentano dunque elementi di tipizzazione, descrittivi di modalità, oggetti o attività, caratterizzati dalla tecnologia informatica, con la inevitabile conseguenza che l'azione penalmente rilevante va correttamente inquadrata secondo le peculiari tecniche di procedure, elaborazioni e componenti informatiche. Sul versante penalistico, alla commissione dei reati informatici hanno così fatto seguito le manifestazioni dei reati telematici, poi comunemente denominati "cibernetici" (*cybercrimes*), realizzati nel c*yberspace* ovvero nello spazio informatico formato dalla integrazione tra tanti sistemi di elaborazione, comunicazione e connessione[25].

Dal "reato informatico" si passa al "reato cibernetico" di pari passo con l'affermazione e la diffusione di *internet*[26] e di altre reti di comunicazione. Per

---

24) M. Bellacosa, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni unite*, 2015.

25) L. Picotti, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Rivista trimestrale di diritto penale dell'economia*, 2011; ID., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, Cedam, 2004.

26) M. Bellacosa, *op. cit.* La parola *internet* deriva da *interconnected networks* = reti interconnesse. *Internet* si afferma negli anni '90: dai 100 mila computer connessi nel 1989 si è passati ai circa 200 milioni di computer nel 1999 (oggi gli utenti di Internet sono 4,39 miliardi). Nel 1982, William Gibson pubblicò negli U.S.A. il romanzo di fantascienza "*Burning Chrome*" e usò per la prima volta il termine "*cyberspace*" per indicare una realtà virtuale. "Cibernetico" deriva dal greco Κυβερνήτης = timoniere, chi guida o governa una nave o anche una città. Con l'affermazione di Internet, "*cyberspace*" è divenuto il termine per indicare il "mondo di internet". La rete *internet* nacque nel 1969, quando i computer di quattro Università americane si misero in collegamento. Nel 1971, l'agenzia militare americana ARPA (*Advanced Research Projects Agency*) collegò 23 computer sparsi sul territorio nazionale..

cybercrime si intende "*any criminal act dealing with computers and networks*": il reato cibernetico è un dunque un concetto più ampio di reato informatico.

Le forme tradizionali di giurisdizione, infatti, si basano sul concetto di "confine" e le leggi su quello di sovranità territoriale. Nei casi di un crimine informatico, avente portata transnazionale, l'individuazione del *locus commissi delicti* risulta assai difficoltosa. Ciò comporta il venir meno di un tassello fondamentale dell'impianto penalistico della maggior parte degli ordinamenti giuridici che si fondano sul principio di territorialità come criterio principe nella definizione del giudice competente a conoscere il fatto illecito.

Essendosi il *cybercrime* ramificato in una dimensione transnazionale, ne consegue che la lotta per contrastare questo fenomeno assuma lo stesso carattere; ciò impone innanzitutto la circolazione delle informazioni e una maggiore cooperazione tra le autorità investigative dei singoli Paesi. Occorre fornire, dunque, a un fenomeno caratterizzato da una ramificazione transnazionale una risposta transnazionale. Diventa, pertanto, imperativo approntare strategie, quali la collaborazione giudiziaria e dotarsi di un sistema normativo comune per contrastare tale tipo di manifestazione delittuosa[27].

Lo spazio immateriale e incalcolabile del *cyber*, realizzatosi con lo sviluppo del *cloud computing*[28], comporta anche diversi rischi circa la "volatilità" delle informazioni memorizzate, la crittografia eventualmente utilizzata e il tipo di approccio alla sicurezza dei dati. Tuttora questi processi si realizzano e si moltiplicano in modo smisurato attraverso l'uso di internet che, da mezzo di interazione e condivisione, è diventato il centro operativo di gran parte delle operazioni politiche, sociali, economiche e commerciali. L'incremento di questa interazione tra individui, aziende e istituzioni per scopi finanziari, economici e sociali, ha creato nuove opportunità anche per le attività criminali tra cui: la pornografia, la pedofilia, i virus informatici, l'uso di droghe, l'incitamento alla violenza e al razzismo, la pirateria *on-line*, la clonazione di carte di credito, la

27) Il *cybercrime* ha assunto i contorni di una vera e propria economia sommersa (fenomeno che comprende non solamente attività illecite, ma anche il reddito non dichiarato, derivante dalla produzione e vendita di beni e servizi e transazioni monetarie e tutte le attività economiche legali, ma non dichiarate, alle quali le autorità fiscali potrebbero applicare un imponibile), globalizzata ed efficiente, dove beni sottratti illegalmente e servizi fraudolenti sono venduti e acquistati e dove il giro d'affari stimato è misurabile in milioni di dollari.

28) In informatica con il termine inglese *cloud computing* si indica un paradigma di erogazione di servizi offerti *on demand* da un fornitore ad un cliente finale attraverso la rete Internet, a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita.

modifica di *smart-card* televisive o telefoniche, le molestie a sfondo sessuale, il cyberterrorismo, gli attacchi informatici a banche di dati, ecc.

Sono queste le attività presenti nel *cyberspace* che vengono definite "*cyber crime*" e si distinguono dalle classiche attività criminali per il fatto che la vittima non può percepire l'attacco fisicamente perché la maggior parte di esse vengono realizzate nel "*dark web*", la parte oscura di *internet*[29].

Gli strumenti utilizzabili per entrare in queste reti sono dei veri e propri protocolli di connessioni, predisposti per garantire la navigazione attraverso una rete parallela quasi impossibile da tracciare. Per poter capire bene questa suddivisione a strati, è necessario immaginare internet come un grande iceberg: nella punta che fuoriesce dall'acqua possiamo collocare il "*surface web*", all'interno del quale navighiamo tutti i giorni, mentre nella parte sommersa, dove comincia a mancare il sole, possiamo collocare il "*deep web*", per poi scendere fino in fondo e trovare il "*dark web*", ossia la parte oscura.

Se il *Surface web* è un web di superficie dove sono presenti le informazioni che tutti possono conoscere, all'interno del *deep web* e soprattutto del *dark web*, che rappresenta circa il 96% dell'intera rete, è possibile reperire informazioni di ogni genere non prelevabili per mezzo dei più comuni motori di ricerca. Si tratta di metadati presenti all'interno dei forum non controllati da password, oppure di informazioni nelle VPN (*Virtual Private Network*) o accessi a siti web che forniscono accessi *free* temporizzati. Da un punto di vista tecnico, l'obiettivo del *dark web* è quello di rendere anonimo l'indirizzo IP[30]. È utilizzato principalmente per traffici illegali quali la compravendita di

29) Occorre distinguere il "*deep web*" dal "*surface web*" ovvero la parte di internet dove sono presenti tutte quelle pagine web e quei contenuti che sono accessibili al grande pubblico e dove le informazioni vengono indicizzate dai motori di ricerca. Questo "strato" di internet è composto essenzialmente da pagine web statiche che risiedono in un server web e sono disponibili ad essere visualizzate dai vari navigatori. Solo il 4% dei contenuti realmente presenti in internet sono accessibili in questo strato superficiale al di sotto del quale troviamo il *deep web*, che erroneamente viene accostato a comportamenti criminosi o illegali. In realtà, questo strato di internet è costituito da tutta una serie di contenuti, non direttamente indicizzati dai normali motori di ricerca per vari motivi che sono di solito assolutamente legali e legittimi. Lo strato più profondo e segreto del *deep web* viene chiamato "*dark web*", formato dalle famose "*dark net*" (reti oscure), dove sono presenti contenuti nascosti intenzionalmente ai comuni navigatori accessibili soltanto attraverso appositi strumenti. I siti presenti in queste reti utilizzano strumenti di anonimato (Tor o I2P) per nascondere la loro effettiva collocazione.

30) Un indirizzo IP (dall'inglese *Internet Protocol address*) – in informatica e nelle telecomunicazioni – è un'etichetta numerica che identifica univocamente un dispositivo detto *host* collegato a una rete informatica che utilizza *l'Internet Protocol* come protocollo di rete.

armi, il traffico di stupefacenti ma anche per la propaganda politica terroristica, la pornografia e pedofilia, quindi una buona parte che viene dal web oscuro è occupato da attività criminali[31]. Il metodo più sicuro e più diffuso per navigare in anonimato attraverso la parte oscura di *internet* è il sistema di comunicazione Tor (*The Onion Router*)[32].

I principali obiettivi degli attacchi *cyber* sono i furti di dati, di denaro e di identità che comportano per le imprese gravi danni non solo economici, ma anche di immagine causati dalla perdita di affidabilità[33]. Le motivazioni che spingono i *cyber* criminali verso questo accanimento possono essere di tipo politico, sociale o finanziario.

Un attacco *Advanced Persistent Threat* (ATP[34]) non si affida solo alla

---

31) Sul tema F. De Vincentis, *La lezione di Teti sul mondo virtuale e l'intelligence "Deep web: istruzioni per l'uso. Virtual Humint Intelligence. Tra fake e realtà"*, nel corso del Master in *intelligence* dell'Università della Calabria, 21/03/2021, su *https://formiche.net*.

32) Il suo utilizzo è finalizzato a proteggere la privacy con la possibilità di condurre delle comunicazioni confidenziali senza che vengano tracciate e monitorate le attività degli utenti. Tor è basato sulla seconda generazione del protocollo *The Onion Router* e il suo funzionamento è concettualmente molto semplice: i dati che appartengono a una comunicazione non transitano direttamente dal client al server, ma passano attraverso i server di Tor, che agiscono da "*Proxy Server*", costruendo un percorso crittografato a strati. Il traffico viene indirizzato ad almeno tre server diversi prima di inviarlo alla destinazione e per ciascuno dei tre server c'è un livello di crittografia diverso.

33) I *malware* sono solo una piccola parte degli strumenti utilizzati dai praticanti del *cyber crime* e la loro massima diffusione è incentrata nel *dark web*, dove si è creato un vero e proprio mondo criminale. Esistono vari tipi di *malware* e più diffusi e utilizzati sono:
– *ransomware,* un programma che blocca l'accesso ai file dei computer e cui segue la richiesta di un riscatto. È molto diffuso nelle *e-mail, link* o *banned* pubblicitari;
– *spyware,* sono programmi che carpiscono informazioni legale alle attività on-line di un utente (password, ecc.).

34) Cfr. "*What is a Malware*", in *https://www.lifewire.com/what-is-malware-262593321/06/201916*. ATP è una recente tipologia di attacco sistemico che si trova sempre più al centro dell'attenzione per due primati "negativi":
– il primo è l'elevato danno che sono in grado di arrecare, ulteriormente aggravato dall'alto livello di efficacia che solitamente riescono a conseguire;
– il secondo è la difficoltà incontrata dalle soluzioni di protezione di tipo più tradizionale nel contrastarle efficacemente. Questo perché le APT rappresentano una minaccia che non si limita a una semplice intrusione rivolta a inserire un *malware* ma che punta, invece, a predisporre un attacco continuativo nel tempo che prosegue fino a quando l'attaccante non è riuscito nel suo intento di penetrare all'interno della rete del suo target. Detti attacchi sono favoriti spesso da un livello basso di protezione dei sistemi che, non essendo protetti, subiscono l'uso dei "*malware*", ossia programmi informatici predisposti per rubare informazioni o recare danni al sistema informatico.

tecnologia ma anche e soprattutto allo studio dei soggetti che utilizzano le tecnologie, per riuscire a individuare il punto di maggiore vulnerabilità all'interno dell'organizzazione attaccata.

La predisposizione di una protezione efficace dovrà quindi confrontarsi con le suddette vulnerabilità predisponendo contromisure in grado di operare non solo in modo efficace ma anche sinergico tra loro.

1.2.1. *Cyber spazio* e minaccia cibernetica: le diverse tipologie di attacco *cyber*

Il quadro delle minacce alla sicurezza nazionale si è progressivamente evoluto in linea con i mutamenti economici, politici e tecnologici del mondo contemporaneo. In questo contesto, le minacce "tradizionali" hanno assunto nuove caratteristiche, dettate dalla dimensione transnazionale, insieme a nuove tipologie di minacce che si sono affacciate sulla scena mondiale. Le nuove minacce che emergono dal *cyber spazio* mettono a dura prova la capacità degli Stati di fronteggiarle adeguatamente, necessitando di un continuo adeguamento normativo e della pronta predisposizione degli opportuni strumenti di contrasto[35]. Le ampie e diversificate opportunità di crescita, correlate all'irrinunciabile evoluzione tecnologica, nascondono elevate vulnerabilità, molto spesso trascurate per la mancanza di una piena consapevolezza da parte degli stessi attori istituzionali, che devono essere affrontate con strumenti adeguati in una prospettiva di sicurezza nazionale e protezione del sistema Paese.

Considerate le problematiche associate alla *cyber threat* (minaccia cibernetica), è evidente la necessità per gli Stati di intervenire attivamente, per

35) Ministero della difesa, *Libro bianco per la sicurezza internazionale e la Difesa* 2015, punto 32 e 103; in ambito internazionale, cfr.: *Conclusioni del vertice dai Capi di Stato e di Governo nel corso del summit di Varsavia, 8-9 luglio 2016*, nel quale si è affermato che "gli attacchi informatici rappresentano una sfida chiara alla sicurezza dell'Alleanza e potrebbero essere dannosi per le società moderne come degli attacco convenzionali". A livello nazionale, da tempo le *Relazioni sulla politica dell'informazione per la sicurezza* trasmesse dal Governo (Presidenza del Consiglio dei Ministri) al Parlamento ai sensi dell'articolo 38 della legge n. 124 del 2007 pongono particolare attenzione all'accresciuto livello di complessità e sofisticatezza della minaccia *cyber* e all'eterogeneità del profilo soggettivo dell'attaccante. Emerge, in proposito, una variegata gamma di attori che si muovono nel *cyberspace* con finalità ed obiettivi diversi, tutti di difficilissima identificazione che vanno dall'*hacker* individuale che agisce a scopo di lucro, fino all'apparato governativo che persegue obiettivi geopolitici o propagandistici.

essere in grado di fronteggiare i rischi e pericoli provenienti dal *cyber spazio*. Ciò non può prescindere dalla realizzazione della cooperazione internazionale, la quale si rivela essenziale, al fine di contenere questa nuova tipologia di minaccia alla sicurezza nazionale degli Stati.

In tutti i principali contesti nazionali, europei ed internazionali nei quali si analizzano le principali sfide alla stabilità, alla sicurezza e alla crescita dei popoli, la minaccia cibernetica viene da tempo considerata come una minaccia assai significativa, mutevole nei suoi tratti essenziali, in continua evoluzione, rapida nel bersaglio da aggredire e capace di produrre effetti a distanze non raggiungibili con gli ordinari strumenti di attacco. Dal punto di vista della pericolosità si passa, quindi, dal vandalismo cibernetico alla vera e propria guerra cibernetica[36].

Non a tutti sono noti i tipi di attacchi informatici utilizzati per danneggiare singoli e organizzazioni pubbliche e private. Come detto, le motivazioni che spingono i criminali informatici ad agire sono essenzialmente economiche. Se poi il danno riguarda il furto di identità la vittima è colpita due volte: sul piano personale sia su quello economico.

I tipi di attacchi informatici imputabili ad *hacktivism* sono maggiormente orientati verso company e organizzazioni per motivi di attivismo e protesta, mentre quelli targetizzati, ovvero orientati verso una vittima in particolare, possono colpire per motivi personali o lucrativi.

Attualmente, le potenziali minacce in tema di sicurezza cibernetica in danno di aziende e privati cittadini vengono prevalentemente dall'uso più o

---

36) Secondo l'ultimo *Cyber Security Report* 2020 emesso da Check Point, l'incidenza dei tipi di attacchi su scala mondiale ricade per il 28% su attacchi da *botnet multipurpose* maligne (reti di computer infettate da malware ed attivabili per sferrare una attacco coordinato, DDOS, contro un target n.d.r.), mentre l'aumento del 20% dei casi di *incident response* è stato causato da un attacco *ransomware* mirato (tipo di *malware* che infetta un PC, spesso ne blocca i dati e le funzioni chiedendo un riscatto per la sua risoluzione n.d.r.). Il panorama del *malware* è ancora dominato da *cryptominer (malware* che usano le risorse computazionali della vittima per minare monete virtuali n.d.r.) che hanno colpito il 38% delle aziende nel 2019. In lieve flessione rispetto al 2018 sembrano risultare gli attacchi mobile sferrati sul 27% delle organizzazioni mondiali nel 2019. In estensione i tipi di attacchi informatici cosiddetti *Magecart* che iniettano codice dannoso nei siti *e-commerce* per rubare i dati di pagamento ed hanno colpito nel 2019 centinaia di siti fra catene alberghiere e giganti del commercio alle PMI. Infine, sono in crescita anche i tipi di attacchi informatici su *cloud* principalmente causati da errata configurazione delle risorse *in-cloud*, ma anche dovuti alla crescita di attacchi rivolti direttamente ai fornitori di servizi *in-cloud*.

meno massivo di "*malware*": i principali metodi sono il "*phishing*" e il "*ransomware*"[37]. La maggior parte dei tipi di attacchi sottovalutati ricadono dunque nella categoria di quelli effettuati via mail usando tecniche di *Social Engineering*: *phishing*, la truffa mirata ad ingannare la vittima in modo che consegni suoi dati personali ed usarli fraudolentemente), truffe del CEO (mail per convincere i dipendenti a trasferire fondi verso i conti bancari controllati dai cyber criminali), lo *spoofing* (falsificazione di alcuni dei dati del mittente per ingannare la vittima), i tipi di attacchi informatici di *Business email compromise*, varie tecniche di dirottamento dell'account e la presenza di allegati malevoli. Si tratta di minacce molto sottovalutate e troppo spesso gestite con leggerezza, poca attenzione e senza alcuna prevenzione.

In particolare, il *phishing* è un tipo di frode ideato allo scopo di rubare importanti informazioni sensibili come numeri di carta di credito, *password* e dati relativi al conto bancario. È uno stratagemma per indurre gli utenti a rivelare, con l'inganno, informazioni personali o finanziarie attraverso un'email o un sito *web*, ma sempre più spesso anche tramite messaggi in arrivo sulle più diffuse piattaforme di social media. Gli attacchi di *phishing* vengono avviati con un messaggio di posta elettronica, oppure con un *link* che viene visualizzato improvvisamente su un social *media* oppure con un avviso pubblicato che compare in qualche applicazione usata dall'utente. L'aspetto è quello tipico delle fonti attendibili, quali ad esempio le banche, ed appare come una notifica ufficiale. Con il messaggio l'utente viene invitato a collegarsi ad un sito *web* che ha una grafica simile al sito originale e ad inserire le cruciali informazioni che proteggono la propria sfera digitale, quali, ad esempio, il numero di conto corrente o la *password* di gestione del conto. Ricevute queste informazioni, i truffatori si appropriano dell'identità digitale del malcapitato e compiono l'azione illegale, in questo caso lo svuotamento del conto *on-line*. In sostanza, l'obiettivo del *phishing* è quello di indurre l'utente in errore per poter acquisire in maniera fraudolenta i suoi dati sensibili[38].

La nuova frontiera del *phishing* è il *vishing* (acronimo di *voice phishing*),

37) Tenuto conto dell'aumento, negli ultimi anni, di attacchi di tipo *Advances Persistent Threat* (ATP), principale rischio per la sicurezza nazionale e per la difesa della proprietà intellettuale, si evidenza come la tecnica del *phishing* tramite posta elettronica, anche certificata, sia utilizzata come mezzo di iniziale penetrazione in sistemi opportunamente protetti, nell'ambito di attacchi mirati ad importanti istituzioni pubbliche e società private.

38) Utenti disattenti possono incappare anche nel *brand phishing*, in cui il reindirizzamento di un *link* fraudolento conduce le vittime alla finta pagina *web*, simile al sito *web* ufficiale di un marchio noto, che infetta il *device* del visitatore a vantaggio dei criminali informatici.

un tipo di truffa riferita ad un finto operatore che chiama al telefono le possibili vittime dell'attacco mediante un sistema vocale automatizzato, configurato falsamente per call center di un istituto di credito, verso utenti telefonici e chiedere loro informazioni private.

Con il termine *ransomware* viene indicata una classe di *malware* che rende inaccessibili i dati del computer infettati e chiede il pagamento di un riscatto per ripristinarli. Il *ransomware* è una vera e propria forma di estorsione di denaro in quanto il suo scopo è quello di "sequestrare", cioè rendere indisponibili per l'utente, i file del proprio personal computer attraverso l'inoculazione di un software crittografico la cui chiave è nota solo al malfattore. La cifratura dei file costituisce il sistema *ransomware* più diffuso sebbene non sia l'unico in grado di rendere inutilizzabile il pc dell'utente. L'utente vede comparire un avviso che propone un'offerta: in cambio di una *password* in grado di sbloccare tutti i contenuti, intima di versare una somma di denaro (quasi sempre sotto i 1.000 euro) con pagamento in *bitcoin*, la valuta virtuale.

Il *cyber espionage* è una pratica in continua crescita usata per rubare *know-how* e informazioni riservate alle aziende pubbliche e private che prevede l'utilizzo di TTP (Tattiche, Tecniche e Procedure), *malware*, *tools* offensivi e infrastrutture di attacco da parte di individui, gruppi, o aziende volte ad ottenere vantaggi individuali, economici o commerciali. Può essere impiegato anche da governi stranieri, o da gruppi loro collegati, al fine di implementare la propria sicurezza nazionale, la competitività economica, la capacità militare ed il proprio patrimonio informativo[39].

Lo spionaggio digitale viene considerato come la minaccia più insidiosa

---

Difendersi è possibile aumentando la soglia della consapevolezza del personale mediante formazione e addestramento, ma anche adottando piattaforme che fanno uso di algoritmi di Artificial Intelligence capaci di filtrare la maggior parte delle minacce dopo un appropriato periodo di apprendimento.

39) Nella *Relazione sulla politica dell'informazione per la sicurezza 2019* si rileva che, per quanto riguarda il nostro Paese, l'obiettivo primario dell'attività di intelligence in ambito *cyber* nel 2019 è stato il contrasto ad operazioni di spionaggio digitale posto in essere da "*gruppi strutturati di cui è stata ritenuta probabile – alla luce sia delle ingenti risorse dispiegate, sia della selezione dei target, quasi sempre funzionale al conseguimento di obiettivi strategici e geopolitici – la matrice statuale*".
Come emerge dalla ricognizione effettuata molte aziende, impegnate nei più disparati settori industriali, risultano essere state oggetto di operazioni di cyber spionaggio.
I principali obiettivi perseguiti durante questo tipo di attività sono:
– furto di dati proprietari dell'azienda: operazioni, stipendi, attività di ricerca e sviluppo, ecc.;

per le sue elevate capacità di rimodulazione rispetto alle misure difensive adottate per ridurre la superfice d'attacco. Sono particolarmente offensivi gli effetti di attacchi di spionaggio digitale nel settore dell'aerospazio e della difesa, finalizzati all'acquisizione di segreti industriali e militari.

La tematica riveste particolare rilievo in relazione allo sviluppo dei noti velivoli multiruolo senza pilota rispetto ai quali gli esperti sottolineano come non possano escludersi a priori possibili attacchi volti a penetrare e riconfigurare i relativi sistemi di comando e controllo sfruttando le vulnerabilità del complesso sistema di navigazione satellitare degli UAV[40]. Al fine di impedire determinate operazioni che avrebbero importanti ripercussioni, in termini di perdite economiche e di danno reputazionale, incidendo fortemente sul perseguimento degli obiettivi strategici, è necessario predisporre una serie di misure volte a proteggere il patrimonio più importante di ogni azienda, cioè le informazioni[41].

La categoria del cyber *terrorism*[42] comprende la molteplicità delle azioni informatiche poste in essere dalle organizzazioni del terrorismo a fini di propaganda, denigrazione o affiliazione e, nei casi estremi, per mettere fuori uso, attraverso l'utilizzo della rete o dei controlli telematici, i gangli di trasmissione critica delle strutture o dei processi che attengono la sicurezza nazionale. Gli attacchi informatici di cyberterrorismo puntano a destabilizzare l'ordine sociale con conseguenze molto più estese e danni correlati gravi nel mondo reale. Con l'attività di propaganda, si intende diffondere un pensiero o un'ideologia al fine di conquistare pubblico e convincere le persone ad aderire alla causa e

---

– furto di proprietà intellettuale: progetti riservati, formule, tecniche di produzione, piani commerciali strategici e tutto ciò che un avversario può ritenere di interesse al fine di aumentare la propria competitività commerciale o nazionale;
– informazioni di clienti: liste di clienti, prezzi applicati, servizi forniti, contratti, ecc.;
– furto di informazioni legate al marketing e alla competitive intelligence: obiettivi di marketing a breve e a lungo termine, andamenti del mercato, informazioni su ulteriori competitors, ecc.

40) M. Nones - A. Marrone, *La trasformazione delle Forze armate: il programma Forza Nec*, Edizioni nuova cultura, 2010, p. 49.

41) A. Strippoli Lanternini, *Cyber espionage, una seria minaccia per le aziende: attori criminali e misure di contrasto*, in *https://www.cybersecurity360.it/nuove-minacce*, 3 aprile 2020.

42) Il termine "*cyber terrorismo*" indica l'utilizzo del cyberspazio (Internet) per fini terroristici, ovvero, diffondere la paura e il panico nella popolazione destabilizzando l'ordine e la sicurezza pubblica, per ragioni politiche, ideologiche o religiose. Il *cyber terrorismo* si manifesta con due attività prevalenti: propaganda e attività diretta.

ad apportare il proprio contributo, utilizzando un mezzo di comunicazione che raggiunga il maggior numero di persone possibili. Uno dei mezzi di propaganda più utilizzati, ad esempio, sono i video che vengono veicolati attraverso vari canali, come i *social network*, da parte delle organizzazioni terroristiche di matrice islamista.

L'attività diretta, non meno pericolosa della precedente, è quella che permette di utilizzare direttamente il *cyber spazio* come mezzo per colpire e dare dimostrazione della propria "potenza di fuoco", partendo da attacchi dimostrativi come il *defacement* di un sito *web* sino alla vera e propria intrusione in un sistema informatico anche complesso[43].

Oltre alle fattispecie sopra richiamate, particolare importanza riveste il cyber riciclaggio, noto anche come *cyberlaundering* che mira, avvalendosi del *web*, ad attribuire una parvenza lecita a capitali derivanti da fatti illeciti, come il narcotraffico, lo sfruttamento della prostituzione, il gioco d'azzardo, le estorsioni, i furti, le truffe. Il *cyberlaundering*, recente forma di criminalità che nasce dalla interconnessione tra riciclaggio[44] "*money laundering*" e reato cibernetico "*cybercrime*", è l'uso di un *device* elettronico per realizzare una transazione o un altro atto su beni patrimoniali provenienti da un reato, che comporti:

– la sostituzione o il trasferimento di tali beni;

---

43) Principali obbiettivi di questa attività possono essere ad esempio le infrastrutture critiche di un Paese, non solo per creare malfunzionamenti e diffondere il panico tra la popolazione, ma anche per poter sottrarre informazioni segrete.

44) Ai sensi dell'Art. 648-*ter* del c.p.: "*Chiunque, fuori dei casi di concorso di reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da cinquemila euro a centocinquemila euro. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita nell'ipotesi di cui al secondo comma dell'art. 648. Si applica l'ultimo comma dell'art. 648*". Presupposto necessario del reato di riciclaggio, analogamente a quanto avviene per il reato di ricettazione *ex* art. 648 c.p., è l' antecedente commissione di un altro fatto delittuoso, che peraltro non si richiede sia stato accertato con sentenza passata in giudicato, essendo sufficiente che il fatto delittuoso risulti dagli atti del processo e che quindi il compimento di tale delitto si sia concluso nel momento di inizio della condotta qui disciplinata. Il riciclaggio tradizionale si realizza sostituendo o trasferendo denaro, beni o altre utilità provenienti da delitto non colposo, o compiendo, in relazione ad essi, altre operazioni finalizzate ad ostacolare l'identificazione della loro provenienza delittuosa. È questa la definizione fornita dal legislatore che all'art. 648-*bis* c.p., tra le condotte antigiuridiche punite con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000, colloca ogni attività tesa a ripulire o a disporre dell'oggetto del delitto presupposto (quindi precedente temporalmente), per impedirne un collegamento con lo stesso fatto criminoso e per renderne sconosciuta la provenienza, la titolarità e la destinazione effettiva.

– l'occultamento o la dissimulazione della vera natura dei beni;
– l'acquisizione, il possesso o l'uso di tali beni.

Poiché il *cyberlaundering* è un crimine che si avvale di internet, nel contrasto al fenomeno emergono i problemi connessi tipicamente con questo ambiente e già più volte rassegnati, quali: l'accesso aperto e illimitato alla rete, la mancanza di barriere o confini e l'anonimato[45]. La rete agevola la realizzazione del riciclaggio elettronico, lo rende più semplice e più rapido. Sono diverse le modalità con le quali è possibile commettere il cyber riciclaggio, essendo la sicurezza delle transazioni monetarie telematiche messa a dura prova, data la difficoltà di individuare in Internet i percorsi del denaro veicolato.

1.2.2. *Cybersecurity* e *privacy*: misure per la prevenzione e l'accertamento dei reati cibernetici

Mentre le minacce a cui è esposta costantemente la sicurezza cibernetica aumentano, i conflitti si spostano sempre più verso una dimensione sostanzialmente priva di un'adeguata cornice di diritto internazionale. Nel contempo, la concreta esigenza di misure efficaci di contrasto a gravi forme di criminalità vale anche rispetto a reati "tradizionali", che trovano nelle nuove tecnologie un essenziale ausilio per la loro realizzazione[46]. In questa direzione, alcune novità sul fronte della prevenzione dei reati e dei mezzi di ricerca delle prove sono state introdotte dal decreto-legge n. 7 del 2015, prevalentemente volto a contrastare il terrorismo internazionale.

Il provvedimento ha, infatti, modificato la disciplina delle norme di at-

45) Nella prospettiva del penalista, il principale problema non è tanto l'introduzione di un nuovo reato, quanto la previsione di specifiche misure per assicurare l'identificazione dell'operatore. Nel contrasto al *cyberlaundering*, le misure tradizionali di lotta al riciclaggio-identificazione dell'operatore/cliente, registrazione dell'operatore/cliente, segnalazione delle operazioni sospette limitazioni all'uso del contante devono essere adattate al *cyberspace*. Dalla lettura della norma emerge inoltre che il bene dovrà provenire solo da delitti di natura dolosa, escludendo dunque le contravvenzioni ed i delitti colposi. Il riciclaggio di denaro sporco è un reato plurioffensivo. Tra beni tutelati dalla norma, oltre al patrimonio, visi annoverano l'amministrazione della giustizia, l'ordine pubblico e l'ordine economico. Il riciclaggio è infine un reato comune poiché può essere commesso da chiunque, tranne che dal concorrente nel reato presupposto. Le modalità di realizzazione di tale reato si sono tuttavia evolute nel tempo, principalmente grazie all'impiego massiccio delle nuove tecnologie.

46) Si pensi alle attività preparatorie di attentati terroristici, che possono trovare in Internet un formidabile mezzo di comunicazione e di pianificazione degli attacchi, oppure alla lotta contro la diffusione di materiale pedopornografico on-line.

tuazione del codice processuale penale sulle intercettazioni preventive, anche in relazione ad indagini per delitti in materia di terrorismo commessi con l'impiego di tecnologie informatiche o telematiche, e con riguardo all'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico.

Ha demandato poi alla polizia postale e delle comunicazioni il compito di tenere aggiornata una *black-list* dei siti *Internet* che vengano utilizzati per la commissione di reati di terrorismo, anche al fine di favorire lo svolgimento delle indagini della polizia giudiziaria, effettuate anche sottocopertura ed ha introdotto in capo agli Internet providers specifici obblighi di oscuramento dei siti e di rimozione dei contenuti illeciti connessi a reati di terrorismo pubblicati sulla rete[47]. Il citato decreto-legge ha, inoltre, introdotto una deroga alla disciplina relativa alla conservazione dei dati di traffico telefonico e telematico contenuta nel Codice della privacy, originariamente temporanea e poi stabilizzata nell'ordinamento dalla legge n. 127 del 2017[48].

L'esempio della "*data retention*"[49] è emblematico di quanto le esigenze repressive e preventive di attività criminose che trovano nel *cyberspace* l'am-

47) Sulla *black list* e sui provvedimenti di oscuramento e rimozione adottati, sono introdotti obblighi di relazione in capo al Ministro dell'interno in apposita sezione della Relazione annuale sull'attività delle forze di polizia e sullo stato dell'ordine e della sicurezza pubblica.

48) L'art. 132 del Codice della *privacy*, infatti, dispone che i dati relativi al traffico telefonico sono conservati dal fornitore per 24 mesi dalla data della comunicazione, per finalità di accertamento e repressione di reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per 12 mesi dalla data della comunicazione. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per 30 giorni. Rispetto a questa disciplina, l'art. 4-*bis* del decreto-legge n. 7 del 2015 ha stabilito che per finalità di accertamento e repressione dei reati di terrorismo, fino al 30 giugno 2017, il fornitore deve conservare i dati relativi al traffico telematico (esclusi i contenuti della comunicazione) ed i dati relativi al traffico telefonico. Analogamente, dovranno essere conservati, fino a tale data, anche i dati sulle chiamate senza risposta. È poi intervenuto l'art. 24 della legge n. 167 del 2017 (Legge europea 2017), in base al quale, al fine di garantire strumenti di indagine efficaci in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione di tali reati il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, è stato stabilito in 72 mesi, in deroga a quanto previsto dall'articolo 132 del Codice della *privacy*.

49) Per *data retention* si deve intendere il *periodo di conservazione dei dati*. Il regolamento UE n. 679/2016, non ha previsto sostanzialmente nulla di nuovo rispetto al Codice Privacy (D.lgs. 196/2003) il quale già contemplava, all'art. 11, che i dati personali dovessero es-

biente esclusivo ed ideale di manifestazione ponga problemi in termini di bilanciamento con altri interessi contrapposti, a partire dai diritti fondamentali dell'individuo, quali il diritto all'integrità, sicurezza e riservatezza dei sistemi informatici ed il diritto all'autodeterminazione informativa, da elevare ad espressioni di "tradizionali" diritti fondamentali.

In tale contesto, l'equilibrio tra la protezione dei dati e la tutela della sicurezza cibernetica è complesso ma anche foriero di nuove sfide e sinergie. La tutela della sicurezza cibernetica, quale dimensione rilevante della sicurezza nazionale, può legittimare limitazioni della *privacy*, in nome del contrasto a minacce potenziali alla difesa nazionale, cui deve corrispondere tuttavia il rispetto dei principi di proporzionalità, unico punto di riferimento per controbilanciare esigenze di prevenzione e libertà[50].

Soprattutto in campo economico-finanziario, il rapporto tra protezione dei dati e sicurezza implica che vengano tutelati contemporaneamente i singoli e la collettività. Spesso, infatti, la vulnerabilità dei sistemi utilizzati dai privati incaricati e la negligenza nell'osservanza degli obblighi di protezione ha esposto a rischio la riservatezza dei cittadini e i dati investigativi, con potenziali riflessi sulla sicurezza nazionale.

Ciò conferma come le minacce globali alla sicurezza cibernetica possano essere fronteggiate efficacemente solo in chiave sovranazionale.

2. L'architettura nazionale *cyber* e le nuove frontiere della sicurezza

2.1. L'ecosistema nazionale *cyber*

La capacità dello Stato di gestire i rischi cibernetici sta diventando una

---

sere: "*conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*", per quanto non ne richiedesse la comunicazione esplicita all'interessato. L'esigenza di stabilire un periodo di conservazione dei dati, invero, nasce in materia normativa sui sistemi di gestione, che trova una declinazione specifica nell'ambito della sicurezza delle informazioni (cfr. ISO/IEC 27001). Si tratta, infatti, di un tempo conservativo, come lo è richiesto ad esempio per i dati di *backup*.

50) Anche che il rapporto tra la protezione dati e *cybersecurity* è foriero anche di strategie e reciproche funzionalità. Infatti, mentre la *cybersecurity* implica innanzitutto la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale e quindi la sicurezza nazionale, le eventuali compromissioni di basi dati appartenenti a soggetti pubblici o privati, i cd. *data breach* previsti dalla normativa in materia di tutela dei dati personali, oltre ad assumere importanza per i singoli cittadini interessati, possono essere di rilievo anche per la sicurezza nazionale in funzione della tipologia dei dati acceduti in maniera illegale.

delle priorità strategiche per le amministrazioni pubbliche al fine di assicurare il giovamento e il beneficio dei vantaggi e delle opportunità derivanti da uno spazio cibernetico sicuro per i cittadini e le imprese. Al fine di erigere un sistema in grado di gestire e rispondere alle minacce derivanti, l'Italia ha sviluppato nel corso degli anni documenti programmatici e operativi che costituiscono la struttura nazionale di *cybersecurity*. Questa, a partire dal 2010 ha subito diverse modifiche fino a quando, a febbraio 2017, il decreto Gentiloni ha riorganizzato l'architettura nazionale poi recepita, a marzo dello stesso anno, dal Piano nazionale per la protezione cibernetica e la sicurezza informatica[51].

Al centro della *governance* per la *cybersecurity* il decreto ha posizionato il Dipartimento Informazioni per la Sicurezza[52] (DIS) della Presidenza del Consiglio, organo apicale il cui compito è quello di assicurare unitarietà nella programmazione della ricerca informativa, nell'analisi e nelle attività operative delle agenzie di intelligence AISE e AISI. Il DIS è il *focal point* unico per quanto concerne l'armonizzazione con gli altri Paesi europei, richiesta dalla direttiva NIS, e presiede il *Nucleo Sicurezza Cibernetica* (NSC). Quest'ultimo è un *board* intergovernativo che svolge funzioni di gestione delle crisi cibernetiche e di raccordo tra le diverse componenti dell'architettura istituzionale di *cybersecurity* che è stata inoltre coinvolta nel recepimento, nel 2018, della Direttiva NIS, il cui obiettivo principale è definire un'unica linea strategica tra i vari Stati dell'Unione europea contro il rischio di incidenti ai danni delle reti informatiche e dei sistemi informativi. La linea strategica prevede,

---

51) Il Decreto Gentiloni ha introdotto la necessità della certificazione nazionale per quanto riguarda la valutazione "delle componenti ICT destinate a essere impiegate nei sistemi di soggetti titolari di funzioni critiche o strategiche", che ha poi trovato realizzazione nella previsione del Centro di valutazione e certificazione nazionale (CVCN) avvenuta nel marzo del 2019.

52) Il *Sistema di informazione per la sicurezza della Repubblica* è l'insieme degli organi e delle autorità che nel nostro Paese hanno il compito di assicurare le attività informative allo scopo di salvaguardare la Repubblica dai pericoli e dalle minacce provenienti sia dall'interno sia dall'esterno. Disciplinato principalmente dalla l. 124/2007, il Sistema di informazione per la sicurezza della Repubblica è composto dal Presidente del Consiglio dei Ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'autorità eventualmente delegata dal Presidente del Consiglio, dal Dipartimento delle Informazioni per la Sicurezza (DIS), e dai servizi di informazione: Agenzia Informazioni e Sicurezza Esterna (AISE) e Agenzia Informazioni e Sicurezza Interna (AISI). A sua volta il Comitato parlamentare per la sicurezza della Repubblica (Copasir), composto da cinque deputati e cinque senatori, è l'organo di controllo parlamentare della legittimità e della correttezza costituzionale dell'attività degli organismi informativi (L. 124/2007, artt. 30-38).

nel concreto, la gestione dei rischi, la protezione contro i *cyber* attacchi, l'individuazione di incidenti e la loro riduzione dell'impatto[53].

L'iniziativa che meglio rappresenta gli sforzi profusi dal Paese sotto il profilo delle *policy cyber* è sicuramente quella del "*Perimetro di sicurezza nazionale cibernetica*". Si tratta di un provvedimento che oltre a prevedere obblighi quali il rispetto di stringenti misure di sicurezza e la notifica degli incidenti, indica specifiche disposizioni in materia di forniture di beni, sistemi e servizi ICT, appartenenti a determinate categorie, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici utilizzati dai soggetti inclusi nel Perimetro per l'esercizio della funzione essenziale per la sicurezza nazionale. Il decreto-legge in materia di perimetro di sicurezza nazionale cibernetica si riferisce in particolare a tutti quei servizi e operatori, sia pubblici che privati, che svolgono un ruolo cruciale per gli interessi dello Stato[54].

La responsabilità di attuazione e vigilanza, per quanto riguarda il perimetro, sono condivise dal Ministero per lo sviluppo economico (per quanto concerne le attività che coinvolgono attori privati) e dalla Presidenza del Consiglio (per le attività che coinvolgono il settore pubblico). Si è, pertanto, dato vita ad un'architettura complessa per la molteplicità degli attori interessati, ma chiara nella definizione dei compiti da ciascuno assicurati, sotto un coordinamento unitario assegnato da tutte le più recenti disposizioni al DIS, quale strumento di diretto supporto alle decisioni del Governo e del Presidente del Consiglio in materia di sicurezza cibernetica[55].

In questo senso, il progressivo rafforzamento dell'architettura nazionale

---

53) Gestire, proteggere, individuare e ridurre: questi i quattro pilastri della linea comune di sicurezza.

54) In tal senso, vi possono essere delle sovrapposizioni con alcuni degli operatori dei servizi essenziali già soggetti alla Direttiva NIS e, in tal caso, essi dovranno continuare a ottemperare alle disposizioni previste dalla Direttiva stessa, aggiungendo *on top* eventuali prescrizioni previste dal perimetro di sicurezza nazionale cibernetica.

55) In questa direzione si è mosso, infatti, già il d.P.C.M. del 17 febbraio 2017 che ha riorganizzato l'architettura nazionale cibernetica, prevedendo la collocazione presso il DIS del Nucleo per la Sicurezza Cibernetica (NSC), che opera a supporto del Presidente del Consiglio e del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. A seguire, con il decreto legislativo 18 maggio 2018, n. 65, è stata recepita la Direttiva UE NIS, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi nei Paesi dell'Unione. In tale contesto, il DIS opera quale Punto di contatto unico NIS, con il compito di coordinare, a livello nazionale, le questioni relative alla sicurezza delle reti e dei

di sicurezza cibernetica perseguito dal 2018 ad oggi ha mirato ad accrescere la resilienza *cyber* del Paese, garantendo, al contempo, unicità di indirizzo e un alto livello di coordinamento attraverso un approccio univoco a una materia complessa e trasversale a diversi settori e realtà. Al raggiungimento di tale traguardo hanno contribuito specifiche misure normative che hanno attribuito al comparto intelligence un ruolo centrale nell'ecosistema cyber nazionale.

All'istituzione, presso il DIS, del *Nucleo per la Sicurezza Cibernetica* (NSC)[56], del *Computer Security Incident Response Team* (CSIRT) italiano[57] e del punto di contatto unico NIS previsto dal decreto legislativo n. 65 del 2018, si è aggiunta, più di recente, l'assegnazione di funzioni di raccordo con le autorità competenti e con i soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica, nonché di supporto al Presidente del Consiglio nell'implementazione di tale disciplina (decreto-legge n. 105 del 2019 convertito, con modificazioni, nella legge n. 133 del 2019).

Molteplici sono, pertanto, i compiti assegnati dal sistema descritto, con una conseguente proiezione delle attività in diversi ambiti di intervento che vanno – in sinergia con gli attori interessati dell'ecosistema nazionale *cyber* – dall'elaborazione delle *policy* in materia di *cybersecurity* e dei contributi per la definizione di atti sovranazionali alla gestione delle *crisi cyber*, dallo svolgimento delle attività dello CSIRT alla realizzazione di analisi tecniche a supporto della sua operatività, per concludere con la promozione di nuove progettualità in materia di innovazione digitale, volte a far sì che l'evoluzione tecnologica dell'Italia sia al passo con gli altri Paesi, in particolare europei, e tenga in debita considerazione gli aspetti di *cybersecurity*.

L'Italia, come gli altri Paesi membri, è stata chiamata, ai sensi della Di-

---

sistemi informativi e, a livello europeo, la cooperazione transfrontaliera, nonché dal 6 maggio 2020 anche come CSIRT italiano. Quest'ultimo è destinatario delle notifiche di incidente da parte degli Operatori di servizi essenziali/Fornitori di servizi digitali (NIS) e dei fornitori di reti e servizi di comunicazione elettronica/Telco (Decreto ministeriale adottato il 12 dicembre 2018, in attuazione del "Codice delle comunicazioni elettroniche"), nonché delle notizie di *data breach* rilevanti ai fini della sicurezza cibernetica, ricevute dall'Autorità garante per la protezione dei dati personali, in virtù del nuovo "*Protocollo d'intenti sulla protezione dei dati personali nelle attività di sicurezza cibernetica*", siglato con il DIS nel marzo 2019.

56) Come disposto dal decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017, art. 8.

57) Come disposto dal decreto del Presidente del Consiglio dei Ministri 8 agosto 2019, art 3.

rettiva NIS, ad indicare quali fossero gli operatori di servizi essenziali e digitali dai quali dipende la società e l'economia del Paese (ad esempio quelli del settore energetico, dei trasporti, ma anche quelli finanziario e sanitario). Inoltre, come sopra accennato, la direttiva ha reso obbligatoria l'istituzione di un unico *Computer Security Incident Response Team*, detto CSIRT, in ogni Paese membro, al quale vengono affidati compiti di natura tecnica nella prevenzione e risposta a incidenti informatici da svolgere in cooperazione con gli altri CSIRT europei. A ciò si affianca l'estensione del *Golden power* per garantire la sicurezza delle nuove infrastrutture di telecomunicazione, in particolare quelle 5G. I poteri speciali sono esercitati nella forma di imposizione di specifiche prescrizioni o condizioni ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale.

2.1.1. Evoluzione delle *policy cyber* a livello nazionale

Negli ultimi anni si sono dunque registrati, a livello sia europeo sia nazionale, interventi sul piano normativo e regolamentare, mirati ad accrescere i complessivi livelli di *cybersecurity*. Come si è già detto, l'Europa ha adottato la Direttiva NIS ed il cd. "*Cybersecurity Act*", in vigore dal giugno 2019, il quale ha, tra l'altro, istituito un quadro europeo di certificazione per prodotti, processi e servizi ICT con l'obiettivo di garantirne la sicurezza per tutto il loro ciclo di vita[58].

Al riguardo, se il 2019 è stato caratterizzato dalla definizione dell'atto normativo e dal relativo iter parlamentare che ha condotto alla sua adozione, il 2020 si è connotato per l'elaborazione dei relativi provvedimenti attuativi tra i quali si annoverano:

– il d.P.C.M. n. 131 del 2020 per la definizione dei criteri per l'identificazione dei soggetti da includere nel Perimetro e di quelli per l'individuazione dei relativi "*beni ICT perimetro*"[59];

– il d.P.C.M. (in fase avanzata di approvazione) per la definizione delle

58) Il *Cybersecurity Act* (Regolamento UE 2019/881) dispone che "*al fine di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cyber-security, cyber-resilience e fiducia all'interno dell'Unione, è istituito un quadro per l'introduzione di sistemi europei di certificazione della sicurezza informatica*".

59) Per "bene ICT" si intende, come da d.P.C.M., l'insieme di reti, sistemi informativi e servizi informatici che permettono le funzioni essenziali dello Stato e l'erogazione dei servizi essenziali.

modalità di notifica degli incidenti e delle misure di sicurezza, comprese quelle sul *procurement* ICT;

– il regolamento – approvato in via definitiva dal Consiglio dei Ministri il 29 gennaio 2021 – relativo alle ispezioni e alle modalità di scrutinio tecnologico da parte del Centro di Valutazione e Certificazione Nazionale (CVCN) e degli altri Centri di Valutazione (CV)[60].

– il d.P.C.M. contenente le categorie di prodotti ICT da sottoporre alle valutazioni del CVCN e dei CV in fase di *procurement* da parte dei soggetti perimetro, esaminato dal Comitato Interministeriale per la Sicurezza della Repubblica (CISR) a fine novembre 2020;

– il d.P.C.M. relativo all'accreditamento e ai raccordi tra CVCN, CV e laboratori. Nel citato d.P.C.M. n. 131 del 2020, in attuazione del criterio di gradualità contemplato dal decreto-legge n. 105 del 2019, sono stati definiti 11 settori di attività, all'interno dei quali devono essere poi individuati i soggetti da includere nel Perimetro[61].

2.1.2. Il perimetro di sicurezza nazionale cibernetica

Il perimetro di sicurezza nazionale cibernetica, i cui confini normativi sono definiti dalla legge 18 novembre 2019 n. 133[62], intende assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle Amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale.

L'attuazione del perimetro è coordinata dal Presidente del Consiglio, avvalendosi del DIS, che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni ai sensi del decreto e con i soggetti inclusi nel perimetro. In tal senso, la menzionata legge si prefigge l'obiettivo di tutelare gli *asset* digi-

---

60) Questi ultimi chiamati ad effettuare verifiche e valutazioni dei beni, dei sistemi e dei servizi ICT che i soggetti inclusi nel Perimetro di Sicurezza nazionale cibernetica intendano acquisire qualora, tramite questi ultimi, vengano erogati e garantiti servizi essenziali al Sistema Paese.

61) Il 25 novembre 2020, su proposta del CISR, previa indicazione da parte delle Amministrazioni competenti, è stato adottato dal Presidente del Consiglio dei Ministri l'atto – non soggetto a pubblicazione e per il quale è escluso il diritto di accesso – contenente l'elencazione dei soggetti inclusi nel Perimetro ai quali, come previsto, il DIS ha dato la relativa comunicazione, il 22 dicembre. Alla luce di quanto descritto, da giugno 2021 inizierà, quindi, l'operatività del "sistema Perimetro", specie in materia di notifiche di incidenti cibernetici.

62) Conversione in legge del decreto-legge 21 settembre 2019, n. 105 sul "*perimetro di sicurezza nazionale cibernetica*".

talizzati che afferiscono alla sicurezza nazionale, prevedendo, rispetto alla direttiva NIS, più stringenti criteri di notifica e livelli di sicurezza, nonché specifiche procedure in materia di *procurement* ICT, così da consentire al Paese di fronteggiare adeguatamente le sfide poste dall'evolversi della minaccia *cyber* nelle sue molteplici forme[63].

Gli obblighi in capo ai soggetti perimetro si sostanziano nella:

– notifica degli incidenti[64] aventi impatto sui "*beni ICT perimetro*"[65], così da assicurare un immediato flusso di informazioni a favore delle strutture deputate alla prevenzione, preparazione e gestione degli eventi cibernetici (in particolare NSC e CSIRT, entrambi incardinati nel DIS);

– adozione di misure di sicurezza per i "*beni ICT perimetro*" relative a organizzazione, processi e procedure, anche in relazione al *procurement* ICT;

– azione di *screening* tecnologico degli approvvigionamenti ICT, destinati ai "*beni ICT perimetro*". La procedura prevede che il soggetto che intenda procedere a tali acquisizioni ne dia comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN, operante presso il Ministero dello sviluppo economico) che, entro un massimo di 60 giorni, può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software[66] (questi ultimi devono essere conclusi nel termine di ulteriori 60 giorni).

---

63) La legge 133 del 2019 interviene anche su procedure, modalità e termini ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici individuati nell'elenco trasmesso alla Presidenza del Consiglio dei Ministri e al Ministero dello sviluppo economico.

64) Nel decreto del Presidente del Consiglio dei Ministri 30 luglio 2020 n. 131, all'art. 2 viene specificato che si parla di incidente per "*ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*". L'art. 3 disciplina l'obbligo e le modalità di notifica a seguito di incidenti. Viene stabilito che, nel caso di incidente, l'azienda violata è tenuta ad informare, entro 6 ore al massimo (e non, come previsto dalla direttiva NIS, entro le 24 ore dal malfunzionamento) il CRSIRT (*Computer security incident response team*) cioè il gruppo di esperti istituito presso il DIS. Quando l'intrusione è grave, si attiva il Nucleo per la sicurezza cibernetica, che propone al Presidente del Consiglio delle ipotesi di risposta all'attacco e coordina il ripristino del servizio. I soggetti inserito nel perimetro di sicurezza nazionale cibernetica rischiano sanzioni fino a 1,5 milioni di euro se non comunicano l'incidente o attacco informatico.

65) Per "*bene ICT*" si intende, come da d.P.C.M. 30 luglio 2020 n.131, l'insieme di reti, sistemi informativi e servizi informatici che permettono le funzioni essenziali dello Stato e l'erogazione dei servizi essenziali.

66) Tali attività sono svolte dai Centri di Valutazione (CV) dei Ministeri dell'interno e della

Il 30 luglio 2020 è stato approvato, con il d.P.C.M. n. 131, il regolamento in materia di *perimetro di sicurezza nazionale cibernetica*[67], che stabilisce le modalità e i criteri procedurali di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica, tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge n.105 del 2019. Il suddetto regolamento istituisce anche il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica, che supporterà il CISR tecnico[68].

Vengono altresì individuati i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica[69].

Nello sviluppo dell'architettura nazionale della *cyber* sicurezza il Sistema di informazione per la sicurezza della Repubblica ha acquisito un ruolo strategico, prima con il d.P.C.M. 24 gennaio 2013 e, successivamente, con il d.P.C.M. 17 febbraio 2017 e il decreto legislativo n. 65 del 2018. Il Presidente del Consiglio, che dirige ed ha la responsabilità generale della politica dell'informazione e della sicurezza – secondo quanto stabilito dall'articolo 1 della legge n. 124 del 2007 – provvede alla tutela della sicurezza nazionale anche nello spazio cibernetico[70] (d.P.C.M. 17 febbraio 2017).

---

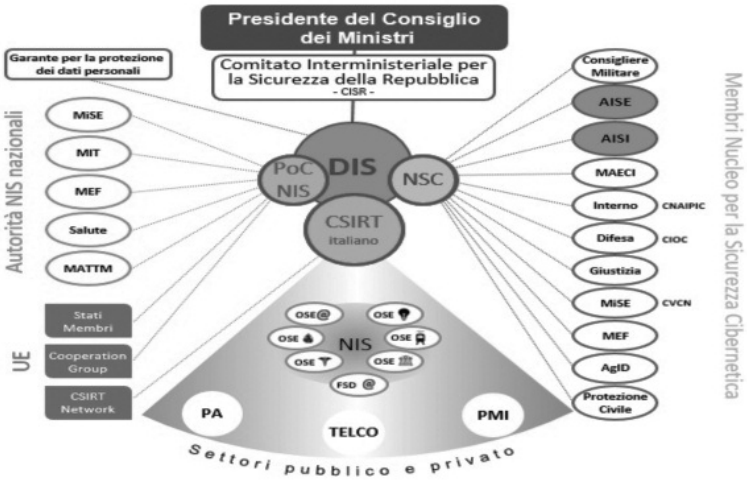
difesa – in stretta sinergia con il CVCN – per le forniture di beni, sistemi e servizi ICT da impiegare sulle rispettive reti, sistemi e servizi informatici.

67) Pubblicato sulla Gazzetta ufficiale n. 261 del 21 ottobre 2020.

68) Il supporto tecnico all'attività del CISR è assicurato dall'organismo collegiale di coordinamento istituito presso il DIS dal d.P.C.M. 24 gennaio 2013, denominato "CISR tecnico" dal d.P.C.M. 17 febbraio 2017 (art.3).

69) Per l'individuazione dei soggetti da includere nel perimetro, le Amministrazioni (Ministero dell'interno, Ministero della difesa, Ministero dello sviluppo economico, Ministero dell'economia e delle finanze, ecc.) predispongono una lista di soggetti – indentificando funzioni e servizi essenziali – e la trasmettono al CISR tecnico. L'elenco dei soggetti inclusi nel perimetro sarà contenuto in un atto amministrativo, adottato e periodicamente aggiornato dal Presidente del Consiglio dei ministri, su proposta del CISR.

70) In particolare, in questo settore il Presidente del Consiglio:
– provvede, nelle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale, a convocare il CISR;
– adotta e aggiorna, su proposta del CISR, il quadro strategico nazionale per la sicurezza dello spazio cibernetico;
– adotta, su deliberazione del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica contenente gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il quadro strategico nazionale;



Schema illustrativo dell'ecosistema italiano cyber. Fonte: Relazione sulla politica dell'informazione per la sicurezza 2020.

In materia di *cybersecurity* il CISR, oltre ai generali compiti di consulenza e proposta nei confronti del Presidente del Consiglio sopra richiamati, ha autonomi poteri di impulso e vigilanza indicati nel d.P.C.M. 17 febbraio 2017 (art. 4) quali:

– l'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico;

– l'approvazione di linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, nonché per la condivisione delle informazioni e per l'adozione di *best pratices* e di misure rivolte all'obiettivo della sicurezza cibernetica;

– l'elaborazione di indirizzi generali e obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali;

– la promozione di iniziative necessarie per assicurare la piena partecipazione dell'Italia ai consessi di cooperazione internazionale, quali quelli in ambito NATO e UE.

– emana le direttive per l'attuazione del Piano nazionale;
– impartisce, sentito il CISR, le direttive al DIS e alle Agenzie per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali.
Inoltre, adotta, sentito il CISR, la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale e le linee di indirizzo per l'attuazione della strategia di sicurezza cibernetica (D.lgs. 65/2018, art. 6).

Infine, il CISR può formulare le proposte di intervento normativo ed organizzativo ritenute necessarie a potenziare le misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi.

Il supporto tecnico all'attività del CISR è assicurato dall'organismo collegiale di coordinamento istituito presso il DIS dal d.P.C.M. 24 gennaio 2013 e presieduto dallo stesso direttore del DIS. L'organismo è stato denominato "CISR tecnico" dal d.P.C.M. 17 febbraio 2017 (art. 3).

La funzione di coordinamento del DIS comprende l'attività di verifica dei risultati sia delle analisi globali da sottoporre al CISR, sia dei progetti di ricerca informativa sui quali decide il Presidente del Consiglio, sentito il CISR (ai sensi dell'articolo 4 della legge n. 124 del 2007).

Schema gli organismi di certificazione nazionali. Fonte: Franchina L., PhD, presentazione Hermesbay, marzo 2020.

2.2. Il coordinamento interforze: gli organismi *cyber investigation* delle forze di polizia e della Difesa

Se la trasformazione digitale comporta un ripensamento del modello architetturale, l'esigenza di tale cambiamento evidenza nuove criticità sul fronte della sicurezza, che vanno affrontate e risolte tenendo conto di un contesto nuovo e di requisiti diversi. Attualmente si assiste infatti ad una riorganizzazione nei Ministeri per rinforzare le difese dello *spazio cyber* nazionale ed approntare le relative strategie di *cyber investigation*.

Schema riassuntivo delle competenze generali in materia cyber delle forze di polizia.

2.2.1. Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche della Polizia di Stato (CNAIPIC)

Il processo di riorganizzazione del Dipartimento della pubblica sicurezza ha previsto l'istituzione della *Direzione centrale per la sicurezza cibernetica*, articolazione destinata ad assorbire le funzioni e le attribuzioni dell'attuale Servizio di Polizia postale e delle comunicazioni.

La futura Direzione centrale avrà principalmente compiti di prevenzione, contrasto e repressione dei crimini informatici e sarà suddivisa in tre servizi: uno di tipo amministrativo per gli affari generali e due operativi. Il primo servizio gestirà il contrasto del cyber bullismo, dei reati associati al fenomeno del *sexting*[71] e più in generale i delitti che vedono coinvolte le cosiddette "fasce deboli", mentre il secondo conterrà al suo interno il *Centro di valutazione del Ministero dell'interno* (CEVA) deputato alle valutazioni tecniche sugli affidamenti di forniture di beni, sistemi e servizi basilari per l'espletamento dei servizi informatici.

Inoltre, il 26 aprile u.s, presso la Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza, è stato inaugurato il *Cyber security operations center* (C-Soc), struttura d'avanguardia finanziata dai fondi europei, per la prevenzione e l'intervento tempestivo sugli incidenti alle ban-

71) Per *sexting* si intende generalmente lo scambio di messaggi, audio, immagini o video – specialmente attraverso smartphone o chat di social network – a sfondo sessuale o sessualmente espliciti, comprese immagini di nudi o seminudi.

che dati delle forze di polizia, di natura accidentale, naturale o dolosa, come gli attacchi hacker[72].

Il *Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche* della Polizia di Stato (CNAIPIC) è l'unità specializzata, attualmente interna al Servizio di Polizia postale e delle comunicazioni[73] dedicata alla prevenzione e alla repressione dei crimini informatici diretti ai danni delle infrastrutture critiche nazionali.

L'operatività del CNAIPIC si realizza attraverso l'esercizio di un Settore operativo e di un Settore tecnico[74].

Il Centro si avvale di una Sala operativa, disponibile 24 ore su 24 e 7 giorni su 7, in qualità di punto di contatto univoco dedicato sia alle infrastrutture critiche, dai collegamenti telematici esclusivi, dedicati e protetti, tra il CNAIPIC e le IC per il condiviso, reciproco e costante trasferimento dei dati e delle informazioni utili all'esercizio delle funzioni di valutazione, prevenzione e repressione delle minacce e dei crimini informatici[75].

---

72) Alla Direzione centrale della polizia criminale fanno capo i sistemi informativi per finalità di polizia, come il sistema informatico interforze Ced-Sdi, il Nue 112, la banca dati del Dna, il Sistema informativo Shengen Nazionale. La funzione del C-Soc è quella di vigilare sulla sicurezza di milioni di informazioni possedute per finalità di polizia (sulle persone, sui documenti, sui veicoli, sulle tracce) affinché siano adeguatamente protette. L'obiettivo è quello di garantire, oltre alla sicurezza del sistema in termini di riservatezza, integrità e disponibilità, la protezione dei dati personali per evitare la dispersione (cosiddetto *data breach*), secondo il principio introdotto dalla direttiva europea 680 del 2016 sul trattamento dei dati per finalità di polizia e di giustizia.

73) Con decreto interministeriale del 19 gennaio 1999, il Servizio Polizia postale e delle comunicazioni viene indicato quale "*organo centrale del Ministero dell'interno per la Sicurezza e la Regolarità dei servizi di telecomunicazioni*". La peculiarità di questa specialità è di avere un Servizio centrale da cui dipende il CNAIP e il CNCPO e i commissariati di PS *on-line*. Il CNAIPIC è stato istituito nell'ambito del Dipartimento della pubblica sicurezza del Ministero dell'interno dall'art. 7-*bis*, comma 1 del d.P.R. 144/2005. La competenza della Polizia delle comunicazioni si distribuisce su un servizio centrale dotato di 20 compartimenti regionali e 80 sezioni provinciali.

74) Il Settore operativo supporta le funzioni di Sala operativa, *Intelligence* e Analisi. Il Settore tecnico è deputato alla gestione ed all'esercizio dell'infrastruttura tecnologica del CNAIPIC e dei collegamenti telematici con le infrastrutture critiche convenzionate, ai processi di individuazione, *testing* ed acquisizione di risorse strumentali ed alla pianificazione di cicli di formazione ed aggiornamento del personale.

75) Il *first response team* è composto da operatori abilitati a rispondere nell'immediatezza del danno subito nonché a ricevere le informazioni, svolgono dunque una attività di monitoraggio su i fenomeni contingenti. Ogni analista è specializzato su un tipo di attacco. Il centro, quando scatta l'emergenza, comincia a lavorare in una situazione di emergenza.

Il Centro ha registrato un andamento crescente del numero di attacchi che, nel corso del 2020, hanno riguardato anche strutture sanitarie[76]. Gli investigatori hanno contribuito, con altri organi di polizia e di intelligence, alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo sia a livello nazionale che internazionale, monitorando circa 36 mila spazi *web* e rimuovendo numerosi contenuti inneggianti alla jihad. Con il crescente uso di strumenti telematici, sono state implementate le campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete, rivolte soprattutto ai giovani. In particolare, la campagna "*Una vita da Social*"[77] negli anni, ha permesso di entrare in contatto con oltre 2 milioni e mezzo di studenti, 220.000 genitori e 125.000 insegnanti, sia nelle piazze che nelle scuole[78].

Una polizia del futuro non potrà dunque non considerare la dimensione cibernetica. Dal CNAIPIC si passerà verosimilmente ai nuclei operativi per la sicurezza cibernetica secondo un sistema non più centrale ma neuronale. In tal senso si delinea l'evoluzione naturale della costituenda Direzione centrale per la sicurezza cibernetica, il cui obiettivo sarà dunque quello di unificare sotto la stessa cabina di regia il CERT (*Computer emergency response team*), la Polizia postale, il CNAIPIC e il Centro nazionale che combatte la pedopornografia *on-line*.

Le notizie acquisite diventano sviluppabili dall'unità investigativa che ha si rapporta con l'autorità giudiziaria, creando una osmosi tra attività investigativa e attività di prevenzione che si autoalimentano reciprocamente.

76) Cfr. *Resoconto della Polizia postale nel 2020*, w*ww.poliziadistato.it*., 04/01/2021. In particolare, nel 2020 sono stati rilevati 507 episodi, a fronte dei 239 dell'anno precedente che hanno portato all'arresto di 21 persone e alla denuncia di 79.

77) Campagna i sensibilizzazione in collaborazione con la Polizia di Stato. Il progetto "*Una vita da social*" vuole calarsi nella filosofia dei giovani interlocutori, interagendo con un linguaggio comunicativo semplice ma esplicito, adatto a tutte le fasce di età, coinvolgendo così dai più piccoli ai docenti ai genitori, con la finalità di combattere la violenza e la prevaricazione dei giovani bulli.

78) Nel corso del *lockdown* l'attività di sensibilizzazione e prevenzione nelle scuole è proseguita attraverso piattaforme di video conferenze. Il rapporto della Polizia Postale, che si riferisce a una analisi relativa al periodo gennaio-dicembre 2020, evidenzia come l'emergenza epidemiologica abbia favorito l'attività criminale condotta con un crescente numero di attacchi informatici e truffe on-line ai danni sia delle infrastrutture critiche che dei comuni cittadini, denotando sia nel caso di attacchi diretti alle grandi infrastrutture erogatrici di servizi essenziali che in quelli apparentemente isolati, diretti a singoli enti, imprese o cittadini, una organizzazione criminale ben strutturata e spesso operante a livello transnazionale. Per tale motivo l'azione di contrasto ai reati di varia natura attuata dal CNAIPIC è stata orientata soprattutto ad assicurare interventi di tipo proattivo e di protezione in

2.2.2. Il Nucleo speciale tutela privacy e frodi tecnologiche del Corpo della Guardia di finanza

La presa di coscienza delle gravi minacce al sistema Paese derivanti dall'utilizzo illecito delle nuove tecnologie, ha portato la Guardia di finanza a rafforzare il dispositivo di contrasto alle conseguenti condotte criminali che impattano sul tessuto economico e finanziario, peraltro in continua evoluzione[79], istituendo il Nucleo speciale tutela privacy e frodi tecnologiche[80].

Il reparto, con sede in Roma, ha competenza sull'intero territorio nazionale[81] ed è composto da personale in possesso di qualifica CFDA, "*Computer forensic data analysis*", deputato a:

– elaborare, integrare e analizzare i dati (*data analysis*) acquisiti nel corso dell'attività investigativa;

– dare supporto tecnologico alle investigazioni per la raccolta di elementi di prova sui sistemi informatici[82] (*computer e network forensics*).

Il Nucleo ha avviato un percorso di scambio informativo con l'*Istituto Superiore delle Comunicazioni e Tecnologie dell'informazione* (ISCT) che, inquadrato nell'ambito del Ministero dello sviluppo economico, si rivolge specificatamente verso le aziende operanti nel settore ICT e l'utenza e riguarda fondamentalmente i servizi alle imprese, la normazione, la sperimentazione e la ricerca di base e applicata, la formazione e l'istruzione specializzata nel campo delle telecomunicazioni. In tema di sicurezza cibernetica, il protocollo prevede che il *Nucleo* possa fornire il proprio qualificato supporto su specifica

---

79) Fonte: Senato della Repubblica, *Audizione 4^ Commissione* (Difesa), audizione Col. G. di F. G. Reccia, Indagine conoscitiva "*I profili della sicurezza cibernetica attinenti alla difesa nazionale*", Roma, 6 agosto 2020.

80) Il Nucleo tutela privacy e frodi tecnologiche opera costantemente gli approfondimenti in rete, sia attraverso metodologie di *Open Source Intelligence* (cd. O.S. Int.), sia mediante sofisticate tecniche di reperimento analisi e filtraggio delle informazioni rinvenute, al fine di isolare potenziali risorse web dedite ad attività illecite.

81) Il Comando generale del Corpo della Guardia di finanza, sin dal 2001, aveva avvertito l'esigenza di istituire un Reparto che quotidianamente fosse impegnato in prima fila in un contesto operativo in esponenziale sviluppo tecnologico, dove gli interessi delle organizzazioni criminali avevano individuato un florido ambiente per proseguire i propri obiettivi in danno del settore economico-finanziario.

82) Il ruolo del Nucleo risulta fondamentale per ricercare ogni elemento utile ai fini dell'individuazione dei soggetti collegati al terrorismo di matrice confessionale, con particole riferimento ai dati, notizie e documenti espressivi, in particolare, di sintomatologie indiziarie di finanziamento del terrorismo.

attivazione del Dicastero in caso di eventi complessi o per situazioni di particolare necessità e gravità[83].

2.2.3. Le capacità *cyber* della Difesa: il *Comando per le Operazioni in Rete* (COR Difesa) e il CERT Difesa

Tra i soggetti pubblici che fanno parte dell'architettura strategica nazionale di *cyber security* un posto di rilievo assumono le strutture della Difesa preposte alla protezione delle reti e dei sistemi digitali delle forze armate quale elemento essenziale per la condotta delle operazioni e la protezione delle informazioni. Il *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* attribuisce, infatti, al dicastero il compito di dotarsi della capacità di pianificare, condurre e sostenere operazioni nello spazio cibernetico e questo per prevenire, localizzare ed individuare la minaccia cibernetica[84].

La Difesa italiana, al pari dei principali Paesi della comunità internazionale, sta da tempo rafforzando le proprie capacità nel dominio cibernetico, sia attraverso apposite strutture di comando e controllo per lo svolgimento di operazioni nel *cyber space*, sia studiando le diverse sfaccettature di tale dominio al fine di poter operare in contesti interconnessi e/o federati[85]. A sua volta il

---

83) Allo stesso modo nel 2018 è stata stipulata dalla Guardia di finanza un'intesa protocollare con l'Agenzia per l'Italia digitale finalizzata alla collaborazione del Nucleo speciale nelle attività ispettive svolte dall'Agenzia nei confronti dei concessionari di servizi di identità digitale SPID e dei servizi di PEC, rivolti ai cittadini.

84) Nel dettaglio, in base a quanto previsto nel *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, spetta al Ministero della difesa definire e coordinare la politica militare, la *Governance* e le capacità militari nell'ambiente cibernetico; pianificare, condurre e sostenere operazioni (*Computer Network Operations* - CNO) nello spazio cibernetico atte a prevenire, localizzare, difendere (attivamente e in profondità), contrastare e neutralizzare ogni possibile minaccia e/o azione avversaria cibernetica, portata alle reti, ai sistemi ed ai servizi della Difesa sul territorio nazionale o nei teatri operativi fuori dai confini nazionali, nel quadro della propria missione istituzionale. In tale quadro, la Difesa negozia le intese e gli accordi internazionali di disciplina della materia, coordina le proprie attività nel settore cyber-militare con NATO, EU e le Difese di atri Paesi amici e alleati.

85) È stato avviato, fin da subito, un processo evolutivo virtuoso, in linea, peraltro, con le priorità e gli obiettivi definiti dapprima in ambito NATO, che ha dichiarato il *Cyberspace* un "dominio" operativo a tutti gli effetti al pari di quelli tradizionali (*Land, Maritime, Air*), e poi recepiti anche in ambito EU dalla Direttiva NIS. Tale processo è teso, da un lato, a realizzare solide capacità di *Cyber Defence* attraverso la realizzazione dei vari progetti di ammodernamento delle proprie infrastrutture ICT e, dall'altro, ad attuare un significativo cambiamento organizzativo.

Piano nazionale per la protezione cibernetica ha previsto inizialmente la realizzazione del *Comando Interforze per le Operazioni Cibernetiche* (CIOC) deputato alla protezione dei sistemi e delle reti del Dicastero della difesa, nonché all'effettuazione delle operazioni in campo cibernetico[86].

Il Ministero della difesa, nella consapevolezza che lo scontro tra gli Stati sposta sempre più spesso il suo fronte verso il "*quinto dominio*", ossia lo spazio cibernetico[87], ha avviato una riorganizzazione che riunisce sotto un unico comando gli uffici che si occupano *cybersecurity* di Aeronautica, Marina, Esercito, Carabinieri e Dicastero tramite la creazione, il 9 marzo 2020, del *Comando per le Operazioni in Rete* (COR), struttura di vertice alle dirette dipendenze del Capo di SMD che coordinerà l'attività *cyber* del Ministero e delle forze armate[88].

In parallelo ha cominciato ad operare il neo Ufficio generale sullo spazio, che sarà prodromico al Comando Operazioni Spaziali (COS), con il compito di coordinare le attività militari nel cosmo[89]. L'obiettivo è "*alzare la cyber defence*", ossia rendere ancora più forte lo scudo delle reti delle forze armate e, in parallelo, migliorare la risposta in caso di attacco.

---

86) A tal proposito si ricorda che nell'ottobre 2018 la NATO ha annunciato l'istituzione a Mons, nell'ambito della struttura di Comando NATO, del *Cyberspace Operations Centre* (CYOC) che sarà pienamente operativo nel 2023. Da collegare all'istituzione del CIOC la definizione di un apposito protocollo d'intesa attraverso il quale il Comparto *intelligence* e lo Stato maggiore della Difesa hanno elaborato un quadro strategico e tattico allineato, tale da permettere il miglior posizionamento del costituendo CIOC con riguardo all'operatività nel dominio digitale anche alla luce dell'esperienze in corso di sedimentazione nell'Alleanza atlantica.

87) Nel suo ultimo rapporto 2020 il CLUSIT, l'Associazione italiana per la sicurezza informatica, riconosce che *l'aspetto più problematico del "new normal" è la possibilità per gli Stati di far "scivolare" senza troppo clamore la gestione dei propri conflitti sempre più verso il piano "cyber", innalzando continuamente il livello dello scontro senza dover fare ricorso a eserciti e armamenti tradizionali*. Una tattica che, concludono gli esperti, apre a "una fase storica di cyber-guerriglia permanente, sempre più feroce anche se non dichiarata.

88) L. Zorloni, in *https://www.wired.it/amp/270448/internet/regole/2020/02/06/cybersecurity-difesa-interni/Dalla Difesa agli Interni, nascono i super team per la cybersecurity*, 6 febbraio 2020.

89) Parte del pacchetto COR sarà anche l'ufficio spazio, a cui spetta scrivere la strategia di difesa nel cosmo. In futuro, quest'ultimo dovrebbe trasformarsi in un comando dedicato, che dovrà monitorare un'altra frontiera strategica per il Paese, visto che lo spazio viene adoperato per attività sensibili come telecomunicazioni, monitoraggio delle infrastrutture e osservazione della terra per studio e business.

Il COR[90] rappresenta l'elemento dell'organizzazione attraverso il quale la Difesa intende riordinare e razionalizzare il settore, per conseguire i seguenti fondamentali obiettivi:

– la direzione, il coordinamento ed il controllo "unitario" nella gestione, in sicurezza, dei sistemi ICT/C4 in servizio;

– la chiara definizione di "pertinenze" e "compiti", sia in area interforze che nel rapporto tra le articolazioni di vertice e le corrispondenti articolazioni delle F.A.;

– l'adozione di un approccio "concorsuale" e la realizzazione di modelli organizzativi uniformi da parte delle F.A., quali presupposti necessari per una gestione maggiormente sinergica e meno dispendiosa dei sistemi in servizio;

– "omogeneità" e "coerenza" negli sviluppi capacitivi, favorendo investimenti più rispondenti; ciò, perseguendo una visione architetturale univoca e l'uniformità tecnologica nel settore di cui trattasi;

– la ricerca dell'"interforzizzazione" di quelle funzioni e servizi ICT che più logicamente e vantaggiosamente si prestano ad una gestione centralizzata.

L'infrastruttura ICT, che il COR Difesa gestisce e di cui garantisce la sicurezza, è in realtà una combinazione di architetture tecnologiche con finalità ed utenti diversi[91], sviluppatesi nel tempo secondo percorsi distinti, che garantisce la fruibilità dei servizi applicativi della Difesa mediante un'infrastruttura di *Private cloud* che consente la virtualizzazione e il bilanciamento delle risorse che, nel processo in atto, consentirà di conseguire anche la piena capacità di "continuità operativa" dei servizi in caso di avaria agli assetti primari (funzione di *Business continuity*), nonché di automatizzare i meccanismi di ripristino dei sistemi in caso di avaria (funzione di *Disaster recovery*)[92].

---

90) Il *Comando per le Operazioni in Rete* (COR) ha la missione di garantire, con visione unitaria e coerente, la condotta delle operazioni nel dominio cibernetico, la gestione tecnico-operativa in sicurezza di tutti i sistemi di *Information & Communications Technology/C4* della Difesa, al fine di armonizzare e distribuire tempestivamente le informazioni prodotte dai sistemi di comando e controllo, *computing, intelligence surveillance & reconnaissance*, necessarie ad abilitare le funzioni del CINC (Comandante in capo) e dei Comandi interessati.

91) Vds. 4ª Commissione (Difesa) del Senato, *Profili della sicurezza cibernetica attinenti alla Difesa nazionale*, Audizione del Vice Comandante del Comando per le operazioni in rete, Gen. Div. C. Massara, Roma, 3 giugno 2020.

92) Il COR Difesa gestisce – in modo accentrato ed a favore di tutte le F.A. – anche l'adeguamento, l'espansione, l'evoluzione e la manutenzione della Rete Integrata della Difesa

Il CERT Difesa, che nelle situazioni di crisi riguardanti i sistemi della difesa, coordina le attività da porre in essere, si articola in due organismi: il CERT *Coordination center*[93] e il CERT *Technical center*[94]. I due CERT svolgono attività di indirizzo, coordinamento e informazione rispetto ai CERT delle singole forze armate.

Nell'Arma dei Carabinieri, i compiti di controllo e monitoraggio e di risposta a eventuali incidenti informatici nonché di analisi proattiva per garantire la sicurezza dell'infrastruttura tecnologica da minacce provenienti sia dall'interno sia dall'esterno sono affidati, rispettivamente, al SOC (*Security Operation Center*) e al CERT (*Computer Emergency Response Team*), unità costituite all'interno del Ce.Si.T. (*Centro di Sicurezza Telematica*) del Comando generale[95].

Il CERT dell'Arma, in particolare, è in costante contatto con i CIRT (*Computer Incident Response Team*) di forza armata e, soprattutto, con il COR - Comando per le Operazioni in Rete, al cui interno è inglobato il CERT Difesa, unico referente operativo del Dicastero per gli aspetti cyber nell'ambito del Nucleo sicurezza cibernetica attivato in seno al DIS. Il COR, nel ga-

---

(RID), in via di totale migrazione alla tecnologia IP, inclusa la sua componente nell'area di ROMA (*Metropolitan Area Network* - MAN), nonché l'*Intranet* dell'Area di vertice interforze (DIFENET). Inoltre, il *Comando per le operazioni in rete* esprime anche una capacità di pianificazione, conduzione e realizzazione dell'intera gamma delle "operazioni militari" nel dominio cibernetico, interfacciandosi con il Centro *intelligence* interforze, per il necessario supporto di *Cyber intelligence*, ed in concorso al Comando operativo di vertice interforze e al Comando interforze per le operazioni delle forze speciali, mediante l'impiego di *Cellule Operative Cibernetiche* (COC) con capacità di proiezione anche "fuori area".

93) Il CERT *Coordination Center,* costituito in seno al II Reparto (Informazioni e Sicurezza) dello Stato maggiore della Difesa svolge attività di informazione e di allertamento anche a scopo di prevenzione e collabora e condivide informazioni con i corrispondenti CERT nazionali e internazionali (come quello della NATO, il Nato *Computer Incident Response Capability* o NCIRC).

94) Il CERT *Technical Center* in seno al Comando C4 Difesa, a sua volta inserito nel VI Reparto (Sistemi C4I e Trasformazione) dello Stato maggiore della Difesa, è invece preposto a prevenire, rilevare e contenere sul piano tecnico-operativo gli incidenti informatici, oltre che a coordinare e supportare l'azione dei CERT di Forza armata in caso di emergenza cibernetica. Il CERT Technical Center è quindi l'organo preposto alla gestione tecnico-operativa di tutti gli assetti e sistemi di *Information and Communication Technology* del comparto Difesa.

95) Posto alle dirette dipendenze del Capo del III Reparto che è, ai sensi dell'art. 543 del Testo unico dell'ordinamento militare, dirigente generale responsabile dei sistemi informativi automatizzati per l'Arma dei Carabinieri (D.G.Re.S.I.A.).

rantire un tempestivo e aderente scambio informativo, assicura la necessaria attività di prevenzione e preparazione ad eventuali situazioni di crisi nonché l'attivazione delle procedure di allertamento. In tale ambito è all'attenzione l'ipotesi di costituzione di un'unità di Polizia militare info/investigativa, composta da personale dell'Arma specializzato, non limitato alla sola parte *Cyber*, in grado di fronteggiare anche minacce, interne e/o esterne.

Il Reparto indagini telematiche del ROS (Raggruppamento operativo speciale), articolato su tre Sezioni, oltre a provvedere alle attività di *digital forensics*, di *Internet investigation* e di *Cyber defence* per le reti e i sistemi, assicura il supporto tecnico alle attività di Polizia militare nei settori della *cyber-security* del comparto Difesa. Quando il supporto richiede un ulteriore, elevata specializzazione interviene il Ra.C.I.S. (Raggruppamento Investigazioni Scientifiche) con il Reparto tecnologie informatiche, che, strutturato su tre Sezioni (Informatica, Elettronica e Cibernetica), garantisce capacità di indagini tecnico-scientifiche su materiale di alta tecnologia (es. memorie di massa complesse, sistemi elettronici, reti e banche dati), attraverso l'estrazione e l'analisi dei dati, anche da dispositivi artigianali, ovvero non standard, la decriptazione dei dati cifrati, nonché attività di *Network forensics*, la *Cyber forensics* e la *Database forensics*.

2.3. Il rafforzamento delle istituzioni di *law enforcement* e la creazione di nuovi strumenti di coordinamento

Attraverso gli interventi statali sul perimetro di sicurezza cibernetica si è cercato di perseguire il coinvolgimento, armoniosamente, di tutte le componenti che potevano offrire un valore aggiunto.

Una volta che viene fatto salvo il principio della riserva sovrana sulla sicurezza nazionale occorre infatti contrapporre, in modo convinto e coordinato, un'altra "rete": quella dei rapporti collaborativi, declinati all'insegna dell'efficienza, dell'efficacia e dell'immediatezza di risultati. Motivo, questo, per cui le relazioni con le forze di polizia degli altri Paesi, le forme di collaborazione all'interno di Interpol ed Europol e le attività nei gruppi internazionali dedicati ad esempio del G7 e dell'Ocse, oltre a rappresentare un essenziale momento di confronto su problematiche e criticità comuni, devono essere sviluppate col massimo impegno, poiché costituiscono fattori essenziali per lo scambio informativo e per l'aggiornamento sulle tecnologie e sulle tecniche investigative.

Il nostro Paese è coinvolto, specie con riguardo ai negoziati di documenti di policy e atti normativi, in ambito ONU, OSCE, UE, NATO, G7 e G20.

Per quel che concerne gli sforzi profusi dall'UE per rafforzare la resilienza ad attacchi *cyber*, è giunto a termine nel dicembre 2020 il negoziato, avviato nel 2018, della "*Proposta di Regolamento per la creazione di un Centro di competenza europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di cybersecurity e della rete dei Centri di coordinamento nazionali*", volta a promuovere la sovranità tecnologica e la leadership dell'UE e dei suoi Stati membri e, conseguentemente, ad accrescerne l'autonomia strategica nel settore e la competitività industriale.

Nell'ambito dei tavoli europei un contributo è stato, altresì, fornito con riguardo a ruolo e funzioni che la futura *Joint cyber unit*[96] andrebbe a svolgere in seno all'ecosistema *cyber* dell'Unione, quale strumento volto a coordinare le diverse realtà europee competenti, a vario titolo, in materia di sicurezza cibernetica.

L'intervento normativo dell'UE più recente in tale settore è la direttiva (UE) n. 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. Gli elementi chiave della direttiva, sostitutiva della precedente decisione quadro 2001/413/GAI del Consiglio, sono: l'ampliamento della portata dei reati, che secondo il nuovo regime include, tra l'altro, le transazioni mediante valute virtuali; l'armonizzazione delle definizioni di alcuni reati *on-line*, quali la pirateria informatica o il *phishing*; l'introduzione di livelli minimi per le sanzioni più elevate per le persone fisiche; norme in materia di competenza giurisdizionale riguardo le frodi transfrontaliere; il miglioramento della cooperazione in materia di giustizia penale; la prevenzione e le attività di sensibilizzazione per ridurre i rischi di frodi.

3. Strategie e politiche europee e nazionali di sicurezza cibernetica

3.1. Nuova strategia UE di sicurezza cibernetica: la direttiva "NIS 2" e la direttiva ICE

Come si è avuto modo di analizzare nel proseguo di questo studio, L'UE ha progressivamente rafforzato le misure volte a contrastare la criminalità informatica, articolando il proprio intervento con riferimento a tre principali categorie di illeciti:

96) A suo tempo annunciata dal Presidente della Commissione europea Von Der Leyen e parte integrante della "*Strategia dell'UE per la cybersecurity nel decennio digitale*", varata il 16 dicembre 2020.

– gli attacchi alle reti e ai sistemi informatici;

– la perpetrazione di reati di tipo comune (ad esempio, crimini essenzialmente predatori) tramite l'uso di sistemi informatici;

– la diffusione di contenuti illeciti (ad es. pedopornografia, propaganda terroristica, *hate speech*/discorso di odio, ecc.) per mezzo di sistemi informatici.

Le politiche di contrasto alle attività illecite e dolose basate sull'uso di sistemi informatici, comprese le iniziative in materia di disinformazione, sono state trattate nei più recenti Consigli europei, in occasione dei quali i leader dell'UE hanno, tra l'altro, chiesto la conclusione dei procedimenti legislativi dei principali strumenti normativi proposti dalla Commissione europea, e dato impulso a nuove iniziative nel campo della *cybersicurezza*[97].

La direttiva NIS definisce *obblighi di sicurezza* per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, l'assistenza sanitaria e la finanza) e i fornitori di servizi digitali (mercati *on-line*, motori di ricerca e servizi di *cloud*), stabilendo, inoltre, che ogni Paese dell'UE è tenuto a designare una o più autorità nazionali per monitorare l'applicazione della direttiva, nonché elaborare una strategia per affrontare le minacce informatiche[98].

L'UE ha recentemente consolidato tale quadro mediante l'adozione del regolamento sulla cybersicurezza n. 2019/881[99] (cd. "*cybersecurity act*"), recante una serie di disposizioni per:

– rafforzare l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), che si tramuterà in *Agenzia UE per la cybersicurezza*;

– introdurre sistemi europei di certificazione della cybersicurezza dei

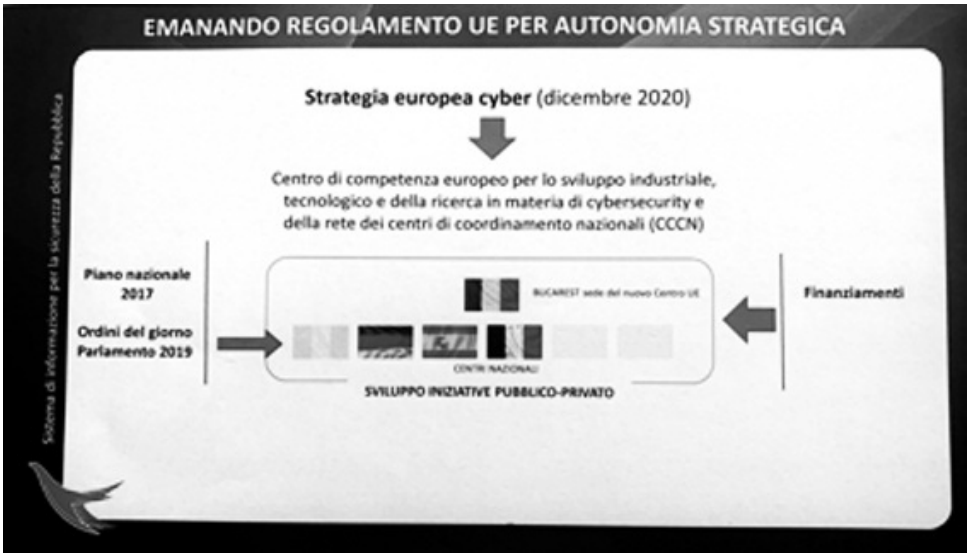
97) Consiglio europeo 28-29 giugno 2018; Consiglio europeo 17-18 ottobre 2018; Consiglio europeo 13-14 dicembre 2018; Consiglio europeo 20-21 giugno 2019.

98) Per minacce ibride – nozione per la quale non esiste una definizione sul piano giuridico universalmente accettata – la Commissione europea intende *una serie di attività che spesso combinano metodi convenzionali e non convenzionali e che possono essere realizzate in modo coordinato da soggetti statali e non statali pur senza oltrepassare la soglia di guerra formalmente dichiarata*. Il loro obiettivo non consiste soltanto nel provocare danni diretti e nello sfruttare le vulnerabilità, ma anche nel destabilizzare le società e creare ambiguità per ostacolare il processo decisionale.

99) Regolamento (UE) n. 2019/881, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento UE n. 526/2013.

prodotti e dei servizi ITC nell'Unione (consistenti in norme, requisiti tecnici e procedure).

Nello stesso ambito, inoltre, il 17 aprile 2019, il Parlamento europeo ha adottato la propria posizione in prima lettura[100] – e il 20 aprile u.s. il Consiglio europeo ha dato il suo via libera – circa la proposta di regolamento istitutivo di un centro europeo di ricerca e di competenza sulla cybersicurezza, affiancato da una rete di centri analoghi a livello di Stati membri. Tra gli obiettivi chiave dell'emanando regolamento, il miglioramento del coordinamento dei finanziamenti disponibili per la cooperazione, la ricerca e l'innovazione in tale ambito.



Schema illustrativo dell'emanando regolamento UE. Fonte: Sistema di informazione per la sicurezza della Repubblica.

La Commissione europea ha dunque annunciato due nuove direttive sui temi della protezione delle infrastrutture critiche e della *cyber security*: la Direttiva NIS 2[101] – che revisiona la *Network and information security* – e la Direttiva ICE che revisiona la direttiva 114/08 sulle infrastrutture critiche euro-

100) Rimane solo il voto in seconda lettura del Parlamento europeo, previsto nel corso della sessione plenaria di metà magio 2021. Poi il regolamento verrà pubblicato sulla Gazzetta ufficiale dell'Unione europea ed entrerà in vigore 20 giorni dopo. Da quel momento gli Stati membri avranno sei mesi di tempo per individuare l'istituto nazionale che si collegherà con il centro di Bucarest.

101) L'aggiornamento della direttiva NIS si è reso necessario alla luce dell'accelerazione del processo di digitalizzazione connessa all'attuale pandemia e all'aumento delle minacce

pee. La proposta di revisione della direttiva NIS si accompagna dunque ed inevitabilmente ad una Direttiva sulla resilienza dei soggetti critici, volta ad introdurre misure a tutela di aziende ed enti operanti in settori critici rispetto a minacce alla loro sicurezza fisica[102]: si tratta di un connubio fondamentale, data la natura sempre più ibrida delle minacce[103]. Il loro combinato disposto può cambiare lo scenario della *cyber security* europea[104].

Entrando nel merito delle proposte europee, le istanze che portano alla sua proposizione sono state raccolte dalla Commissione con un sondaggio sottoposto a tutti gli Stati membri. È emerso che il livello di *cyber security* nel *business* è ancora basso in tutta Europa, che il livello di resilienza è ancora inconsistente in molti settori e in molti Paesi, che manca una condivisione delle informazioni che sia organizzata, costante e che veda tutti gli Stati membri

---

cybernetiche collegate alla stessa. Ad esempio, in alcuni Stati membri, gli ospedali del sistema sanitario non sono stati inclusi tra i soggetti sottoposti all'obbligo di adottare le misure di sicurezza imposte dalla NIS, e sono quindi risultati maggiormente esposti a minacce cibernetiche della crisi legata alla Covid-19. Si osserva come non saranno più i singoli Stati membri ad identificare gli "operatori di servizi essenziali" soggetti agli obblighi della Direttiva, ma è la direttiva stessa a definire il proprio ambito di applicazione. Ciò è dovuto al fatto che, nella pratica, gli attuali criteri per l'identificazione degli "operatori di servizi essenziali" sono risultati poco chiari e sono stati applicati in maniera diversa nei diversi Stati membri.

102) La Commissione ha presentato a dicembre 2020 anche la proposta legislativa volta ad aggiornare la Direttiva NIS per raggiungere un più elevato livello comune di sicurezza informatica in tra l'Unione e una nuova direttiva sulla resilienza delle entità critiche che coprano un'ampia gamma di settori. Entrambe le nuove direttive mirano ad affrontare i rischi attuali e futuri sia *on-line* sia *offline*: dagli attacchi cibernetici alla criminalità o ai disastri naturali, in modo coerente e complementare.

103) Con la suddetta proposta di riforma delle norme sulla sicurezza delle reti e dei sistemi di informazioni, la Commissione europea si pone l'obiettivo di aumentare il livello di resilienza informatica dei settori pubblici e privati critici: ospedali, reti energetiche, ferrovie, ma anche *data center*, amministrazioni pubbliche, laboratori di ricerca e produzione di dispositivi medici e medicinali critici, nonché di altre infrastrutture e servizi critici con l'obiettivo di renderli "impermeabili" in un contesto di minaccia sempre più rapido e complesso.

104) Cfr. *Documento di sicurezza nazionale 2020. Allegato alla relazione annuale al Parlamento ai sensi dell'art. 38, comma 1-bis, legge 124/2007*. L'implementazione della Direttiva NIS ha previsto le attività propedeutiche, in sede UE per la revisione della direttiva UE 114/2008 sulle Infrastrutture Critiche Europee (ICE), al fine di garantire l'armonizzazione delle due normative, evitando in tal modo eventuali accresciuti oneri per gli operatori. Analogamente, di stretta intesa con il Ministero dell'economia e delle finanze, si è proceduto rispetto all'avvio delle negoziazioni a livello UE relative alla proposta di Regolamento sulla resilienza operativa digitale per il settore finanziario ("DORA").

partecipare allo stesso modo, e infine che manca una organizzazione di gestione delle crisi europea comune. La direttiva proposta individua due tipi di "grandi potenziali vittime": le definisce entità, essenziali e importanti. Le entità "essenziali" sono individuate in: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio.

La novità interessante è l'ingresso delle "entità importanti", quindi con obblighi minori, ma comunque attenzionati. Questi sono individuati nei servizi postali e corrieri, smaltimento rifiuti, manifattura, produzione e distribuzione di prodotti chimici, produzione, elaborazione e distribuzione di alimenti, manifattura e provider di servizi digitali.

La Direttiva ICE 2 è dedicata al tema della resilienza delle entità critiche rispetto a minacce fisiche, o, come si usa dire oggi, *cinetiche*. Essa incaricherà le autorità competenti di condividere informazioni e intraprendere misure complementari alla NIS 2, riguardanti la resilienza cinetica. Gli operatori pubblici e privati che saranno identificati sotto l'egida di tale direttiva saranno soggetti a maggiori e più chiari obblighi di protezione e resilienza.

La NIS 2 imporrà di adottare una strategia nazionale di *cybersecurity* in ogni Stato membro, con una autorità competente alla attuazione designata per legge. Gli operatori essenziali e importanti avranno obblighi di valutazione e gestione del rischio, di notifica all'autorità competente e di condivisione delle informazioni. Il tenore della proposta evidenzia un legislatore molto più maturo, consapevole e deciso a concretare una vera svolta europea sul tema cyber. Tuttavia, lo scopo della Direttiva era soprattutto uniformare il concetto di infrastruttura critica, cosa che è stata raggiunta anche se il panorama normativo in termini di sicurezza è comunque divergente nei vari Paesi europei.

Gli operatori verranno identificati e designati sulla base di una analisi del rischio basata su indicatori standardizzati e saranno soggetti a obblighi aggiuntivi riguardanti la resilienza da minacce cinetiche. L'analisi del rischio prenderà in considerazione minacce naturali e antropiche, inclusi incidenti, disastri naturali, emergenze di pandemie pubbliche, minacce antagoniste e terroriste. Viene inoltre costituito un gruppo per la resilienza delle entità critiche[105].

---

105) Secondo L. Franchina, *Cyber security, le due nuove direttive europee che cambieranno tutto*, in *https://www.agendadigitale.eu*., 18 gennaio 2021, la proposta è un'ottima controparte della NIS 2, volta a garantire che la sicurezza tutta, e non solo la *cyebrsecurity*, sia curata, normata e attenzionata opportunamente. Finalmente un panorama completo sulle Infrastrutture critiche, che riconosce a queste e ai loro operatori una necessità di protezione e sicurezza a tutto tondo e non solo *cyber*.

L'obiettivo dell'UE è quello di rafforzare ulteriormente la cooperazione tra gli Stati membri e sviluppare capacità di difesa informatica all'avanguardia, basandosi sul lavoro dell'Agenzia europea per la difesa e incoraggiando gli Stati membri ad avvalersi pienamente della cooperazione strutturata permanente e del fondo europeo per la difesa.

Schema illustrativo della nuova strategia europea di sicurezza cybernetica. Fonte: Sistema di informazione per la sicurezza della Repubblica.

3.2. Sviluppo delle reti di nuova generazione (5G)

Il 5G, il nuovo standard di comunicazione mobile che consente velocità e connessioni multiple sino ad ora impensabili, viene considerato cruciale per una connettività di alta qualità nell'intero territorio dell'Unione, ai fini del completamento del mercato unico digitale e a sostegno dell'innovazione in tutti settori. A tal proposito, la direttiva (UE) n. 2018/1972 che istituisce il Codice delle comunicazioni elettroniche, ha previsto che entro il 2020 tutti gli Stati membri dell'UE avessero assegnato le frequenze necessarie per l'introduzione della rete 5G[106].

106) A tal proposito si ricordano:
– la risoluzione non legislativa (2019/2575 (RSP), adottata dal Parlamento europeo il 12 marzo 2019, sulle "*minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione a livello di Unione per ridurre tali minacce*". Nell'atto di indirizzo si esprime forte preoccupazione in relazione alla possi-

La quinta generazione di sistemi di telecomunicazione mobili e senza fili (5G) offre una connessione superveloce che supporta, oltre ai singoli utenti, un ingente numero di dispositivi e oggetti connessi, cioè l'apparato noto come "*Internet delle cose*" *(Internet of things)*. Si compie in tal modo un balzo rivoluzionario rispetto agli standard precedenti delle reti 3G e 4G[107]. Essa costituirà un fattore abilitante per lo sviluppo di molti servizi digitali e le relative reti 5G saranno l'infrastruttura portante non solo di nuovi servizi di comunicazione elettronica, ma anche di una vasta gamma di servizi essenziali, quali l'energia, i trasporti, i servizi bancari e sanitari, i sistemi di controllo industriale.

Il 5G, inoltre, tramite le sue soluzioni tecniche, basate sullo sfruttamento di elevate porzioni dello spettro elettromagnetico e anche sulla diffusione capillare di antenne e microcelle, assicurando estesa copertura della rete, grande velocità di trasferimento, elevato numero di connessioni simultanee a bassissima latenza, incrementerà in maniera esponenziale l'utilizzo dell'*internet of things* e dei *big data* all'interno della società. Come rilevano gli esperti, si tratta di un insieme molto ampio di servizi che presentano diversi aspetti di vulnerabilità da considerare, ai fini della messa in sicurezza della relativa rete.

L'attenzione della Commissione europea rispetto alla sicurezza delle reti 5G degli Stati membri è stata costante. In tale ambito, in continuità con le ini-

---

bilità che le infrastrutture cinesi per le reti 5G possano avere incorporate delle '*backdoors'* in grado di consentire a fornitori ed autorità cinesi un accesso non autorizzato ai dati personali e alle telecomunicazioni nell'UE;

– la comunicazione congiunta del "*UE - Cina una prospettiva strategica*" della Commissione europea e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, nella quale si sottolinea la necessità di un approccio comune per la cybersicurezza delle reti 5G;

– la raccomandazione del 26 marzo 2019, con la quale la Commissione europea (in attuazione dell'indirizzo espresso dal Consiglio europeo del 22 marzo 2019 a favore di un approccio concertato alla sicurezza delle reti 5G) propone un approccio comune dell'UE ai rischi per la sicurezza delle reti 5G, basato su una valutazione coordinata dei rischi e su misure coordinate di gestione dei rischi, su un quadro efficace per la cooperazione e lo scambio di informazioni e su una conoscenza comune della situazione delle reti di comunicazione.

107) Secondo uno studio della Commissione europea, con l'introduzione delle capacità della rete 5G si otterranno benefici del valore di 113 miliardi di euro all'anno in quattro importanti settori strategici: automobilistico, sanitario, dei trasporti ed energetico. Lo studio indica inoltre che, negli Stati membri, gli investimenti per il 5G creeranno probabilmente 2,3 milioni di posti di lavoro.

ziative avviate con la raccomandazione del 26 marzo 2019, il NISCG (*NIS Cooperation Group*) ha adottato il Toolbox[108] delle misure di sicurezza, pubblicato il 29 gennaio 2020. Il Toolbox contiene una serie di misure strategiche e tecniche, nonché azioni di supporto destinate, su base volontaria, agli Stati membri al fine di promuovere un approccio armonizzato alla sicurezza delle reti 5G[109].

Un altro motivo per cui il 5G richiede un approccio concertato a livello di UE risiede nella natura transfrontaliera della sua infrastruttura e delle potenziali minacce per la sicurezza. Qualsiasi vulnerabilità significativa o incidente di *cybersicurezza* riguardante le reti in uno Stato membro si ripercuoterebbe su tutta l'UE che, pertanto, negli ultimi anni, ha destinato a progetti per il 5G negli Stati membri finanziamenti consistenti, tra cui prestiti dalla Banca europea per gli investimenti[110].

Le reti 5G costituiranno un'ulteriore tecnologia abilitante per la trasmissione di servizi digitali ancora più pervasivi nei settori essenziali. Tutti gli Stati membri hanno avviato un processo di revisione e rafforzamento delle misure di sicurezza in vista del 5G, anche se in alcuni Paesi i lavori sono ancora in corso e che dunque non sono state ancora adottate misure definitive[111].

---

108) Sulla base dei risultati emersi dal *risk assessment* coordinato dell'Unione europea, il *toolbox* delinea una serie di misure di sicurezza che permettono un'efficace mitigazione dei rischi al fine di progettare e implementare le reti 5G in modo sicuro in tutta Europa.

109) Fonte: *Relazione sulla politica dell'informazione per la sicurezza*, 2020. Al riguardo, come descrive la relazione, l'Italia non si è limitata ad uniformarsi alle citate linee guida, ma le ha recepite all'interno dell'ordinamento giuridico nazionale. Attraverso il cd. Decreto liquidità (D.l. n. 23/2020, convertito dalla legge n. 40/2020), la disciplina sul *Golden Power* (D.l. n. 21/2012 convertito, con modificazioni, dalla legge n. 56/2012) è stata, infatti, emendata prevedendo un richiamo alle linee guida europee, e quindi al Toolbox, quale riferimento per il processo istruttorio delle notifiche relative all'acquisto di tecnologia 5G da fornitori extra-europei.

110) Il piano d'azione dell'UE prevedeva il varo dei servizi 5G in tutti gli Stati membri entro la fine del 2020; a ottobre di quest'anno, il 5G era disponibile in 17 Paesi dell'UE e nel Regno Unito. Eventuali ritardi nel raggiungere un'appropriata copertura 5G, così come i problemi di sicurezza, potrebbero avere enormi implicazioni per la competitività e l'indipendenza strategica dell'UE.

111) Nell'ambito del pacchetto di strumenti, gli Stati membri hanno convenuto di rafforzare i requisiti di sicurezza mediante una possibile serie di misure ad hoc, in particolare per valutare i profili di rischio dei fornitori, applicare le restrizioni pertinenti per i fornitori considerati ad alto rischio (comprese le necessarie esclusioni per gli *asset* chiave considerati critici e sensibili, come le funzioni della rete centrale) e predisporre strategie per garantire la diversificazione dei fornitori. Le misure volte a limitare la partecipazione dei fornitori sulla base del loro profilo di rischio sono già in vigore in alcuni Stati membri e in una fase avanzata di preparazione in molti altri.

Il modo in cui il 5G sarà offerto nell'UE influirà su molti aspetti della vita dei cittadini, grazie a sviluppi quali la sanità elettronica, le automobili intelligenti e le reti elettriche intelligenti. Il 5G avrà ripercussioni anche sull'opera di digitalizzazione in Europa e, data la sua natura transfrontaliera, sul funzionamento del mercato unico. È indispensabile, pertanto, che questa nuova fondamentale tecnologia trovi una realizzazione rapida, sicura e concertata.

Lo sviluppo correlato al 5G porterà nuove sfide per le autorità di sicurezza e, per superarle, sarà necessaria un'azione di concerto tra tutte le istituzioni interessate al fine di delineare un piano d'azione efficace. Sarà fondamentale uno sforzo comune per raggiungere lo sviluppo tecnologico, consapevoli che non esiste un rischio zero in termini di sicurezza né un automatismo immediato in termini di benefici economici[112].

3.3. *Golden power* e sicurezza cibernetica nel nuovo assetto asimmetrico degli equilibri globali

Il decreto-legge n. 105 del 2019, nell'introdurre il perimetro della sicurezza cibernetica, ha costituito anche l'occasione per un ulteriore rafforzamento del c.d. *golden power*, con precipuo riferimento alle reti di comunicazione elettronica a banda larga con tecnologia 5G, secondo una nuova linea evolutiva sviluppata nella legislazione nazionale a partire dal 2012.

L'esigenza di assicurare ogni possibile tutela agli assetti strategici nazionali ha indotto dunque il Governo a dare corso, dopo gli aggiornamenti del 2019, a nuovi, mirati interventi normativi intesi a rafforzare il dispositivo. Sul piano legislativo, il riferimento è alle modifiche al decreto-legge n. 21 del 2012 introdotte dagli articoli 15 e 16 del decreto-legge n. 23 del 2020 (cd. "Liquidità") – convertito, con modificazioni, dalla legge n. 40 del 2020 – che hanno ampliato gli strumenti a disposizione del decisore politico per contrastare il rischio di acquisizioni predatorie od opportunistiche di aziende e di *asset* strategici per il Paese da parte di investitori esteri[113].

Particolare attenzione è stata rivolta alla tutela degli attivi di rilevanza

112) I maggiori organismi di standardizzazione internazionale sono al lavoro per implementare un insieme di standard di sicurezza internazionali (SCAS e NESAS) con molteplici vantaggi sia per i fornitori di apparecchiature e gli operatori di rete, sia per i singoli Stati.

113) Tra le principali novità apportate dal decreto si segnala, in particolare, l'introduzione di un regime temporaneo, che ha esteso (inizialmente fino al 31 dicembre 2020, poi fino al 30 giugno 2021) l'ambito di applicazione della disciplina *Golden Power* rispetto al regime ordinario (ad es. sottoponendo a scrutinio anche gli acquisti, da parte di investitori europei,

strategica nel settore finanziario, creditizio e assicurativo, in quello del trattamento e dell'archiviazione dei dati, nonché dell'accesso e controllo di dati e informazioni sensibili[114]. Attraverso le previsioni del decreto-legge n. 21 del 2012, dunque, nel recepire la giurisprudenza europea, in specie attraverso la definizione della minaccia che legittima il ricorso ai poteri speciali – individuata nel *grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale* – è stato introdotto l'obbligo, relativamente ai settori della difesa e della sicurezza nazionale (oltre che relativamente ad ambiti ritenuti strategici quali l'energia, i trasporti e le telecomunicazioni), di preventiva notificazione alla Presidenza del Consiglio dell'acquisto di partecipazioni in società che detengono infrastrutture strategiche.

Il decreto delinea i presupposti che legittimano l'esercizio di tali poteri ed il loro contenuto, secondo i principi di proporzionalità ed adeguatezza ed alla luce della potenziale influenza dell'acquirente sulla società, anche in ragione della entità della partecipazione acquisita, con definizione dei criteri di valutazione della minaccia che considerano anche "*la sussistenza di legami fra l'acquirente e paesi terzi che non riconoscono i principi di democrazia o dello Stato di diritto, che non rispettano le norme del diritto internazionale o che hanno assunto comportamenti a rischio nei confronti della comunità internazionale, desunti dalla natura delle loro alleanze*" [articolo 1, comma 3, lettera b].

Nel procedimento definito da tale disciplina (decreto-legge e relativi atti attuativi), che presuppone la gestione da parte della società di *asset* strategici[115], nel caso di una minaccia da fronteggiare, viene dunque legittimato il ricorso a poteri prescrittivi, interdittivi e oppositivi[116].

---

di partecipazioni di controllo in società che detengono *asset* di rilevanza strategica). Inoltre, il legislatore ha previsto: il rafforzamento della tutela *Golden Power* nell'ambito finanziario (incluso quello creditizio e assicurativo); l'introduzione di norme che prevedono e disciplinano il potere della Presidenza del Consiglio di avviare d'ufficio il procedimento per l'esercizio dei poteri speciali, nei casi in cui sia stata accertata una violazione dell'obbligo di notifica; in tema 5G, l'inserimento, tra i criteri guida dello scrutinio operato ai sensi dell'art. 1-*bis*, d.l. n. 21/2012, di un riferimento esplicito ai principi e agli attori internazionali, che, facendo ricorso a strumenti competitivi non convenzionali, tendono ad insidiare quote di mercato e *know how* pregiato della nostra industria.

114) Fonte: *Relazione del 12 dicembre 2019 del Comitato parlamentare per la sicurezza della Repubblica*, nella quale si richiama l'esigenza della tutela "sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale".

115) Le categorie degli *asset strategici* sono state individuate con il regolamento recato dal decreto del Presidente della Repubblica n. 85 del 2014, mentre con il decreto del Presi-

L'impianto che ne è scaturito ha, nel complesso, assicurato un equilibrio tra libertà di iniziativa economica ed interessi sensibili in settori strategici, delineando l'esercizio della discrezionalità dei poteri pubblici, con un certo livello di trasparenza e di certezza per gli operatori e con adeguate garanzie di

---

dente della Repubblica n. 86, emanato in pari data, sono state definite le procedure per l'attivazione dei poteri speciali. In particolare, l'art. 3 del citato decreto del Presidente della Repubblica n. 85 ha individuato, con riferimento al settore delle comunicazioni tre categorie: le reti dedicate, la rete di accesso pubblica agli utenti finali in connessione con le reti metropolitane, i router di servizio e le reti a lunga distanza; gli impianti utilizzati per la fornitura dell'accesso agli utenti finali dei servizi rientranti negli obblighi del servizio universale e dei servizi a banda larga e ultralarga. La disposizione specifica, altresì, l'inclusione degli elementi dedicati, anche laddove l'uso non sia esclusivo, per la connettività (fonia, dati e video), la sicurezza, il controllo e la gestione relativi a reti di accesso di telecomunicazioni in postazione fissa.

116) B. Bruno, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *Federalismi.it*, Rivista di diritto pubblico, comparato, europeo, ISSN 1826-3534, n. 14/2020. L'art. 1, comma 1 del d.l. n. 21 del 2012, prevede, in particolare, la possibilità di: «*a) imposizione di specifiche condizioni relative alla sicurezza degli approvvigionamenti, alla sicurezza delle informazioni, ai trasferimenti tecnologici, al controllo delle esportazioni nel caso di acquisto, a qualsiasi titolo, di partecipazioni in imprese che svolgono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale; b) veto all'adozione di delibere, atti od operazioni dell'assemblea o degli organi di amministrazione di un'impresa di cui alla lettera a), aventi ad oggetto la fusione o la scissione della società, il trasferimento dell'azienda o di rami di essa o di società controllate, il trasferimento all'estero della sede sociale, la modifica dell'oggetto sociale, lo scioglimento della società, la modifica di clausole statutarie eventualmente adottate ai sensi dell'articolo 2351, terzo comma, del codice civile ovvero introdotte ai sensi dell'articolo 3, comma 1, del decreto-legge 31 maggio 1994, n. 332, convertito, con modificazioni, dalla legge 30 luglio 1994, n. 474, come da ultimo modificato dall'articolo 3 del presente decreto, le cessioni di diritti reali o di utilizzo relative a beni materiali o immateriali o l'assunzione di vincoli che ne condizionino l'impiego, anche in ragione della sottoposizione dell'impresa a procedure concorsuali; c) opposizione all'acquisto, a qualsiasi titolo, di partecipazioni in un'impresa di cui alla lettera a) da parte di un soggetto diverso dallo Stato italiano, enti pubblici italiani o soggetti da questi controllati, qualora l'acquirente venga a detenere, direttamente o indirettamente, anche attraverso acquisizioni successive, per interposta persona o tramite soggetti altrimenti collegati, un livello della partecipazione al capitale con diritto di voto in grado di compromettere nel caso specifico gli interessi della difesa e della sicurezza nazionale. A tale fine si considera altresì ricompresa la partecipazione detenuta da terzi con i quali l'acquirente ha stipulato uno dei patti di cui all'articolo 122 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di quelli di cui all'articolo 2341-bis del codice civile*».

verifica, sul piano legittimità, in sede contenziosa innanzi al giudice amministrativo.

L'allargamento dell'area di rilevanza strategica ad interi settori e l'ampiezza della discrezionalità del Governo sia nella relativa definizione sia nell'apprezzamento dei rischi determina una connotazione dei poteri di incidenza pubblica sulle iniziative economiche sempre meno speciale e straordinaria e sempre più ordinaria.

3.4. Trasformazione digitale e sicurezza cibernetica

In linea con il contesto internazionale, l'Italia sta vivendo un processo di trasformazione e innovazione dei servizi ai cittadini e alle imprese in un'ottica di semplificazione, anche attraverso l'utilizzo di tecnologie digitali.

L'effetto delle nuove tecnologie, nella prospettiva *digital first*, porta non solo ad un sistema più efficiente, ma soprattutto ad accorciare le distanze tra pubblica amministrazione e utenti ed a facilitare l'accesso ai servizi e a rilanciare l'economia, in particolare di alcuni settori produttivi strategici per il Paese.

L'articolo 76 del decreto cd. "Cura Italia"[117] prevede l'introduzione di soluzioni di innovazione tecnologica attraverso un gruppo di esperti per lo sviluppo della trasformazione. Infatti, la trasformazione digitale non riguarda solo gli informatici, non attiene unicamente allo strumento utilizzato dalla pubblica amministrazione, ma rappresenta un nuovo modo di intendere ed operare della stessa e necessita di un insieme di competenze tecnologiche, giuridiche e organizzative.

Sebbene il livello di digitalizzazione nelle pubbliche amministrazioni sia ancora basso, il quadro normativo che disciplina tale aspetto ed anche gli strumenti tecnologici esistenti si è oggi evoluto[118].

Il *Codice dell'Amministrazione Digitale* (CAD), il testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della pubblica amministrazione nei rapporti con i cittadini e le imprese[119], all'articolo 17 obbliga tutte le Amministrazioni ad individuare un ufficio per la transizione alla mo-

---

117) Decreto legge 17 marzo 2020 n. 18 "*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da Covid-19*".

118) L. Facondini, *La transizione al digitale della Pubblica Amministrazione*, in *Diritto.it*, sezione di Diritto amministrativo, 30 luglio 2020.

119) Il *Codice dell'Amministrazione Digitale* (CAD), istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato numerose volte, in particolare,

dalità digitale – il cui responsabile è il RTD – con la funzione di garantire la trasformazione digitale della pubblica amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di modelli di relazione trasparenti e aperti con i cittadini[120].

Dopo l'accelerazione del processo di trasformazione digitale imposto dalla pandemia *Covid-19* che ha portato ad un sensibile aumento degli attacchi cibernetici, il programma di finanziamento "*Next generation EU*" ha posto i presupposti per un'ulteriore fase di allargamento e velocizzazione del processo, al fine di aumentare la resilienza del Paese e dell'Europa.

Nel *Recovery plan* (PNRR - Piano Nazionale di Ripresa e Resilienza[121])

---

di recente, è stato modificato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale. Con l'ultimo intervento normativo il CAD è stato ulteriormente razionalizzato nei suoi contenuti. Attraverso il decreto legislativo n. 217/17 è stata sottolineata con maggior forza la natura di carta di cittadinanza digitale della prima parte del CAD con disposizioni volte ad attribuire a cittadini e imprese i diritti all'identità e al domicilio digitale, alla fruizione di servizi pubblici *on-line* e *mobile oriented*, a partecipare effettivamente al procedimento amministrativo per via elettronica e a effettuare pagamenti on-line; è stata promossa l'integrazione e l'interoperabilità tra i servizi pubblici erogati dalle pubbliche amministrazioni in modo da garantire a cittadini e imprese il diritto a fruirne in maniera semplice; è stata garantita maggiore certezza giuridica alla formazione, gestione e conservazione dei documenti informatici prevedendo che non solo quelli firmati digitalmente – o con altra firma elettronica qualificata – ma anche quelli firmati con firme elettroniche diverse possano, a certe condizioni, produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria senza prevedere l'intervento di un giudice caso per caso; è stata rafforzata l'applicabilità dei diritti di cittadinanza digitale e promosso l'innalzamento del livello di qualità dei servizi pubblici e fiduciari in digitale, sia istituendo presso l'AgID l'Ufficio del Difensore civico per il digitale, sia aumentando la misura delle sanzioni irrogabili qualora i fornitori di servizi fiduciari violino le norme; è stato promosso un processo di valorizzazione del patrimonio informativo pubblico riconducendolo tra le finalità istituzionali di ogni amministrazione.

120) L'articolo 17 del *Codice dell'Amministrazione digitale* obbliga tutte le amministrazioni ad individuare un ufficio per la transizione alla modalità digitale – il cui responsabile è il RTD – a cui competono le attività e i processi organizzativi ad essa collegati e necessari alla realizzazione di un'amministrazione digitale e all'erogazione di servizi fruibili, utili e di qualità.

121) *Il Piano Nazionale di Ripresa e Resilienza* (PNRR) è il programma di investimenti che l'Italia deve presentare alla Commissione europea nell'ambito del *Next Generation EU*, lo strumento per rispondere ala crisi pandemica provocata dal *Covid-19*. La proposta di *Linee guida* per la definizione del Piano nazionale di ripresa e resilienza è stata approvata nei suoi contenuti essenziali dal Comitato interministeriale per gli affari europei del 9 settembre 2020, in coordinamento con tutti i Ministeri e le rappresentanze delle Regioni e degli enti locali, e trasmessa alle Camere il 16 settembre 2020.

si individuano chiaramente quali vincoli di progetto: semplificazione burocratica, costruzione di modelli organizzativi a supporto dell'amministrazione digitale, costruzione di burocrazie trasparenti; amministrazioni accessibili, amministrazioni nativamente digitali (stop ai sistemi misti), Amministrazioni partecipate e sostenibili, formazione per dirigenti e dipendenti[122].

Il *Recovery plan* italiano (PNRR) articola i tre assi strategici di cui si compone in complessive 6 missioni, che, a loro volta, raggruppano 16 componenti funzionali a realizzare gli obiettivi ivi contenuti attraverso 47 linee di intervento per progetti di investimento. Gli interventi di digitalizzazione sono distribuiti in tutte le sei missioni e dunque non limitati soltanto alla *Missione 1* chiamata "*Digitalizzazione, innovazione, competitività e cultura*", che tuttavia contiene gli specifici interventi relativi alla pubblica amministrazione digitale oltre che quelli relativi alla digitalizzazione delle imprese e al rilancio del turismo. Gli obiettivi generali sono: cambiare la P.A. per favorire l'innovazione e la trasformazione digitale del settore pubblico, dotandola di infrastrutture moderne, interoperabili e sicuri; accelerare i tempi della giustizia; favorire la diffusione di piattaforme, servizi digitali e pagamenti elettronici presso Pubbliche Amministrazioni e cittadini.

È evidente come l'emergenza pandemica abbia cambiato la prospettiva, portando al centro dell'attenzione l'urgente necessità di una trasformazione

---

122) Per far ripartire l'Europa dopo la pandemia da *Covid-19*, a luglio 2020 l'UE ha approvato il *Next generation EU*, noto in Italia come *Recovery fund* o "Fondo per la ripresa". Si tratta di un fondo speciale volto a finanziare la ripresa economica del vecchio continente nel triennio 2021-2023 con titoli di Stato europei (*Recovery bond*) che serviranno a sostenere progetti di riforma strutturali previsti dai Piani nazionali di riforme di ogni Paese: i *Recovery plan*. Lo stanziamento complessivo è di 750 miliardi di euro, da dividere tra i diversi Stati. L'Italia e la Spagna figurano tra i maggiori beneficiari di questa misura. Il testo del *Recovery plan* approvato nella riunione del Consiglio dei Ministri del 12 gennaio 2021 stabilisce le misure che dovranno dare attuazione in Italia al programma *Next generation EU*, definita come la grande occasione per lo sviluppo dell'Italia, e che richiedere uno sforzo collettivo ed urgente. Il PNRR punta a rendere l'Italia più inclusiva e sostenibile, con una serie di riforme ritenute necessarie per superare la crisi causata dal *Covid-19*. Il testo del *Recovery plan* è articolato in 6 missioni, aree tematiche strutturali di intervento:
– digitalizzazione, innovazione, competitività e cultura;
– rivoluzione verde e transizione ecologica;
– infrastrutture per una mobilità sostenibile;
– istruzione e ricerca;
– inclusione e coesione;
– salute.

digitale di processi e servizi pubblici in un senso che aiuti cittadini e imprese a usare i mezzi tecnologici per fare a distanza ciò che diventa difficile o impossibile fare in presenza, abilitando una generale maggiore efficienza e sburocratizzazione.

3.4.1. Il passaggio della pubblica amministrazione al *cloud computing* e la reingegnerizzazione dei processi amministrativi

Il primo elemento che viene descritto nel dettaglio progettuale del *Recovery plan* riguarda il passaggio al *cloud computing*[123] delle pubbliche amministrazioni, con la costituzione di un *cloud storage*[124] nazionale inserito nell'ambito del progetto UE denominato GAIA-X[125]. Scopo di questo intervento è la riqualificazione e messa in sicurezza dei dati attualmente residenti nelle infrastrutture locali che, infatti, per poter essere trasferiti in *cloud*, devono essere verificati, standardizzati e ne deve essere controllata la sicurezza.

Il piano dichiara che l'intervento sul *cloud* consentirà notevoli risparmi sulle spese di manutenzione e aggiornamento dei *data-center* nel prossimo

123) Il *cloud computing* (in italiano nuvola informatica) indica, in informatica, un paradigma di erogazione di servizi offerti *su richiesta* da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita. La ridondanza dei dati e l'elevata misura di sicurezza garantisce un'elevata continuità operativa. Usufruire di un servizio di *cloud computing* equivale ad un abbattimento dei costi fissi riguardanti strumenti informatici, costi di manutenzione e di aggiornamento.

124) Il *cloud* (termine inglese che significa nuvola) è uno spazio di archiviazione personale, chiamato talvolta anche *cloud storage* che risulta essere accessibile in qualsiasi momento ed in ogni luogo utilizzando semplicemente una qualsiasi connessione ad internet. Il *cloud storage*, dunque, non fa altro che sincronizzare tutti i propri file preferiti in un unico posto, con il conseguente vantaggio di riscaricarli, modificarli, cancellarli e/o aggiornarli, senza avere dunque il bisogno di portare con sé *hard disk* esterni, *pen drive USB*, o qualsiasi altra cosa che normalmente è possibile perdere o dimenticare.

125) Lanciato nel 2018 GAIA-X è un progetto franco-tedesco che promuove la creazione di una infrastruttura europea dei dati, puntando su sicurezza, innovazione, open source e trasparenza. L'obiettivo è creare una piattaforma che sia in grado di aggregare dati sulla base di standard condivisi, mettendo sempre al centro gli utenti, la chiave di volte per una economia digitale di successo. L'adesione al progetto è aperta a tutti gli *stakeholders*, imprese, PMI e start up (28 imprese italiane aderiscono oggi a GAIA-X). Il progetto GAIA-X sostiene la costituzione e lo sviluppo di un *cloud federato UE*, una piattaforma europea per definire criteri e standard comuni di gestione dei dati e dei servizi in *cloud*, in linea con il concetto di sovranità tecnologica europea.

triennio, liberando risorse per gli investimenti che saranno mirati alla realizzazione e consolidamento di centri per elaborare e ospitare i servizi più strategici della P.A. centrale, e alla realizzazione dei servizi di *cloud enabling*, necessari alla transizione *cloud*, nonché alla sicurezza dei dati[126].

Anche il *cloud*, tuttavia, se utilissimo per razionalizzare la gestione dei dati e la sicurezza, deve necessariamente abbinarsi ad altri investimenti presenti nel PNNR, tra cui quello sulle reti ed infrastrutture. Risulta infatti inutile portare in *cloud* i dati di un'Amministrazione che non ha soddisfacente accesso alla banda ultralarga per accedere ed utilizzare i dati ed i servizi, perché se ne rallenterebbe e complicherebbe il lavoro[127].

L'intervento sul *cloud* mira inoltre a costruire quello che viene definito "sistema operativo del Paese" realizzando una standardizzazione delle base dati e delle interfacce operative che renda i servizi delle pubbliche amministrazioni "interoperabili" tra loro: un'Amministrazione potrà facilmente ottenere e recuperare dati dall'altra e il cittadino e l'impresa, a loro volta, avranno un unico punto di accesso per ottenere i dati dalla pubblica amministrazione.

L'emergenza *Covid-19* ha dimostrato che le imprese più resilienti sono state proprio quelle in grado di adottare immediatamente modalità innovative di lavoro agile sfruttando le potenzialità delle connessioni digitali. Sebbene le rilevazioni internazionali fotografino l'arretratezza italiana in questo campo come confermato dall'Indice DESI[128] secondo cui per quota di piccole e medie

---

126) L'investimento complessivo per la transizione al *cloud* e la sicurezza previsto è di 1.250 milioni di euro. Non si tratta di un investimento così rilevante se si considera che il solo "Lotto 1" (lo *storage*) del precedente bando SPC *Cloud* aveva un valore di circa 2 miliardi di euro ed è stato sostenuto senza alcun supporto UE.

127) Occorre poi regolare l'uso dei dati in *cloud* da parte delle Amministrazioni centrali e dei soggetti a cui sarà affidata la relativa gestione sulla scorta delle *best practice* del bando *Cloud-SPC*, il quale ha dato ottimi risultati in termini di *cloudizzazione* dei dati delle pubbliche amministrazioni italiane, con il sistema dei contratti quadro che le abilitano a stipulare direttamente accordi esecutivi per i servizi necessari.

128) Il *Digital Economy and Society Index* (DESI) è un indice creato dalla Commissione europea che misura i progressi dei Paesi europei in termini di digitalizzazione dell'economia e della società. L'indice è la sintesi di diversi indicatori raccolti in 5 aree principali:
– *connettività*: misura lo sviluppo della banda larga, la sua qualità e l'accesso fatto dai vari *stakeholder*;
– *capitale umano*: misura le competenze necessarie a trarre vantaggio dalle possibilità offerte dalla società digitale;
– *uso di internet*: misura le attività che i cittadini compiono grazie a internet, connettività e competenze digitali;

imprese (Pmi) in grado di vendere direttamente on-line, il nostro Paese si posiziona terz'ultimo nell'Ue[129].

In questo contesto le risorse Ue dovranno essere utilizzate per dare continuità al cd. "Piano transizione 4.0". Tra le azioni chiave la stabilizzazione degli incentivi per almeno un triennio; l'immediata fruibilità del credito d'imposta per le imprese, introducendo ove possibile il meccanismo dello sconto in fattura e della cedibilità al sistema finanziario; l'innalzamento delle aliquote, in particolare per gli investimenti in ricerca, sviluppo e innovazione e per i progetti *industria 4.0* ed economia circolare[130].

3.5. Il Centro di competenza UE e il Centro di coordinamento nazionale

Entro sei mesi dall'entrata in vigore del relativo regolamento UE che prevede un centro di competenza europeo per lo sviluppo industriale, tecnologico e della ricerca in materia di *cybersecurity* che avrà sede a Bucarest e della rete dei centri di coordinamento nazionali, ogni Stato membro è chiamato a costituire un proprio Centro di coordinamento nazionale da individuare in un ente pubblico, o a maggioranza pubblica, e che abbia la capacità di supportare e relazionarsi con il citato Centro UE e la connessa rete dei diversi Centri nazionali di coordinamento, gestire fondi, possedere o avere accesso diretto a capacità tecniche e di ricerca in materia di *cybersecurity*, coinvolgere e coordinarsi con i settori pubblico (incluse le autorità NIS) e privato, con l'accademia, il mondo della ricerca e la società civile.

Il 20 aprile u.s. il Consiglio europeo ha dato il suo via libera al suddetto regolamento. Il nuovo Centro e la nuova rete saranno chiamati a svolgere un

---

– *integrazione delle tecnologie digitali*: misura la digitalizzazione delle imprese e l'impiego del canale on-line per le vendite;

– *servizi pubblici digitali:* misura la digitalizzazione della PA, con un *focus* sull'*eGovernment.*

Ognuna di queste cinque aree contiene diversi indicatori che sono raccolti annualmente per tutti i Paesi europei e opportunamente pesati a seconda della loro rilevanza. Nel rapporto DESI 2018 sono stati 34 gli indicatori utilizzati.

129) Seguito solo da Romania e Bulgaria.

130) Fonte: F. Meta, *Recovery Plan, Confindustria Digitale:* "*Priorità a Transizione 4.0 e PA*", 28 dicembre 2020, in *Corrierecomunicazioni.it*. L'industria 4.0 favorisce il passaggio ad una economia sempre più circolare. Per economia circolare si intende un approccio diverso ai metodi di produzione. In altri termini, si tratta di passare da un processo lineare che contempla l'utilizzo di materie prima e la generazione di scarti, a un modello che si rigenera, trasformando in risorsa ciò che comunemente viene considerato rifiuto. Si tratta di una passaggio che è prima di tutto culturale.

ruolo fondamentale nel contribuire a garantire la sicurezza informatica anche di settori cruciali quali la sanità, i trasporti, l'energia, i mercati finanziari e i sistemi bancari. Rispetto alla proposta iniziale della Commissione, il testo ha subito alcune modifiche concordate da entrambi i colegislatori europei. In particolare, è stato rafforzato il ruolo dell'*Enisa* (Agenzia dell'Unione europea per la cybersicurezza), che sarà un osservatore permanente nel consiglio di direzione del Centro di competenza e potrà fornire consulenza e contributi per l'elaborazione dell'agenda e dei programmi di lavoro annuale e pluriennale. Sono anche state introdotte nuove disposizioni relative ai centri nazionali di coordinamento, in particolare per quanto riguarda la designazione dei centri e la valutazione della Commissione[131].

Il Centro avrebbe quindi l'obiettivo, da un lato, di favorire lo sviluppo e il potenziamento di una industria italiana ed europea competitiva, in grado di fornire tecnologie e servizi abilitanti ad elevato grado di sicurezza, con particolare riguardo all'ambito delle infrastrutture critiche digitali, alle principali filiere industriali nazionali e, dall'altro, di operare – in termini di supporto, studio e sviluppo – in stretta sinergia con i diversi soggetti che compongono l'architettura nazionale di sicurezza cibernetica[132].

La sicurezza delle reti e dell'informazione, nonché dei nostri dati, passa

---

131) Fonte: G. Carrer, *Rete cyber europea, il Consiglio dice sì. Italia al lavoro per il centro*, SU *Formiche.net*, 29/04/2021. Il paragrafo 5 dell'articolo 6 del regolamento precisa i criteri per la designazione del Centro nazionale di coordinamento, che dev'essere "*un ente del settore pubblico o un ente a partecipazione pubblica maggioritaria che esercita funzioni amministrative pubbliche ai sensi del diritto nazionale, anche per delega, ed è in grado di sostenere il Centro di competenza e la rete nell'assolvimento della loro missione*". E ancora: "*Esso dispone di competenze in materia di cibersicurezza nell'ambito della ricerca e della tecnologia o vi ha accesso. Esso è in grado di interagire e di coordinarsi efficacemente con l'industria, il settore pubblico, la comunità accademica e della ricerca e i cittadini, nonché con le autorità designate a norma della direttiva (Ue) 2016/1148*" (direttiva Nis). Il Centro e la rete verranno finanziati da due programmi dell'Unione europea, Orizzonte Europa e Europa digitale con 5 miliardi di euro in totale per i 27 Stati membri. Si tratta di ***matching fund***, ossia finanziamenti che richiedono pari stanziamenti da parte dello Stato membro. Intanto, il Piano nazionale di ripresa e resilienza italiano già prevede per la cybersicurezza 620 milioni di euro per rafforzare il livello delle nostre difese cyber, a partire dalla piena attuazione del Perimetro di sicurezza nazionale cibernetica.

132) La menzionata nuova struttura, inoltre, costituirebbe la naturale interfaccia dei Centri di competenza previsti dal Piano nazionale Impresa 4.0, che fa seguito all'iniziativa della Commissione europea "*Digitising European Industry*" dell'aprile 2016, volta a promuovere la trasformazione digitale delle imprese, rafforzando i collegamenti tra ricerca e industria, oltre che dei *Digital Innovation Hub*, distribuiti sul territorio a supporto delle

infatti per una potente capacità di innovazione tecnologica che richiede investimenti importanti e pluralità di menti e di intenti verso uno scopo comune. Ogni Paese non può che affrontare a livello nazionale, prima di tutto, questa necessità, se vuole continuare a proporsi anche all'estero come driver di soluzioni e tecnologie e attrattore di investimenti. Dimostrare di "saper proteggere sé stessi e il proprio ambiente" è oggi di fatto un vantaggio competitivo nella proposizione di qualsiasi attività. La tematica ampiamente dibattuta delle tecnologie e delle soluzioni 5G è una dimostrazione lampante della "nazionalità" del problema di sicurezza.

La sicurezza cibernetica è, come abbiamo visto, un tema pervasivo, che interessa ogni singolo cittadino, come ogni realtà imprenditoriale e ogni istituzione pubblica. L'approccio alla *cybersecurity* non può che vedere la sintesi tra l'interesse nazionale e quello privato, tra sfera collettiva e sfera privata. La scelta europea, confermata dal regolamento 881 del 2019, è quella di lasciare totalmente alla competenza degli Stati membri l'apparato sanzionatorio della cybersicurezza, con la conseguenza che dovrà essere ponderata l'influenza sulle strategie degli operatori delle diverse discipline nazionali anche in funzione di prevenzione del ricorso a pratiche elusive.

In relazione al modello delle competenze interne all'amministrazione italiana, emerge che anche il decreto-legge n. 105 del 2019 riserva massima cura nella descrizione e nel bilanciamento tra il ruolo dei diversi Ministeri, comitati e agenzie, il tutto inevitabilmente affiancato dalla necessità di mantenere il più possibile invariati gli oneri per il bilancio dello Stato[133]. L'auspicata creazione di un'Agenzia dedicata, prevista dalla direttiva NIS e poi dal citato regolamento 881 del 2019, potrebbe costituire l'occasione per concentrare risorse e competenze umane, costituendo quell'interlocutore unico con il settore privato auspicato dalle Direttive. In questo contesto, in Italia

---

piccole e medie imprese e delle Pubbliche Amministrazioni locali per il relativo incremento delle capacità di prevenzione e di valutazione del livello di maturità digitale e tecnologica, nonché per l'accrescimento della consapevolezza.

133) La frammentazione delle competenze in materia di cybersicurezza era già stata descritta in modo chiaro dalle direttive della Presidenza del Consiglio dei Ministri del 2013 e del 2015 in tema di cybersicurezza: quest'ultima aveva espressamente indicato come "*il quadro di competenze rimane ancora frammentato sotto il profilo legislativo*". L'adozione del d.l. n.105 del 2019 non ha agevolato il dipanare delle competenze e in un settore così strategico come quello della *cyber security*, il modello del "coordinamento", per come sino ad ora concepito ed attuato non appare coerente con la dimensione e la velocità d'azione del fenomeno cybersicurezza.

si è sviluppato nelle aule parlamentari un acceso dibattito sulla condivisa necessità di creare l'*Istituto Italiano di Cybersicurezza* (IIC)[134].

L'Istituto si propone due scopi principali:

– promuovere e sostenere l'accrescimento delle competenze e delle capacità tecnologiche, industriali e scientifiche nazionali nel campo della sicurezza cibernetica e della protezione informatica;

– favorire lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni in una cornice di sicurezza e il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica, a tutela dell'interesse della sicurezza nazionale nel settore.

È dunque di fondamentale importanza avere anche in Italia, quanto prima, e al pari di altri Paesi europei, un laboratorio di ricerca e sviluppo sulla *cybersecurity* che metta in relazione il mondo della ricerca accademica, quello dello sviluppo industriale e quello degli stakeholder pubblici. In questo modo potranno essere messe a disposizione le innovazioni internazionali nel settore, e definite nuove metodologie e tecnologie che il mondo accademico utilizzerà per pubblicazioni, insegnamento e *spin off*, le aziende per sviluppare nuovi prodotti e il comparto governativo e di *law enforcement* per avere visione delle ultime tecnologie e beneficiare di un'osmotica collaborazione e interazione con un ambiente di ricerca innovativo.

3.5.1. Collaborazione pubblico-privato: quale approccio per una struttura nazionale di *cybersecurity*. Comparazione con le strategie dei Paesi UE

A livello europeo e internazionale sono presenti diverse tipologie di collaborazione tra attori pubblici e privati (anche sotto forma di Partenariati Pubblico-Privato - PPP) sviluppate al fine di garantire una migliore cooperazione attraverso un concetto di sicurezza compartecipata. E sono varie le organiz-

134) Come cita la relazione illustrativa, "*la Fondazione denominata Istituto Italiano di Cybersicurezza (IIC) ha lo scopo di promuovere e sostenere l'accrescimento delle competenze e delle capacità tecnologiche, industriali e scientifiche nazionali nel campo della sicurezza cibernetica e della protezione informatica, nonché di favorire lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni in una cornice di sicurezza e il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica, a tutela dell'interesse della sicurezza nazionale nel settore*".

zazioni che, seppur differenti per forma giuridica e organizzazione, sono simili all'IIC negli obiettivi che si prefigurano di perseguire[135].

Sul piano normativo, l'implementazione delle direttive europee (ECI e NIS) e la strategia europea di *cybersecurity*, oltre alle forme di sviluppo di PPP sovranazionali, hanno spinto gli Stati membri verso forme di collaborazione a livello operativo, volte al rafforzamento delle misure di *cybersecurity* delle organizzazioni secondo le indicazioni dei *policy maker* europei. Da questo punto di vista, come visto per i PPP sovranazionali, le *best practice* internazionali suggeriscono un tipo di approccio *bottom-up*, teso a coinvolgere gli stakeholder sin dalle fasi iniziali, costitutive delle strutture e delle policy nazionali[136].

Per quanto riguarda la *governance* interna dei centri dei Paesi europei, il modello tedesco si è concentrato sulla responsabilità politica, in capo al Ministero della difesa, con un modello di *governance* agile, che prevede un amministratore delegato. Il modello francese del Cyber Campus si è dotato di una *governance* mista attraverso la creazione di una SAS, con capitale pubblico (49%) e privato (51%). La Finlandia ha annunciato il NSAB (*Network Security Advisory Board*), un organismo che riunisce agenzie del Governo, intelligence e imprese. In Inghilterra dal 2018 è attivo il programma LORCA[137](*London Office for Rapid Cybersecurity Advancement*) che punta su una

---

135) R. De Nicola - L. De Martino (a cura di), *Istituto italiano di cybersicurezza: perché serve ora e come impostarlo bene (guardando alla UE)*, in *www.agendadigitale.eu* - Sicurezza nazionale. In Europa si è deciso di localizzare in Romania il centro di competenza europeo per la sicurezza informatica che si collegherà con una rete di centri di coordinamento nazionali e che sarà il principale organismo per la gestione delle risorse finanziarie dell'UE dedicate alla ricerca sulla sicurezza informatica nell'ambito dei due programmi proposti – *Digital Europe* e *Horizon Europe* – nell'ambito del prossimo quadro finanziario pluriennale, per il periodo 2021-2027. L'analisi ha portato alla luce le evidenze per poter valutare e, quindi, comparare gli sviluppi nazionali delle forme di collaborazione tra settore pubblico, privato, centri di ricerca e università sulla *cybersecurity* con particolare riferimento allo sviluppo di capacità di difesa nazionali e all'affidamento di tale compito a strutture nazionali.

136) Una distinzione fondamentale si pone, relativamente alle scelte degli Stati, sul ruolo che deve avere una struttura nazionale che si occupi di *cybersecurity.* L'esempio della nascente agenzia di *cybersecurity* tedesca e del futuro *Cyber Campus* francese suggeriscono di puntare su un approccio inclusivo, al fine di svolgere non solo un'azione di sintesi nell'ambito della ricerca, ma anche di favorire, allo stesso tempo, la nascita di un ecosistema e di un indotto di *cybersecurity* intorno alla struttura stessa. Esse sembrano puntare a concentrare, anche geograficamente, le capacità di difesa nazionali in una struttura fondante che funzioni da centro attrattivo principale.

137) Il modello inglese del LORCA ha un budget di 13,5 milioni di sterline all'anno per sostenere lo sviluppo di oltre 72 aziende nel settore della *cybersecurity.*

governance delegata a una struttura privata, pur mantenendo salda e continuativa la collaborazione con il NCSC, garantendo sia lo sviluppo di tecnologie rilevanti per la sicurezza nazionale sia l'eventuale accompagnamento nei mercati internazionali.

Una questione centrale si concentra, dunque, sul target principe della struttura, ovvero se questa debba basarsi su un output specifico come quello relativo alla gestione di un evento critico o se, invece, il perseguimento di un obiettivo comune condiviso possa stabilire il rapporto di fiducia necessario tra gli attori coinvolti (università, agenzie governative e attori privati) tale da poter determinare il successo della collaborazione. Questa condizione è alla base, ad esempio, del modello israeliano di *Beer Sheva*, dove si è deciso di puntare sulla convergenza di obiettivi tra i principali attori di un ecosistema, con il fine ultimo di fornire allo Stato le capacità cyber, operative e tecniche, necessarie per la sua sicurezza favorendo, allo stesso modo, lo sviluppo economico del Paese e la leadership a livello internazionale nel settore tecnologico.

A tal riguardo, si evidenzia la recente proposta del Prefetto Franco Gabrielli, autorità delegata per la sicurezza della Repubblica, per la creazione di una agenzia nazionale per la *cybersicurezza* presso la Presidenza del Consiglio ma fuori dal comparto dell'intelligence, "*con una partnership più forte*", che tratti in maniera olistica il tema della sicurezza cibernetica, nell'ottica di "*affrancarsi da una modalità emergenziale*"[138]. L'agenzia avrà il compito di sviluppare nel Paese le capacità di resilienza di fronte a minacce ed attacchi di varia natura. Il Prefetto Gabrielli ha dunque sottolineato, in tema di *cybersecurity*, il bisogno "*di un salto di qualità tra pubblico e privato fondato su trasparenza e correttezza di rapporti*"; in tal senso, ha annunciato una revisione del d.P.C.M. di attuazione del perimetro cibernetico contenente le regole per le aziende in caso di incidenti.

Si prevede, quindi, da un lato, un centro di competenza privato ma di operatività nel mondo dell'intelligence e destinato solo a ricerca e sviluppo degli investimenti *tech*; dall'altro, *una nuova agenzia per la cybersicurezza*, anch'essa fuori del sistema DIS, che risponda al Presidente del Consiglio operando in raccordo con il centro.

La costituzione di un Istituto dedicato alle problematiche di *cybersecurity* può sradicare, alla fonte, i motivi scatenanti di un indebolimento delle ca-

138) M. Ludovico, *Gabrielli: Un'agenzia nazionale per la cybersecurity fuori dall'intelligence*, in *Il sole 24 ore*, 10 aprile 2021. Secondo Gabrielli la nuova struttura dovrebbe collocarsi presso la Presidenza del Consiglio, fuori dal comparto intelligence, perché quest'ultimo si occupa di un aspetto ma non della complessità della resilienza.

pacità nazionali: non solo, infatti, gli attori coinvolti non sarebbero più in una condizione di estraneità rispetto alla difesa dello Stato, ma la relazione collaborativa garantirebbe il superamento di eventuali difficoltà operative. Inoltre, il coordinamento della ricerca da parte di un attore statale permetterebbe di mantenere la responsabilità e la direzione strategica per la sicurezza nazionale in capo all'attore pubblico.

Conclusioni

Il 2021 e gli anni a venire si caratterizzeranno per una sempre maggiore e necessaria attenzione verso uno dei principali fattori strutturali e abilitanti dell'innovazione digitale, quello della *sicurezza legata all'archiviazione*, *all'accesso e all'uso delle informazioni digitalizzate* ma anche delle *infrastrutture e dei servizi chiave collegati a tali informazioni*. Nel contesto di sempre maggiore competizione globale e di necessario ampliamento della digitalizzazione, come l'emergenza *Covid-19* ha dimostrato, un obiettivo di fondamentale importanza è anche quello della garanzia di un elevato e comune livello di resilienza cibernetica.

A tal fine, la definizione del quadro europeo di certificazione della *cybersecurity* diviene utile all'armonizzazione dei sistemi di certificazione impiegati nei vari Stati membri e alla creazione di un mercato unico digitale per i servizi di rete. Tale sistema, come si è avuto modo di descrivere, prevede la creazione di un meccanismo capace di attestare che le funzioni, i prodotti, i servizi e i processi, opportunamente valutati, durante tutto il loro ciclo di vita, siano conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati. Per fare ciò si rende necessaria anche la differenziazione dei livelli di affidabilità dei sistemi di certificazione in relazione al relativo livello di rischio.

In questa prospettiva, importante diventerà il ruolo attuativo degli Stati membri nell'ottica delineata dal legislatore europeo. Su questo versante, come si è avuto modo di analizzare, l'Italia ha introdotto il *Piano nazionale per la protezione cibernetica e la sicurezza informatica* che mira a potenziare l'architettura nazionale cibernetica attraverso l'implementazione degli standard minimi di sicurezza comuni. Ma ancora moltissimo resta da fare. Anche a seguito dei repentini cambiamenti generati dall'emergenza pandemica, infatti, assumono maggiore importanza quelle infrastrutture e quei servizi che svolgono attività civili, sociali o economiche fondamentali per gli interessi dello

Stato e della comunità dei cittadini. Nel difficile momento di emergenza sanitaria è stato possibile rilevare con chiarezza quali e quanti siano gli operatori, pubblici e privati, che garantiscono tali funzioni e la cui continuità si è dimostrata essenziale per la tenuta non solo economia, ma ancor più sociale, delle nostre comunità.

È, quindi, di primaria importanza la realizzazione di un sistema che consenta un'efficace valutazione sotto il profilo tecnico della sicurezza e della resilienza degli apparati e dei prodotti forniti e che valuti la presenza di fattori di vulnerabilità che possano compromettere l'integrità e la sicurezza delle reti utilizzate da questi operatori.

La *sicurezza cibernetica* procede, così, di pari passo con la resilienza del servizio essenziale offerto poiché è volta a prevenirne il blocco e a consentirne la regolare e continua fruizione a servizio della società.

Dal punto di vista delle imprese sono fondamentali, da una parte l'enorme criticità del rischio *cyber* nella valutazione complessiva del rischio aziendale, dall'altra, la rilevanza del coinvolgimento dei *board aziendali* la cui *awareness* è cruciale per l'impostazione di sane strategie di *cybersecurity*. E questo è ancora più vero oggi che assistiamo a un'esponenziale diffusione di metodologie lavorative prima poco utilizzate e ora, a causa della pandemia, entrate prepotentemente nell'uso quotidiano.

La direttiva UE 2018/1972 ha istituito il *Codice delle comunicazioni elettroniche* che ha previsto, dal 2020, l'assegnazione, da parte di ogni Stato membro, delle frequenze necessarie per la rete 5G. Anche in questo settore, dunque, non può esistere una sovranità nazionale che non faccia i conti con una nuova dimensione, che impone la condivisione di strategie operative, informazioni sensibili, capacità informative e tecniche di indagine. Sfide come la lotta alla criminalità organizzata, al terrorismo, al crimine informatico, non possono essere affrontate a livello di singolo Paese.

I risvolti politici, economici, sociali ma anche etici saranno tanti e tali che, oltre a dover essere affrontati in modo sistemico, chiameranno l'umanità stessa a porsi in termini più incisivi il problema della propensione della potenza tecnica al dominio assoluto. E, con esso, dovremo anche porci il problema di recuperare l'unitarietà del sapere a fronte della strutturazione a compartimenti stagno delle discipline scientifiche attraverso le quali cerchiamo attualmente di decifrare la complessità dell'ambiente che ci circonda.

La risposta delle forze di polizia deve essere *coerente e coordinata*, secondo un *approccio omnicomprensivo* che affianchi, alla repressione dei reati, la prevenzione, la presa di coscienza dei rischi, la formazione e la resilienza, nonché secondo un metodo che si focalizzi, per l'appunto, sull'impatto che

gli sviluppi tecnologici possono avere sul contesto di riferimento, dando vita a nuove figure di reato, oppure offrendo nuove modalità per perpetrare reati tradizionali.

La strategia della *cybersecurity* costituisce asse portante di questo sistema che richiede, nel contempo, un *quadro regolatorio chiaro e completo*, inserito in una strategia reale, coerente ed unitaria e supportato da un coordinamento imprescindibile nella definizione, gestione e sviluppo infrastrutturale, con il rafforzamento di forme di collaborazione pubblico privato nella combinazione di modelli differenti, necessariamente integrati, ma con una regia unitaria.

Le priorità per la *cybersecurity* su cui lavorare nel 2021 dovrebbero puntare a sviluppare iniziative per favorire l'integrazione dei processi di sicurezza informatica all'interno delle dinamiche aziendali e delle pubbliche amministrazioni; a ripensare i sistemi di certificazione della *cybersecurity* secondo nuovi approcci; a favorire il coordinamento tra gli attori pubblici e privati coinvolti nel sistema della *cybersecurity* e a sviluppare iniziative per favorire l'integrazione dei processi di resilienza informatica all'interno delle dinamiche aziendali.

Ed è in tale quadro che il rafforzamento del sistema delle comunicazioni nel suo complesso si pone quale premessa ineludibile, in quanto insostituibile strumento per promuovere un virtuosismo, *in primis*, tra economia della conoscenza ed economia dei servizi a beneficio dell'intera collettività, in assenza della quale ogni iniziativa si esaurirebbe entro i ristretti margini della gestione della contingenza.

La radice valoriale è, in ultima analisi, il fondamento unico e portante di ogni politica di sicurezza, inclusa quella per lo spazio cibernetico.

Bibliografia

Alberici A., *Imparare sempre nella società della conoscenza*, Bruno Mondadori, Milano, 2002

Balsano A.M. - Del Monte L., *Il diritto internazionale di fronte al cyberspace*, in Osservatorio per la sicurezza nazionale (a cura di), *Cyberworld. Capire, proteggersi e capire gli attacchi in rete*, Hoepli, Milano, 2013

Bellacosa M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni unite*, in *Diritto penale contemporaneo*, 2015

Belluta H., *Cybercrime e responsabilità degli enti*, in Luparia (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009

Bruno B., *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *Rivista di diritto pubblico, comparato, europeo*, ISSN 1826-3534, n. 14/2020, su *Federalismi.it*

Castells M., *The rise of the network society*, Oxford University Press, Oxford, 2001

Cazorla L. - Alcaraz C. - Lopez J., *Cyber stealth attacks in critical information infrastructures*, in *IEEE Systems Journal*, 12.2.2016

De Nicola R. - De Martino L., *Istituto italiano di cybersicurezza: perché serve ora e come impostarlo bene (guardando alla UE)*, in *www.agendadigitale.eu* - Sicurezza nazionale, 21 dicembre 2020

De Vincentis F., *La lezione di Teti sul mondo virtuale e l'intelligence "Deep web: istruzioni per l'uso. Virtual Humint Intelligence. Tra fake e realtà*, nel corso del Master in *intelligence* dell'Università della Calabria, su *https://formiche.net*., 21/03/2021

Di Nunzio R. - Rapetto U., *Le nuove guerre. Dalla Cyberwar ai Black Bloc, dal sabotaggio mediatico a Bin Laden*, Rizzoli, Milano, 2001

Facondini L. *La transizione al digitale della Pubblica Amministrazione*, in *Diritto.it*, sezione di Diritto amministrativo, 30 luglio 2020

Flor R., *Social networks e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Rivista trimestrale di diritto penale dell'economia*, 2012

Floridi L., *La rivoluzione dell'informazione*, Codice Edizioni, Torino, 2012

Franchina L., *Cyber security, le due nuove direttive europee che cambieranno tutto*, in *https://www.agendadigitale.eu*., 18 gennaio 2021

Heim M., *Metafisica della realtà virtuale*, ed. it. a cura di D. Rossi, Guida, Napoli, 2015

Luparia L. (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009

Manes V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, in *Rivista trimestrale diritto penale dell'economia*, 1-2/2004

Martino L., *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, fascicolo 1, gennaio - aprile 2018, Il Mulino

Meta F., *Recovery Plan, Confindustria Digitale:* "*Priorità a Transizione 4.0 e PA*", in *Corrierecomunicazioni.*it, 28 dicembre 2020

Morcellini M., *Oltre la sudditanza digitale*, in Rivista *Formiche.net*, Lo specchio, marzo 2021

NONES M. - MARRONE A., *La trasformazione delle Forze armate: il programma Forza NEC*, Edizioni nuova cultura, 2010

PECORELLA C., *Enciclopedia del Diritto*, *Reati informatici*, annale X, Cedam, Padova, 2017

PICOTTI L., *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Rivista trimestrale di diritto penale dell'economia*, 2011

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, Cedam, 2004

PROSPERETTI E., *La PA digitale nel Recovery Plan: cosa c'è e cosa manca.*, su *www.agenda digitale.eu - l'approfondimento*, 25 gennaio 2021

RUGGIERO F., *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002

SARZANA C., *Criminalità e tecnologia: il caso dei "computer-crimes"*, in *Rassegna penitenziaria e criminologica*, 1979

SAVONA U., *Processi di globalizzazione e criminalità organizzata transnazionale*, in *Transcrime*, *working paper*, n. 29, dicembre 1998

SEMINARA S., *La pirateria su Internet e il diritto penale*, in *Rivista trimestrale di diritto penale dell'economia*, 1997

STRIPPOLI LANTERNINI A, *Cyber espionage, una seria minaccia per le aziende: attori criminali e misure di contrasto*, 3 aprile 2020, in *https://www.cybersecurity360.it/nuove-minacce*

TENORE V., *La libertà di pensiero tra riconoscimento costituzionale e limiti impliciti ed espliciti: gli argini normativi e giurisprudenziali per giornalisti, dipendenti pubblici (e privati), magistrati nell'uso dei social media*, in *www.rivistacorteconti.it*, 2019

TETI A., *Cyber espionage e cybercounterintelligence. Spionaggio e controspionaggio cibernetico*, Rubbettino, Soveria Mannelli, 2018

TETI A., *Open Source Intelligence & cyberspace. La nuova frontiera della conoscenza*, Rubbettino, Soveria Mannelli, 2015

TOFFLER A. - TOFFLER H., *Creating a new civilization: the politics of the third wave*, Turner Publishing, Nashville, 1995

ZONARO M., *Le 50 parole della Digital forensics più utilizzate nelle aule di giustizia*, Roma, 2014, p. 27

ZORLONI L. *Dalla Difesa agli Interni, nascono i super team per la cybersecurity*, in *https://www.wired.it/amp/270448/internet/regole/2020/02/06/cybersecurity-difesa-interni*, 6 febbraio 2020

Documenti consultati

4ª Commissione (Difesa) del Senato, *Profili della sicurezza cibernetica attinenti alla Difesa nazionale*, audizione del Gen. Div. C. Massara, Roma, 3 giugno 2020

Audizione del Capo di Stato maggiore della Difesa *pro-tempore*, Gen. C. Graziano, Commissione difesa della Camera, seduta del 12 febbraio 2019

Cassazione penale, sez. V, 17 novembre 2000, n. 4741

Commissione difesa della Camera dei Deputati, *Documento conclusivo dell'indagine conoscitiva sulla difesa e sicurezza dello spazio cibernetico*, seduta del 9 febbraio 2016, audizione del Prof. BALDONI R.

Convenzione ONU contro la criminalità organizzata transnazionale, Palermo 2000, in *https://uif.bancaditalia.it/normativa/norm-antiricic/convenzioni/conv-palermo.pdf*

Documento di sicurezza Nazionale 2020, allegato alla Relazione annuale al Parlamento ai sensi dell'art. 38, comma 1-*bis*, legge 124/2007

Libro bianco per la sicurezza internazionale e la Difesa, Ministero della difesa, 2015

Quadro strategico nazionale per la sicurezza dello spazio cibernetico, Presidenza del Consiglio dei Ministri, dicembre 2013

Rapporto CLUSIT 2019 sulla sicurezza ICT in Italia

Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia - Cyber Security Report 2020

Relazione annuale al Parlamento sulla politica dell'informazione per la sicurezza, 2018

Relazione annuale al Parlamento sulla politica dell'informazione per la sicurezza, 2020

Relazione del Nucleo investigativo centrale della Polizia penitenziaria, II sem. 2020

Report "We Are Social", 2020

Resoconto della Polizia postale nel 2020, 04/01/2021, in *www.poliziadistato.it*

Senato della Repubblica, *Audizione 4^ Commissione* (Difesa), audizione Col. G. di. F. G. Reccia, Indagine conoscitiva "*I profili della sicurezza cibernetica attinenti alla difesa nazionale*", Roma, 6 agosto 2020

Sitografia

www.agendadigitale.eu
www.cybersecurity360.org
www.europarl.europa.eu
www.formiche.net
www.ispionline.it
www.lifewire.com
www.poliziadistato.it
www.sicurezzanazionale.gov.it
www.slideshare.net
www.uif.bancaditalia.it

Parte II

Articoli e Saggi

Criticità tra la presentazione dell'istanza di ammonimento, ai sensi dell'art. 8 legge 38/2009 e dell'art. 3 legge 119/2013, e l'obbligo di trasmissione da parte della polizia giudiziaria all'autorità giudiziaria degli atti relativi ai fatti esposti dalla vittima previsto dall'art. 1 della legge 69/2019

di Carmelo Alba*

Abstract

L'apparente specificità e natura tecnica di dettaglio della traccia in trattazione sottende, in realtà, l'approccio al più ampio e suggestivo tema connesso al rapporto tra procedimento amministrativo (per l'adozione del provvedimento di ammonimento questorile) e procedimento penale (a carico dell'ammonito).

A sua volta, siffatto tema permette – o impone – di traguardarne un altro ancora, riassumibile nei delicati termini della convivenza ed interazione tra due distinti ordini di poteri: quelli (ben noti) dell'autorità giudiziaria e quelli (per certi versi meno conosciuti ai non addetti ai lavori) dell'autorità di pubblica sicurezza e segnatamente – per quanto concerne i provvedimenti di prevenzione di cui qui si tratta – dell'autorità tecnica di p.s. di livello provinciale, ossia il Questore.

Ciò, peraltro, in un contesto normativo in cui l'esigenza di approntare un sempre maggiore e più efficace statuto di tutela della vittima pare passare, sempre più spesso, oltre che per il tramite di un irrobustimento delle previsioni sostanzial-penalistiche e degli strumenti procedural-penalistici (e quindi dei poteri/doveri dell'autorità giudiziaria), attraverso l'implementazione delle prerogative e degli strumenti dell'autorità di pubblica sicurezza e segnatamente dei poteri di prevenzione del Questore.

Pare quindi imprescindibile, per una corretta impostazione dell'analisi del problema in trattazione, muovere dalla preliminare fissazione del ruolo e

(*) Vice Questore della Polizia di Stato, già frequentatore del XXXVI corso di Alta formazione presso la Scuola di perfezionamento per le forze di polizia.

delle prerogative istituzionali del Questore nel nostro ordinamento (specificamente in materia di misure di prevenzione), per poi passare in rassegna la natura e la disciplina degli istituti degli ammonimenti questorili introdotti dai decreti-legge n. 11 del 2009 e n. 93 del 2013, con precipuo riguardo allo spazio di operatività di essi rispetto all'azione penale esercitata dall'autorità giudiziaria (ed ai doveri della polizia giudiziaria funzionali ad assicurare l'obbligatorietà della predetta azione penale), ed infine giungere ad affrontare la disamina delle novità introdotte dalla legge n. 69/2019 recante disposizioni in materia di tutela delle vittime di violenza domestica e di genere (il c.d. codice rosso), con particolare attenzione alla novella dell'art. 347 c.p.p., in punto di obbligo della polizia giudiziaria di immediata trasmissione alla a.g. delle notizie di reato relative a taluni delitti, nel cui novero sono state ora ricomprese le fattispecie ex art. 612-bis c.p. e art. 582 c.p. (non anche quella ex art. 581), per le quali è ammesso il parallelo istituto preventivo dell'ammonimento questorile.

* * *

The manifest peculiarity and technical content of this dissertation includes, as a matter of fact, a wider and interesting topic related to the correlation between administrative procedure (for the adoption of the admonition measure enacted by the Questore - Chief of Local Police) and the criminal proceedings (against the admonished person).

Moreover, this topic includes another issue concerning the cohexistence and interaction between two different types of powers: the ones (well-known) of the judicial authority and the ones (perhaps less well-known to non-professional individuals in this field) of the public security authority and, in particular, the technical public security authority at provicial level, that is to say the Questore, as regards the prevention measures which are dealt with in this dissertation.

As a matter of fact, this is to be related to the legal framework in which the need to ensure more appropriate and effective measures to protect the victims involves the strenghtening of substantial and criminal provisions, procedural and criminal law instruments (and therefore the powers/duties of the judicial authority) as well as the implementation of the powers and legal tools of the public security authority, in particular the Questore's prevention powers.

Therefore, it is necessary to analyze, first of all, the institutional role and the powers of the Questore in our legislation (in particular in relation to the prevention measures), with the aim of carrying out a comprehensive survey

of the problem under examination. Then, the nature and the shape of the admonition measures enacted by the Questore and provided for by decree-laws nr. 11 of 2009 and nr. 93 of 2013 are taken into account, with a special focus on their range of operability in relation to the judicial powers exercised by the judicial authority (and the duties of criminal police, involving the obligation to implement the above mentioned measure). Finally, the study of the innovations introduced by Law nr. 69/2019 providing for measures aimed at protecting the victims of domestic and gender violence (the so called red code) has been conducted in this publication. A special attention has been focused on the new content provided for by Art. 347 of the Code of Criminial Procedure in relation to the obligation for criminal police to immediately transmit to the judicial authority the crime reports concerning some types of offences now including those provided for by Art. 612-bis of the Criminal Code and Art. 582 of the Criminal Code (not the one provided for by Art. 581), for which the parallel preventive admonition measure enacted by the Questore is accepted.

* * *

1. Il Questore quale autorità di pubblica sicurezza

1.1. Inquadramento ordinamentale e prerogative funzionali

La figura del Questore, nell'ordinamento italiano, è connotata da attribuzioni, ruoli e competenze suscettibili di frequenti incertezze e malintesi, anche tra gli addetti ai lavori, di tal ché si impone preliminarmente la fissazione dell'esatta posizione istituzionale occupata da essa e delle correlative responsabilità.

Ed invero, la ricorrente immagine del Questore quale vertice provinciale della Polizia di Stato coglie, in modo peraltro parziale od approssimativo, solo uno degli aspetti in cui è declinabile il suo ruolo istituzionale, con la duplice conseguenza, per un verso, di ridimensionarne sbrigativamente le prerogative sul piano della gestione di una forza di polizia o addirittura (ed erroneamente) alla stregua di una sorta di alto dirigente dei servizi di polizia giudiziaria esperiti dalla Polizia di Stato nella provincia (direzione che invece non gli appartiene affatto, essendo privo peraltro di qualsivoglia qualifica di p.g.) e, per altro verso, oscurare completamente la vera sfera di competenza assegnatagli dal legislatore e, quindi, l'essenza stessa del suo ruolo, che è quello di "autorità di pubblica sicurezza".

In tale ultima veste, il Questore è titolare di esclusive responsabilità e

attribuzioni di natura amministrativa, su un piano di assoluta autonomia e distinzione rispetto ad altri poteri dello Stato e segnatamente rispetto alle autorità giudiziarie.

Quanto al primo profilo, l'affermazione secondo cui il Questore sia il vertice della Polizia di Stato che presta servizio in una provincia merita qualche precisazione.

Intanto, quella del Questore è una funzione riservata ai dirigenti della Polizia di Stato, che siano titolari della qualifica apicale di "dirigente superiore" o "dirigente generale di pubblica sicurezza": con la precisazione che non tutti i dirigenti titolari di quelle qualifiche svolgano sempre la funzione questorile, per essi essendone previste anche altre, di diverso contenuto. In questo senso, quindi, l'associazione tra la figura del Questore e quella dell'alto dirigente della Polizia di Stato è vera solo in un senso (quello per cui il primo è necessariamente anche il secondo, ma non il contrario).

Il Questore è poi certamente il titolare dell'ufficio della Questura, di cui all'art. 32 della legge n. 121/1981, sicché egli è posto in posizione di sovraordinazione rispetto a tutto il personale (dell'Amministrazione civile dell'interno e della Polizia di Stato) che opera all'interno dei suoi uffici, compresi quelli decentrati dei Commissariati, sezionali e distaccati, e dei Posti di polizia.

Al riguardo, tuttavia, pare opportuno segnalare che, all'interno di siffatte articolazioni questorili, sono istituiti anche taluni uffici investigativi che, pur composti da personale sottordinato gerarchicamente al Questore, sono posti a disposizione delle autorità giudiziarie, siccome costituenti "*servizi di polizia giudiziaria*" ex art. 56 c.p.p. (essenzialmente Squadra mobile e Digos, nonché le squadre investigative dei Commissariati). Per altro verso, nella provincia, possono essere istituiti ed operare altri uffici della Polizia di Stato, strutturalmente non inquadrati nella Questura (ad esempio quelli dei Reparti mobili o Reparti prevenzione crimine, delle Scuole o delle Specialità della Polizia stradale, ferroviaria, postale e delle comunicazioni, delle frontiere), che, pur diretti da dirigenti della Polizia di Stato non gerarchicamente sottordinati al Questore (bensì, normalmente, ai titolari di uffici compartimentali sovraprovinciali o addirittura dei servizi dipartimentali centrali), sono comunque sottoposti a talune forme di coordinamento o poteri del Questore: ciò avviene, per esempio, per l'avvio dell'inchiesta disciplinare finalizzata all'irrogazione della sanzione della sospensione o destituzione dal servizio, che compete al Questore, ex art. 19 d.P.R. n. 737/1981, per tutto il personale della Polizia di Stato con qualifica non direttiva o dirigenziale che opera nella provincia (a prescindere dall'ufficio di appartenenza); per la comunicazione istituzionale della Polizia di Stato, che è accentrata in capo al portavoce del

Questore, con cui devono coordinarsi anche gli altri uffici della provincia, nonché per taluni aspetti logistici.

Occorre tuttavia rilevare che, su questo piano, la figura del Questore non presenti ancora tratti differenziali rispetto a quelli di ogni altro comandante o dirigente di una delle quattro forze di polizia, insediata su una provincia, sia pure con modalità particolarmente articolate.

La specificità e singolarità del ruolo del Questore nel nostro ordinamento si coglie, piuttosto, laddove si superi l'orizzonte della *Polizia di Stato* e si allarghi il campo di visione alla distinta e più ampia dimensione istituzionale della "*Amministrazione della pubblica sicurezza*", di cui si avvale il Ministro dell'interno, quale autorità nazionale, per l'espletamento dei suoi compiti in materia di ordine e sicurezza pubblica.

Essa è disciplinata nell'ambito della legge n. 121/1981, il cui art. 3, dopo avere precisato che l'Amministrazione della pubblica sicurezza è civile ed ha un ordinamento speciale, aggiunge che le sue funzioni sono esercitate da organi e soggetti che operano in dimensioni articolabili su quattro piani:

– il livello centrale del "*Dipartimento della pubblica sicurezza*" che, oltre alla direzione e amministrazione della Polizia di Stato, provvede all'attuazione della politica dell'ordine e della sicurezza pubblica ed al coordinamento tecnico-operativo delle forze di polizia: vi è preposto il Capo della Polizia - Direttore generale della pubblica sicurezza (si tratta, anche per tale figura, di funzione distinta da quella di vertice nazionale della Polizia di Stato);

– il livello delle "*autorità provinciali di pubblica sicurezza*", sia sul piano amministrativo generale (il Prefetto, ex art. 13 legge n. 121/1981)[1], sia sul piano tecnico-operativo (il Questore, ex art. 14 legge n. 121/1981);

---

1) Art. 13. "Prefetto".

Il prefetto è autorità provinciale di pubblica sicurezza.

Il prefetto ha la responsabilità generale dell'ordine e della sicurezza pubblica nella provincia e sovraintende all'attuazione delle direttive emanate in materia.

Assicura unità di indirizzo e coordinamento dei compiti e delle attività degli ufficiali ed agenti di pubblica sicurezza nella provincia, promuovendo le misure occorrenti.

A tali fini il prefetto deve essere tempestivamente informato dal questore e dai comandanti provinciali dell'Arma dei carabinieri e della Guardia di finanza su quanto comunque abbia attinenza con l'ordine e la sicurezza pubblica nella provincia.

Il prefetto dispone della forza pubblica e delle altre forze eventualmente poste a sua disposizione in base alle leggi vigenti e ne coordina le attività.

Il prefetto trasmette al Ministro dell'interno relazioni sull'attività delle forze di polizia in riferimento ai compiti di cui al presente articolo.

Il prefetto tiene informato il commissario del Governo nella regione sui provvedimenti che adotta nell'esercizio dei poteri ad esso attribuiti dalla presente legge.

– il livello comunale delle "*autorità locali*" di pubblica sicurezza, coincidenti con i Dirigenti dei Commissariati distaccati di pubblica sicurezza nel comune sede del presidio della Polizia di Stato (anche per essi, la qualità di autorità locale di p.s., nel comune, si cumula alla distinta responsabilità dell'ufficio della forza di polizia cui appartengono, che ha normalmente competenza sovracomunale) e, nei comuni in cui tali presìdi non sono istituiti, i Sindaci, quali ufficiali del Governo (art. 15 legge n. 121/1981)[2];

– il livello (per così dire diffuso) degli "*ufficiali ed agenti di pubblica sicurezza*", ovunque essi si trovino, i quali devono operare "*sotto la direzione delle autorità centrali e provinciali di pubblica sicurezza*".

In questo articolato sistema, il Questore occupa il posto peculiare e nevralgico di autorità provinciale di pubblica sicurezza (oltre che di autorità locale nel comune capoluogo), cui spetta la direzione, la responsabilità ed il coordinamento, a livello tecnico-operativo, dei servizi di ordine e di sicurezza pubblica e dell'impiego, a tal fine, della forza pubblica e delle altre forze eventualmente poste a sua disposizione (art. 14 legge n. 121/1981).

Il Questore, quindi, oltre ad essere il titolare e responsabile di un ufficio provinciale della Polizia di Stato (e come tale in posizione gerarchicamente sovraordinata ad altri pubblici ufficiali con attribuzioni di polizia giudiziaria e pubblica sicurezza in esso in servizio) è esso stesso un'autorità amministrativa, titolare di attribuzioni e responsabilità, con una *mission* istituzionale distinta, strumenti e risorse paralleli a quelli giudiziari e prerogative pregnanti che gli competono in via esclusiva[3].

Siffatte prerogative attengono innanzitutto al governo degli eventi inci-

---

2) Art. 15. "Autorità locali di pubblica sicurezza".
Sono autorità locali di pubblica sicurezza il questore nel capoluogo di provincia e i funzionari preposti ai commissariati di polizia aventi competenza negli altri comuni.
Ove non siano istituiti commissariati di polizia, le attribuzioni di autorità locale di pubblica sicurezza sono esercitate dal sindaco quale ufficiale di Governo.
Quando eccezionali esigenze di servizio lo richiedono, il prefetto, o il questore su autorizzazione del prefetto, può inviare funzionari della Polizia di Stato, nei comuni di cui al comma precedente, per assumere temporaneamente la direzione dei servizi di pubblica sicurezza. Resta in tale caso sospesa la competenza dell'autorità locale di pubblica sicurezza.
Le autorità provinciali di pubblica sicurezza, ai fini dell'ordine e della sicurezza pubblica e della prevenzione e difesa dalla violenza eversiva, sollecitano la collaborazione delle amministrazioni locali e mantengono rapporti con i sindaci dei comuni.

3) Cfr. S. Licciardello, *Il Questore*, Ed. Franco Angeli, 2016, secondo cui "il Questore agisce per la tutela dell'ordine e della sicurezza pubblica attraverso procedimenti amministrativi ed esercizio di discrezionalità tecnica che esprimono autonomia e responsabilità decisionale".

denti sull'ordine e la sicurezza pubblica: al Questore compete la pianificazione e direzione tecnica dei servizi, che si esprime in un potere di adottare "ordinanze di servizio", ai sensi dell'art. 37 d.P.R. n. 782/1985[4], indirizzate a tutti i soggetti coinvolti, volte a stabilire le modalità di svolgimento dei servizi stessi, la forza da impiegare, l'equipaggiamento necessario, i responsabili del servizio e le finalità da conseguire[5]. Nella stessa prospettiva, al Questore spettano i poteri ex art. 18 r.d. n. 773/1931 (TULPS) in materia di divieto o disciplina delle riunioni e manifestazioni pubbliche, che gli organizzatori sono invero tenuti a preannunciargli almeno tre giorni prima. Analogamente, il Questore può vietare, per ragioni di ordine pubblico o di sanità pubblica, le funzioni, le cerimonie, le pratiche religiose e le processioni o può prescrivere l'osservanza di determinate modalità (art. 26 TULPS), così come può vietare che il trasporto funebre avvenga in forma solenne ovvero può determinare speciali cautele a tutela dell'ordine pubblico e della sicurezza dei cittadini (art. 27 TULPS). Rientra, poi, nella dimensione delle attribuzioni assegnate al Questore, quale autorità di pubblica sicurezza, il potere (sancito dall'art. 100 TULPS) di so-

---

4) Art. 37 d.P.R. n. 782/1985. "Ordinanza di servizio in materia di ordine e sicurezza pubblica".
Per i servizi di ordine e sicurezza pubblica il Questore emana apposita ordinanza di servizio stabilendo le modalità di svolgimento dei servizi stessi, la forza da impiegare, l'equipaggiamento necessario, i responsabili del servizio e le finalità da conseguire.
L'ordinanza va comunicata al Prefetto e indirizzata per l'esecuzione ai dirigenti degli uffici, ai funzionari impiegati nonché alle altre forze di polizia ed altri enti eventualmente interessati.
L'ordinanza emanata dal Questore di Roma va inoltre inviata per conoscenza al Dipartimento della pubblica sicurezza e agli ispettorati della Polizia di Stato esistenti nella capitale.
L'ordinanza di servizio numerata progressivamente va conservata agli atti per un periodo di cinque anni.

5) G. Aliquó, "*Il Questore, autorità nel sistema della sicurezza complementare*", Quaderno della Rivista trimestrale della Scuola di perfezionamento per le forze di polizia, II/2015, sottolinea che "la primazia del questore si afferma, proprio in fase di coordinamento tecnico dei servizi delle Forze di polizia, per il quale utile strumento è il Tavolo tecnico, che può essere convocato dal questore in vista dell'emanazione della ordinanza di servizio ex art. 37 d.P.R. n. 782/1985. Il Tavolo tecnico, istituito al punto 4 del decreto del Ministro dell'interno del 12 febbraio 2001, è il luogo in ci, ottenute le direttive e gli eventuali indirizzi del prefetto, sarà possibile raggiungere le intese per l'esecuzione dei servizi. Esso si atteggia come organismo consultivo tecnico del questore [...] ". Al riguardo, la direttiva del Capo della polizia – Direttore generale della pubblica sicurezza n. 555/OP/490/2009/1/NC del 1 gennaio 2009 segnala che il tavolo tecnico costituisca "proiezione esterna – di governo tecnico dell'evento – raccogliendo il testimone del Comitato provinciale [...]".

spendere o revocare le licenze concernenti tutti gli esercizi pubblici (anche quelli, come i bar, la cui apertura non presuppone autorizzazioni questorili, bensì solo commerciali), laddove gli stessi costituiscano – anche alla stregua di valutazioni che prescindono da profili di responsabilità dei titolari o gestori – oggettivo pericolo per l'ordine pubblico, per la moralità pubblica e il buon costume o per la sicurezza dei cittadini.

Al Questore, quale autorità amministrativa, compete il governo e controllo di settori della vita privata ed economica dei cittadini, ritenuti sensibili per i profili della sicurezza pubblica e quindi suscettibili di un articolato regime autorizzatorio, in cui si esplica un potere provvedimentale, proprio o talora delegato: si pensi al rilascio di passaporto o titolo di viaggio per minori (su delega del Ministero degli affari esteri e della cooperazione internazionale) onde legittimare l'espatrio dei cittadini italiani; all'adozione di provvedimenti autorizzatori in materia di armi (nulla osta all'acquisto di arma, autorizzazione al porto d'arma lunga); alle autorizzazioni in materia di pubblici spettacoli (come ad esempio la licenza per concerti o incontri di calcio allo stadio o gare sportive in genere) o in materia di attività economiche ritenute sensibili (quali gioiellerie, compro oro, sale scommesse, *internet point*, agenzie di noleggio auto, agenzie investigative ed altro).

Al Questore spetta poi, ai sensi del d.lgs. n. 286/1998 (T.U. Immigrazione), la gestione del fenomeno immigratorio sul territorio nazionale, sia in punto di potestà provvedimentale in materia di rilascio dei titoli di soggiorno per gli stranieri, sia in punto d'istruzione ed esecuzione dei provvedimenti di espulsione ed allontanamento dal territorio nazionale dei cittadini stranieri (rispettivamente extracomunitari e comunitari), emessi dal Prefetto: al riguardo, al Questore compete l'adozione del decreto di trattenimento dell'espellendo, nei centri di permanenza per i rimpatri di cui all'art. 14 T.U. Immigrati, oltre che la ricezione delle istanze di asilo e protezione internazionale in genere.

Ma al Questore competono attribuzioni esclusive anche in un ulteriore campo, particolarmente delicato e sempre più strategicamente attuale nel panorama legislativo italiano: quello delle *misure di prevenzione*, alle quali pare opportuno riservare specifica attenzione.

1.2. Le competenze del Questore in materia di *misure di prevenzione*

Fin dalla legge n. 1423/1956 (per restringere il campo allo scenario successivo all'emanazione della Costituzione repubblicana), l'ordinamento italiano contempla un sistema di "misure di prevenzione", espressione dell'avvertita esigenza di approntare strumenti *ante delictum*, idonei a scongiurare la

stessa verificazione di quelle lesioni ai beni giuridici tutelati, che il diritto penale reprime solo dopo la loro commissione[6].

Il catalogo delle misure preventive è stato successivamente implementato da leggi speciali, sovente di emergenza, fino a confluire in una, seppur parziale, codificazione sistematica tracciata nell'ambito del d.lgs. n. 159/2011 (peraltro noto come "codice delle leggi antimafia", ancorché intitolato anche alla codificazione delle misure preventive, disciplinate nel libro I del testo normativo)[7].

---

6) Sulla recente riscoperta degli strumenti preventivi, cfr. (pur con considerazioni critiche) F. Basile, *Le misure di prevenzione dopo il c.d. Codice Antimafia. Aspetti sostanziali e aspetti procedurali. Brevi considerazioni introduttive sulle misure di prevenzione*, in *Giur. it*., 2015, 6, 1520, che parla di "crisi della pena" e "boom delle misure di prevenzione", precisando: "Che le misure di prevenzione svolgano una funzione di surrogato rispetto alle pene potrebbe essere vero anche in un'ulteriore prospettiva. La crisi di certezza ed efficacia di cui oggi soffre notoriamente la pena potrebbe, infatti, in qualche modo aver favorito la forte espansione – legislativa e applicativa – conosciuta dalle misure di prevenzione negli ultimi anni: legislatore e giudice, insomma, non potendo più 'contare' sulla pena, avrebbero rivolto le loro preferenze alle misure di prevenzione, ritenute più certe, più celeri e più efficaci. Al punto che forse dovremmo riscrivere le pagine dei manuali dove si parla del "doppio binario" su cui si fonda il sistema penale, giacché questo ormai corre in realtà anche su un "terzo binario" – quello delle misure di prevenzione – il quale, peraltro, si sta rivelando, rispetto al binario delle pene e delle misure di sicurezza, un binario ad alta velocità! Le misure di prevenzione sono, infatti, oggigiorno divenute un pilastro dell'opera statale di contrasto di alcune forme di criminalità, la cui efficacia risiede anche nell'intreccio, che esse assicurano, tra profili di prevenzione e profili di repressione, e in ogni caso nel loro grado di afflittività che, per taluni aspetti, può risultare pari, se non superiore, a quello delle pene vere e proprie". Nello stesso senso, sia pure con riguardo a diverse misure preventive (come le interdittive antimafia) cfr. V. Antonelli, *Il diritto amministrativo preventivo a servizio della sicurezza pubblica*, in *Dir. pen. e processo*, 2019, 11, 1503: "Con la crescente introduzione da parte del diritto amministrativo di istituti finalizzati a garantire la sicurezza pubblica si consolida la tendenza del nostro ordinamento a spostare sul versante della prevenzione il contrasto alle molteplici forme di illegalità e di criminalità. Lo scopo perseguito dal legislatore è quello di rafforzare l'efficacia dissuasiva delle norme penali e di agevolare la repressione dei fenomeni criminali attraverso la prevenzione amministrativa. [...] La finalizzazione alla "sicurezza pubblica" da parte del diritto amministrativo di alcuni istituti consolida la tendenza del nostro ordinamento a spostare e al contempo a rafforzare sul versante della prevenzione il contrasto alle molteplici forme di illegalità e di criminalità. Una "sicurezza pubblica" perseguita attraverso misure amministrative che trova nella cosiddetta normativa "antimafia" e in quella "anticorruzione" due importanti antecedenti. Lo scopo perseguito dal legislatore è quello di rafforzare l'efficacia dissuasiva delle norme penali e di agevolare la repressione dei fenomeni criminali attraverso misure a carattere amministrativo: si passa in tal modo dalla repressione penale alla prevenzione amministrativa".

7) Il d.lgs. n. 159/2017 è stato integrato dalla legge n. 161/2017 e più da ultimo, dal decreto-legge 4 ottobre 2018, n. 113 convertito, con modificazioni, dalla legge 1 dicembre 2018, n. 132, che ha riscritto il comma 3-*bis* dell'articolo 17 del Codice delle leggi antimafia (ru-

Si tratta, come noto, di misure la cui natura è tradizionalmente ricondotta nell'ambito del diritto amministrativo, segnatamente del diritto amministrativo di polizia, e con riguardo alle quali spicca corrispondentemente il ruolo centrale dell'autorità tecnica di pubblica sicurezza di livello provinciale, ossia del Questore (che peraltro si muove in un contesto la cui autonomia, segnatamente rispetto al piano giudiziario, è esplicitamente sancita dall'art. 29 d.lgs. n. 159/2011).

Siffatta centralità è evidente sotto vari punti di vista.

Innanzitutto, il Questore (quello territorialmente competente, in relazione al luogo di dimora dell'indiziato) è legislativamente individuato quale autorità responsabile dell'*esecuzione* delle misure preventive *personali*.

Ai sensi dell'art. 11 comma 1 d.lgs. n. 159/2011, gli vanno quindi comunicati i relativi decreti autorizzativi delle misure. E l'art. 69 comma 2 del Codice antimafia disciplina gli obblighi, gravanti in capo alle cancellerie, circa puntuali comunicazioni, al riguardo, verso le Questure, che curano peraltro l'inserimento delle relative segnalazioni nella banca dati interforze.

Il Questore è poi titolare – oggi unitamente al Procuratore della Repubblica, al Procuratore nazionale antimafia ed antiterrorismo ed al Direttore della DIA – di un autonomo *potere di proposta* in materia di adozione di misure di

---

bricato "titolarità della proposta") in materia di proposta preventiva patrimoniale, con l'intento di restituire centralità alla figura del Questore in un sistema di prevenzione nel quale i titolari del potere di proposta sono collocati in posizione paritetica (così circolare esplicativa Ministero dell'interno del 14 gennaio 2019). Ed invero, il d.l. n. 113/2018, pur continuando a riconoscere in capo al Procuratore della Repubblica distrettuale la fondamentale funzione di coordinamento informativo in materia di misure di prevenzione patrimoniali, ha innovato la disciplina complessiva degli oneri di comunicazione previsti dal citato comma 3-*bis* dell'art. 17. In primo luogo, è stata disposta l'abrogazione dell'intera lettera d), che imponeva al Questore e al Direttore della D.I.A. di comunicare al Procuratore della Repubblica distrettuale, qualora avessero ritenuto di non dover esercitare l'azione di prevenzione, provvedimento motivato. In secondo luogo, il legislatore è intervenuto sulla lettera c) prevedendo che la comunicazione della proposta al Procuratore della Repubblica presso il tribunale del capoluogo del distretto – da dare almeno dieci giorni prima della sua presentazione al Tribunale – sia "sintetica". Inoltre, è stata eliminata la "sanzione" dell'inammissibilità della proposta, nel caso di mancata presentazione entro il termine previsto nel precedente capoverso, ed è stato contestualmente introdotto l'onere per il Procuratore della Repubblica distrettuale, nei dieci giorni successivi alla comunicazione della proposta, di informare l'autorità proponente dell'eventuale sussistenza di pregiudizi per le indagini preliminari. In questi casi, l'autorità giudiziaria e il Questore o il Direttore della D.I.A. potranno concordare modalità per la presentazione congiunta della proposta, già proficuamente sperimentate in varie realtà territoriali.

prevenzione, sia personale (la *sorveglianza speciale di pubblica sicurezza*, con o senza obblighi o divieti di soggiorno in determinati Comuni), sia patrimoniale (sequestro, confisca, amministrazione giudiziaria dei beni connessi ad attività economiche) nei confronti di una serie di soggetti, il cui corposo elenco è fissato all'art. 4 del d.lgs. n. 1598/2011: in quest'ultimo, attualissimo ambito, peraltro, la legge riconosce al Questore l'iniziativa di avviare autonomamente indagini patrimoniali, finalizzate alla richiesta di misure ablative, addirittura con un potere di delega dei relativi accertamenti alla polizia giudiziaria (che pure è istituzionalmente posta a disposizione dell'autorità giudiziaria) ed anche alla Guardia di finanza (art. 19 d.lgs. n. 159/2019).

Ma, ai fini che qui ci occupano, pare opportuno sottolineare che al Questore competa anche, in via esclusiva, il potere decisorio, da esercitarsi in forma provvedimentale, circa l'adozione di molte misure di prevenzione di natura personale, il cui novero peraltro ha conosciuto, nell'ultimo trentennio, un sempre maggiore e puntuale ampliamento.

Invero, il capo I del titolo I del libro I del c.d. Codice antimafia (esplicitamente intitolato alle "*Misure di prevenzione personali applicate dal Questore*") contempla le c.d. misure preventive questorili "tipiche", già recepite fin dalla legge del 1956 come rimesse al potere provvedimentale del Questore:

– l'ordine di rimpatrio con foglio di via obbligatorio (art. 2);
– l'avviso orale (art. 3).

Riguardo a quest'ultima misura, si segnala che l'art. 3, comma 4, del d.lgs. n. 159/2011 prevede una *forma aggravata di avviso orale*, irrogabile nei confronti di coloro i quali hanno riportato condanne definitive per delitti non colposi. In tal caso, il Questore può imporre al destinatario il divieto di possedere o utilizzare, in tutto o in parte, tra gli altri oggetti, qualsiasi apparato di comunicazione radiotrasmittente (compreso il cellulare o tablet).

Ma il legislatore, spinto dall'esigenza di infrenare fenomeni particolarmente insidiosi per la sicurezza pubblica, ovvero assicurare una tutela anticipata ed efficace alle vittime di fatti avvertiti come particolarmente gravi e pericolosi, ha sempre più arricchito il panorama con altri strumenti "atipici", che partecipano pacificamente della stessa natura giuridica preventiva e che sono stati attribuiti esclusivamente al potere provvedimentale del Questore.

Tra essi, si segnala il c.d. "D.A.SPO" (Divieto di avvicinamento ai luoghi di manifestazioni sportive, eventualmente con prescrizione di comparizione personale ad un ufficio di polizia), originariamente introdotto dall'art. 6 della legge n. 401/1989, con precipuo riguardo al contrasto delle violenze negli stadi ed impianti sportivi.

Si tratta di una misura amministrativa svincolata dalla condanna, che può essere adottata nell'immediatezza dei fatti e prima del processo penale e, pertanto, differisce da quello irrogabile dall'autorità giudiziaria con sentenza di condanna, per i reati commessi in occasione o a causa di manifestazioni sportive (art. 6, comma 7, l. n. 401/1989, c.d. *D.A.Spo. giudiziario*).

Mutuando la disciplina dell'avviso orale aggravato, di cui all'art. 3 comma 4 d.lgs. 159/2011, il legislatore, con il decreto-legge n. 53/2019, ha inserito nell'art. 6 legge n. 401/1989, il comma 8-*ter*, che consente al Questore, all'atto dell'adozione del provvedimento di D.A.Spo., di imporre alle persone che risultino definitivamente condannate, per delitti non colposi, il divieto di possedere o utilizzare, in tutto o in parte, qualsiasi apparato di comunicazione radiotrasmittente, oltre ad altri oggetti sensibili.

Si tratta del c. d "D.A.SPO Aggravato".

Di recente, il modello del D.A.SPO è stato assunto a riferimento per l'elaborazione di innovative misure di prevenzione attagliate sui fenomeni di degrado e pregiudizio della sicurezza urbana, con l'istituzione del c.d. ordine di allontanamento e conseguente "*daspo urbano*" o "D.A.C.UR" (di cui agli artt. 9 e 10 del d.l. 20 febbraio 2017, n. 14, convertito nella l. 18 aprile 2017, n. 48), e di un analogo provvedimento interdittivo per denunciati e/o condannati per reati in materia di droga, ex art. 73 d.P.R. n. 309/1990, recante divieto di accedere o stazionare nei pressi di scuole, locali o esercizi analoghi a quelli in prossimità dei quali risultassero avere commesso i fatti penalmente rilevanti (art. 13 d.l. 20 febbraio 2017, n. 14, convertito nella l. 18 aprile 2017, n. 48)[8].

Tra le misure preventive attribuite alla potestà provvedimentale del Questore, poi, rientrano gli "ammonimenti": quello introdotto per gli *atti persecutori* (art. 8 d.l. n. 11 del 2009, convertito in legge n. 38/2009); quello per fatti di *violenza domestica* (art. 3 d.l. n. 93/2013, convertito in legge n. 119

8) Da ultimo, il d.l. n. 113/2018 ha introdotto, nell'impianto normativo del d.l. n. 14/2017, un nuovo art. 13-*bis*, a norma del quale il Questore può disporre la speciale misura anche nei confronti delle persone condannate con sentenza definitiva o confermata in grado di appello nel corso degli ultimi tre anni per reati commessi in occasione di gravi disordini avvenuti in pubblici esercizi ovvero in locali di pubblico trattenimento, per delitti non colposi contro la persona e il patrimonio, nonché per i delitti previsti dall'articolo 73 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309: per essi è previsto il divieto di accesso agli stessi locali o ad esercizi pubblici analoghi, specificamente indicati, ovvero di stazionamento nelle immediate vicinanze degli stessi, limitato a specifiche fasce orarie e con possibile prescrizione di comparire personalmente una o più volte, negli orari indicati, nell'ufficio o comando di polizia competente in relazione al luogo di residenza dell'obbligato o in quello specificamente indicato.

del 2013) e quello, più recentemente introdotto, finalizzato al contrasto del c.d. *cyberbullismo* (art. 7 della legge 29 maggio 2017 n. 71, recante "disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo").

Su tali ultimi istituti monitori ci si soffermerà nelle pagine seguenti.

1.3. Disponibilità degli "Ufficiali ed agenti di pubblica sicurezza"

Prima di addentrarsi nell'esame delle problematiche connesse ai procedimenti monitori questorili ed ai loro rapporti con i procedimenti giudiziari penali, pare però il caso di fissare una preliminare precisazione circa la rete di soggetti di cui il Questore (beninteso, ancora una volta, nella sua distinta qualità di autorità provinciale di pubblica sicurezza) disponga, per lo svolgimento dei propri compiti istituzionali.

Nozione

Invero, nel declinare il testé ribadito ruolo istituzionale del Questore, si è già accennato alla previsione dell'art. 3 della legge n. 121/1981, secondo cui l'Amministrazione della pubblica sicurezza svolge i suoi compiti tramite le "*autorità di pubblica sicurezza*" e gli "*ufficiali ed agenti di pubblica sicurezza*", i quali ultimi operano "*sotto la direzione*" dei primi: *rectius*, delle sole "*autorità centrali e provinciali*".

Ciò premesso, non pare residuare alcun dubbio sulla circostanza che il Questore, nei limiti delle sue competenze di *autorità di p.s.* provinciale, sul piano tecnico-operativo, possa certamente avvalersi – come in effetti avviene – di *ufficiali ed agenti di p.s.* che sono sottoposti alla sua "direzione", all'insegna di un modello che pare tradire un suggestivo parallelismo con quello disegnato, nella distinta dimensione della procedura penale, dai rapporti di disponibilità degli ufficiali ed agenti di *polizia giudiziaria* da parte dell'autorità giudiziaria.

Ricorrono, del resto, ulteriori elementi di analogia.

Come per la polizia giudiziaria, anche gli ufficiali ed agenti di pubblica sicurezza costituiscono un insieme eterogeneo di figure appartenenti trasversalmente a tutte le forze di polizia, oltre che ad altre istituzioni (come *infra* si specificherà).

Quanto all'impiego, abbiamo già sopra intravisto come, in analogia alla possibilità di delega magistratuale indirizzata alla polizia giudiziaria, anche il Questore possa disporre degli ufficiali ed agenti di p.s., tramite il pregnante strumento formale dell'ordinanza di servizio, ex art. 37 d.P.R. n. 782/1985,

con cui prevedere e disciplinare l'impiego, in servizio di ordine pubblico, anche di consistenti aliquote di personale ed addirittura designare nominativamente un ufficiale di pubblica sicurezza quale responsabile del servizio, con le connesse responsabilità giuridiche.

Del resto, poi, il Questore può anche ricorrere a modalità più dirette e speditive di disposizione: si pensi ai frequenti casi di delega ad ufficiali di p.s. (anche non appartenenti alla Polizia di Stato), circa l'esecuzione di misure di prevenzione "tipiche" disposte dall'autorità provinciale (tipicamente, laddove la segnalazione iniziale provenga dagli stessi ufficiali), ovvero alle richieste di informazioni utili all'istruttoria di procedimenti amministrativi finalizzati al rilascio di licenze di polizia, di competenza questorile (esemplificativamente, in materia di armi).

Occorre tuttavia prendere atto che, se la *polizia giudiziaria* ed i suoi rapporti con l'autorità giudiziaria costituiscono oggetto di un'organica e dettagliata disciplina normativa (essenzialmente codicistica, siccome fissata dal titolo III del libro I del Codice di procedura penale), non altrettanto avviene per gli *ufficiali ed agenti di pubblica sicurezza* ed i loro rapporti con le autorità di p.s., di tal ché residuano molti dubbi, segnatamente – per ciò che più attiene al tema del presente lavoro – con riguardo ai profili della segnalazione di fatti rilevanti per l'attivazione delle attribuzioni questorili ed ai compiti istruttori attraverso i quali l'autorità provinciale possa disporre del sostrato informativo idoneo a svolgere il percorso valutativo e decisionale che gli compete per esercitare le sue competenze provvedimentali.

Invero, le leggi relative agli *ufficiali ed agenti di pubblica sicurezza* sono raccolte in un testo unico adottato con r.d. n. 690 del 31 agosto 1907. Ulteriori indicazioni si colgono nel Testo Unico delle leggi di Pubblica Sicurezza (TULPS), adottato con il r.d. n. 773 del 18 giugno 1931 e nel regolamento di esecuzione al TULPS di cui al r.d. n. 635/ 1940. Si tratta, tuttavia, di una disciplina molto risalente e comunque oltremodo scarna, anche in ordine ai punti di interesse sopra cennati[9].

9) Sul parallelismo citato nel testo, cfr. C. Mosca, *La sicurezza come diritto di libertà*, Cedam, Padova, 2012: "Il sistema della pubblica sicurezza incentrato sulle autorità, sugli ufficiali e sugli agenti ai quali è affidata la gestione degli interventi in materia viene, con la legge n. 121/81, a configurarsi come parallelo al sistema giudiziario […]. Due sistemi, quindi, che meritano uno specifico raccordo, pur restando essi stessi fondamentalmente autonomi, ma richiedono al contempo una loro attenta definizione, soprattutto sul versante delle funzioni espletate sul fronte della sicurezza". Sulle lacune normative, al riguardo, Cfr. C. Mosca, *Teoria generale del coordinamento delle Forze di polizia*, in M. Morcel-

Elenco

Già l'elencazione dei soggetti titolari di tali qualifiche – si ribadisce: del tutto distinte e diverse da quelle di polizia giudiziaria – è ricavabile da una serie estremamente frammentaria di forti normative, nel cui ambito sono distinguibili:

– *ufficiali di pubblica sicurezza*: sono tali i funzionari della Polizia di Stato (art. art. 2 d.lgs. n. 334/2000), gli ufficiali dell'Arma dei Carabinieri (art. 179 d.lgs. n. 66/2010), nonché il Sindaco, nel territorio del proprio comune, se privo di altri ufficiali di p.s. (artt. 6-12 r.d. n. 690/1907)[10];

– *sostituti ufficiali di p.s.* (destinati ad esercitare le funzioni dell'ufficiale solo in caso di sua assenza o impedimento): sono tali i funzionari della Polizia penitenziaria (artt. 6-21 d.lgs. n. 146/2000); i Sostituti Commissari e gli Ispettori S.U.P.S. della Polizia di Stato (art. 26 d.P.R. n. 335/1982); i Luogotenenti ed i Marescialli Aiutanti S.U.P.S. dell'Arma dei Carabinieri;

– *agenti di pubblica sicurezza*: sono tali tutti gli appartenenti alle forze di polizia, non titolari di altra delle qualifiche sopra citate; i militari delle forze armate posti a disposizione delle autorità di p.s. per servizi di pubblica sicurezza (si pensi ai militari impiegati in specifiche e sempre più frequenti operazioni di pattugliamento del territorio nazionale in relazione a fenomeni emergenziali); gli appartenenti al Corpo dei Vigili del fuoco, ai sensi dell'art. 8, comma 1, della legge 27 dicembre 1941, n.1570; gli appartenenti ai Corpi di Polizia municipale cui sia stata attribuita la qualifica dal Prefetto (art. 5 legge n. 65/1986), nonché una serie amplissima di altri soggetti tra cui rientrano, solo esemplificativamente, gli appartenenti a corpi di vigilanza, guardie campestri, boschive, cantonieri ed altri soggetti privati, nominati agenti di pubblica sicurezza, con decreto del Prefetto ai sensi dell'art. 4-*bis* del r.d. 06/05/1940, n. 635.

LINI - C. MOSCA (a cura di), *La sapienza della sicurezza*, Maggioli, Santarcangelo di Romagna, 2014. L'A. indica la "necessità che, come avvenuto per l'autorità giudiziaria e per gli ufficiali e agenti di polizia giudiziaria, in base a quanto puntualmente chiarito dal codice di procedura penale, vengano sottolineati nel testo unico delle leggi di pubblica sicurezza ruoli, funzioni e distinzioni" per l'autorità di pubblica sicurezza nonché per gli ufficiali e agenti di pubblica sicurezza.

10) Il decreto legislativo 29 maggio 2017 n. 95 ha inoltre previsto che gli ufficiali del ruolo normale e gli ispettori del Corpo della Guardia di finanza, comandanti di reparti navali e di unità navali, sono *ufficiali di pubblica sicurezza*, limitatamente alle funzioni esercitate in mare. La previsione è collegata alla previsione dell'articolo 2 del decreto legislativo 19 agosto 2016 n. 177, che affida alla Guardia di finanza il comparto di specialità inerente alla polizia del mare.

Compiti

Siffatta variegata ed ampia schiera di figure è connotata, oltre che dalla già chiarita soggezione alla direzione delle "autorità di pubblica sicurezza", per le finalità dell'Amministrazione della pubblica sicurezza, dal comune orientamento funzionale del relativo servizio ai compiti sanciti dall'art. 34 r.d. n. 690/1907 (il cui contenuto è stato poi ripreso dall'art. 1 TULPS in punto di fissazione delle competenze dell'autorità di p.s.), secondo cui "*gli ufficiali ed agenti di pubblica sicurezza vegliano al mantenimento dell'ordine pubblico, all'incolumità e alla tutela delle persone e delle proprietà, in genere alla prevenzione dei reati, raccolgono le prove di questi e procedono alla scoperta, ed in ordine alle disposizioni della legge, all'arresto dei delinquenti; curano l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle province e dei comuni, come pure delle ordinanze delle pubbliche autorità; prestano soccorso in casi di pubblici e privati infortuni*".

Pare il caso di sottolineare, al riguardo, come già il testo unico del 1907 contemplasse, tra i primissimi obiettivi istituzionali assegnati agli agenti ed ufficiali di pubblica sicurezza, la "*tutela delle persone*" e della loro "*incolumità*": una previsione di straordinaria modernità che sembra anticipare, di molti decenni, non solo il principio della tutela della persona umana fissato dalla Costituzione repubblicana ma, per ciò che qui ci occupa, il doveroso impegno statuale nella direzione di approntare un'efficace prevenzione e protezione della vittima[11].

Atti

Ma altrettanto complessa è la ricostruzione di uno statuto disciplinare organico degli *atti* dei predetti soggetti, segnatamente quelli istruttori, in un quadro normativo in cui difetta una regolamentazione sistematica (a differenza di quanto avviene nel campo penale ma anche in quello, pure affine, degli illeciti amministrativi ex art. 13 legge n. 689/1981) e occorre piuttosto valorizzare diffusi riferimenti e variegati istituti.

---

11) Il dovere di effettiva protezione della vittima (segnatamente delle vittime di violenza domestica e delle persone vulnerabili in genere, come donne e bambini), oltre a costituire il perno degli interventi legislativi e degli istituti che saranno trattati nel presente lavoro, è oggi sempre più sottolineato anche in seno alla giurisprudenza della Corte europea dei diritti dell'uomo: cfr. al riguardo, la celebre sentenza CEDU n. 41237/14 del 2 marzo 2017 (nella causa Talpis c. Italia), che – in applicazione degli artt. 2 e 3 della Convenzione europea dei diritti dell'uomo – ha condannato l'Italia per non avere adottato adeguate misure di tutela di una donna e del figlio, a fronte delle minacce e violenze del marito.

In questo quadro, certamente rilevante pare la previsione ex art. 15 TULPS, che riconosce all'autorità di pubblica sicurezza, tramite i suoi ufficiali ed agenti, un *potere di convocazione*, tutelato da sanzione amministrativa ed assistito dalla possibilità di ricorrere all'impiego della forza pubblica, evidentemente funzionale all'acquisizione di informazioni dai convocati, utili all'esercizio dei compiti dell'autorità.

L'*audizione dello stesso interessato* è, nei casi in cui le attribuzioni dell'autorità di p.s. si esplichino in forme tecnicamente "procedimentali", momento imposto dalle previsioni della legge n. 241/1990 in materia di garanzie partecipative (con talune possibili eccezioni connesse all'urgenza, ex art. 7 legge medesima), ma è senz'altro possibile, per gli agenti ed ufficiali di p.s., anche *sentire soggetti terzi*, informati sui fatti, la cui conoscenza sia utile ai fini di pubblica sicurezza. Del resto, la necessaria acquisizione e valutazione di un adeguato patrimonio informativo (che deve risultare nella motivazione del provvedimento ex art. 3 legge n. 241/1990) è, in generale, coessenziale al ponderato svolgimento dell'azione amministrativa in forma procedimentale, oltre che spesso prevista esplicitamente dalle discipline dei singoli procedimenti (come, infatti, si vedrà anche per quelli monitori questorili, oggetto del presente lavoro).

Nessun particolare ostacolo, poi, sembra frapporsi alla possibilità, per gli agenti ed ufficiali di pubblica sicurezza (che procedano per compiti di istituto e segnatamente per l'istruzione di procedimenti di competenza dell'autorità di p.s.), di acquisizione di documenti detenuti da pubbliche amministrazioni, oltre che di ispezioni di luoghi pubblici o, col consenso di chi possa disporne, anche privati.

Quanto agli obblighi di documentazione di tali attività, poi, soccorre la previsione ex art. 37 r.d. n. 690/1907, secondo cui "*gli ufficiali ed agenti di pubblica sicurezza dovranno distendere verbale e fare rapporto di quanto hanno eseguito o potuto osservare in servizio*".

Agli agenti ed ufficiali di p.s. competono poi taluni esclusivi poteri-doveri, funzionali ad aspetti specifici delle relative attività, ma suscettibili di assicurare ampi spettri di conoscenza di fatti rilevanti per le finalità di pubblica sicurezza. In tal senso, rileva la previsione dell'art. 16 TULPS in punto di facoltà di accedere, in qualunque ora, nei locali destinati all'esercizio di attività soggette a qualsivoglia autorizzazione di polizia, ovvero quella dell'art. 4 TULPS, relativa alla facoltà di ordinare rilievi segnaletici nei confronti di persone ritenute pericolose o sospette, ovvero ancora quella ex art. 4 legge n. 152/1975, circa la facoltà di procedere all'identificazione e perquisizione, sul posto, di persone la cui presenza non appaia ivi giustificabile, onde rintracciare

il possesso di armi o strumenti di effrazione. Né va sottaciuta la possibilità di conoscere situazioni suscettibili di rilievo anche nel corso di quella *composizione dei privati dissidi* che l'art. 35 r.d. n. 690/1907 e l'art. 1 r.d. n. 773/1931 (TULPS) assegnano alla competenza dell'autorità di pubblica sicurezza, per il tramite dei suoi ufficiali di p.s., su istanza di parte.

Ciononostante, le lacune ed i dubbi che permangono sull'efficacia gnoseologica degli atti così acquisiti nei procedimenti questorili, nonché sulla stessa sufficienza di essi a supportare adeguatamente le ampie prerogative ed attribuzioni funzionali dell'autorità di pubblica sicurezza, denunciano una vera e propria lacuna nel nostro ordinamento giuridico, che si appalesa sempre più grave[12].

Obblighi informativi

Occorre conclusivamente dare atto di un'ulteriore funzione essenziale ascrivibile agli *agenti ed ufficiali di pubblica sicurezza* nell'articolato sistema delineato dal legislatore (su cui peraltro è percepibile un'altra possibile analogia con la parallela ma distinta articolazione della polizia giudiziaria): essi costituiscono, sul territorio nazionale e nell'ambito di istituzioni o contesti di appartenenza dalla natura molto diversa, un sistema trasversale e diffuso di capillare presidio, idoneo ad intercettare costantemente ogni situazione di pregiudizio per l'ordine e la sicurezza pubblica, ed a veicolarne la segnalazione verso le autorità di pubblica sicurezza, provinciali e nazionali[13].

Questo flusso informativo sembra anche esplicitamente contemplato dall'art. 36. r.d. n. 690/1907, secondo cui "*gli agenti di pubblica sicurezza debbono informare prontamente, per iscritto, gli ufficiali di sicurezza, nella cui circoscrizione si trovano, di ogni reato, e di ogni avvenimento importante che accada nei luoghi dove prestano servizio* [...]", nonché dal comma 3 dell'art. 14 della legge n. 121/1981, recante precisi obblighi informativi verso il Questore, gravanti sui comandanti locali dell'Arma dei Carabinieri e della Guardia di finanza, su quanto comunque abbia attinenza con l'ordine e la sicurezza pubblica nei territori di competenza.

---

12) In questi termini cfr. G. Aliquó, *La violenza domestica. L'ammonimento del Questore*, Pacini Giuridica, 2019, p. 130.

13) G. Aliquó, *Il Questore, autorità nel sistema della sicurezza complementare*, cit., evoca, al riguardo, l'immagine di una "rete aperta" di sensori che deve garantire la circolarità delle informazioni e delle analisi, "quale strumento di conoscenza per l'Amministrazione della pubblica sicurezza, ai fini della migliore tutela dell'ordine e della sicurezza pubblica, ma anche per il Sistema della sicurezza nazionale nel suo complesso". Un sistema reticolare aperto, peraltro, alle potenzialità offerte dalle interazioni tra soggetti pubblici e privati, in un articolato sistema governato dall'Amministrazione e dalle autorità di p.s.

Il tema impone però uno scandagliamento ulteriore.

Invero, il tenore delle predette disposizioni sembra definire l'oggetto delle informazioni, che devono essere avviate verso le autorità di pubblica sicurezza, con riguardo alla sola ricorrenza di fatti pregiudizievoli per la convivenza civile, in una prospettiva di circolarità informativa, verso l'alto, essenzialmente finalizzata ad un'accentrata e puntuale gestione della situazione dell'ordine pubblico sul territorio nazionale.

Ma, ragioni connesse alle sopra rievocate finalità istituzionali assegnate dallo stesso legislatore precostituzionale ai protagonisti del sistema della pubblica sicurezza (in punto di tutela delle persone e della loro incolumità), nonché un obbligo di rilettura costituzionalmente orientata degli strumenti normativi e degli istituti giuridici previgenti, impone di ritenere gli *agenti ed ufficiali di pubblica sicurezza* tenuti a veicolare verso l'alto, immediatamente (o almeno con quella tempestività che assicuri la persistente efficacia degli interventi successivi), anche le segnalazioni di fatti suscettibili di rilevare per la tutela del "diritto alla sicurezza" dei cittadini[14].

In altri termini, pur in difetto di una disciplina esplicita e dettagliata al riguardo (e con i limiti e le incertezze applicative connesse a tale lacuna), nell'attuale quadro ordinamentale pare doversi ritenere che l'*agente* o *ufficiale di pubblica sicurezza* che conosca un fatto rilevante per la tutela della sicurezza pubblica, nel senso appena precisato (e quindi anche con riferimento ad un fatto sottendente un possibile pregiudizio dei diritti dei cittadini, e precipuamente di quelli afferenti alla sfera personale), assuma immediatamente, al riguardo, una posizione di garanzia che gli imponga di farne compiuta e tempestiva comunicazione al Questore, onde consentirgli di attivare, se del caso, gli strumenti provvedimentali di sua competenza nella prospettiva di assicurare adeguata ed efficace protezione preventiva alla persona minacciata[15].

Anche per tale via, pertanto, in capo agli *agenti ed ufficiali di pubblica*

---

14) Sul "diritto alla sicurezza" come "diritto di libertà" cfr. C. Mosca, *La sicurezza come diritto di libertà*, Padova, 2012, p. 71 ss., secondo cui esso è "diritto fondamentale autonomo, non solo servente o strumentale rispetto ad altri diritti pure costituzionalmente ed espressamente riconosciuti, quanto come bene percepito e, finalmente, giuridicamente riconosciuto ai cittadini di una moderna democrazia. [....]. Un diritto di libertà, quello alla sicurezza, che attiene allo stesso bene della vita e dell'incolumità fisica".

15) Sulla ricorrenza di tale obbligo di tempestiva segnalazione degli agenti ed ufficiali di p.s. onde consentire al Questore – in particolare, nel campo della violenza domestica – di "adottare gli opportuni provvedimenti preventivi di sua competenza e così assicurare, in chiave anticipatoria e di concreta difesa sociale, il diritto alla sicurezza", cfr. G. Aliquó, *La violenza domestica. L'ammonimento del Questore*, cit., p. 203 ss.

sicurezza è isolabile un obbligo di tempestiva informazione, verso il Questore, che si appalesa analogo a quello che l'art. 347 c.p.p. pone in capo agli *agenti ed ufficiali di polizia giudiziaria* in ordine al rilievo di notizie di reato da segnalare all'ufficio di Procura.

2. L'ammonimento per "atti persecutori"

2.1. Introduzione del delitto ex art. 612-*bis* c.p. e dell'ammonimento

L'istituto dell'*ammonimento* questorile è stato introdotto nel nostro ordinamento dall'art. 8 del decreto-legge n. 11 del 23 febbraio 2009 (convertito dalla legge n. 38 del 23 aprile 2009), recante "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori"[16].

L'intervento normativo, dopo avere interpolato nel Codice penale (e segnatamente nella sezione III del titolo XII dedicata ai "delitti contro la libertà morale") l'art. 612-*bis*, ivi tipizzando il nuovo reato di "*atti persecutori*" (il c.d. stalking)[17], ha poi previsto (all'art. 8) la speciale misura monitoria, nella disponibilità provvedimentale del Questore (quello territorialmente competente, in relazione al luogo in cui è avvenuto il fatto o, nel caso in cui il fatto

16) Alla stregua dei dati pubblicati dalla Direzione Centrale della Polizia Criminale (DCPC) del Dipartimento della pubblica sicurezza, il 25 novembre 2020, in occasione della *Giornata Internazionale per l'eliminazione della violenza contro le donne*, gli ammonimenti ex art. 8 d.l. n. 11/2009 complessivamente emessi dai Questori della Repubblica sono: n. 1269 nel 2018; n. 1300 nel 2019; n. 1055 per il periodo del 2020 fino al 19 novembre.

17) L'obiettivo del legislatore era quello di colmare un vuoto di tutela verso i comportamenti persecutori, assillanti ed invasivi della vita altrui, di cui sono vittime soprattutto, ma non esclusivamente, le donne. Il delitto di atti persecutori (c.d. "stalking") comprende comportamenti che in precedenza risultavano solo parzialmente tipizzati nelle preesistenti norme – "maltrattamenti in famiglia", "minaccia", "violazione di domicilio" "disturbo alle persone", ecc. – le quali certamente non esaurivano l'ambito di riferimento bisognoso di tutela penale. Alla stregua della sentenza della Corte costituzionale n. 172 del 11 giugno 2014 (chiamata a pronunciarsi sulla legittimità costituzionale della nuova fattispecie penale, di cui era stata denunciata una pretesa indeterminatezza), con l'art. 612-*bis* c.p. il legislatore ha ulteriormente connotato le condotte di minaccia e molestia, richiedendo che le stesse siano realizzate in modo reiterato e idoneo a cagionare almeno uno degli eventi indicati nel testo normativo (stato di ansia o di paura, timore per l'incolumità e cambiamento delle abitudini di vita). Tale ulteriore caratteristica è volta ad individuare specifici fenomeni di molestia assillante che si caratterizzano per un atteggiamento predatorio nei

sia commesso mediante rete telematica, al luogo di residenza della vittima) da esercitarsi, su istanza della vittima del delitto di atti persecutori, nei confronti dell'autore della condotta[18].

Lo strumento, che mira a garantire alla vittima di *stalking* una tutela rapida ed anticipata, tramite il solenne richiamo dello *stalker* ad astenersi da con-

---

confronti della vittima, la quale subisce ripercussione nella vita emotiva (stato di ansia e di paura ovvero timore per l'incolumità) e pratica (cambiamento delle abitudini di vita). Il delitto di atti persecutori, dunque, viene a configurarsi come reato abituale che differisce dai reati di molestie e minacce – che pure ne possono rappresentare un elemento costitutivo – per la produzione di un evento di "danno" (consistente nell'alterazione delle proprie abitudini di vita o in un perdurante e grave stato di ansia e di paura) ovvero, in alternativa, di un evento di "pericolo" (consistente nel fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva). Affinché venga integrato il requisito dell'abitualità proprio del reato di stalking occorre che la minaccia o la molestia non sia isolata, ma avvenga con condotte reiterate nel tempo (ache due sole condotte tra quelle descritte dall'art. 612-*bis*, pure se commesse in un arco di tempo molto ristretto, sono idonee a costituire la reiterazione richiesta dalla norma incriminatrice di cui all'art. 612-*bis* c.p., sempreché la vittima, per le reiterate molestie subite, manifesti un perdurante e grave stato d'ansia e sia costretta a modificare le proprie abitudini di vita: Cass. 3 luglio 2015, n. 45453). Il reato di cui all'art. 612-*bis* è un reato comune, potendo essere commesso da chiunque, a prescindere dal tipo di relazione con la persona offesa. Il secondo comma dell'articolo prevede, però, una circostanza aggravante, ad efficacia comune, in cui tale relazione assume rilievo. Il testo originario dell'art. 612-*bis*, comma 2, si riferiva al fatto commesso dal coniuge legalmente separato o divorziato o da un soggetto che in passato era stato legato alla persona offesa da una relazione affettiva. Con il d.l. n. 93 del 2013, nel testo modificato dalla legge di conversione n. 119 del 2013, è stata estesa l'applicazione della circostanza aggravante sia ai fatti commessi dal coniuge separato soltanto di fatto, sia ai fatti commessi in costanza del rapporto di coniugio o affettivo. Sotto il profilo processuale, il delitto di atti persecutori è procedibile a querela, il cui termine di presentazione è di sei mesi e la remissione può essere soltanto processuale. La querela è comunque irrevocabile se il fatto è stato commesso mediante minacce reiterate, nei modi di cui all'articolo 612, secondo comma. È prevista la procedibilità d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità, oppure quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio.

18) Il testo dell'art. 8 del d.l. n. 11/2009 (convertito dalla legge n. 38/2009), come modificato dall'art. 1, comma 4, d.l. 14 agosto 2013, n. 93, convertito, con modificazioni, dalla l. 15 ottobre 2013, n. 119 (su cui *infra* nel testo), è il seguente.
1. Fino a quando non è proposta querela per il reato di cui all'articolo 612-bis del codice penale, introdotto dall'articolo 7, la persona offesa può esporre i fatti all'autorità di pubblica sicurezza avanzando richiesta al questore di ammonimento nei confronti dell'autore della condotta. La richiesta è trasmessa senza ritardo al questore.
2. Il questore, assunte se necessario informazioni dagli organi investigativi e sentite le persone informate dei fatti, ove ritenga fondata l'istanza, ammonisce oralmente il soggetto nei cui confronti è stato richiesto il provvedimento, invitandolo a tenere una condotta con-

dotte pregiudizievoli per la vittima ed a tenere un comportamento conforme alla legge, ha pacifica natura di misura amministrativa preventiva, siccome funzionale ad assicurare una forma avanzata di prevenzione e di dissuasione dei comportamenti sanzionati dall'art. 612-*bis* c.p. (Consiglio di Stato, sez. III, 25 maggio 2015, n. 2599; 7 settembre 2015, n. 4127; 15 febbraio 2019, n. 1085).

Esso rappresenta, quindi, l'espressione di un sistema integrato di misure per prevenire o interrompere sul nascere, prima ancora che punire, condotte che, per la loro attitudine o idoneità, possono creare il pericolo di verificazione di eventi molesti o lesivi della libertà di autodeterminazione di soggetti in posizione, se non altro psicologica, di minorata difesa, potenziando con strumenti *ad hoc* i poteri dell'autorità di pubblica sicurezza a tutela dei cittadini (cfr. Consiglio di Stato, sez. III, 6 settembre 2018, n. 5259).

In questo senso, l'ammonimento introdotto dal d.l. n. 11/2009 costituisce traduzione legislativa (e quindi applicativa), nell'ordinamento italiano, di una volontà statuale e sovranazionale, sempre più pressante e consapevole (come sopra anticipato), di assicurare alla vittima uno statuto di protezione che, ferma restando la necessità di risposte repressive adeguate e puntuali, miri anche – e soprattutto – a scongiurare la stessa aggressione alla sua sfera giuridica, in una dimensione di effettiva ed anticipata prevenzione e protezione.

2.2. La disciplina

Coerentemente alla testé precisata natura giuridica dell'istituto, il procedimento relativo all'adozione dell'ammonimento questorile è di natura essenzialmente amministrativa e preventiva, di tal ché ad esso si applicano certamente le norme ed i principi di cui alla legge n. 241/1990, laddove non risultino sufficienti le specifiche norme procedurali fissate dallo stesso art. 8 del d.l. n. 11/2009, alle quali è opportuno riservare ora particolare attenzione.

Presupposti di applicazione

Il presupposto dell'ammonimento disegnato dall'art. 8 d.l. n. 11/2009

---

forme alla legge e redigendo processo verbale. Copia del processo verbale è rilasciata al richiedente l'ammonimento e al soggetto ammonito. Il questore adotta i provvedimenti in materia di armi e munizioni.

3. La pena per il delitto di cui all'articolo 612-bis del codice penale è aumentata se il fatto è commesso da soggetto già ammonito ai sensi del presente articolo.

4. Si procede d'ufficio per il delitto previsto dall'articolo 612-bis del codice penale quando il fatto è commesso da soggetto ammonito ai sensi del presente articolo.

risiede nella circostanza che sia stato commesso un reato ex art. 612-*bis* c.p.: l'affermazione va contestualizzata alla stregua della natura del provvedimento che si tratta di adottare (costituente misura preventiva e non misura di sicurezza) e del procedimento nel cui ambito vanno accertati gli estremi della sua legittimazione.

Corrispondentemente, proprio in ragione del fatto che il procedimento amministrativo di cui all'art. 8 del d.l. n. 11 del 2009 si muove su un diverso piano (cautelare e preventivo) da quello del procedimento penale per il reato di cui all'art. 612-*bis* c.p., il provvedimento conclusivo (decreto di ammonimento) presuppone, non l'acquisizione di prove tali da poter resistere in un giudizio penale avente ad oggetto un'imputazione per il reato di *stalking*, bensì la sussistenza di elementi dai quali sia possibile desumere la ricorrenza di un comportamento astrattamente qualificabile in termini persecutori o gravemente minacciosi che, nel contesto di relazioni intersoggettive, possa degenerare e preludere a condotte costituenti reato. Pertanto, ai fini dell'ammonimento, non occorre che si sia raggiunta la prova della commissione del reato, risultando sufficiente il riferimento ad elementi dai quali sia possibile desumere, con un sufficiente grado di attendibilità, un comportamento persecutorio che ha ingenerato nella vittima un perdurante e grave stato di ansia e di paura. In altri termini ancora, il provvedimento di ammonimento non presuppone l'acquisizione della prova del fatto penalmente rilevante, punito dall'art. 612-*bis* c.p., ma – nel quadro di un potere valutativo ampiamente discrezionale dell'amministrazione – richiede la sussistenza di un quadro indiziario che renda verosimile, secondo collaudate massime di esperienza, l'avvenuto compimento di atti persecutori. Per questo motivo, il Questore deve apprezzare la fondatezza dell'istanza, formandosi il ragionevole convincimento sulla plausibilità e attendibilità delle vicende esposte, senza che sia necessario il compiuto riscontro dell'avvenuta lesione del bene giuridico tutelato dalla norma penale incriminatrice.

Del resto, ciò che è essenziale è che l'ammonimento raggiunga, nella sua configurazione *ex ante*, quella funzione tipicamente cautelare e preventiva tesa ad evitare che gli atti persecutori posti in essere contro la persona non siano più ripetuti e non cagionino esiti irreparabili, a prescindere dalla loro successiva sottoposizione al vaglio del giudice penale e perfino dalla ritenuta successiva irrilevanza degli stessi sotto il profilo di tale tipo di responsabilità" (Cons. Stato, sentenza n. 5259 del 2018, cit.).

All'ammonimento deve quindi applicarsi quella "logica dimostrativa a base indiziaria e di tipo probabilistico che informa l'intero diritto amministrativo della prevenzione" (Consiglio di Stato, sez. III, 15 febbraio 2019, n. 1085).

Alla stregua dei più recenti arresti del Consiglio di Stato, ai fini dell'adozione dell'ammonimento di cui all'art. 8 del d.l. n. 11/2009 non è richiesta la piena prova della responsabilità dell'ammonito ovvero di comportamenti di cui sia accertato il carattere persecutorio, ma è sufficiente il sospetto che vi sia una tale finalità o idoneità nelle condotte ripetute dallo stesso tenute, con la conseguenza che a sostegno del provvedimento dell'ammonimento orale è sufficiente un quadro istruttorio da cui emergano, anche solo su un piano indiziario, eventi che rechino un *vulnus* alla riservatezza della vita di relazione o, in senso lato ed in forma anche potenziale, all'integrità della persona vittima di comportamenti minacciosi o molesti (Cons. Stato, sez. III, 25/06/2020, n. 4077).

Richiesta della vittima

La legge prevede, quale condizione di procedibilità, che la persona offesa dalla condotta persecutoria (nel senso appena precisato) rivolga al Questore apposita "*richiesta*" di ammonimento.

In questo senso, l'istituto è connotato da una marcata disponibilità da parte della vittima, alla quale viene riconosciuta la libera valutazione in ordine allo strumento da attivare, in relazione alla situazione personale che la riguarda ("*la persona offesa può esporre i fatti all'autorità di pubblica sicurezza avanzando richiesta al questore di ammonimento nei confronti dell'autore della condotta*").

La formulazione dell'art. 8 d.l. n. 11/2009 sul punto, tuttavia, non pare particolarmente puntuale laddove prevede che la vittima possa chiedere l'emissione dell'ammonimento da parte del Questore, esponendo i fatti patiti alle "autorità di pubblica sicurezza", così finendo, per un verso, con l'evocare quale possibile recettore dell'istanza indirizzata al Questore finanche il Prefetto, oltre che il Sindaco (il cui ruolo al riguardo è peraltro particolarmente importante, attesa la contestuale preposizione dello stesso alla rete dei servizi sociali comunali)[19] e, per altro verso, non contemplando tra i soggetti ai quali consegnare la formale volontà di attivare il procedimento monitorio gli "agenti ed ufficiali di p.s.".

In relazione a quanto premesso nel capitolo precedente, si deve ritenere, tuttavia, che l'impropria formulazione dell'art. 8 d.l. n. 11/2009 non impedisca affatto la materiale presentazione dell'istanza di ammonimento ad ognuno di

19) Sulla importanza del ruolo del Sindaco in materia, cfr. G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, Pacini giuridica, 2019, p. 79 ss.

tali ultimi attori dell'Amministrazione della p.s., che risulterà obbligato, conseguentemente, alla ricezione di essa ed alla sua immediata trasmissione al Questore.

Più dubbia potrebbe rivelarsi la ricezione di una valida richiesta di ammonimento da parte di soggetti che non siano titolari di alcuna qualifica di pubblica sicurezza (si pensi, ad esempio, ai funzionari dei servizi sociali comunali). La previsione normativa in esame, che subordina la valida instaurazione di un procedimento monitorio per atti persecutori (a differenza di quanto si vedrà per i fatti di violenza domestica) alla sola ricorrenza di una formale richiesta della vittima, esplicitamente qualificata dalla presentazione a soggetti selettivamente connotati dall'appartenenza all'Amministrazione della pubblica sicurezza (seppure estensivamente intesi nel senso prima segnalato), pare ostare a siffatta equiparazione: ciò non impedisce, ovviamente, che l'istanza irritualmente ricevuta da soggetti diversi possa (ed anzi, si ritiene, debba tempestivamente) essere trasmessa all'autorità di p.s. dinnanzi alla quale l'istanza potrà essere formalizzata (salva la possibilità che la persona offesa abbia cambiato frattanto idea, anche orientandosi per la proposizione di una querela).

Alternatività rispetto alla querela

L'art. 8 del d.l. n. 11/2009 ha introdotto nel nostro ordinamento l'ammonimento questorile per atti persecutori quale strumento, non solo rimesso alla sola disponibilità della vittima, ma anche alternativo alla tutela penale, siccome esperibile "*fino a quando non è proposta querela per il reato...*".

La scelta legislativa del 2009 (verosimilmente indicativa di un concomitante intento deflattivo dei giudizi penali) sembra disinnescare, a monte, i problemi connessi ai rapporti tra procedimento penale giudiziario e procedimento monitorio questorile: laddove ricorra la querela, non vi sarà spazio per l'intervento dell'autorità di pubblica sicurezza (salvi diversi provvedimenti di competenza, ad esempio in materia di armi); se invece è stata avanzata la richiesta di ammonimento, il Questore avvierà e farà istruire da ufficiali ed agenti di pubblica sicurezza (segnatamente quelli in servizio presso l'Ufficio polizia anticrimine della Questura, competenti al riguardo) un procedimento amministrativo che si concluderà con un eventuale provvedimento di ammonimento o di motivato rigetto della richiesta della vittima.

Tuttavia, la realtà applicativa può porre questioni più dinamiche e sfumate, suscettibili di conseguenti minori certezze schematiche.

Un primo problema si pone laddove la vittima richieda l'ammonimento per fatti nuovi, rispetto a quelli per i quali abbia già sporto querela, in precedenza.

La questione si è posta all'attenzione della giurisprudenza, in seno alla quale è stata valorizzata l'autonomia dello strumento preventivo questorile, rispetto a quello giudiziario, giungendo alla conclusione che il procedimento penale pendente o concluso, in relazione ad un primo fatto persecutorio, non impedisca affatto che la stessa vittima richieda un ammonimento per nuove condotte poste in essere dallo *stalker* nei suoi confronti: in tal senso, in particolare, si è espresso TAR Lombardia (Brescia), sezione I, nella sentenza n. 1189 del 12 luglio - 2 ottobre 2017.

Rimane poi il problema connesso alla qualificazione dei fatti segnalati dalla vittima, nella propria richiesta di ammonimento, ben potendo accadere che, in essa o nella successiva istruzione amministrativa, emerga che i fatti segnalati vadano qualificati in termini diversi da quelli di atti persecutori, integrando estremi di un reato procedibile d'ufficio o, in aggiunta ad essi, constino ulteriori fatti di tale natura penale.

In tal caso, ferma la trasmissione degli atti alla a.g., ci si chiede se comunque il Questore abbia il potere o dovere di provvedere all'ammonimento richiesto. La risposta affermativa a tale quesito pare imposta dalla necessità di assicurare alla vittima la tutela immediata ed anticipata sottesa allo strumento preventivo esplicitamente richiesto, vieppiù a fronte del rischio che la tutela giudiziaria arrivi tardi (in sede di condanna o anche solo cautelare) o addirittura non arrivi mai (laddove la a.g. non ravvisasse alfine gli estremi per addivenire ad un provvedimento giudiziario o non aderisse alla stessa qualificazione dei fatti in termini di reato procedibile d'ufficio)[20]. Tuttavia, questa soluzione pare legittima e doverosa solo quando, nel fatto emergente in seno al procedimento amministrativo, sia enucleabile – astrattamente, si intende – una condotta comunque qualificabile come *persecutoria*, ancorché poi costitutiva di una fattispecie penale più grave o comunque procedibile d'ufficio. La tesi secondo cui il Questore possa o debba, invece, ammonire (ovviamente a fronte di una richiesta in tal senso della vittima) anche l'autore di condotte qualificabili in termini diversi da quelli (anche solo astrattamente) declinabili come persecutorie ex art. 612-*bis* (richiamato dall'art. 8 d.l. n. 11/2009), cozzerebbe con il principio di legalità e tassatività che vale anche nel campo delle misure di prevenzione, quale espressione del generale principio di certezza del diritto, a sua volta immanente alle fondamenta stesse dello Stato di diritto[21].

---

20) In tal senso, G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, cit., p. 310 ss.

21) Sulla dimensione del principio di certezza del diritto, cfr. G. Alpa, *I principi generali*, Milano, 2006.

Partecipazione dell'interessato al procedimento

Come anticipato, al procedimento questorile monitorio si applicano, in quanto compatibili, le norme della legge n. 241/1990 e, tra esse, anche quelle relative agli istituti partecipativi di cui agli artt. 7 e seguenti.

Conseguentemente, ove non sussistano specifiche ragioni di urgenza (da indicare nell'atto), l'Amministrazione deve dare comunicazione dell'avvio del procedimento al soggetto destinatario dell'ammonimento, con conseguente possibilità per l'interessato di manifestare le proprie deduzioni ed osservazioni nel corso del procedimento (T.A.R. Abruzzo, sez. I, 28 maggio 2015, n. 428) ed integrare la stessa istruttoria del procedimento con il proprio apporto: sia nella forma di presentazione di documentazione e memorie scritte, che nella forma della audizione personale. In tal senso, soccorre il recente arresto di Cons. Stato, sez. III, 24/04/2020, n. 2620, secondo cui, in una prospettiva di contemperamento di esigenze istruttorie e necessità di tempestività e non aggravamento dell'azione amministrativa, "*la norma di cui all'art. 8, comma 2 del d.l. n. 11/2009 nella parte in cui subordina ad una valutazione di necessità l'acquisizione di informazioni dagli organi investigativi e dalle persone informate dei fatti, affida alla valutazione discrezionale dell'autorità competente la modulazione degli strumenti di approfondimento istruttorio offrendole la possibilità di una interlocuzione con il diretto interessato nella duplice e alternativa forma delle deduzioni scritte oppure dell'audizione diretta, in forma orale*".

Dalla comunicazione di avvio del procedimento, invece, può prescindersi nel caso in cui sussistano, in concreto ed eccezionalmente, ragioni di impedimento derivanti da particolari esigenze di celerità del procedimento, che non consentano di dar luogo alla comunicazione di avvio del procedimento (T.A.R. Lombardia, sez. III, 2 aprile 2015, n. 877): così, è tipicamente, quando consti – alla stregua degli elementi di fatto noti all'autorità di p.s. – che la vittima sia esposta ad imminenti pericoli connessi alla condotta dello *stalker*, ovvero tale minaccia sia destinata ad integrarsi proprio in esito alla conoscibilità dell'avvio del procedimento (tenuto conto che il procedimento monitorio di cui qui si tratta, per definizione, si attiva solo su richiesta della persona offesa)[22].

22) Tra le ultime pronunce al riguardo, cfr. ancora Cons. Stato, sez. III, 24/04/2020, n. 2620: «Ai fini dell'adozione di un provvedimento di ammonimento, l'inoltro della comunicazione di avvio del procedimento, previsto dall' art. 7 della legge n. 241/1990 è obbligatorio solo laddove sussistano circostanze che effettivamente consentano di avvisare il possibile destinatario dell'atto atteso che altrimenti specifiche ragioni di urgenza possono essere fronteggiate solo attraverso un intervento "illico et immediate"».

In merito alla partecipazione dell'interessato al procedimento questorile monitorio, peraltro, occorre precisare che lo stesso diritto di accesso agli atti amministrativi sottesi all'adozione dell'ammonimento può incontrare delle limitazioni, ai sensi dell'art. 24 comma 6 lettera c) della legge n. 241/1990 e dell'art. 3 d.m. n. 415 del 10 maggio 1994, connesse alla necessità di assicurare, intanto, il segreto investigativo ex art. 329 c.p.p., sotteso a paralleli procedimenti penali (per reati diversi) o possibili sviluppi di polizia giudiziaria (TAR Campania, sez. I Salerno, sentenza n. 818 del 7 giugno - 8 luglio 2007).

Siffatta limitazione al diritto di accesso, in una materia contigua a quella penale quale è quella preventiva in esame, si appalesa oltremodo opportuna laddove essa consente di utilizzare – sulla base di intese con l'a.g. – anche atti di polizia giudiziaria, superando l'altrimenti insormontabile ostacolo di un'indebita ostensione di essi in sede amministrativa.

Ma dal diritto di accesso agli atti acquisiti nel procedimento amministrativo, finalizzato all'adozione dell'ammonimento questorile, possono essere esclusi anche atti riservati (e nei limiti in cui sia necessario che lo rimangano) di competenza dell'autorità di pubblica sicurezza in quanto tale, segnatamente connessi ai documenti che attenessero "*alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte*" (art. 24 comma 6 lettera c della legge n. 241/1990). In tal senso, Consiglio di Stato, sezione I, parere n. 243 del 16 - 21 gennaio 2019 e TAR Emilia Romagna, sezione I, sentenza n. 280 del 8 febbraio - 6 aprile 2017.

Per altro verso, siffatti limiti vanno contemperati con l'essenziale diritto di difesa del soggetto interessato, oltreché con fondamentali principi di ponderatezza ed imparzialità dell'azione amministrativa, con la conseguente necessità di trovare – di volta in volta – equilibrati assetti di reciproca tutela, anche ad esempio attraverso secretazioni parziali dei documenti, occultamento dei soli nomi o altro accorgimento (Consiglio di Stato, sezione III, sentenza n. 4187 del 15 maggio - 9 luglio 2018)[23].

Il provvedimento

Ai sensi dell'art. 8 d.l. n. 11/2009, il Questore "*assunte se necessario informazioni dagli organi investigativi e sentite le persone informate dei fatti, ove ritenga fondata l'istanza, ammonisce oralmente il soggetto nei cui confronti è stato richiesto il provvedimento*".

23) Per una approfondita analisi di siffatti limiti all'accesso agli atti e la relativa casistica, cfr. G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, *op. cit*., p. 135 ss.

Alla stregua di siffatta formulazione, si è sottolineato che il provvedimento monitorio per atti persecutori sia connotato da obbligatorietà ed oralità.

Sotto il primo profilo, cioè, si ritiene che, ove l'istruttoria consegni la conferma della ricorrenza della condotta persecutoria dedotta nell'istanza dalla vittima, il Questore sia tenuto ad adottare il provvedimento richiesto.

Per altro verso, il provvedimento di ammonimento deve avere forma orale, non risultando legittima la mera notifica di un atto scritto[24]. Al riguardo, tuttavia, occorre precisare che:

– il Questore possa delegare all'uopo un ufficiale di p.s. (Cass., sez. III, n. 30644 del 9 novembre 2016, sulla scia di quanto pacificamente avviene in materia di Avviso orale);

– dell'avvenuto ammonimento orale vada comunque redatto verbale da consegnare in copia all'ammonito ed alla vittima istante;

– non sia affatto vietato concludere il procedimento questorile (anche) con un atto scritto, che anzi pare idoneo a dare contezza formale anche del percorso motivazionale che sorregge il provvedimento, purché esso non sia meramente sostitutivo dell'essenziale momento orale.

La previsione dell'essenziale oralità dell'ammonimento è forse espressione di una prospettiva legislativa che voglia imporre un contatto umano tra l'autorità di pubblica sicurezza e lo *stalker*, sia al fine di imprimere maggiore efficacia preventiva al richiamo monitorio, sia al fine di ottimizzare l'approccio rieducativo dello stesso autore della condotta persecutoria, chiaramente considerato anche come un soggetto da curare. Ed invero, l'art. 3, comma 5-*bis* d.l. n. 93/2013 ha previsto che, quando il Questore proceda all'ammonimento ai sensi dell'articolo 8 del decreto-legge 23 febbraio 2009, n. 11, debba informare – senza indugio – l'autore del fatto circa i servizi disponibili sul territorio, inclusi i consultori familiari, i servizi di salute mentale e i servizi per le dipendenze, come individuati dal Piano di cui all'articolo 5, d.l. n. 93/2013, finalizzati ad intervenire nei confronti degli autori di violenza domestica o di genere[25].

---

24) Sugli effetti della violazione di tale previsione, T.A.R. Lombardia Milano, sez. III, 25/08/2010, n. 4182, ha precisato che "l'adozione da parte del Questore del provvedimento di ammonimento di cui all'art. 8 del d.l. n. 11 del 2009, convertito in legge n. 38 del 2009, in forma scritta in luogo dell'atto orale seguito dalla verbalizzazione, ferma restando la comunicazione data all'interessato mediante convocazione e consegna dell'atto ad opera di un ufficiale di pubblica sicurezza, integra una mera irregolarità in quanto, pur non riflettendo esattamente il paradigma normativo, soddisfa chiaramente le esigenze di certezza e garanzia cui tende il meccanismo procedimentale delineato dalla richiamata norma".

25) Sul diverso piano della tutela della vittima, lo stesso l'art. 11, d.l. n. 11/2009, invece, impone alle forze dell'ordine, ai presidi sanitari ed alle istituzioni pubbliche che ricevono

2.3. Gli effetti del provvedimento monitorio e della sua inosservanza

Il provvedimento di ammonimento determina taluni effetti associati alla stessa adozione di esso, da parte del Questore, nonché altri connessi alla sua eventuale trasgressione od inosservanza da parte dell'interessato.

Quanto al primo aspetto, il comma 2 dell'art. 8 d.l. n. 11/2009 (come modificato dal d.l. n. 93/2013) prevede che "*il Questore adotta i provvedimenti in materia di armi*". Ne discende, in concreto, che il Questore debba immediatamente disporre:

– l'eventuale ritiro materiale delle armi da parte di agenti ed ufficiali di p.s. (funzionale all'adozione del conseguente divieto prefettizio di detenzione ex art. 39 TULPS);

– l'avvio del procedimento amministrativo per la revoca delle eventuali licenze di porto d'arma lunga (di sua competenza) ex art. 11 e 42 TULPS ovvero per l'imposizione di specifiche prescrizioni al riguardo[26].

Dai provvedimenti in materia di armi, peraltro, discendono ulteriori possibili conseguenze sui rapporti di lavoro dell'ammonito, segnatamente laddove

---

dalla vittima notizia del reato di cui, tra l'altro, all'art. 612-*bis* del codice penale, l'obbligo di fornire alla vittima stessa tutte le informazioni relative ai centri antiviolenza presenti sul territorio e, in particolare, nella zona di residenza della vittima. Le forze dell'ordine, i presidi sanitari e le istituzioni pubbliche provvedono a mettere in contatto la vittima con i centri antiviolenza, qualora ne faccia espressamente richiesta.

26) Sul tema dei provvedimenti in materia di armi che il Questore "adotta" in caso di ammonimento cfr. G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, cit., p. 216 ss., che sostiene la non necessità di provvedimenti interdittivi in conseguenza dell'ammonimento, ben potendo il Questore – soprattutto nei casi di appartenenti a forze di polizia o forze armate o, in genere, di coloro la cui professione postuli l'uso delle armi – orientarsi su "*adeguate misure prescrittive, ragionevolmente proporzionate e altrettanto efficaci ma meno impattanti sul rapporto di lavoro, lasciandone l'esecuzione ai superiori gerarchici dell'ammonito*". Cons. Stato, sez. III, 07/01/2020, n. 65 ha statuito che "a seguito del provvedimento di ammonimento, l'adozione di provvedimenti in materia di armi e munizioni è atto dovuto per il Questore, ex art. 8, comma 2, d.l. n. 11 del 2009. In particolare, il Questore adotta misure di tipo cautelare, riconducibili all'art. 39, comma 2, del r.d. 18 giugno 1931, n. 773 (TULPS) (immediato ritiro di armi, munizioni, materiale esplodente) e ne dà comunicazione al Prefetto. Il Prefetto, ai sensi dell'art. 39, comma 1, TULPS, con valutazione ampiamente discrezionale, da esercitarsi con riguardo, innanzitutto, al prioritario interesse all'incolumità delle persone coinvolte, oltre che nell'interesse della sicurezza pubblica, ha facoltà di vietare in via definitiva la detenzione dei materiali di cui sopra e ne ordina la cessione a terzi entro un termine di 150 giorni, quando sia riscontrabile una "capacità di abusarne". Il parere del Consiglio di Stato, sezione I, n. 659 del 16 luglio 2014 - 4 marzo 2015 precisa che l'ammonimento sottende una presunzione legislativa di

essi postulino la necessità di essere armati (si pensi a tutti gli appartenenti alle forze di polizia o forze armate, ovvero ai titolari della qualifica di GPG addetti di istituti di vigilanza)[27].

Ma la legge contempla anche precisi effetti connessi all'eventuale trasgressione dell'ammonimento questorile: si tratta di previsioni che, esponendo l'ammonito a conseguenze differenziali, di natura sia amministrativa che penale (sostanziale e procedurale), mirano a tutelare l'osservanza del provvedimento adottato, la sua efficacia e, in definitiva, l'effettività della sottesa protezione rivolta alla vittima.

In questa prospettiva, innanzitutto, occorre rilevare che, laddove il soggetto ammonito trasgredisse all'invito solennemente rivoltogli dal Questore (il cui contenuto, come anticipato, è essenzialmente polarizzato sul divieto di reiterare condotte astrattamente persecutorie), il suo comportamento potrebbe rilevare ad integrare, indiziariamente, il quadro di pericolosità sociale qualificata fissato dall'art. 4 comma 1 lettera i-*ter* del d.lgs. n. 1549/2011 (lettera interpolata nel c.d. Codice antimafia dall'art. 1 comma 1 lettera d della legge n. 161/2017). Tale norma ricomprende ora anche i "*soggetti indiziati dei delitti di cui agli articoli* [...] *612-bis del Codice penale*" tra i destinatari delle misure di prevenzione personali applicate dall'autorità giudiziaria (segnatamente la sorveglianza speciale di pubblica sicurezza) ed addirittura – per l'effetto del richiamo all'art. 4 contenuto nell'art. 16 del medesimo decreto – delle misure di prevenzione patrimoniale di cui al titolo II del Codice: beninteso, si tratta di misure preventive giudiziarie che hanno uno spazio autonomo di formale operatività rispetto all'ammonimento ma che, evidentemente, nell'eventuale

---

inaffidabilità dell'ammonito in ordine all'uso delle armi, con la conseguente necessità della revoca delle autorizzazioni rilasciate al riguardo e dell'adozione di misure interdittive, anche quando si tratti di appartenente alle forze di polizia e armate. Lo stesso parere precisa: "avuto riguardo alla ratio del modificato comma 2 dell'art. 8 del d.l. n. 11 del 2009, non possono sussistere dubbi che nel bilanciamento dei contrapposti interessi (salvaguardia dell'incolumità delle potenziale vittime degli atti persecutori e necessità di disporre dell'arma d'ordinanza per l'assolvimento del servizio di polizia) debba prevalere il primo sul secondo. Pertanto, nel caso dell'ammonizione di appartenente alle forze di polizia, il questore dovrà disporre che allo stesso siano ritirate le armi detenute a qualsiasi titolo, compresa l'arma di ordinanza, anche se ciò comporti per l'interessato l'impossibilità di adempiere a pieno ai compiti d'istituto e lo esponga a provvedimenti disciplinari e di stato. Ovviamente, nel caso di appartenenti a corpi diversi dalla Polizia di Stato, il provvedimento con cui si dispone il ritiro dell'arma in dotazione non potrà che essere indirizzato ai superiori dell'interessato, sui quali graverà l'obbligo di ottemperare".

27) L'ammonimento può rilevare, peraltro, quale fonte di eventuali responsabilità disciplinari.

inosservanza di quest'ultimo provvedimento questorile (e quindi nella rilevata persistenza di condotte persecutorie, nonostante il previo ammonimento) potrebbero rinvenire una più solida giustificazione[28].

Né sarebbe da escludere, nel caso d'inosservanza dell'ammonimento, l'adozione di misure di aggravamento di quelle già eventualmente adottate circa le armi dell'ammonito[29].

Laddove, poi, la condotta del soggetto già ammonito si rivelasse integrare gli estremi del reato di atti persecutori ex art. 612-*bis* c.p., l'inosservanza del provvedimento questorile dispiegherebbe effetti di natura penale, tanto sostanziale, quanto procedurale.

Ed invero, l'art. 8, comma 3, d.l. n. 11/2009, prevede che la pena per il delitto di cui all'articolo 612-*bis* del Codice penale è aumentata se il fatto è commesso da soggetto già destinatario di ammonimento. Inoltre, la previa irrogazione dell'ammonimento incide sulla procedibilità del delitto di atti persecutori, il quale, come anticipato, ordinariamente è procedibile a querela della persona offesa, ma diventa procedibile d'ufficio quando il fatto è commesso da soggetto già ammonito.

Al riguardo, il tenore del comma 4 dell'art. 8 d.l. n. 11/2009 (secondo cui "*si procede d'ufficio per il delitto previsto dall'articolo 612-bis del Codice penale quando il fatto è commesso da soggetto ammonito ai sensi del presente articolo*") pare sottolineare solo lo *status* (di già ammonito) dell'autore della

28) Nei confronti dello *stalker*, inoltre, sarà possibile corredare la proposta di applicazione della misura di prevenzione con l'imposizione di quelle prescrizioni che – avuto riguardo alle esigenze del caso concreto (che andranno ben specificate con l'indicazione di precisi elementi di fatto) – possano salvaguardare le esigenze di difesa sociale e della vittima, che il Tribunale può adottare ai sensi dell'art. 8, comma 5, d.lgs. n. 159 del 2011. Pertanto, potrà chiedersi al Tribunale di vietare al proposto di utilizzare, in tutto o in parte, l'autovettura o gli altri mezzi con cui risulta stazionare davanti all'abitazione della vittima perseguitata, ovvero il computer o il telefono cellulare dal quale partono le chiamate e sono inviati i messaggi minacciosi o molesti, ecc. In tal senso le "Linee guida in materia di misure di prevenzione personali" elaborate dal Servizio centrale anticrimine della Direzione centrale anticrimine della Polizia di Stato. Lo stesso documento ritiene invece non percorribile in concreto, il ricorso alla misura di prevenzione patrimoniale del sequestro che l'art. 16, comma 1, del Codice delle leggi antimafia estende anche ai soggetti indicati all'art. 4, comma i-*ter*), del predetto decreto legislativo, trattandosi di provvedimento di carattere reale che presuppone l'acquisizione dei beni attraverso condotte "lucro genetiche" ovvero una disponibilità di carattere sproporzionato al reddito dichiarato o all'attività svolta.

29) Ciò, beninteso, laddove non si ritenga obbligatoria, per il Questore, l'adozione di provvedimenti interdittivi, fin dall'adozione dell'ammonimento: sul punto cfr. nota 26.

condotta, a prescindere dall'identità della vittima della nuova condotta persecutoria, che quindi si ritiene potrebbe non coincidere con quella del fatto per il quale è stato adottato l'ammonimento. Del resto, tale soluzione interpretativa pare più coerente anche con il contenuto del richiamo monitorio questorile che, ai sensi del comma 2 dell'art. 8 d.l. n. 11/2009, reca invito all'ammonito a conformare alla legge la propria condotta in genere (non già i soli rapporti con l'istante)[30].

Inoltre, l'inosservanza dell'ammonimento questorile potrebbe rilevare quale indice, rispettivamente, della personalità e capacità a delinquere dell'indagato o imputato, in sede cautelare e nel momento della quantificazione giudiziaria della pena ex art. 133 c.p.

3. L'ammonimento per "violenza domestica"

3.1. Cenni sulle novità introdotte nel 2013

Il 25 ottobre 2012, veniva emanata la direttiva 2012/29 UE del Parlamento europeo e del Consiglio recante norme minime in materia di diritti, assistenza e protezione delle vittime del reato, che prevede una protezione individuale "ritagliata" segnatamente per le vittime vulnerabili, tra cui minori e vittime di violenze di genere.

L'11 maggio 2011, era stata approvata la Convenzione internazionale di Istanbul finalizzata alla protezione delle donne contro qualsiasi forma di violenza, innovativamente qualificata alla stregua di forma discriminatoria in violazione dei diritti umani. La Convenzione veniva ratificata dall'Italia il 27 giugno 2013 ma, prima ancora che il testo convenzionale entrasse in vigore (il numero minimo di convalide dagli Stati parte si è superato il 1 agosto 2014), il nostro ordinamento ne ha attuato le prescrizioni con un decreto-legge d'urgenza, il d.l. 14 agosto 2013, n. 93, convertito in l. 15 ottobre 2013, n. 119, ribattezzato dai mass-media e altresì da numerosi esponenti governativi e parlamentari "legge contro il femminicidio", ancorché tale nozione non venga mai impiegato dal legislatore.

Nella parte introduttiva dello stesso decreto, si legge che "il susseguirsi di eventi di gravissima efferatezza in danno di donne e il conseguente allarme

30) In senso apparentemente contrario cfr. invece G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, cit., p. 310 ss. (nota 13).

sociale che ne è derivato rendono necessari interventi urgenti volti a inasprire, per finalità dissuasive, il trattamento punitivo degli autori di tali fatti, introducendo, in determinati casi, misure di prevenzione finalizzate alla anticipata tutela delle donne e di ogni vittima di violenza domestica".

Il decreto, segnatamente nel capo I, contiene una serie di previsioni di natura penale sostanziale, penale processuale ed amministrative-preventive, oltre ad altre disposizioni in materia di misure educative, sostegno ai centri antiviolenza ed altro[31], rivolte ad arginare il fenomeno della "violenza di genere", sempre più percepito come una piaga sociale da contrastare con la massima risolutezza[32].

3.2. Novità di diritto penale sostanziale

Le modifiche di diritto penale sostanziale, contenute all'art. 1 d.l. n. 93/2013, riguardano innanzitutto l'introduzione di talune circostanze aggravanti, in materia di c.d. violenza assistita (cioè i casi in cui il delitto non colposo contro la vita e l'incolumità personale, contro la libertà personale nonché quello di maltrattamenti ex art. 572 c.p. sia commesso in presenza o in danno di un minore o persona in stato di gravidanza), di violenza sessuale ex art. 609-*ter* c.p. (commesso nei confronti di persona minore o legata all'autore da relazioni affettive) e nel delitto di atti persecutori di cui all'art. 612-*bis* c.p. (prevedendo l'aggravante della relazione affettiva anche tra coniugi o partner sentimentali attuali oltre al caso di condotte persecutorie "commesse attraverso strumenti informatici e telematici").

Al riguardo, anche per le ricadute sullo spazio di operatività dell'istituto monitorio passato in rassegna nel capitolo precedente, si segnalano le innovazioni relative alla procedibilità del suddetto delitto. Il testo originario dell'art. 612-*bis* c.p., quale introdotto dal d.l. 11/2009 (convertito in l. 38/2009), pre-

---

31) Si segnala la novità contenuta nell'art. 4 del decreto che, inserendo l'art. 18-*bis* al testo unico sull'immigrazione approvato con d.lgs. 286/98, istituisce un'ipotesi di permesso di soggiorno temporaneo per le vittime di alcuni gravi reati commessi nell'ambito di violenze domestiche, qualora siano accertate situazioni di violenza o abuso nei confronti di uno straniero ed emerga un concreto ed attuale pericolo per la sua incolumità, come conseguenza della scelta di sottrarsi alla medesima violenza o per effetto delle dichiarazioni rese nel corso delle indagini preliminari o del giudizio. Il permesso è rilasciato dal Questore "per consentire alla vittima di sottrarsi alla violenza".

32) F. Macrí, *Le nuove norme penali sostanziali di contrasto al fenomeno della violenza di genere*, in *Dir. pen. e processo*, 2014, 1, 11.

vedeva infatti la procedibilità a querela del reato, con estensione del termine di proposizione a sei mesi, in analogia con i reati sessuali, ma senza prevederne l'irrevocabilità disposta per questi ultimi dall'art. 609-*septies*, comma 3°, c.p.

Il Governo, nel testo del d.l. n. 93/2013 (art. 1, comma 3, lett. b), accoglieva le critiche di coloro che ritenevano che la revocabilità della querela implicasse il rischio di esporre la vittima del reato ad ulteriori episodi di violenza o minaccia da parte dello stalker, sancendo l'irrevocabilità della querela presentata per il delitto di "atti persecutori". In sede di conversione in legge, tuttavia, tale previsione è stata ridimensionata (conservando in capo alla persona offesa il potere di chiudere completamente la parentesi persecutoria vissuta), attraverso la previsione della revocabilità della querela nella sola sede processuale, salvo che si verifichi la duplice condizione:

a) che le condotte persecutorie siano commesse mediante minacce reiterate;

b) che le minacce siano gravi oppure commesse con armi, o da persona travisata, o da più persone riunite, o con scritto anonimo, o in modo simbolico, o valendosi della forza intimidatrice derivante da segrete associazioni, esistenti o supposte (art. 612, comma 2°, c.p., che rinvia all'uopo all'art. 339 c.p.).

Rimangono fermi i casi di procedibilità d'ufficio già sanciti legislativamente sin dal 2009, ex art. 612-*bis*, comma 4°, c.p., quando la vittima è minorenne o disabile ex art. 3 della l. n. 104/1992, oppure ove il fatto sia connesso con altro delitto per il quale si debba procedere d'ufficio.

3.3. Novità di diritto penale procedurale

L'art. 2 del d.l. n. 93/2013 come convertito dalla legge n. 119/2013 prevede modifiche al Codice di procedura penale, attraverso disposizioni volte ad ampliare le misure coercitive adottabili a tutela delle vittime e a prevedere obblighi di informazione a tutela della persona offesa.

È stato novellato l'art. 266 c.p.p., onde consentire il ricorso alle intercettazioni anche nelle indagini relative agli atti persecutori ex art. 612-*bis* c.p.

È stato modificato l'art. 282-*bis* c.p.p., così estendendo l'applicabilità della misura dell'allontanamento dalla casa familiare, anche in deroga ai limiti di pena previsti dall'art. 280 c.p.p., anche ai delitti di lesioni personali procedibili d'ufficio o comunque aggravate (art. 582 c.p.) e di minaccia grave ovvero aggravata (art. 612 cpv c.p.) in danno dei prossimi congiunti o del convivente.

È stato modificato l'art. 299 c.p.p., con la previsione di specifici doveri di avviso in caso di richiesta di revoca o di sostituzione delle misure di cui

agli artt. 282-*bis* e *ter* c.p.p. (allontanamento dalla casa familiare e divieto di avvicinamento ai luoghi frequentati dalla persona offesa), nonché in caso di adozione dei provvedimenti di revoca o sostituzione di dette misure. La richiesta di revoca o sostituzione di cui al novellato art. 299 c.p.p. – sia che essa provenga dal pubblico ministero, sia che essa provenga dall'imputato (o indagato) o dal suo difensore – deve essere contestualmente notificata, a cura della parte richiedente, al difensore della persona offesa o, in mancanza di questo, alla persona offesa a pena di inammissibilità. Invece la revoca o sostituzione delle anzidette misure, disposta ai sensi dell'art. 299 commi 1 e 2, c.p.p. dev'essere immediatamente comunicata al difensore della persona offesa o, in mancanza di questo, alla persona offesa e ai servizi socio-assistenziali del territorio.

Di particolare rilievo è la modifica dell'art. 380 c.p.p. nel senso di estendere l'arresto obbligatorio in flagranza anche ai casi di maltrattamenti in famiglia (art. 372 c.p.) e atti persecutori (art. 612-*bis* c.p.).

Infine, la novità procedurale più nota è costituita dall'introduzione dell'art. 384-*bis* c.p.p. che prevede, nei casi di cui all'art. 282-*bis* comma 6 c.p.p., la misura dell'allontanamento d'urgenza dalla casa familiare ed il contestuale divieto di avvicinamento ai luoghi abitualmente frequentati dalla persona offesa: misura che può essere disposta dalla polizia giudiziaria, su autorizzazione anche orale del pubblico ministero (successivamente confermata per iscritto o per via telematica).

3.4. L'ammonimento c.d. per "violenza domestica"

Come anticipato, la stessa premessa del decreto-legge n. 93/2013 dava conto della volontà legislativa di apprestare una tutela rafforzata alle vittime della violenza di genere, attraverso la duplice direttrice dell'inasprimento del trattamento punitivo degli autori di tali fatti, nonché "*introducendo, in determinati casi, misure di prevenzione finalizzate alla anticipata tutela delle donne e di ogni vittima di violenza domestica*".

Il legislatore del 2013, quindi, procede nella scia tracciata fin dall'intervento del 2009 in materia di *stalking*, sottendente la convinzione della necessità di affiancare al tradizionale canale di tutela penale un parallelo sistema di tutela amministrativa, di natura segnatamente preventiva, con una funzione marcatamente anticipatoria e di protezione della vittima, finalizzata a scongiurare effettivamente ed efficacemente – prima ancora che reprimere – la stessa aggressione della stessa.

In questo senso, l'art. 3 del d.l. n. 93/2013 (rubricato "Misura di preven-

zione per condotte di violenza domestica") introduce la previsione di un nuovo (caso di) ammonimento questorile per le ipotesi di ricorrenza di taluni fatti di violenza domestica[33].

Peraltro, nel tentativo di approntare strumenti di tutela sempre più efficaci, il legislatore del 2013 non si limita affatto a recepire, con riguardo ai fenomeni di violenza domestica, lo strumento monitorio introdotto dal d.l. n. 11/2009 per gli atti persecutori ma, pur mutuandone gli estremi, ne introduce una disciplina applicativa sensibilmente diversa, al punto da legittimare la convinzione che si tratti di istituto completamente o significativamente diverso: esso è invero strumento sottratto alla disponibilità della vittima, connotato da profili di marcata autonomia rispetto alla tutela penale con cui può contestualmente coesistere ed ha effetti diversi rispetto a quelli dell'ammonimento per atti persecutori.

Tali caratteristiche postulano peraltro problemi differenziali, rispetto a quelli affrontati con riguardo al primo istituto monitorio del 2009, cui occorre riservare particolare attenzione di seguito.

3.5. Il presupposto dell'ammonimento per violenza domestica

Il presupposto applicativo perché il Questore possa procedere ad adottare un ammonimento ex art. 3 d.l. n. 93/2013 risiede nella ricorrenza (ancora una volta, da accertare alla stregua del peculiare livello gnoseologico indiziario, sotteso ad un procedimento preventivo, in cui quel fatto vale peraltro quale indice di una pericolosità sociale dell'ammonendo) di "*un fatto che debba ritenersi riconducibile ai reati di cui agli articoli 581, nonché 582, secondo comma, consumato o tentato, del Codice penale*"[34].

L'art. 581 c.p. riguarda il delitto di "percosse", procedibile a querela della persona offesa.

---

33) Alla stregua dei dati pubblicati dalla Direzione Centrale della Polizia Criminale (DCPC) del Dipartimento della pubblica sicurezza, il 25 novembre 2020, in occasione della Giornata internazionale per l'eliminazione della violenza contro le donne, gli ammonimenti ex art. 3 d.l. n. 93/2013 complessivamente emessi dai Questori della Repubblica sono: n. 1300 nel 2018; n. 1249 nel 2019; n. 956 per il periodo del 2020 fino al 19 novembre.

34) Il ricorso normativo alla nozione di *riconducìbilità* (alle previsioni del codice penale), sottolinea che, nel procedimento preventivo, non rileva la perfetta e piena sussumibilità del fatto nella fattispecie penale tipizzata dalla norma (in tutti i suoi elementi costitutivi), bensì la ricorrenza di una condotta astrattamente qualificabile in quei termini, secondo un apprezzamento indiziario. Cfr. F. Pittaro, *La legge sul femminicidio: le disposizioni penali di una complessa normativa*, in *Famiglia e diritto*, 2014, 7, 715: "i reati di percosse

L'art. 582 comma 2 c.p. prevede invece la fattispecie di lesioni personali procedibili a querela: si tratta delle lesioni c.d. "lievi" (con prognosi sotto 20 giorni), sempreché non sussistano le aggravanti ex art. 583 c.p. (relativo alle lesioni gravi e gravissime) né le aggravanti ex art. 585 c.p., tranne quelle ex art. 577 n. 1 (fatto commesso "*contro l'ascendente o il discendente anche per effetto di adozione di minorenne o contro il coniuge anche legalmente separato, contro l'altra parte dell'unione civile o contro la persona stabilmente convivente con il colpevole o ad esso legata da relazione affettiva*") e tranne quelle "*indicate nell'ultima parte dell'art. 577*" (laddove il riferimento testuale pare doversi riferire al comma 2 dell'art. 577 relativo ai fatti commessi "*contro il coniuge divorziato, l'altra parte dell'unione civile, ove cessata, la persona legata al colpevole da stabile convivenza o relazione affettiva, ove cessate, il fratello o la sorella, l'adottante o l'adottato nei casi regolati dal titolo VIII del libro primo del codice civile, il padre o la madre adottivi, o il figlio adottivo, o contro un affine in linea retta*"). Quindi le "lesioni lievi" (e non altrimenti aggravate ex art. 585 c.p.) commesse in danno di congiunti o ex congiunti (nel senso ex art. 577 comma 1 n. 1 e art. 577 comma 2) rientrano nelle previsioni dell'art. 582 comma 2 e sono quindi procedibili "a querela".

Beninteso: ciò vale a meno che non ricorrano ulteriori aggravanti. Tra queste ultime circostanze che possono concorrere (e rendere quindi procedibili d'ufficio il reato) se ne segnala una in particolare. Si sottolinea invero che, a seguito delle novità normative introdotte dalla legge n. 69/2019 (su cui *infra* nel testo), le "lesioni lievi" (anche se non altrimenti aggravate ex art. 585) commesse dal soggetto già ammonito per stalking (ex art. 8 legge 2009) in danno della vittima degli atti persecutori (cioè della stessa vittima che aveva

---

o di lesioni lievi sono rilevanti non di per sé, ma in quanto sintomatici di un comportamento grave o non episodico di violenza domestica e vengono considerati, in sostanza, come dei "reati sentinella" di forme di violenza o di aggressione che possono precedere delitti di stalking, di maltrattamenti in famiglia, oppure delitti di sangue, ovvero ancora, per ritornare al tema da cui avevamo preso le mosse, lo stesso femminicidio". Per altro verso, pare doversi sottolineare che la scelta del legislatore del 2013 di richiamare selettivamente, quale presupposto, i fatti "riconducibili" (sia pure negli astratti ed ampi termini suddetti) alle sole condotte perseguibili *a querela*, ex art. 581 e 582 cpv c.p. (come aveva fatto il legislatore del 2009 per l'ammonimento collegato a fatti ex art. 612-*bis* c.p.) pare rispondere ad una *ratio* non del tutto comprensibile, vieppiù laddove l'ammonimento per violenza domestica, a differenza di quello per atti persecutori, è stato istituito (come si vedrà nel testo) come strumento di tutela cumulativa rispetto all'eventuale procedimento penale ed indipendente dall'iniziativa della persona offesa.

fatto istanza di ammonimento) sono sussumibili nell'alveo delle lesioni ex art. 582 comma 2 aggravate ex art. 585 e 576 comma 1 n. 5.1 c.p., sicché sono procedibili d'ufficio (e peraltro con l'accelerazione del rito previsto dalla novella dell'art. 347 c.p.p. recata dall'art. 1 d.l. n. 69/2019, su cui *infra*).

Orbene, se la vittima dello *stalking* fosse stata un *familiare o ex congiunto* dell'ammonito (nel senso ex art. 577 comma 1 n. 1 o comma 2), le successive lesioni commesse nei suoi confronti dallo *stalker* ammonito saranno procedibili d'ufficio.

Ma vi è di più.

L'art. 3 d.l. n. 93/2013 consente di adottare l'ammonimento questorile a condizione che i fatti riconducìbili alle fattispecie di cui all'art. 582 comma 2 c.p., oltre che all'art. 581, siano stati tentati o consumati nell'ambito di "*violenza domestica*", situazione tipizzata dallo stesso art. 3 nei seguenti termini: "*Uno o più atti, gravi ovvero non episodici, di violenza fisica, sessuale, psicologica o economica che si verificano all'interno della famiglia o del nucleo familiare o tra persone legate, attualmente o in passato, da un vincolo di matrimonio o da una relazione affettiva, indipendentemente dal fatto che l'autore di tali atti condivida o abbia condiviso la stessa residenza con la vittima*".

In realtà, laddove ricorra un fatto riconducìbile, in astratto, nelle fattispecie (anche solo tentate) di percosse o lesioni (l'art. 3 lo postula sempre), la situazione di "*violenza fisica*" evocata dalla nozione di "violenza domestica" pare doversi ritenere già per definizione, ancorché essa possa essere isolata e non grave, come richiesto dalla norma. In tal caso, bisognerà verificare se quella violenza fisica, unica e lieve (e cioè di per sé insufficiente ex art. 3), si inscriva in un rapporto familiare o affettivo (nel senso sopra precisato e quindi anche concluso) connotato da *violenza psicologica e/o economica* e/o *sessuale*. Se non si rintracciasse alcuna di tali evenienze, non si potrebbe dare corso all'adozione dell'ammonimento.

3.6. L'avvio del procedimento: segnalazione e indisponibilità dalla vittima

Il dato procedurale più nettamente innovativo che connota l'ammonimento per violenza domestica, rispetto a quello per atti persecutori, riguarda l'avvio del procedimento ex d.l. n. 93/2013, che risulta sottratto all'esclusiva disponibilità della vittima.

L'art. 3 del decreto in esame, infatti, prevede che il procedimento monitorio questorile per violenza domestica sia avviato sulla base di una mera "*segnalazione*" proveniente da chiunque abbia contezza della ricorrenza del

suddetto presupposto applicativo dell'istituto, purchè essa sia "*non anonima*"[35].

L'autore della segnalazione è peraltro tutelato dalla correlativa previsione secondo cui "*in ogni atto del procedimento per l'adozione dell'ammonimento di cui al comma 1 devono essere omesse le generalità del segnalante, salvo che la segnalazione risulti manifestamente infondata*".

Si tratta di scelta legislativa evidentemente finalizzata a superare il limite delle comprensibili resistenze che la persona offesa da tali fenomeni delittuosi può frequentemente frapporre all'emersione e denuncia dei fatti di cui è vittima. Se da una parte, tale scelta espone la stessa vittima a iniziative statuali potenzialmente ignorate (peraltro con conseguenti maggiori responsabilità di tutela in capo all'autorità questorile a fronte del rischio di ritorsioni dell'ammonito), per altro verso, la previsione della possibilità che l'impulso al procedimento monitorio arrivi da terzi pare idonea (oltre che ad acuire la reattività del sistema di protezione) a spersonalizzare quell'impulso procedurale stesso o comunque ad affievolire la percezione dell'ammonimento come il risultato di un'iniziativa esclusivamente propria della vittima, suscettibile di innescare reazioni da parte dell'interessato.

Per altro verso, il maggiore rischio per la vittima connesso all'indisponibilità dell'avvio del procedimento monitorio, sembrerebbe bilanciato dalla maggiore discrezionalità apparentemente riconosciuta al Questore in punto di adozione del provvedimento di cui si tratta, all'esito dell'istruttoria, da esercitarsi proprio in relazione alla delicata valutazione della sua compatibilità effettiva con gli altri interessi familiari in campo e segnatamente con la reale rispondenza dell'ammonimento all'esigenza di tutelare la vittima. Invero, l'art. 3 d.l. n. 93/2013 prevede che, all'esito dell'istruttoria, il Questore "può procedere" all'ammonimento per violenza domestica, mentre l'art. 11 d.l. n. 11/2009 non sembrava lasciare alcun margine di discrezionalità al riguardo all'autorità di pubblica sicurezza ("*Il Questore* [...] *ove ritenga fondata l'istanza, ammonisce oralmente il soggetto nei cui confronti è stato richiesto il provvedimento*")[36].

---

35) L'art. 3 d.l. n. 93/2013 testualmente evoca una segnalazione alle "forze dell'ordine", laddove tale ultima nozione – che non trova precisi ed inequivoci contorni definitori nel nostro ordinamento giuridico, come avviene per quelle più tecniche e note di forze armate e forze di polizia – sembra più opportunamente e sistematicamente declinabile con riguardo agli *agenti ed ufficiali di pubblica sicurezza* In senso parzialmente diverso, G. Aliquó, *La violenza domestica. L'ammonimento del Questore*, *op. cit.*, p. 82, ritiene che la formula andrebbe intesa come equivalente a quella di "*forze di polizia*".

36) Cfr. al riguardo G. Aliquó, *La violenza domestica. L'ammonimento del Questore*, *op. cit.*, p. 83, che, con plurimi richiami giurisprudenziali del Consiglio di Stato, sottolinea l'ampia

L'art. 3 d.l. n. 93/2013 impone un'istruttoria particolarmente accurata, atteso che "*la segnalazione è utilizzabile soltanto ai fini dell'avvio del procedimento*".

In concreto, la segnalazione può provenire da terzi testimoni dei fatti, estranei al nucleo familiare o da soggetti intranei allo stesso, così come da soggetti istituzionali che siano venuti a conoscenza delle vicende di violenza domestica per ragioni di istituto (si pensi al personale sanitario o dei servizi sociali).

La segnalazione può provenire anche dalla vittima, con l'avvertenza che ella può contestualmente manifestare la volontà dell'anonimato: in tal caso, le dichiarazioni della stessa non potranno essere dedotte nella motivazione del procedimento monitorio.

La segnalazione può provenire ovviamente da ogni agente o ufficiale di pubblica sicurezza che, laddove abbia contezza dei fatti potenzialmente integranti il suddetto presupposto legittimante l'ammonimento per violenza domestica, ha senz'altro il dovere di farne segnalazione al Questore.

Al riguardo, attesa peraltro la non alternatività con il procedimento penale (su cui *infra*), più delicato si rivela il caso in cui l'agente o ufficiale di pubblica sicurezza abbia conosciuto del fatto in ragione della propria (normalmente compresente) qualifica di polizia giudiziaria. Sul punto, si ritornerà più diffusamente in seguito.

3.7. Effetti dell'ammonimento per violenza domestica e della sua inosservanza

Al netto delle peculiarità disciplinari sin qui rassegnate e della non alternatività col procedimento penale, su cui *infra*, l'istituto monitorio previsto dall'art. 3 d.l. n. 93/2013 partecipa della stessa natura giuridica dell'ammonimento per atti persecutori, introdotto dall'art. 8 del d.l. n. 11/2009, il contenuto della cui ultima norma è esplicitamente richiamato dal legislatore del 2013 come applicabile anche al procedimento per l'adozione del più recente provvedimento per violenza domestica ("*Si applicano, in quanto compatibili, le disposizioni dell'articolo 8, commi 1 e 2, del decreto-legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38, come modificato dal presente decreto*").

---

discrezionalità del Questore al riguardo, anche in relazione alla possibilità di esperire alternativamente il diverso istituto della composizione del privato dissidio ex art. 1 comma 2 TULPS.

Piuttosto, occorre segnalare che lo stesso richiamo normativo sia palesemente circoscritto ai soli primi due commi dell'art. 8 d.l. n. 11/2009 e non anche agli ultimi due commi, di tal ché all'ammonimento per violenza domestica non si applicano le norme sui peculiari effetti penalistici dell'ammonimento per atti persecutori, in punto di aggravamento della pena e procedibilità d'ufficio a carico dell'ammonito (salva la possibile rilevanza dell'ammonimento in sede valutativa della personalità e capacità di delinquere dell'indagato o imputato, nella prospettiva cautelare o di quantificazione della pena).

Ma vi è di più.

L'eventuale inosservanza dell'ammonimento "per violenza domestica" pare avere effetti più lievi di quella concernente l'ammonimento per *stalking*, non solo sul piano penale (per il caso in cui il già ammonito commettesse un reato), ma anche su quello delle conseguenze di natura amministrativo-preventiva.

Ed invero, occorre prendere atto che il già sopra citato combinato disposto degli artt. 16 e 4 comma 1 lettera i-*ter* del d.lgs. n. 159/2011 (all'esito dell'integrazione recata dalla legge n. 69/2019, su cui *infra*) ricomprenda tra i destinatari delle misure di prevenzione personali applicate dall'autorità giudiziaria (segnatamente la sorveglianza speciale di pubblica sicurezza e, in ipotesi, le misure di prevenzione patrimoniale di cui al titolo II del Codice), oltre agli indiziati di atti persecutori, i soli "*soggetti indiziati dei delitti di cui agli articoli 572*" del Codice penale: in difetto di un quadro indiziario sintomatico di condotte riconducibili al predetto delitto di maltrattamenti familiari, quindi, l'inosservanza dell'ammonimento adottato ex art. 3 d.l. n. 93/2013 non varrebbe a legittimare, di per sé, la richiesta di una misura di prevenzione giudiziaria nei confronti del già ammonito (come invece sarebbe possibile nel caso dello *stalking*)[37].

Se l'inosservanza del provvedimento di ammonimento c.d. "per violenza domestica" pare comportare conseguenze sanzionatorie incomprensibilmente più lievi, rispetto a quelle conseguenti alla trasgressione dell'ammonimento "per atti persecutori", gli effetti diretti associati all'adozione del primo prov-

37) G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, cit., p. 214 e 309, stigmatizza siffatta lacuna normativa ed auspica la previsione organica di effetti più pregnanti per l'ammonimento e l'avviso orale, onde scongiurare – come paventato da G. Fiandaca - C. Visconti, *Il codice delle leggi antimafia: risultati, omissioni e prospettive*, in *La legislazione penale*, 2012, p. 183 ss. – che siffatti strumenti presentino "*caratteristiche patetiche di arnesi obsoleti, privi di plausibile funzionalità in una seria ottica special preventiva*".

vedimento questorile sembrano, al contrario, risultare più gravosi rispetto a quelli associati al secondo.

Ed invero, nel caso di ammonimento per violenza domestica, il Questore, non solo "adotta" i provvedimenti in materia di armi, analogamente a quanto previsto per l'altro istituto monitorio introdotto nel 2009, ma ha la possibilità – contemplata dall'art. 3 comma 2 del d.l. 93/2013 – di chiedere al "*Prefetto del luogo di residenza del destinatario dell'ammonimento l'applicazione della misura della sospensione della patente di guida per un periodo da uno a tre mesi*" (sempreché non vi ostino esigenze lavorative dell'interessato).

La discrezionalità riconosciuta al Questore al riguardo (al netto della ricorrenza di ostativi – e prevedibilmente frequenti – motivi professionali), pare postulare un ricorso prudente alla richiesta di siffatto effetto gravoso per l'ammonito, che potrebbe forse essere valorizzato, in una prospettiva di gradualità dell'approccio preventivo, anche quale strumento sanzionatorio dell'inosservanza del precedente provvedimento monitorio, così integrando gli strumenti di tutela della sua efficacia, di cui si sono appena segnalate le apparenti debolezze.

Pare oltremodo opportuno soggiungere, infine, che il comma 5-*bis* dell'art. 3 d.l 93/2013 abbia previsto che: "*quando il Questore procede all'ammonimento* (…) *informa senza indugio l'autore del fatto circa i servizi disponibili sul territorio, inclusi i consultori familiari, i servizi di salute mentale e i servizi per le dipendenze, come individuati dal Piano di cui all'articolo 5, finalizzati ad intervenire nei confronti degli autori di violenza domestica o di genere*". Si tratta di un approccio legislativo multidisciplinare al problema, alla cui stregua l'ammonito (la cui pericolosità postula l'adozione di una tutela avanzata per la vittima) si rivela egli stesso oggetto di attenzioni assistenziali, il cui effettivo avvio (pur sempre subordinato al necessario consenso dell'interessato) passa per un'iniziativa assegnata dal legislatore, anche qui, al Questore[38].

38) Al riguardo, si segnala che la Direzione centrale anticrimine della Polizia di Stato, con la recente circolare del 25 febbraio 2021, già sopra segnalata in nota, abbia invitato i Questori a favorire la stipula di protocolli d'intervento e d'intesa con le amministrazioni locali, le ASL, gli uffici scolastici provinciali, i centri antiviolenza e le associazioni che si occupano della tutela delle donne, in armonia con i protocolli diffusi a livello nazionale. Tra questi ultimi, la stessa circolare rievoca la positiva esperienza della Questura di Milano, che, il 5 aprile 2018, ha stipulato un protocollo di collaborazione (denominato "ZEUS") con il Centro italiano per la promozione e la mediazione, in virtù del quale, peraltro, il Questore inserisce nel testo del decreto di ammonimento la c.d. "*ingiunzione trattamentale*", ossia l'invito rivolto all'ammonito di rivolgersi al centro stesso, onde intraprendere un percorso di crescita personale in punto di controllo delle proprie emozioni.

3.8. Non alternatività col procedimento penale

L'ulteriore rilevante tratto distintivo del procedimento finalizzato all'adozione dell'ammonimento per violenza domestica, rispetto a quello per atti persecutori, risiede nella circostanza che il primo, a differenza del secondo, può svolgersi a prescindere dalla pendenza di un eventuale procedimento penale ma quindi anche parallelamente ad esso.

Invero, a fronte della previsione dell'art. 8 d.l. n. 11/2009 secondo cui la vittima può richiedere l'ammonimento "*fino a quando non è proposta querela*", l'art. 3 d.l. n. 93/2013 – con una formula non ineccepibile – precisa che il Questore possa procedere "*anche in assenza di querela*", da cui si deduce che, analogamente, possa fare laddove una querela sia stata sporta, all'insegna di una netta autonomia reciproca tra il potere preventivo dell'autorità di pubblica sicurezza e l'azione penale esercitata dall'autorità giudiziaria nel procedimento penale.

Ed invero, la disciplina dell'ammonimento per violenza domestica costituisce espressione dell'autonomia del "*diritto della prevenzione*", in cui risiede il suo indubbio valore aggiunto nello statuto di tutela della vittima[39].

Il principio di non alternatività tra procedimento monitorio questorile per l'ammonimento per violenza domestica e l'eventuale procedimento penale pone sul campo il problema dei reciproci rapporti tra siffatti distinti procedimenti in cui si esprimono le prerogative di autorità altrettanto diverse.

Si tratta di problemi estremamente delicati.

Prima di esaminarne i termini, pare opportuno fissare alcuni utili chiarimenti circa l'oggetto del procedimento monitorio e la sua istruzione.

4. Istruzione del procedimento monitorio

4.1. L'oggetto del procedimento amministrativo monitorio

Dopo avere fissato i termini delle prerogative del Questore nel nostro

39) In tal senso, Consiglio di Stato, sentenza n. 1085 del 7-15 febbraio 2019 e sentenza n. 758 del 24-30 giugno 2019, che ribadisce il difetto di qualsivoglia "*rapporto di pregiudizialità condizionalità o ancillarità tra il giudizio penale e quello amministrativo*" nonché la necessità che la materia del diritto amministrativo di prevenzione sia affrancata "*da valori e logiche proprie del diritto punitivo, alla quale non appartiene, e da un più o meno consapevole, inappropriato panpenalismo*".

ordinamento, nonché i lineamenti dell'istituto dell'ammonimento questorile, per come risulta dagli interventi legislativi del 2009 e del 2013, pare opportuno, prima di affrontare il tema dei rapporti tra procedimento monitorio e procedimento penale, soffermarsi sull'esatta definizione dell'oggetto del primo e sugli strumenti istruttori attraverso i quali l'autorità di pubblica sicurezza perviene a maturare il proprio convincimento (i cui estremi andranno puntualmente esplicitati nella motivazione del provvedimento) circa l'adozione dell'ammonimento.

Al riguardo, preso atto della natura di misura di prevenzione del provvedimento monitorio, occorre sottolineare come, nel procedimento amministrativo finalizzato all'adozione dell'ammonimento questorile, non si ricerchi affatto la "prova" della colpevolezza di un soggetto in ordine alla commissione di un reato, secondo i canoni processuali della ragionevole certezza, bensì un sufficiente quadro "indiziario", ancorché basato su elementi di fatto legislativamente tipizzati, circa la pericolosità del soggetto.

Più precisamente, il giudizio preventivo – mutuando categorie elaborate nelle aule dei Tribunali per le misure di prevenzione ma applicabili anche nei paralleli contesti procedimentali amministrativi di competenza del Questore – postula un duplice passaggio logico-giuridico: un primo momento di constatazione della ricorrenza (sempre alla stregua dei predetti canoni indiziari) del presupposto tipizzato dal legislatore, segnatamente coincidente – nei casi in esame – con la ricorrenza di condotte persecutorie o di violenza domestica; un secondo momento, di valutazione prognostica, circa il rischio che l'autore di quelle condotte reiteri in futuro comportamenti lesivi della persona offesa[40].

Il primo momento del giudizio preventivo attiene, quindi, all'accertamento della ricorrenza di una fattispecie tipizzata dal legislatore, siccome evidentemente sintomatica della futura possibilità di compiere condotte pregiudizievoli per la sicurezza pubblica.

Beninteso, tale accertamento (come recentemente ribadito dal Consiglio di Stato, sez. III, sent., 4-25 giugno 2020, n. 4077 con riferimento ad un caso di ammonimento per atti persecutori) riguarda «*un quadro istruttorio da cui emergano, anche solo su un piano indiziario, eventi che recano un vulnus alla riservatezza della vita di relazione o, in senso lato e in forma anche potenziale,*

40) Su tale struttura logico-giuridica del giudizio preventivo, cfr. Cassazione, sezione I penale, sentenza n. 349 del 15 giugno 2017 - 9 gennaio 2018 che richiama Corte costituzionale, sentenza n. 177 del 16-22 dicembre 1980.

all'integrità della persona. Anche all'ammonimento, infatti, deve applicarsi quella logica dimostrativa a base indiziaria e di tipo probabilistico che informa l'intero diritto amministrativo della prevenzione. [...]. *Pertanto, il provvedimento di ammonimento presuppone non l'acquisizione della prova richiesta ai fini della condanna per il reato di stalking, di cui all'art. 612-bis c.p., ma la sussistenza di soli elementi indiziari dai quali sia possibile desumere, con un adeguato grado di attendibilità, un comportamento reiterato anomalo, minaccioso o semplicemente molesto, come tale avvertito dal destinatario della condotta, che sia atto a determinare uno stato di "ansia e paura" nella vittima*».

Sotto questo aspetto, l'oggetto del procedimento monitorio è quindi essenzialmente l'*indizio*, sottendente la qualificata possibilità che il soggetto di cui si tratta leda il bene tutelato della vittima[41].

---

41) Sulla nozione di indizio, cfr. G. Aliquó, *La violenza domestica. L'ammonimento del Questore*, *op. cit.*, p. 272 ss. L'A. si interroga sulle nozioni di *fatto*, *sospetto*, *indizio*, (elemento di) *prova*, ricercando gli incerti limiti di esse, con l'obiettivo di rintracciare ed isolare i criteri ermeneutici che permettano di cogliere e definire, innanzitutto, gli estremi di rilevanza giuridica delle vicende, in un contesto istituzionale di tutela della vittima costituzionalmente orientato, nonché la soglia entro la quale l'operatore di polizia si confronti con una materia gnoseologica suscettibile di rilevare in sede preventiva e oltre la quale, invece, debba riferirne all'autorità giudiziaria: "La prova rappresentativa e quella indiziaria, pur mirando allo stesso *thema probandum*, differiscono tra loro per l'atteggiarsi del ragionamento inferenziale: nella prima la "prova" è l'effetto della rappresentazione di una percezione diretta del fatto da provare, che si acquisisce mediante la fonte di prova; con l'indizio, invece, si ha solo un fatto che, mediante un ragionamento probabilistico fondato su criteri esperienziali o scientifici, deve sostenere logicamente (unitamente ad altri indizi) una distinta conclusione presuntiva. [...]. Nella fase istruttoria del procedimento giudiziario, più che di prove o indizi, è comunque il caso di parlare di "*elementi di prova*" o "*elementi d'indizio*", trattandosi di materiale che, introdotto regolarmente nel procedimento (civile, penale o amministrativo), è destinato a essere utilizzato per la specifica attività valutativa richiesta, nel contraddittorio tra le parti, all'Organo chiamato alla decisione. Solo con le garanzie del dibattimento tali elementi possono condurre, a seconda dei casi, a un esito probatorio o arrestarsi a uno meramente indiziario. A maggior ragione non si ritiene che possa parlarsi di formazione della "prova" nel procedimento amministrativo di prevenzione: per quanto il procedimento amministrativo sia garantito, manca la pienezza del contraddittorio tra le parti e, in ogni caso, è l'*indizio* che, nella cornice della prevenzione, è sufficiente e determinante per sostenere le decisioni". [...] Non è necessario, in altre parole, che gli indizi raccolti nel procedimento di prevenzione abbiano né la forza di prova né quella degli elementi induttivi atti a sostenere la qualificata probabilità che le condotte del soggetto maltrattante possano condurre alla futura affermazione della sua responsabilità penale. Per l'applicazione delle misure di prevenzione ci si muove,

Ciò, beninteso, con la duplice seguente precisazione:

– per un verso, tale sufficiente indizio non è – e non può essere – un semplice "sospetto"[42];

– per altro verso, attesa peraltro la coessenziale natura urgente del provvedimento che si tratta di adottare, non sarà necessario pervenire a livelli di qualificata gravità indiziaria (richiesta, per esempio, per l'adozione delle misure cautelari in sede giudiziaria), né tampoco ad un quadro di indizi "gravi, precisi e concordanti", integranti gli estremi della prova (indiretta) del reato nel giudizio penale[43].

Il secondo momento valutativo, in cui è articolabile il processo logico che presiede all'adozione del provvedimento preventivo, è invece riassumibile in un giudizio prognostico circa la *pericolosità sociale* dell'interessato.

Al riguardo, occorre precisare che la pericolosità sociale sottesa ai procedimenti monitori questorili in esame pare qualificata da un differenziale e marcato orientamento verso la persona fisica della singola vittima

---

in realtà, nello spazio più ampio della "*qualificata possibilità*". L'indizio "semplice" – che in questa sede è idoneo a fondare il ragionamento inferenziale – coincide con il concetto di "*fondato sospetto*", ovvero di elemento di fatto dotato di quel sufficiente grado di concordanza (anche se non di precisione e gravità) che, nella relazione con altri elementi di fatto raccolti nel corso del procedimento amministrativo, consente di sostenere logicamente la prognosi di pericolosità. La motivazione del provvedimento, allora, dovrà avere alla sua base un ragionamento probabilistico che, forte degli indizi raccolti, attinga la soglia logica della qualificata possibilità, ovvero della "*ragionevole verosimiglianza*" dell'ipotesi del quadro di violenza domestica e della sua attualità. [...]. L'indizio, anche nel campo delle misure di prevenzione, non può essere considerato in maniera parcellizzata, in modo avulso da un più ampio contesto ricostruttivo degli altri elementi raccolti. È nella reciproca relazione dei singoli indizi, infatti, che il quadro complessivo assume effettiva significanza. Occorre, allora, una ricognizione globalmente unitaria e compiuta dell'intero compendio indiziario, finalizzata a far affermare, nella tendenziale univocità della lettura logica degli elementi di fatto raccolti, la concreta possibilità di un attuale clima di violenze domestiche e un quadro prognostico di pericolosità del maltrattante. Si sarebbe, invece, in presenza di indizi penalmente rilevanti – e dunque di una notizia di reato – ove l'analisi globale degli stessi porti a superare la soglia del "fondato sospetto" (ovvero dell'indizio semplice), consentendo di affermare la sussistenza di plurimi elementi di fatto costituenti, nel loro insieme, ipotesi di reato perseguibili d'ufficio. Gli elementi raccolti che consentano di percepire un fatto come verificato e, da un punto di vista di diritto, di ipotizzarne l'inquadramento in una fattispecie penalmente rilevante, integrano, dunque, la *notizia di reato*".

42) In tal senso Cassazione, sezioni unite, sentenza n. 51407 del 21 giugno 2018 - 13 novembre 2018.

43) Cfr. in tal senso Cass., sez. unite, sentenza n. 13426 del 25 marzo - 9 aprile 2010.

di atti persecutori o violenza domestica, oltre che da una imprescindibile attualità[44].

4.2. L'investigazione preventiva di pubblica sicurezza

Il predetto processo decisorio del Questore postula la disponibilità di un quadro gnoseologico adeguato, raggiunto all'esito di un'istruzione procedimentale che – laddove gli elementi indiziari non siano già agli atti dell'autorità questorile – può passare attraverso una vera e propria attività investigativa, qualificabile come *di pubblica sicurezza*, affidata agli agenti ed ufficiali di p.s.[45]: si tratta – beninteso – di attività investigativa assolutamente distinta da quella di *polizia giudiziaria* che, sotto la direzione dell'autorità giudiziaria, compete agli agenti ed ufficiali di p.g., normalmente appartenenti ai diversi uffici costituenti servizi di polizia giudiziaria ex art. 56 c.p.p. (in Questura, la Squadra mobile e, per alcuni ambiti criminali, la Digos), per le diverse finalità repressive dei reati consumati o tentati[46].

Del resto, sia il d.l. n. 11/2009 istitutivo dell'ammonimento per atti persecutori, che (con formula normativa pressoché analoga) l'art. 3 d.l. n. 93/2013, per l'ammonimento per c.d. violenza domestica, prevedono esplicitamente che il Questore – si intende: tramite gli ufficiali ed agenti di p.s. – provveda all'ammonimento "*sentite le persone informate dei fatti*" e assunte, se necessario, "*informazioni dagli organi investigativi*".

Quanto all'audizione di persone informate dei fatti, va preliminarmente precisato che, al netto di una formulazione normativa apparentemente assertiva, si tratta di atto istruttorio cui ricorrere solo se necessario[47].

---

44) In tal senso, Corte costituzionale, n. 291del 25 settembre - 2 dicembre 2013 che ha dichiarato l'incostituzionalità dell'art. 12 legge n. 1423/1956, nella parte in cui esso non prevedeva che, nel caso in cui l'esecuzione di una misura di prevenzione personale restasse sospesa per l'espiazione di una pena, l'organo che aveva applicato la misura preventiva dovesse rivalutare la persistente ed attuale pericolosità sociale del sottoposto con riguardo l momento in cui si trattava di ripristinarne l'esecuzione.

45) Tale istruttoria è curata dall'Ufficio misure di prevenzione, istituito in seno all'Ufficio di polizia anticrimine di ogni Questura e sotto il coordinamento funzionale, per tutto il territorio nazionale, di un Servizio centrale anticrimine istituito nella Direzione centrale anticrimine della Polizia di Stato. Sul problema della forma degli atti degli agenti ed ufficiali di pubblica sicurezza cfr. *supra* capitolo 1, paragrafo 1.3.

46) Sulla necessità, in generale, di un'attività istruttoria di pubblica sicurezza finalizzata a riscontrare la segnalazione o richiesta di ammonimento, cfr. TAR Abruzzo, sezione I, sentenza 428 del 13/28 maggio 2015.

47) In tal senso TAR Lazio, sez. I-*ter*, sentenza n. 10628 del 23 ottobre - 5 novembre 2018,

Ed invero, analogamente a quanto avviene nel procedimento penale (ad esempio per l'applicazione delle misure cautelari), le dichiarazioni della vittima – nel caso di specie, rassegnate nella richiesta o segnalazione (non anonima) di ammonimento – se soggettivamente credibili ed intrinsecamente attendibili e coerenti, ben possono risultare di per sé sufficienti a fondare il convincimento del Questore circa la necessità di adottare il provvedimento monitorio di competenza (in tal senso Consiglio di Stato, sez. I, parere n. 2794 del 25 settembre - 7 novembre 2019)[48].

Quanto all'identità delle persone da sentire, il riferimento più proprio ed immediato è ovviamente a soggetti terzi, che (per ragioni contingenti o anche connesse al proprio lavoro o servizio) siano a conoscenza delle vicende che rilevano ai fini di cui si tratta: gli stessi sono convocabili ex art. 15 TULPS ed escutibili dagli agenti ed ufficiali di p.s. che procedono[49].

Non va tuttavia dimenticato che, tra le persone suscettibili di essere sentite, rientra anche la vittima, segnatamente quando l'avvio del procedimento fosse avvenuto sulla base di un atto di impulso diverso dall'istanza o segnalazione della stessa (il riferimento è al caso di ammonimento per violenza do-

---

secondo cui "spetta al Questore, quindi, valutare discrezionalmente se sia necessario effettuare ulteriori indagini, ben potendo comunque ritenere sufficienti gli elementi a sua conoscenza per provvedere immediatamente". T.A.R. Piemonte Torino, sez. I, 02/03/2012, n. 290 (Marinetti c. Ministero dell'interno e altri): "Ai sensi dell'art. 8 d.l. n. 11/2009, deve ritenersi adeguatamente motivato il decreto di ammonimento che, per quanto non preceduto dall'audizione di persone informate dei fatti, si fonda su dati fattuali precisi ed emergenti dalle risultanze istruttorie, non contestati dall'ammonito, tali da integrare un quadro indiziario che rende verosimile, secondo criteri di ragionevolezza, la sussistenza dei presupposti per l'adozione del decreto di ammonimento nei suoi confronti".

48) Anche se, ovviamente, un provvedimento motivato sulla sola versione della vittima si espone a elevati rischi di successiva censura giurisdizionale: così, ad esempio, TAR Umbria, sentenza 486 del 18 giugno - 2 settembre 2019, ha annullato un provvedimento questorile basato sulle sole dichiarazioni della vittima.

49) Sulla possibilità e modalità di escussione di soggetti minori cfr. G. Aliquó, *La violenza domestica. L'ammonimento del Questore*, *op. cit.*, p. 157 ss. L'A. segnala la necessità (il cui fondamento giuridico ravvisa nell'art. 1 legge n. 241/1990 che richiama i principi generali dell'ordinamento comunitario e quindi anche quelli discendenti dalla direttiva 2012/29/UE sulla protezione delle vittime di reato) che tali delicatissimi atti vengano esperiti dagli ufficiali di p.s. con le medesime modalità previste nell'ambito dei procedimenti penali (ivi comprese le videoregistrazioni e l'assistenza di psicologi), al fine di consentire ex art. 220 disp. att. c.p.p. l'utilizzabilità di quelle informazioni anche nel procedimento penale e scongiurare comunque fenomeni di c.d. vittimizzazione secondaria, oltre che inficiare la genuinità delle dichiarazioni raccolte.

mestica, atteso che quello per *stalking* presuppone, per definizione, siffatta richiesta della persona offesa)[50].

Come anticipato, poi, l'applicazione dei generali principi di partecipazione procedimentale ex legge n. 241/1990 impone già – salvi i casi in cui "*sussistano ragioni di impedimento derivanti da particolari esigenze di celerità del procedimento*", da esplicitare caso per caso con adeguata motivazione[51] – di avvisare dell'avvio del procedimento lo stesso ammonendo, che potrà intervenire nel procedimento tramite la richiesta di sua audizione personale, in aggiunta o alternativa alla produzione di eventuali osservazioni o memorie scritte[52].

Ma il Questore può assumere anche "*informazioni dagli organi investigativi*".

La formula non pare chiarissima.

Il riferimento ad "organi investigativi" – attesa la natura preventiva di pubblica sicurezza che connota l'istruttoria di cui qui si tratta ed esclusa la disponibilità in capo al Questore dei servizi di polizia giudiziaria in quanto tali – pare doversi intendere come relativo, innanzitutto, all'articolazione della Questura il cui personale (costituito da agenti ed ufficiali di p.s. appartenenti ai ruoli della Polizia di Stato) è prioritariamente preposto alle attività istruttorie in materia di misure di prevenzione.

---

50) Per contro, non si procederà ad escutere la vittima laddove sia stata proprio ella ad inoltrare la segnalazione finalizzata ad ottenere l'ammonimento per violenza domestica, con richiesta di anonimato ex art. 3 comma 4 d.l. n. 93/2013.

51) È tipico il caso in cui dall'istanza o segnalazione o dai primissimi atti istruttori emerga già una situazione di insostenibilità per la vittima o la prospettiva di imminenti (ulteriori) pregiudizi per la stessa o altri familiari: cfr. Consiglio di Stato, sezione I, parere 2439 del 4/13 settembre 2019; Consiglio di Stato, sezione III, sentenza n. 4241 del 29 settembre/13 ottobre 2016.

52) Sulla possibilità che la partecipazione dell'interessato al procedimento amministrativo avvenga indifferentemente con memorie scritte o audizione orale cfr., *ex plurimis*, Consiglio di Stato, sezione I, parere n. 2794 del 25 settembre - 7 novembre 2019. Piuttosto, T.A.R. Emilia-Romagna Parma, sez. I, sent. 14/07/2009, n. 637 (Saouf A. c. Ministero dell'interno) ha ribadito che "l'audizione dell'interessato è una forma di partecipazione al procedimento che non rientra tra quelle contemplate dalla l. n. 241/90, sicché l'Amministrazione è tenuta ad ammetterla solo quando vi si sia preventivamente autovincolata". Ciononostante, se l'ammonendo chiedesse di essere sentito, pare oltremodo opportuno che le sue dichiarazioni vengano acquisite al quadro conoscitivo sulla base del quale il Questore deve provvedere, attesa la natura del provvedimento adottando, significativamente incisivo sulla sfera giuridica dello stesso interessato. Ed invero non mancano pronunce del giudice amministrativo nel senso della necessità di un'audizione orale dell'ammonendo: cfr.TAR Toscana, sez. III, sentenza n. 1379 del 8/23 ottobre 2019.

Ma non può negarsi, in relazione all'inquadramento ordinamentale premesso nelle pagine precedenti, che il Questore abbia possibilità di richiedere ogni utile informazione ostensibile, al riguardo, anche ad altri uffici di diverse forze di polizia (magari quelle appartenenti a presidi territorialmente più prossimi ai soggetti interessati), della Polizia locale o di altri uffici pubblici che dispongano di quel patrimonio informativo in ragione dei propri compiti istituzionali, in senso ampio.

Anche la nozione di "informazione", suscettibile di essere assunta dai predetti organi – a fronte del diverso patrimonio conoscitivo orale, acquisibile "*sentite*" le persone informate (tra cui possono ben rientrare anche i rappresentanti di uffici) – pare doversi intendere estensivamente come relativa a qualsivoglia dato gnoseologico idoneo ad integrare il quadro conoscitivo del Questore, così ricomprendendo anche l'acquisizione di dati documentali (referti, certificati, relazioni di servizio, documentazione videofotografica, ecc.)[53].

4.3. Rapporti con le prove del procedimento penale

L'autonomia del procedimento amministrativo finalizzato all'adozione delle misure di prevenzione, rispetto al procedimento penale, è corollario della reciproca autonomia dell'autorità di pubblica sicurezza rispetto all'autorità giudiziaria, discendente da basilari ed inderogabili principi di ripartizione dei poteri statuali amministrativi e giudiziari.

In tal senso, pare opportuno richiamare ancora il recente arresto del Consiglio di Stato, sezione III (sentenza 758 del 24-30 gennaio 2019 n. 758**)** che, pronunciandosi sui confini del diritto amministrativo di prevenzione (nello specifico campo delle interdittive antimafia), esclude esplicitamente ogni "*rapporto di pregiudizialità, condizionalità o ancillarità tra il giudizio penale e quello amministrativo*", che finirebbe peraltro per pregiudicare l'efficacia e tempestività dello strumento preventivo monitorio e quindi la *ratio* della sua stessa previsione legislativa quale strumento per scongiurare una condotta aggressiva che si abbia fondato motivo di ritenere possibile ed imminente.

Ne discende che le stesse attività istruttorie poste in essere nel procedimento preventivo non sono condizionate da quelle svolte nel giudizio penale, rimanendo libero il Questore di fondare il proprio convincimento anche su elementi già vagliati in un parallelo o precedente giudizio penale, i cui atti po-

53) Sull'acquisibilità ed utilizzabilità in sede amministrativa di materiale videofotografico cfr. TAR veneto, sezione III, sentenza n. 711 del 12/17 giugno 2019.

trebbero essere richiesti ed utilizzati in sede preventiva, ad esempio, a seguito dell'emergere di un nuovo indìzio che riattualizzi il pericolo sotteso ad una vicenda giudiziariamente trattata: e ciò è vero anche se il giudizio penale non abbia condotto a condanna (per es. per archiviazione, remissione di querela[54], proscioglimento[55], prescrizione)[56].

Il Questore non è nemmeno vincolato dal giudicato penale, atteso che la stessa assoluzione irrevocabile dell'ammonendo, in sede penale, non impedisce all'autorità di pubblica sicurezza di inferirne comunque – sempre attraverso un puntuale e coerente processo logico motivazionale che muova da fatti oggettivamente apprezzabili, nella diversa prospettiva del procedimento preventivo – una pericolosità sociale che postuli l'adozione del provvedimento monitorio[57].

Due limiti paiono tuttavia enucleabili, al riguardo, per l'autorità questorile.

Il primo limite riguarda i rapporti tra il procedimento monitorio ed il processo penale già precedentemente concluso: in sede di procedimento preventivo, il Questore non potrà assumere come sussistenti, sia pure indiziariamente, fatti la cui ricorrenza sia stata esclusa da sentenze passate in giudicato[58].

---

54) Remissione della querela che, pur potendo comportare la conclusione del procedimento penale, non solo non impedisce affatto l'avvio o prosecuzione di un procedimento finalizzato all'adozione dell'ammonimento per c.d. violenza domestica ex art. 3 d.l. n. 93/2013 ma addirittura può assumere particolare valore indicativo della soggezione della vittima remittente la querela rispetto a pressioni o intimidazioni dell'ammonendo. In tal senso Cassazione, sezione VI penale, sentenza n. 175 del 15 novembre 2018 - 4 gennaio 2019

55) L'art. 651-*bis* c.p.p. prevede piuttosto che la sentenza di proscioglimento *per particolare tenuità del fatto*, pronunciata a seguito di dibattimento, faccia stato in sede amministrativa (come in quella civile) quanto all'accertamento della sussistenza del fatto, della sua illiceità penale e della sua commissione da parte dell'imputato.

56) Il soggetto a carico del quale è avviato procedimento monitorio ben può essere stato già sottoposto a procedimento penale, non ostandovi il principio del *ne bis in idem* pacificamente escluso nel campo del diritto di prevenzione, anche dopo la celebre sentenza della CEDU 4 marzo 2014, Grande Stevens c. Italia, atteso che le misure di prevenzione nell'ordinamento italiano sono misure dirette ad evitare la commissione di atti criminali e mai a sanzionare la realizzazione di essi, di tal ché non partecipano di natura (nemmeno sostanzialmente) penale: in tal senso Cass., sez. II, sentenza n. 26235 del 4 giugno 2015 (in Rivista di Polizia Anno LXIX, fascicolo I-II, 2016, pag. 114).

57) In tal senso Cassazione, sezioni unite sentenza n. 13426 del 25 marzo/9 aprile 2010 nonché Consiglio di Stato, sez. I parere n. 2794 del 25 settembre - 7 novembre 2019.

58) In tal senso Cassazione, sez. II, sentenza n. 11846 del 19 gennaio - 15 marzo 2018; Cassazione, sez. VI, sentenza n. 49541 del 13 settembre - 27 ottobre 2017.

Il secondo limite riguarda invece i rapporti tra il procedimento monitorio, in corso d'istruzione, ed il procedimento penale che (eventualmente) si avvierà o celebrerà successivamente: in questa prospettiva, l'acquisizione degli atti istruttori in sede amministrativa deve tenere conto della necessità di assicurare gli elementi di prova destinati al processo penale. Ne discende la necessità che gli atti stessi siano acquisiti con le forme previste dal Codice di procedura penale, ai sensi dell'art. 220 disp. att. c.p.p. che – regolando la materia di confine tra investigazioni amministrative e penali (le c.d. "*indagini anfibie*") – dispone che "*quando nel corso di attività ispettive o di vigilanza previste da leggi o decreti emergono indizi di reato, gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale sono compiuti con l'osservanza delle disposizioni del codice*"[59].

La norma (testualmente relativa al corso di "attività ispettive o di vigilanza" previste da leggi e decreti) si ritiene applicabile anche al procedimento

59) Cfr. M. Rampioni, *Le c.d. indagini "anfibie": linee di fondo sul controverso legame tra attività ispettive e processo penale*, nella rivista on-line *Processo penale e giustizia* 1/2019, che, sottolineando il diverso contenuto della disposizione ex art. 220 disp. att. c.p.p. rispetto a quello più pregnante dettato dall'art. 223 disp. att. c.p.p. in materia di analisi di campione, si sofferma sui rischi di violazione delle garanzie difensive per l'indagato sottesi all'applicazione del primo istituto (soprattutto nel rapporto tra procedimento ispettivo tributario e processo penale). L'A. segnala due alternative soluzioni al problema: «*De jure condendo*, e al fine di salvaguardare le garanzie fondamentali del soggetto che subisce l'accertamento ispettivo, si potrebbero prospettare soluzioni alternative. Innanzitutto, l'attuazione di un sistema in cui la separazione delle funzioni è totale. Per cui, tutto ciò che emerge in sede d'indagine amministrativa non può essere utilizzato in alcuna fase del processo penale. Alla polizia amministrativa spetterà il solo compito di comunicare all'autorità giudiziaria un'eventuale anomalia; il magistrato del pubblico ministero, poi, applicando le disposizioni del codice di rito, dovrà verificare, autonomamente o in collaborazione con la polizia giudiziaria, se tale segnalazione è fondata o meno. Eliminando ex tunc qualsiasi forma di collaborazione, si risolverebbero (per altro) altre due problematiche strettamente connesse fra loro: quella relativa al binomio indizi-sospetti e quella concernente il momento applicativo delle garanzie difensive. Una simile ricostruzione tuttavia, non solo, appare eccessivamente drastica e perciò di difficile applicazione, risultando inverosimile l'ipotesi di nessun contatto tra i diversi organi; inoltre, non sembra neppure rispondere alle esigenze di economia, in quanto la netta separazione delle funzioni provocherebbe la ripetizione dei medesimi accertamenti. Altra soluzione, forse l'unica (almeno ad avviso di chi scrive) in grado di salvaguardare le garanzie del soggetto che subisce l'accertamento, quella di anticipare massimamente le tutele difensive: sin dall'inizio dell'accertamento amministrativo (pertanto quando ancora non sono emersi indizi) si informa il soggetto passivo della verifica del diritto di farsi assistere dal proprio difensore di fidu-

amministrativo monitorio del Questore, la cui istruttoria – come precisato – postula un'attività investigativa amministrativa (di pubblica sicurezza) i cui esiti possono rilevare ai fini dell'accertamento in sede di giudizio penale[60].

In definitiva, gli atti istruttori del procedimento amministrativo, prima che emergano indizi di reato, saranno assumibili liberamente nelle ordinarie forme dell'investigazione preventiva di pubblica sicurezza. Gli stessi atti, in linea generale, potrebbero confluire nel successivo procedimento penale, attraverso l'acquisizione al fascicolo del dibattimento come prova documentale ex art. 431 c.p.p.[61].

---

cia. Così facendo, non solo si consente la collaborazione tra autorità giudiziaria e amministrativa (espressione di «armonia» tra i diversi poteri dello Stato al fine di raggiungere obiettivi comuni), ma, inoltre, si risolverebbero in radice tutte le questioni fin qui segnalate (sia quella relativa al binomio "indizio-sospetto", che quella concernente il momento applicativo delle garanzie difensive) che affliggono l'istituto».

60) La volontà del legislatore di estendere il più possibile l'ambito applicativo dell'art. 220 disp. att., per le irrinunciabili garanzie che ne derivano, è sottolineata da N. ROMBI, *La circolazione delle prove penali*, Cedam, Padova, 2003, p. 159. In tal senso anche G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, *op. cit.*, p. 284 ss. che richiama a sua volta F. Roia, *Crimini contro le donne. Politiche, leggi, buone pratiche*, Milano, 2017, p. 148. L'A. sottolinea come, opinando diversamente, si delineerebbe il rischio di far entrare nel processo penale (alla stregua di ogni altro documento acquisibile ex art. 234 e ss c.p.p. al fascicolo dibattimentale) anche atti postulanti specifiche forme e garanzie: si pensi all'assunzione delle dichiarazioni dello stesso autore delle condotte violente, eventualmente sentito in sede di partecipazione al procedimento quale controinteressato, senza le garanzie che il c.p.p. assicura all'indagato o imputato. Sul problema dell'utilizzabilità in dibattimento delle dichiarazioni rese dal soggetto destinatario dell'accertamento amministrativo attraverso la testimonianza de auditu dell'organo amministrativo, cfr. M. Rampioni, *Le c.d. indagini "anfibie": linee di fondo sul controverso legame tra attività ispettive e processo penale*, cit., p. 246. che sottolinea come il divieto ex art. 62 c.p.p. (di per sé orientato verso le sole dichiarazioni pre-assunte in sede procedimentale penale) sia stato valorizzato come ostativo alla testimonianza su dichiarazioni rese anche in contesti amministrativi da Cass., sez. un., 28 novembre 2001, n. 45477, in *Arch. nuova proc. pen*., 2002, p. 35.

61) Anche tale impostazione solleva talune riserve dottrinarie. Cfr. N. Rombi, *La circolazione delle prove penali*, Cedam, Padova, 2003, p. 160, secondo cui, in ossequio ai principi dell'oralità e dell'immediatezza cui dovrebbe ispirarsi il processo penale, non è acquisibile, quand'anche formatasi prima dell'emersione indiziaria, la documentazione di atti effettuata nel corso di una procedura amministrativa (a meno che non si tratti di atti amministrativi "irripetibili") "dovendo i medesimi contenuti conoscitivi essere ricavati attraverso l'assunzione diretta di una prova costituenda". Facendo diversamente, infatti, "il ricorso agli organi amministrativi […] diverrebbe l'escamotage per ottenere elementi probatori utilizzabili come prova dei fatti nel processo penale ma al di fuori del rispetto di ogni garanzia difensiva in esso operante".

Dal momento in cui emergessero indizi di reato, invece, l'istruttoria amministrativa dovrà tenere conto della necessità di rispettare le forme del codice di rito penale (e gli atti acquisiti, salvi casi di irripetibilità, confluiranno nel fascicolo del p.m.).

E ciò beninteso, a pena di inutilizzabilità di quegli atti nell'instaurando procedimento penale[62] e di responsabilità disciplinare dell'ufficiale di p.s. procedente (siccome normalmente titolare di qualifiche di polizia giudiziaria che lo espongono al riguardo).

Considerata la contiguità ontologica tra aspetti penali e amministrativo-preventivi della materia in esame, appare oltremodo opportuno, anche sotto tale profilo, che il procedimento questorile e l'indagine penale si svolgano all'insegna di una costante intesa e sintonia tra le autorità cui essi competono.

5. Procedimento monitorio e procedimento penale

5.1. I concreti termini del problema

Nelle pagine precedenti, affrontando direttamente la disciplina degli istituti degli ammonimenti questorili, sono stati lambiti incidentalmente i problematici ed incerti termini in cui taluni aspetti del relativo procedimento amministrativo interagiscono con le previsioni normative (talora di rango costituzionale) che presiedono allo svolgimento del distinto procedimento giudiziario penale.

In realtà, la contiguità tra l'oggetto del procedimento giudiziario e quello del procedimento questorile, in uno alla chiara volontà del legislatore di cumulare strutturalmente i due distinti binari della tutela penale e di quella preventiva, in un unico, articolato ed auspicabilmente più efficace statuto di protezione della vittima (almeno nella materia della violenza domestica), postulano la necessità di un più approfondito e diretto inquadramento dei termini in cui sono destinati, non solo a convivere, ma a potenziarsi le prerogative istituzionali del Questore e dell'autorità giudiziaria su questo campo.

Al riguardo, è opportuno ribadire schematicamente che il ricorso all'isti-

62) Tuttavia, secondo Cass. pen., sez. III, sent., 21/11/2019, n. 9977 (rv. 278423-01), La violazione dell'art. 220 disp. att. cod. proc. pen. non comporta automaticamente l'inutilizzabilità dei risultati probatori acquisiti nell'ambito di attività ispettive o di vigilanza, essendo invece necessario che tale sanzione processuale sia autonomamente prevista dalle norme del codice di rito cui la disposizione citata rimanda.

tuto dell'ammonimento (*rectius* ai diversi istituti di ammonimento) del Questore è ipotizzabile con riguardo a fatti astrattamente *riconducibili* (nel senso sopra precisato) a tre situazioni fattuali, per la cui descrizione il legislatore richiama i reati di[63]:

– atti persecutori ex art. 612-*bis* c.p. (art. 8 d.l. n. 11/2009);

– percosse ex art. 581 C.P, tentate o consumate in un contesto di "violenza domestica" (art. 3 d.l. n. 93/2013);

– lesioni personali c.d. lievi, ex art. 582 comma 2 c.p., tentate o consumate in un ambito di "violenza domestica" (ai sensi del già citato art. 3 d.l. 93/2013).

Come è ormai chiaro, quelle situazioni fattuali potrebbero costituire oggetto anche di un distinto procedimento penale avviato dall'autorità giudiziaria, talora alternativamente, talaltra contestualmente al procedimento amministrativo dell'autorità di pubblica sicurezza.

Beninteso, l'affermazione va intesa nel senso precisato nel capitolo precedente, cioè con costante riferimento alla diversità dell'oggetto, rispettivamente, del procedimento amministrativo (preventivo) e di quello giudiziario. Il primo non mira come il secondo, all'accertamento di un quadro probatorio ragionevolmente certo circa l'effettiva commissione del reato (nella sua struttura tipica e nei suoi profili di antigiuridicità e colpevolezza) e tantomeno alla responsabilità soggettiva del suo autore. Esso, piuttosto, può e deve attestarsi allo stadio della ricorrenza di un ragionevole o sufficiente quadro indiziario che collochi l'interessato nel contesto "criminologico" disegnato dal legislatore (c.d. fase constatativa del giudizio preventivo), per poi passare al giudizio circa la soggettiva pericolosità sociale dell'interessato (fase della c.d. valutazione prognostica, concernente la prospettiva di una sua futura lesione di beni giuridici tutelati).

In questo senso, come appena sopra chiarito, è bene ribadire altresì che le stesse istruttorie dei due procedimenti hanno – in astratto – obiettivi diversi, ricercando il procedimento penale "elementi di prova" ed il procedimento preventivo "indizi".

Tuttavia, è altrettanto innegabile che quella prima fase del giudizio preventivo tesa a riscontrare o constatare, sia pure indiziariamente, la condotta del soggetto tipizzata legislativamente (da cui inferire la successiva prognosi

63) Prescindendo dall'ultima ipotesi di ammonimento introdotta nel nostro ordinamento dalla legge 29 maggio 2017 n. 71, in materia di *cyberbullismo,* che non rientra nell'oggetto del presente lavoro.

di pericolosità), sottenda in concreto un'attività gnoseologica e valutativa molto vicina o contigua a quella tipicamente propria del giudizio penale.

E ciò è ancor più vero ed evidente laddove la "fattispecie preventiva", da cui desumere elementi prognostici circa la futura pericolosità del soggetto, sia stata tipizzata dal legislatore essenzialmente con esplicito riferimento alla commissione di uno o più reati, come avviene appunto nel caso di cui all'art. 3 d.l. n. 93/2013 (che evoca la preventiva commissione da parte dell'ammonendo di fatti riconducibili ai reati ex artt. 581 e 582 cpv. c.p. sia pure con l'ulteriore contestualizzazione di essi in un ambito di violenza domestica).

La delicatezza di siffatta interazione e delle connesse conseguenze operative è acuita dalla notoria circostanza per cui gli ufficiali ed agenti di pubblica sicurezza, che ricevono gli atti di impulso del procedimento amministrativo monitorio o ne curano l'istruzione, sono contestualmente – di fatto tutti – titolari anche della qualifica di ufficiali ed agenti di polizia giudiziaria, soggiacendo ai correlativi doveri.

Tanto premesso, pare necessario scandagliare siffatto problematico rapporto tra i due procedimenti ed i relativi riflessi sui doveri degli operatori, con l'avvertenza che, conformandosi esso in termini diversi a seconda (quantomeno) del tipo di ammonimento questorile di cui si tratta, si ritiene opportuno condurre tale analisi con distinta attenzione al caso dell'ammonimento c.d. per *stalking* rispetto a quello per c.d. violenza domestica.

5.2. Il caso dell'ammonimento per *stalking*

Come anticipato sopra, l'art. 612-*bis* c.p. ha introdotto nel nostro ordinamento il delitto di atti persecutori, prevedendo al riguardo la procedibilità a querela (proponibile entro sei mesi e rimettibile solo in sede processuale). Con il d.l. n. 93/2013 (lo stesso intervento che ha istituito il diverso ammonimento per violenza domestica), per il reato di atti persecutori è stata introdotta la previsione dell'arresto obbligatorio in flagranza ex art. 380 comma 2 lettera l-*ter* (sempreché sussista la condizione di procedibilità nella forma ex art. 380 comma 3 c.p.p.).

Orbene, come ampiamente anticipato *supra*, l'art. 8 d.l. n. 11/2009 contempla l'ammonimento del Questore per atti persecutori, configurandolo esplicitamente quale strumento *alternativo* alla proposizione della querela, all'insegna di un diritto di disponibilità della vittima, che può scegliere quale via percorrere.

Tanto premesso, pare di poter riassumere il ventaglio delle ipotesi che si offrono potenzialmente all'attenzione degli ufficiali o agenti di p.s./p.g.,

nel caso del reato di atti persecutori, nei seguenti termini alternativi:

A) se la vittima ha sporto querela (o ha esternato la propria volontà al riguardo nella forma prevista dall'art. 380 comma 3 c.p.p., in occasione di un intervento in flagranza, con conseguente arresto obbligatorio del responsabile), non c'è spazio per l'ammonimento questorile dell'autore della condotta[64]. Gli atti assunti, siccome esclusivamente di polizia giudiziaria, saranno trasmessi all'a.g. (oggi, peraltro, con accelerazione del rito, ex art. 347 c.p.p. come modificato dalla legge n. 69/2019, su cui più diffusamente *infra*);

B) qualora, invece, la vittima, astenendosi dalla proposizione di querela, rivolga la già sopra esaminata "richiesta di ammonimento" al Questore, si procederà amministrativamente in sede preventiva, attraverso i già spiegati meccanismi di istruzione del procedimento, postulanti, se del caso, la citata investigazione di pubblica sicurezza.

Come anticipato sopra, gli atti di questa investigazione preventiva sono essenzialmente di diritto amministrativo. Tuttavia, considerato che la querela per atti persecutori potrebbe sopravvenire in un momento successivo (e fino a sei mesi dal fatto), con la conseguente instaurazione di un procedimento penale successivo all'istruttoria amministrativa, occorre segnalare come, in questo contesto procedurale, si ritengano suscettibili di opportuna e massima valorizzazione due ordini di previsioni normative:

– la già sopra esaminata norma ex art. 220 disp. att. c.p.p. che impone, laddove "*emergono indizi di reato*", di ricorrere alle forme del codice di rito, per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale;

– il disposto dell'art. 346 c.p.p. secondo cui, in mancanza di una condizione di procedibilità che può ancora sopravvenire, possono (e piuttosto devono) essere compiuti gli atti di indagine preliminare necessari ad assicurare le fonti di prova (oltre che assumere le prove previste dall'articolo 392, se vi è pericolo nel ritardo), che la polizia giudiziaria trasmetterà all'Ufficio di Procura ai sensi dell'art. 112 disp. att. c.p.p. (su cui *infra*).

Ora è vero che l'oggetto dell'istruzione del procedimento amministrativo è formalmente diverso da quello dell'eventuale giudizio penale e che la prima istruzione è riservata agli *ufficiali di pubblica sicurezza* mentre l'indagine penale coinvolge la *polizia giudiziaria*, ma è altrettanto vero, nei fatti, che, per un verso, le predette qualifiche soggettive (ed i connessi obblighi) si rinven-

64) Almeno per la condotta per cui è già stata sporta querela. Circa l'ammissibilità di una richiesta di ammonimento per fatti nuovi e successivi, cfr. quanto precisato nel testo al capitolo 2.

gono contestualmente nelle stesse persone fisiche (il più delle volte appartenenti alle forze di polizia e segnatamente a quelle a competenza generale: Polizia di Stato e Arma dei Carabinieri), e, per altro verso, il presupposto applicativo dell'ammonimento per *stalking* è costituito dalla ricorrenza (sia pure indiziariamente ritenuta) di una condotta qualificabile alla stregua dell'art. 612-*bis* c.p.

La contiguità delle materie e la conseguente vischiosità delle valutazioni delle autorità di P.S e giudiziarie, al riguardo, postulano l'opportunità – anche per ragioni di economie procedurali, non dispersione delle prove e di esclusione di fenomeni di c.d. vittimizzazione secondaria – che l'assunzione degli atti istruttori nel procedimento amministrativo (che pure è connotato da una marcata celerità connessa alla funzione preventiva e cautelare di esso) tenga in massima considerazione la prospettiva dell'eventuale successivo procedimento penale e della conseguente applicazione delle forme del codice di rito nell'acquisizione degli atti conoscitivi.

Quanto al momento della trasmissione di siffatti atti all'autorità giudiziaria, l'art.112 disp. att. c.p.p. dispone che la polizia giudiziaria riferisca "*senza ritardo*" al pubblico ministero l'attività di indagine prevista dall'articolo 346 del Codice, salvi i casi di urgenza (connessi per esempio all'esecuzione di un sequestro) o quelli in cui il pubblico ministero faccia richiesta che la documentazione delle attività compiute gli sia trasmessa "*prontamente*".

Ne discendono, quindi, di regola, le seguenti possibili alternative:

– a fronte di una querela proposta, gli atti frattanto acquisiti ai sensi dell'art. 346 c.p.p. si trasmetteranno senz'altro all'a.g., di regola unitamente all'atto integrante la condizione di procedibilità stessa;

– se invece non venisse sporta la querela, gli atti di indagine assunti ex art. 346 c.p.p. sarebbero trasmissibili in ogni momento ed anche alla scadenza del termine massimo di proponibilità della querela (di sei mesi)[65].

Piuttosto, in tale secondo caso (in cui non fosse sopravvenuta la querela), potrebbe risultare opportuna una soluzione temporale che contempli la trasmissione all'autorità giudiziaria delle annotazioni e dei verbali eventualmente assunti ex art. 346 c.p.p., a conclusione del procedimento amministrativo que-

65) In tal senso, cfr. direttive del Procuratore della Repubblica di Bologna del 9 settembre 2016, che segnala la legittimità di questa prassi invalsa negli uffici ed addirittura consente, nel proprio distretto, la trasmissione degli atti assunti ex art. 346 c.p.p. con unica informativa riepilogativa inviata con cadenza annuale. Il Procuratore, invero, sottolinea come l'inciso temporale "*senza ritardo*", contenuto nell'art. 112 att. vada letto come concetto "*elastico*" che non impone alcun immediato inoltro alla Procura.

storile, che accoglie o rigetta la richiesta di ammonimento ex art. 8 d.l. n. 11/2009: con l'occasione, invero, l'a.g. riceverebbe gli atti (di polizia giudiziaria), così assunti, ma anche la segnalazione del provvedimento questorile emesso (o della reiezione dell'istanza di esso), nella prospettiva di alimentare – beninteso su un piano di reciproca autonomia tra autorità diverse – un circuito di virtuosa circolazione delle informazioni, utile ad amplificare le possibilità di tutela della vittima.

5.3. Il caso dell'ammonimento c.d. "per violenza domestica"

I rapporti tra procedimento penale e procedimento amministrativo finalizzato all'ammonimento per violenza domestica ex art. 3 d.l. n. 93/2013 sottendono maggiori profili di fluidità ed incertezza, connessi alla non alternatività del procedimento monitorio rispetto a quello giudiziario.

Invero, come anticipato, ai sensi dell'art. 3 citato, laddove un fatto "riconducibile" alle fattispecie penali ex art. 581 e 582 comma 2 c.p. fosse stato tentato o consumato in ambito di "violenza domestica", su segnalazione non anonima anche di terzi, il Questore può avviare procedimento per l'adozione dell'ammonimento dell'autore della condotta: ciò può avvenire a prescindere dalla proposizione o meno della querela da parte della persona offesa, di tal ché ben potrà ricorrere una contestuale pendenza del procedimento monitorio amministrativo e di quello penale[66].

I due strumenti sono quindi, non solo distinti, ma anche potenzialmente paralleli. In tale contesto, quindi, ben possono porsi problemi di non poco momento, soprattutto per gli operatori che rivestono attribuzioni e qualifiche di polizia giudiziaria e di pubblica sicurezza, riassumibili quantomeno nei seguenti termini schematici.

Gli obblighi dell'ufficiale o agente di p.s. verso l'a.g.

L'operatore che, conoscendo quale *ufficiale o agente di pubblica sicurezza* ed ai fini amministrativi-monitori una vicenda di violenza domestica, vi ravvisi una notizia di reato o elementi di prova al riguardo, deve porsi il problema di adempiere anche agli obblighi, connessi alle proprie attribuzioni di *polizia giudiziaria*, di riferirne all'autorità giudiziaria, con trasmissione degli atti assunti[67].

---

66) In tal senso, *ex plurimis*, Tar Trento, sentenza n. 33 del 7 - 18 febbraio 2019.

67) Come noto, peraltro, si tratta di obbligo presidiato da tutela penale ex art. 361 c.p. e disciplinare ex art. 16 disp. att. c.p.p.

Al riguardo, potranno verificarsi i seguenti casi:

– se non è stata sporta querela (o all'operatore di polizia non è noto che lo sia), all'autorità giudiziaria saranno trasmessi gli atti d'indagine eventualmente assunti, ai sensi dei già sopra esaminati artt. 346 c.p.p. e 112 disp. att. c.p.p.;

– se invece la querela risulti sporta, ovvero si tratti di fatti rilevanti in relazione a fattispecie procedibili d'ufficio, la notizia di reato e gli atti assunti andranno trasmessi all'autorità giudiziaria ai sensi degli artt. 347 e 357 c.p.p., fermo restando che il procedimento monitorio preventivo continuerà a seguire il suo corso innanzi all'autorità questorile.

Gli obblighi dell'ufficiale o agente di p.g. verso il Questore

Ancora più problematico pare, invece, risolvere il dubbio se un operatore di polizia, che conosca della vicenda per ragioni di *polizia giudiziaria* (per esempio: perché riceva denuncia o querela dei fatti o perché riceva una delega dell'a.g. al riguardo), abbia il potere-dovere, connesso alla qualifica di *ufficiale o agente di pubblica sicurezza*, di segnalazione della vicenda al Questore (sempreché in essa abbia ravvisato il presupposto ex art. 3 legge 2013 della commissione del fatto in ambito di "violenza domestica", nonché gli estremi indiziari di una pericolosità del soggetto).

Alla stregua dei principi ordinamentali rassegnati nelle pagine precedenti e dell'evidente volontà del legislatore di rafforzare, sempre più, un articolato statuto di protezione della vittima che affianchi alla tutela penale repressiva strumenti di anticipata difesa preventiva, su binari reciprocamente autonomi e di non pregiudizialità, pare doversi ritenere vigente un siffatto obbligo di segnalazione.

Pare opportuno ribadire come tale obbligo si ritenga, piuttosto che corollario del già sopra spiegato dovere informativo incombente ex art. 24 comma 3 legge n. 121/1981 sui comandanti locali dell'Arma dei Carabinieri e della Guardia di finanza, come più pregnante predicato di quella funzione di tutela dell'incolumità delle persone, coessenziale al ruolo istituzionale di tutti gli agenti ed ufficiali di p.s., siccome appartenenti all'Amministrazione della pubblica sicurezza ex art. 3 legge n. 121/1981.

In altri termini, il potere/dovere dell'autorità di p.s. (e quello strumentale o funzionale degli agenti ed ufficiali di pubblica sicurezza) di vagliare la situazione connessa alla pericolosità sociale dell'indagato (quale indiziato di condotte pericolose) attiene alla tutela della vittima rispetto ad un'esposizione a rischio che riguarda spesso la sua salute o comunque beni – essi pure – costituzionalmente tutelati ai livelli più alti[68].

68) È vero che l'autorità giudiziaria dispone della possibilità di misure cautelari: ma i presupposti sono diversi ed i tempi possono essere molto più lunghi.

Né può sottacersi il fatto che lo stesso operatore, che conosca della vicenda per ragioni di polizia giudiziaria, pare doversi ritenere titolare, nella sua contestuale veste di ufficiale o agente di pubblica sicurezza, di una specifica "posizione di garanzia" della vittima (o addirittura delle altre possibili vittime) in ordine ad ulteriori condotte lesive dei suoi beni attinenti alla persona[69].

Consentire quindi la parallela attivazione degli strumenti giudiziari e di quelli monitori amministrativi significa, non solo rispettare la volontà del legislatore (che nella legge del 2013 non ha riproposto per l'ammonimento per c.d. violenza domestica il principio di alternatività rispetto al procedimento penale che invece presiede all'istituto di cui all'art. 8 d.l. n. 11/2009), ma anche consentire l'effettiva esplicazione degli autonomi e distinti poteri dell'autorità di p.s. e dell'autorità giudiziaria e soprattutto la possibilità di assicurare quella pienezza ed efficacia dello statuto di tutela della vittima i cui addentellati assiologici e giuridici sono stati rassegnati nelle pagine precedenti.

Del resto, la valorizzazione della specifica disciplina normativa dell'am-

69) Pare utile ribadire, sul punto, che l'obbligo delle autorità dello Stato di intervenire tempestivamente (a fronte di un quadro significativamente sintomatico che fosse noto) per la protezione e prevenzione efficace contro le offese all'integrità della persona di minori e vittime vulnerabili (quali quelle delle violenze domestiche) è stato sancito dalla CEDU in consolidata giurisprudenza relativa alla portata dell'art. 2 della Convenzione europea dei diritti dell'uomo ("Il diritto alla vita di ogni persona è protetto dalla legge [...]"). In particolare cfr. la già citata Corte europea dei diritti dell'uomo – prima sezione – sentenza 2 marzo 2017 (ricorso n. 41237/14). Sul punto, ancora una volta, soccorre l'autorevole insegnamento di C. Mosca, *La Sicurezza - Valori, modelli e prassi istituzionali*, Editoriale scientifica, 2021, p. 109 ss.: "il diritto alla sicurezza deve essere pure considerato diritto sociale di libertà, soprattutto per le persone più fragili, per coloro, cioè, le cui condizioni economiche e sociali non consentono, laddove previsto dalla legge, agevoli forme di «autodifesa» e per le quali lo Stato, anche attraverso le Forze di polizia e la Magistratura, deve apprestare il necessario sostegno. È evidente, allora, che il successivo intervento giudiziario, in chiave repressiva, nei confronti di condotte che abbiano già leso l'intangibilità dei diritti individuali, non esaurisce il dovere dello Stato a garantire effettivamente la pari dignità tra le persone, ma soprattutto può arrecare una lesione più grave – perché individualmente non evitabile o sanabile – per gli appartenenti alle fasce più deboli. E il «diritto alla sicurezza» inteso nella sua pienezza che, specie quando anticipa preventivamente la tutela al momento in cui l'offesa ancora non si è consumata, consente dunque di sostanziare, oltre alla «giustizia intersoggettiva» (che regola, normalmente in modo diretto ed *ex post*, i conflitti tra i singoli consociati) e alla «giustizia sociale» (o della società), l'effettivo valore della coesistenzialità tra i singoli consociati, dando così effettività al principio di uguaglianza sostanziale. Un diritto tutt'altro che astratto e che, anche con riguardo alle responsabilità delle autorità tenute a garantirlo, è azionabile secondo quanto prevede l'articolo 24 della Costituzione".

monimento per violenza domestica, dettata dal d.l. n. 93/2013 pare consentire il rispetto dei delicati limiti che consentono la convivenza tra poteri dell'autorità di p.s. e dell'a.g., salvaguardandone la reciproca autonomia.

Ciò emerge segnatamente:

– nella concreta regolamentazione dell'avvio del procedimento amministrativo ex art. 3 d.l. n. 93/2013, per cui è sufficiente una "segnalazione" non anonima che provenga da chiunque e quindi anche dallo stesso ufficiale o agente di p.g.;

– nella possibilità di non rivelare il nome del segnalante e così il contesto "giudiziario" in cui il segnalante abbia appreso della vicenda, rilevante anche sul piano amministrativo;

– nella diversità dell'oggetto dei procedimenti e della relativa istruzione (che – in astratto – sottende la possibilità che il Questore acquisisca e valorizzi elementi istruttori non utili e/o non acquisiti nel procedimento penale);

– nella previsione ex art. 220 att. c.p.p. che prevede esplicitamente uno strumento di raccordo tra procedimento amministrativo e quello penale che, nello scongiurare la perdita di elementi di prova per il processo penale, legittima ulteriormente la ritenuta ritualità di paralleli canali procedurali.

Si ritiene quindi che l'ufficiale di p.s. che – sia pure per ragioni o in un contesto di polizia giudiziaria – conosca (direttamente o per esserne stato informato a sua volta dall'agente di p.s.) di un fatto che possa rilevare per l'incolumità di una persona, possa – *rectius*, in linea generale, debba – segnalarlo al Questore, onde porlo nella condizione di valutare l'eventuale parallela attivazione del procedimento preventivo monitorio di propria competenza.

Tale assunto tuttavia deve essere contemperato e bilanciato con la necessaria tutela del segreto investigativo ex art. 329 c.p.p. e la salvaguardia delle prerogative costituzionali in materia di autonomia della direzione magistratuale dell'indagine penale e diretta disponibilità della polizia giudiziaria ex art. 109 Cost., vieppiù dopo la celebre pronuncia della Corte costituzionale sentenza n. 229 del 7 novembre/6 dicembre 2018[70], di tal ché si impone un assetto trasparente e puntuale nei rapporti informativi verso (e tra) le autorità di pubblica sicurezza e giudiziaria, che tuttavia pare potersi declinare in termini parzialmente diversi a seconda delle situazioni suscettibili di essere isolate.

Più precisamente: se l'ufficiale di p.s. conosce di un fatto rilevante, ai

70) Come noto, relativa al conflitto di attribuzione tra poteri dello Stato sollevato in riferimento all'art. 18 comma 5 d.lgs. n. 177/2016 circa la previsione di trasmissione alla c.d. scala gerarchica di notizie sull'inoltro delle informative di reato all'a.g.

fini della possibile attivazione questorile di una tutela preventiva in favore della vittima, in un contesto in cui gli è chiaro che sia già iscritto un procedimento penale (è il caso tipicamente associato alla ricezione di una delega d'indagine), non pare possibile – e compatibile con i principi costituzionali – che la segnalazione di quel fatto all'autorità di pubblica sicurezza avvenga senza il preventivo nulla osta dell'autorità giudiziaria, titolare dell'indagine che si assume, per definizione, pendente.

Più sfumata pare, invece, la necessità di richiedere il preventivo nulla osta giudiziario, al fine di avviare un eventuale procedimento per ammonimento questorile (il riferimento è in particolare a quello per violenza domestica), laddove non esista alcun (noto) procedimento penale già iscritto, nel momento in cui l'ufficiale o agente di p.s./p.g. riceva notizia del fatto, contestualmente rilevante in termini di reato e di preventiva tutela della vittima:

– è il caso della ricezione, da parte di un ufficiale di p.g./p.s., di una denuncia–querela, relativa a casi di reati in contesti di violenza domestica, potenzialmente rientranti nella fattispecie tipizzata dall'art. 3 d.l. n. 93/2013. La denuncia-querela, come tale, va certamente trasmessa alla sola autorità giudiziaria competente, ai sensi dell'art. 347 c.p.p., ma non pare peregrino sostenere che (pur dandone esplicita ed immediata contezza all'a.g., onde consentirle le iniziative ritenute opportune) l'ufficiale di p.g./p.s. possa (ed anzi debba) anche darne una segnalazione, seppur essenziale o eventualmente riassuntiva dei soli estremi di rilievo ai fini di sicurezza pubblica, al Questore, onde consentirgli l'esercizio delle prerogative assegnategli dalla legge sul distinto piano del diritto di prevenzione;

– ma è anche il caso in cui sia l'agente o ufficiale di p.s./p.g. che intervenga direttamente (come avviene tipicamente durante gli ordinari servizi continuativi di pronto intervento)[71] in un contesto domestico in cui si ravvisino fatti potenzialmente rilevanti in termini penali e di prevenzione amministrati-

71) A tale compito, nell'organizzazione della Questura, è preposto il personale dell'Ufficio prevenzione generale e soccorso pubblico (in cui sono inquadrati gli equipaggi automontati in servizio di volante) che, con tutte le altre componenti ed i reparti specialistici impegnati nel controllo del territorio, sono coordinati a livello nazionale dal Servizio controllo del territorio istituito nell'ambito della Direzione centrale anticrimine della Polizia di Stato. Si tratta, emblematicamente di attività di *pubblica sicurezza* ma con una forte contiguità con le attività di *polizia giudiziaria*, atteso che il personale di p.s./p.g. che opera in tale settore interviene estemporaneamente in contesti in cui si soccorrono le vittime ma si acquisiscono notizie di reato da trasmettere all'a.g. Non, è un caso, peraltro che proprio in seno agli UPGSP siano istituiti gli Uffici denunce.

va. In tal caso, le annotazioni ed i verbali di polizia giudiziaria andranno trasmessi senz'altro all'ufficio di Procura, con la comunicazione di notizia di reato del caso. Ma la relazione di fine servizio redatta dal personale operante (come agenti di p.s.), con contenuto riassuntivo dei fatti rilevati nel servizio (che era pur sempre di soccorso e sicurezza pubblica), si ritiene debba essere contestualmente – e quindi senza necessità di previo nulla osta giudiziario[72] – portata a conoscenza, per il tramite dell'ufficiale di p.s. sovraordinato agli operatori, dell'autorità questorile, per le iniziative preventive di competenza[73].

6. Le novità introdotte dalla legge n. 69/2019

6.1. La legge istitutiva del c.d. *Codice rosso*

La testé rassegnata previsione di diversi ed intrecciati istituti di tutela della vittima e correlativi poteri-doveri degli ufficiali ed agenti di pubblica si-

72) Quel "nulla osta" giudiziario sarà invece necessario laddove il Questore, o l'ufficiale di p.s. delegato all'istruttoria nel procedimento monitorio, volesse acquisire, in quella sede amministrativa, il verbale in sé o l'atto di p.g. assunto dalla p.g. (per esempio, una copia della querela o degli atti con cui è stata data esecuzione alla delega giudiziaria: verbali di sommarie informazioni, annotazioni di p.g., ecc.).

73) In tal senso, e nella consapevolezza delle potenzialità sottese al duplice canale di tutela tracciato nel testo, si segnala che la Direzione centrale anticrimine della Polizia di Stato, nella recente circolare del 25 febbraio 2021, di aggiornamento della precedente N.225/UAG/2019 - 66981 U del 6 settembre 2019 in materia di "Violenza di genere", nel richiamare le nuove prassi operative conseguenti all'istituzione dell'innovativo applicativo interforze denominato SCUDO (accessibile a tutti gli operatori di polizia individuati, onde agevolarne la fase di primo intervento d'urgenza anche in caso di violenza domestica, consentendo l'acquisizione estemporanea di informazioni su indirizzo o anagrafica, e la conseguente individuazione di informazioni relative a pregresse attività), ha invitato i Questori a sensibilizzare i dirigenti degli UPGSP e dei Commissariati ad un prudente, preventivo apprezzamento della relazione di servizio e/o annotazione, compilata dagli equipaggi impiegati nel controllo del territorio al termine dell'intervento per le cd. "liti" in ambito familiare, curando che tutti gli atti citati (relazioni/annotazioni), attraverso l'Ufficio di gabinetto, confluiscano giornalmente all'attenzione dei dirigenti delle Divisioni anticrimine e Squadre mobili. Qualora, nel medesimo contesto/ambito familiare, si ripeta un intervento da parte di una pattuglia, per situazioni che potrebbero risultare comunque "indicatrici" di violenza domestica, i dirigenti degli UPGSP e dei Commissariati dovranno tempestivamente interessare la Divisione/Ufficio anticrimine, allo scopo di anticipare l'irrogazione di misure di prevenzione da parte del Questore, nonché la Squadra mobile, qualora la dinamica dei fatti richieda l'intervento della polizia giudiziaria specializzata.

curezza - polizia giudiziaria, a fronte di altrettanto variegate fattispecie delittuose richiamate quali presupposti di legittimazione dell'uno o dell'altro dei predetti strumenti (fattispecie fissate spesso con una tecnica di redazione normativa non esemplare e comunque in modo disallineato) pone all'interprete, e soprattutto all'operatore, oggettive difficoltà di orientamento.

Siffatti problemi applicativi si sono ulteriormente acuiti all'indomani dell'emanazione della legge n. 69/2019, recante "*Modifiche al Codice penale, al Codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere*" e ribattezzata presto, dagli stessi esponenti politici, quale legge istitutiva del c.d. *Codice rosso*.

La legge, nei suoi 21 articoli, prevede disposizioni attinenti il diritto penale sostanziale ed il diritto processuale penale (oltre ad altre norme in materia di misure di prevenzione, formazione del personale di polizia, indennizzo e sostegno alle vittime del reato, centri antiviolenza)[74].

Le norme di diritto penale sostanziale

Sotto il primo profilo, pare opportuno ricordare che l'art. 4 della l. n. 69/2019 introduce nel Codice penale l'art. 387-*bis*, rubricato "*Violazione dei provvedimenti di allontanamento dalla casa familiare e del divieto di avvicinamento ai luoghi frequentati dalla persona offesa*", che punisce con la reclusione da sei mesi a tre anni chiunque, essendovi legalmente sottoposto, violi gli obblighi o i divieti derivanti dal provvedimento che applica le misure cau-

74) Pare necessario sottolineare che l'art. 5 della legge 69/2019 preveda obblighi formativi per il personale delle forze di polizia onde affinare l'esercizio delle funzioni che competono loro nella duplice direzione delle "funzioni di pubblica sicurezza" e di "polizia giudiziaria", in un consapevole e deliberato quadro ordinamentale in cui il legislatore mostra inequivocabilmente di volere contrastare il fenomeno criminale di cui si tratta attraverso il duplice binario, tratteggiato nel testo, dell'attività amministrativa di "prevenzione" e di quella giudiziaria del "perseguimento dei reati": [Art. 5] "*Entro dodici mesi dalla data di entrata in vigore della presente legge, la Polizia di Stato, l'Arma dei carabinieri e il Corpo di Polizia penitenziaria attivano presso i rispettivi istituti di formazione specifici corsi destinati al personale che esercita funzioni di pubblica sicurezza e di polizia giudiziaria in relazione alla prevenzione e al perseguimento dei reati di cui agli articoli 1, 2 e 3 o che interviene nel trattamento penitenziario delle persone per essi condannate. La frequenza dei corsi è obbligatoria per il personale individuato dall'amministrazione di appartenenza. 2. Al fine di assicurare l'omogeneità dei corsi di cui al comma 1, i relativi contenuti sono definiti con decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri per la pubblica amministrazione, dell'interno, della giustizia e della difesa*".

telari di cui agli artt. 282-*bis* e 282-*ter* del Codice di procedura penale o dell'ordine di cui all'art. 384-*bis* del medesimo codice[75].

L'art. 7 della l. n. 69/2019 introduce nel Codice penale l'art. 558-*bis*, rubricato "*Costrizione o induzione al matrimonio*": la norma punisce con la reclusione da uno a cinque anni chiunque, con violenza o minaccia, costringe una persona a contrarre matrimonio o unione civile, ovvero chiunque, approfittando delle condizioni di vulnerabilità o di inferiorità psichica o di necessità di una persona, con abuso delle relazioni familiari, domestiche, lavorative o dell'autorità derivante dall'affidamento della persona per ragioni di cura, istruzione o educazione, vigilanza o custodia, la induce a contrarre matrimonio o unione civile.

L'art. 12, comma 1, della l. n. 69/2019 introduce nel Codice penale l'art. 583-*quinquies*, rubricato "*Deformazione dell'aspetto della persona mediante lesioni permanenti del viso*": viene punito, con la reclusione da otto a quattordici anni, chiunque cagioni ad alcuno lesione personale dalla quale derivino la deformazione o lo sfregio permanente del viso. Tale fattispecie rientrava, in precedenza, nella previsione dell'art. 583, comma 2, c.p., il quale puniva con la reclusione da sei a dodici anni le lesioni gravissime, fra le quali era contemplata, al n. 4, la deformazione, ovvero lo sfregio permanente del viso: disposizione ora abrogata dal comma 3 del citato art. 12, l. n. 69/2019.

L'art. 10 della l. n. 69/2019 ha introdotto nel Codice penale l'art. 612-*ter*, rubricato "*Diffusione illecita di immagini o video sessualmente espliciti*": si tratta del c.d. "*Revenge porn*", sotteso alla condotta di soggetti che diffon-

75) Prima dell'introduzione di tale sanzione penale, la violazione degli obblighi stabiliti dalle misure cautelari ex artt. 282-*bis* e 282-*ter* c.p.p. avrebbe comportato solamente la sostituzione con una misura cautelare più severa, mentre nessuna conseguenza avrebbe comportato la violazione dell'ordine ex art. 384-*bis* c.p.p. Il che, peraltro, si poneva in contrasto con quanto stabilito dalla convenzione del Consiglio d'Europa del 2011 sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica (c.d. Convenzione di Istanbul), la quale stabilisce all'art. 53 che la violazione delle ordinanze di ingiunzione o di protezione sia "oggetto di sanzioni penali o di altre sanzioni legali efficaci, proporzionate e dissuasive": l'introduzione dell'art. 387-*bis* c.p. viene dunque a colmare una lacuna legislativa e ad ottemperare ad un obbligo sovranazionale. In tal senso F. PITTARO, *Il c.d. Codice Rosso sulla tutela delle vittime di violenza domestica e di genere*, in *Famiglia e diritto*, 2020, 7, 735 (commento alla normativa). Si soggiunge, al riguardo, che forse sarebbe stata questa l'occasione per colmare legislativamente anche la lacuna, segnalata sopra, nel testo, che si ritiene di ravvisare nella disciplina delle conseguenze (apparentemente troppo lievi) dell'inosservanza dell'ammonimento questorile, segnatamente di quello cd. per violenza domestica, ex art. 3 d.l. n. 93/82013.

dono immagini sessualmente rilevanti di una persona, come ritorsione o vendetta nei suoi confronti.

Sempre sul piano del diritto sostanziale, la l. n. 69/2019 ha peraltro operato un inasprimento del trattamento sanzionatorio già previsto per le fattispecie criminali tipicamente connesse a contesti di violenza domestica e di genere: *gli atti persecutori* (la pena per i quali è stata elevata prevedendo la reclusione da un anno a sei anni e sei mesi); i *maltrattamenti contro famigliari e conviventi* ex art. 572 c.p. (la cui pena base ex comma 1 passa dalla reclusione da due a sei anni alla reclusione da tre a sette anni, oltre a prevedere aggravamenti per talune situazioni tra cui quella di violenza assistita); il *delitto di violenza sessuale* di cui all'art. 609-*bis* c.p. (la cui pena viene elevata con la previsione della reclusione da sei a dodici anni, oltrea rimodulare le circostanze aggravanti di cui al successivo art. 609-*ter*); il *delitto di atti sessuali con minorenne* ex art. 609-*quater* c.p. (prevedendo l'aggravamento della pena se il delitto di atti sessuali con minorenne infraquattordicenne, compiuto senza violenza, con il soggetto immaturo, ma consensuale, avviene in cambio di denaro o di qualsiasi altra utilità, anche solo promessi, fermo restando che se il tutto avviene con il minore di età compresa fra i quattordici ed i diciotto anni si ricade nel delitto di "prostituzione minorile", di cui all'art. 600-*bis*, comma 2, c.p., il quale prevede la pena della reclusione da uno a sei anni e la multa da 1.500 a 6.000 euro); il *delitto di violenza sessuale di gruppo* ex art. 609-*octies* c.p. (la cui pena viene elevata dalla reclusione da sei a dodici anni alla reclusione da otto a quattordici anni).

Le norme procedurali

Tra le novità introdotte dalla legge n. 69/2019, tuttavia, in questa sede rilevano soprattutto le modifiche apportate alle norme del codice di rito, ed in particolare agli artt. 347 e 362 c.p.p., onde tracciare, nel procedimento penale, una sorta di corsia preferenziale per le notizie di reato in materia di violenza di genere (appunto il c.d. *Codice rosso*), con lo scopo di assicurare che l'autorità giudiziaria sia posta in condizione, in tempi strettissimi, di conoscere le stesse ed altrettanto velocemente approfondire gli estremi di fondatezza e gravità della vicenda, nell'evidente prospettiva di adottare tempestivi provvedimenti al riguardo, segnatamente di natura cautelare[76].

76) La relazione tecnica che accompagnava il disegno di legge approvato come legge n. 69/2019 dava conto esplicitamente dell'obiettivo di perfezionare la tutela delle vittime di violenza domestica e di genere, in attuazione della direttiva 2012/29/UE, "mediante il potenziamento degli strumenti propri delle indagini e dell'azione giudiziaria, favorendo l'im-

Agli ufficiali ed agenti di polizia giudiziaria sono stati così imposti nuovi obblighi, funzionali al perseguimento dei predetti obiettivi, che postulano ulteriori problemi di compatibilità con il delicato assetto dei rapporti tra attribuzioni connessi alle qualifiche di polizia giudiziaria e di pubblica sicurezza sopra tracciati, vieppiù in un quadro normativo in cui la novella del 2019 si segnala per alcune asimmetrie rispetto agli interventi precedenti, con il connesso, ulteriore problema interpretativo di tracciare esattamente il campo di applicazione delle novità rispetto alla disciplina previgente.

Per intendere appieno la portata delle novità introdotte dalla legge n. 69/2019 (limitatamente ai temi che ci occupano in questa sede) pare opportuno soffermarsi sul contenuto e l'ambito applicativo di tale novella.

6.2. La modifica dell'art. 347 c.p.p. ed il relativo ambito di applicazione

Come noto, l'art. 347 c.p.p. prevede che la polizia giudiziaria debba[77] trasmettere all'ufficio di Procura la notizia di reato acquisita "*senza ritardo*"[78], laddove la locuzione temporale va intesa con elasticità, nel senso di escludere – per un verso – inerzie ingiustificate, anche alla stregua dei carichi di lavoro

---

mediata instaurazione e progressione del procedimento penale e prevedendo, ove necessario, l'adozione, senza ritardi, di eventuali provvedimenti cautelari e preventivi, attraverso un deciso intervento sui tempi e sulle modalità di svolgimento delle diverse fasi del procedimento penale". Sul punto, cfr. anche G. Aliquó, *La violenza domestica. L'ammonimento del Questore*", cit., p. 355, secondo cui "la legge vuole anticipare il più possibile il contatto tra vittima e autorità giudiziaria, con una sorta di presunzione legale d'urgenza che, per evitare qualsiasi forma di stasi o ritardo nel procedimento, assicuri una corsia preferenziale alle notizie di reato ed ai procedimenti per violenza di genere e violenza domestica".

77) Come anticipato sopra, gli obblighi della polizia giudiziaria di comunicazione della notizia di reato alla Procura sono presidiati da responsabilità penale ex art. 361 cpv. c.p. e disciplinare ex art. 16 disp. att. c.p.p.

78) La polizia giudiziaria riferisce "*per iscritto, gli elementi essenziali del fatto e gli altri elementi sino ad allora raccolti, indicando le fonti di prova e le attività compiute, delle quali trasmette la relativa documentazione. 2. Comunica, inoltre, quando è possibile, le generalità, il domicilio e quanto altro valga alla identificazione della persona nei cui confronti vengono svolte le indagini, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti*" (art. 347 c.p.p.). L'art. 357 c.p.p. comma 4-5 prevede che "*la documentazione dell'attività di polizia giudiziaria è posta a disposizione del pubblico ministero. 5. A disposizione del pubblico ministero sono altresì poste le denunce, le istanze e le querele presentate per iscritto, i referti, il corpo del reato e le cose pertinenti al reato*". Pare opportuno ricordare, tuttavia, che l'art. 107-*bis* disp. att., introdotto dall' art. 50, l. 16.12.1999, n. 479, prevede che «*le denunce a carico di*

dell'ufficio pubblico di cui si tratta, ma – per altro verso – assicurare la compatibilità dei termini di trasmissione con una previa, doverosa attività di verifica, controllo, implementazione della notizia cui la polizia giudiziaria medesima deve ritenersi tenuta ex art. 55 c.p.p. (anche) prima di riferirne compiutamente al p.m. (in tal senso, *ex plurimis*, Cassazione, sez. VI, 19.3.2007, n. 18457, O.V., in CED Cassazione, 2007, 236501).

Che la locuzione predetta vada ordinariamente intesa in termini relativamente elastici, si desume peraltro già dalla previsione del comma 2-*bis* dello stesso art. 347 che contempla l'obbligo della trasmissione "*entro quarantotto ore"* nei soli casi in cui "*siano stati compiuti atti per i quali è prevista l'assistenza del difensore della persona nei cui confronti vengono svolte le indagini*"[79], così confermando che, negli altri casi, il termine può ben essere superiore.

Ma lo stesso art. 347 c.p.p. comma 3 – con tutt'altro tenore letterale – prevede taluni casi in cui la trasmissione della *notitia criminis* all'autorità giudiziaria debba avvenire addirittura prima delle quarantotto ore e cioè "*immediatamente*", anche in forma orale, seguita da quella scritta: si tratta dei casi in cui "*sussistono ragioni di urgenza*", nonché di quelli in cui si proceda per un reato rientrante in un elenco tracciato dalla stessa norma codicistica, con evidente attenzione a fattispecie criminali ritenute postulanti l'immediata assunzione della direzione delle indagini in capo al magistrato della Procura: la norma, in particolare, prima del 2019, richiamava i delitti previsti nell'ar-

---

ignoti sono trasmesse all'ufficio di procura competente da parte degli organi di polizia, unitamente agli eventuali atti di indagine svolti per la identificazione degli autori del reato, con elenchi mensili»: ciò beninteso con l'eccezione dei casi di cui all'art. 347 comma 3 c.p.p. (su cui *infra* nel testo). Infine, si ricorda altresì che, nel caso di reati procedibili a querela, per la polizia giudiziaria l'obbligo di informativa all'autorità giudiziaria trova una disciplina particolare nel combinato disposto degli artt. 346 e 112 disp. att. Infatti, in mancanza di querela, quando questa può essere ancora presentata, la polizia giudiziaria può (anzi, deve) compiere gli atti di indagine necessari ad assicurare le fonti di prova (ad esempio, in caso di incidente stradale con feriti, la polizia stradale intervenuta in loco deve procedere ad eseguire i rilievi dell'incidente stradale ed a sentire le persone informate che hanno assistito all'incidente), riferendone senza ritardo all'autorità giudiziaria (valgono, a ben vedere, le regole generali di cui si è detto supra); a quest'ultima, però, rimetterà la relativa documentazione (solo) se e quando la querela venga successivamente presentatae, comunque, quando il p.m. ne abbia fatto formale richiesta.

79) Si tratta dei c.d. "atti garantiti": per esempio, l'assunzione di sommarie informazioni dall'indagato (art. 350 c.p.p.), la perquisizione (352) ed il sequestro (354), rispetto a cui il p.m. è tenuto al deposito dei verbali in segreteria ex art. 366 c.p.p. oltreché (per gli ultimi due) alla convalida ex art. 352 comma 4 e 355 c.p.p.

ticolo 407, comma 2, lettera a), numeri da 1) a 6), del medesimo Codice di rito.

In tali casi, la polizia giudiziaria è tenuta a rispettare il più rigoroso e netto termine temporale, fermo restando impregiudicato il potere-dovere di attivarsi per riscontrare la notizia di reato, identificare il possibile autore ed assicurare le relative fonti di prova[80].

Orbene, l'art. 1 della legge n. 69/2019 ha esteso tale ultima accelerazione del rito – con conseguente previsione dell'obbligo della polizia giudiziaria di riferire immediatamente all'ufficio di Procura la notizia di reato e gli atti assunti – anche ai casi in cui si proceda per i delitti previsti dagli articoli 572, 609-*bis*, 609-*ter*, 609-*quater*, 609-*quinquies*, 609-*octies*, 612-*bis* e 612-*ter* del Codice penale, ovvero dagli articoli 582 e 583-*quinquies* del Codice penale nelle *ipotesi aggravate ai sensi degli articoli 576, primo comma, numeri 2, 5 e 5.1, e 577, primo comma, numero 1, e secondo comma*, del medesimo Codice penale[81].

La novella che ha riguardato l'art. 347 c.p.p. è peraltro evidentemente collegata alla parallela riforma dell'art. 362 c.p.p., al quale l'art. 2 della legge n. 69/2019 ha aggiunto un comma 1-*ter*, a norma del quale «*quando si procede per i delitti previsti dagli articoli 572, 609-bis, 609-ter, 609-quater, 609-quinquies, 609-octies e 612-bis del Codice penale, ovvero dagli articoli 582 e 583-quinquies del Codice penale nelle ipotesi aggravate ai sensi degli articoli 576, primo comma, numeri 2, 5 e 5.1, e 577, primo comma, numero 1, e secondo comma, del medesimo codice, il pubblico ministero assume informazioni dalla persona offesa e da chi ha presentato denuncia, querela o istanza, entro il ter-*

---

80) L'art. 347 comma 3 introduce una deroga al solo regime temporale della trasmissione della notizia di reato, non anche allo spazio ed ai limiti della competenza della polizia giudiziaria anche in termini di attività di iniziativa ad essa demandata dal codice. Purtuttavia, è evidente che – vieppiù in casi, come quelli di cui alla legge n. 69/2019, di marcata delicatezza o sottendenti possibili rischi di esposizione delle vittime o dei minori a conseguenze deleterie in conseguenze di reiterazione di atti procedimentali – sarà opportuno che la polizia giudiziaria si raccordi (anche oralmente) sin dai primi momenti con l'autorità giudiziaria: in tal senso, cfr. direttive della Procura di Mantova prot. 1068 del 31 luglio 2019.

81) Art. 1. "Obbligo di riferire la notizia del reato 1". *All'articolo 347, comma 3, del codice di procedura penale, dopo le parole: «nell'articolo 407, comma 2, lettera a), numeri da 1) a 6)» sono inserite le seguenti: «, del presente codice, o di uno dei delitti previsti dagli articoli 572, 609-bis, 609-ter, 609-quater, 609-quinquies, 609-octies, 612-bis e 612-ter del codice penale, ovvero dagli articoli 582 e 583-quinquies del codice penale nelle ipotesi aggravate ai sensi degli articoli 576, primo comma, numeri 2, 5 e 5.1, e 577, primo comma, numero 1, e secondo comma, del medesimo codice penale»*.

mine di tre giorni dall'iscrizione della notizia di reato, salvo che sussistano imprescindibili esigenze di tutela di minori di anni diciotto o della riservatezza delle indagini, anche nell'interesse della persona offesa».

Ed ancora, l'art. 3 della legge n. 69/2019 ha interpolato due commi nell'art. 370 c.p.p., relativo agli atti di polizia giudiziaria delegati, che ora prevede che, nei procedimenti relativi allo stesso ambito di delitti sopra elencati dall'art. 347 comma 3, "*la polizia giudiziaria procede senza ritardo al compimento degli atti delegati dal pubblico ministero*" e sempre "senza *ritardo*" pone a disposizione del pubblico ministero la documentazione dell'attività espletata ex art. 357[82].

Orbene, nell'elenco dei reati appena tracciato (dedotto rispettivamente negli artt. 347 comma 3, 362 comma 1-*ter* e 370 commi 2-*bis* e 2-*ter* c.p.p.), per i quali il legislatore del 2019 ha introdotto il rassegnato *codice rosso*, figurano evidentemente due dei reati per i quali – per quanto esposto nei capitoli precedenti – si può porre un problema di sovrapposizione tra procedimento monitorio del Questore e procedimento penale dinnanzi all'autorità giudiziaria: invero, gran parte delle fattispecie delittuose dedotte nel suddetto elenco di reati di cui agli artt. 347/362/370 c.p.p. come sensibili sotto il profilo del contrasto alla violenza di genere, non figurano tra i presupposti di avvio di paralleli o alternativi procedimenti monitori; per altro verso il delitto di "percosse" ex art. 581 c.p. che, laddove commesso in un contesto di violenza domestica, comporta la possibilità di avviare un procedimento finalizzato all'adozione dell'ammonimento questorile ex art. 3 d.l. n. 93/2013, non è stato

82) Art. 3. "Atti diretti e atti delegati": *1. Dopo il comma 2 dell' articolo 370 del codice di procedura penale sono inseriti i seguenti:«2-bis. Se si tratta di uno dei delitti previsti dagli articoli 572, 609-bis, 609-ter, 609-quater, 609-quinquies, 609-octies, 612-bis e 612-ter del codice penale, ovvero dagli articoli 582 e 583-quinquies del codice penale nelle ipotesi aggravate ai sensi degli articoli 576, primo comma, numeri 2, 5, 5.1, e 577, primo comma, numero 1, e secondo comma, del medesimo codice, la polizia giudiziaria procede senza ritardo al compimento degli atti delegati dal pubblico ministero. 2-ter. Nei casi di cui al comma 2-bis, la polizia giudiziaria pone senza ritardo a disposizione del pubblico ministero la documentazione dell'attività nelle forme e con le modalità previste dall'articolo 357»*. Al riguardo, G. Aliquò, *La violenza domestica. L'ammonimento del Questore*, cit., p. 357, segnala l'asimmetria per cui l'art. 362 comma 1-*ter* c.p.p. non ricomprenda nel proprio ambito applicativo la fattispecie delittuosa di cui all'art. 612-*ter* c.p. che invece è richiamata sia dall'art. 347 comma 3 che dall'art. 370 commi 2-*bis* e 2-*ter* c.p.p. (di tal ché, per il reato di diffusione illecita di video o immagini sessualmente espliciti, il legislatore sembra avere ritenuto sufficiente l'accelerazione impressa alla sola fase di trasmissione della notizia di reato dalla polizia giudiziaria alla a.g.).

ricompreso tra quelle fattispecie per cui si ritiene necessario che l'ufficio di Procura sia notiziato immediatamente dalla polizia giudiziaria.

In definitiva, quindi, il problema delle conseguenze (soprattutto in punto di doveri degli operatori di polizia in senso ampio) recate dalle novità introdotte dalla legge n. 69/2019, sul sistema dei rapporti tra procedimento penale e procedimento monitorio questorile, pare doversi restringere al solo ambito di ricorrenza di due delitti contro la persona:

– delitto art. 612-*bis* c.p., la condotta del cui autore può essere oggetto di (alternativo) procedimento preventivo finalizzato all'adozione dell'ammonimento del Questore ex art. 8 legge 2009;

– delitto ex art. 582 c.p. aggravato ex art. 576 comma 1 n. 2/5/5.1 nonché 577 comma 1 numero 1 e comma 2: la condotta del cui autore – limitatamente alle ipotesi di cui all'art. 582 comma 2 e sempreché il reato sia stato commesso in un contesto di "violenza domestica" – può essere oggetto del (parallelo) procedimento preventivo finalizzato all'adozione dell'ammonimento del Questore ex art. 3 d.l. n. 93/2013.

Pare opportuno esaminare partitamente le ipotesi di cui sopra.

6.3. Il caso dello stalking

Nonostante il contesto criminale in cui si inscrive potenzialmente la fattispecie ex art. 612-*bis* c.p. sia molto più ampio – di per sé – rispetto alla sfera della violenza domestica e dei rapporti tra soggetti (già) legati da relazioni affettive, in senso ampio, la legge n. 69/2019 ha previsto anche tale fattispecie tra quelle rientranti nel novero dei reati per i quali il novellato art. 347 c.p.p. comma 3 prevede ora l'obbligo della polizia giudiziaria di riferire "*immediatamente*" la *notitia criminis* all'autorità giudiziaria, nel senso sopra precisato[83].

Per altro verso, come ormai noto, gli atti persecutori costituiscono anche il presupposto applicativo dell'istituto monitorio previsto dall'art. 8 d.l.n. 11/2009.

Tuttavia, attesa la già spiegata alternatività tra i due strumenti appena ricordati (quello giudiziario e quello preventivo questorile), le novità introdotte

83) Il reato è tipicamente associato a contesti di relazioni affettive traumaticamente o non consensualmente concluse, ma ciò non è vero necessariamente: esiste, ad esempio, ampia casistica giurisprudenziale e letteratura dottrinaria per i casi di stalking in ambito professionale (cfr. al riguardo M. De Paolis, *Il fenomeno dello stalking occupazionale*, in *Azienditalia* - Il Personale, 2014, 3, 145) o condominiale.

dalla legge n. 69/2019 non sembrano sollevare differenziali dubbi interpretativi o incertezze applicative.

Ancora una volta, invero, se la vittima ha sporto querela (o ha esternato la propria volontà al riguardo nella forma prevista dall'art. 380 comma 3 c.p.p., in occasione di un intervento in flagranza, con conseguente arresto obbligatorio del responsabile), non si potrà procedere all'ammonimento questorile dell'autore della condotta.

La querela e gli atti assunti, siccome esclusivamente di polizia giudiziaria, saranno trasmessi all'autorità giudiziaria *immediatamente*, ex art. 347 comma 3 c.p.p. come modificato dalla legge n. 69/2019, onde consentire al magistrato di procedere all'escussione ex art. 362 c.p.p. (o più spesso a delegarne l'esecuzione alla polizia giudiziaria) nel ristretto termine dei tre giorni dall'iscrizione della notizia di reato: ciò, evidentemente, nella prospettiva dell'eventuale adozione di una misura cautelare oltre che del tempestivo esercizio dell'azione penale.

Se invece non vi fosse querela, si procederà ad ammonimento questorile (sempreché sia stato richiesto).

In tale ultima evenienza, gli eventuali atti d'indagine acquisiti ex art. 346 c.p.p. – anche in occasione dell'investigazione di pubblica sicurezza – prima che trascorra il termine entro cui la querela potrebbe sempre essere proposta, andranno trasmessi alla autorità giudiziaria ai sensi dell' art. 112 disp. att. c.p.p.

Al riguardo, occorre sottolineare che l'art. 346 c.p.p. prevede che se "*si tratta di taluno dei delitti indicati nell'articolo 407, comma 2, lettera a), numeri da 1) a 6), la comunicazione è data immediatamente anche in forma orale*". Tuttavia, la legge n. 69/2019 ha novellato l'art. 347 c.p.p. ma non anche l'art. 346 c.p.p. (né la parte dell'art. 407 richiamata dall'art. 346), di tal ché ne discende che agli atti d'indagine compiuti in difetto di una querela per *stalking* – che possa ancora essere proposta – non si applicherà l'accelerazione del rito imposto per la trasmissione degli atti di polizia giudiziaria quando sussiste la condizione di procedibilità.

6.4. Il caso delle lesioni personali

Alla stregua della novella recata dalla legge n. 69/2019, il "codice rosso" (per come risultante dal nuovo contenuto delle previsioni degli artt. 347, 362 e 370 c.p.p.) si applica a tutti i casi in cui ricorra una notizia di reato per il delitto di *lesioni personali* ex art. 582 c.p., sempreché sussista uno dei casi di

aggravamento sanzionatorio tipizzato nelle seguenti norme, esplicitamente evocate dalla legge stessa:

A. Art. 576 comma 1 n. 2;
B. Art. 576 comma 1 n. 5;
C. Art. 576 comma 1 n. 5.1;
D. Art. 577 comma 1 n. 1;
E. Art. 577 comma 2.

Per contro, occorre ricordare che l'art. 3 d.l. n. 93/2013 preveda il possibile ricorso all'ammonimento questorile (quello per c.d. violenza domestica) per i soli casi di lesioni personali, perseguibili a querela, di cui all'art. 582 comma 2 c.p. Tale comma, a sua volta, presuppone la duplice circostanza per cui:

– la malattia che deriva dalla lesione abbia "*una durata non superiore ai venti giorni*";

– *non* concorra alcuna delle circostanze aggravanti previste (oltre che negli artt. 61, numero 11-*octies* e 583) dall'art. 585 c.p.; norma, quest'ultima, che – tra le altre – richiama le "*circostanze aggravanti previste dall'art. 576*" del Codice penale.

Ne discende, pertanto, che i casi di lesioni aggravate dalle circostanze ex art. 576 c.p. (sopra distinte sub lettere A, B e C) esulino pacificamente dall'ambito applicativo dell'art. 582 comma 2 c.p. e, per ciò stesso, da quello dell'art. 3 d.l. n. 93/2013, in materia di ammonimento questorile per violenza domestica.

Quanto invece ai casi di lesioni aggravate sopra distinte sub lettere D) ed E), occorre rilevare che, se le aggravanti di cui all'art. 577 c.p. sono – esse pure – richiamate dall'art. 585 c.p., l'art. 582 comma 2 c.p. sembra ricomprenderle nella propria fattispecie (e conseguentemente nell'ambito applicativo dell'art. 3 d.l. n. 93/2013), laddove ricorre alla clausola di esclusione "*ad eccezione di quelle indicate nel n. 1 e nell'ultima parte dell'art. 577*"[84].

Per quanto sin qui premesso, dei sopra rassegnati casi di lesioni aggravate cui è ora esteso il c.d. *codice rosso*, è evidente che solo gli ultimi due (rispettivamente contrassegnati sub D ed E) postulino la possibilità di ricorrere – contestualmente al procedimento penale e sempreché vi siano i presupposti dell'art. 3 d.l. n. 93/2013 (segnatamente in punto di contestualizzazione in un ambito di *violenza domestica*) – all'ammonimento questorile. Ciò, beninteso,

84) La locuzione "*nell'ultima parte dell'art. 577*", contenuta nell'art. 582 cpv. c.p., sembra invero potersi intendere riferita alla previsione del comma 2 dello stesso articolo.

a condizione che si tratti di lesioni procedibili a querela, ex art. 582 comma 2 (solo questa fattispecie essendo, infatti, richiamata dall'art. 3 del decreto-legge citato).

Riassumendo, il problema di possibili sovrapposizioni tra procedimento questorile monitorio ex art. 3 d.l. n. 93/2013 e procedimento penale da avviare secondo l'accelerazione del rito, connesso al c.d. *codice rosso* ex legge n. 69/2019, con i connessi profili di problematicità, in capo agli operatori di polizia (costituenti l'oggetto del presente lavoro), può porsi per i soli fatti *riconducibili* a lesioni personali lievissime procedibili a querela ex art. 582 comma 2, tentati o consumati – nell'ambito di un contesto di "*violenza domestica*" ex art. 3 legge 2013 – nei seguenti casi di contiguità familiare in senso ampio, attuale o cessata:

– *caso ex art. 582 comma 2 c.p. aggravato ex art. 577 comma 1 n. 1 (585 c.p.).*

Si tratta (alla stregua della novella dell'art. 577 c.p. recata dalla legge n. 69/2019) delle lesioni personali lievissime, procedibili a querela, tentate o consumate "*contro l'ascendente o il discendente anche per effetto di adozione di minorenne o contro il coniuge, anche legalmente separato, contro l'altra parte dell'unione civile o contro la persona stabilmente convivente con il colpevole o ad esso legata da relazione affettiva*";

– *caso ex art. 582 comma 2 c.p. aggravato ex art. 577 comma 2 (585 c.p.).*

Si tratta (alla stregua della novella dell'art. 577 c.p. recata dalla legge n. 69/2019) delle lesioni personali lievissime, procedibili a querela, tentate o consumate "*contro il coniuge divorziato, l'altra parte dell'unione civile, ove cessata, la persona legata al colpevole da stabile convivenza o relazione affettiva, ove cessate, il fratello o la sorella, l'adottante o l'adottato nei casi regolati dal titolo VIII del libro primo del codice civile, il padre o la madre adottivi, o il figlio adottivo, o contro un affine in linea retta*".

Così delimitato l'esatto ambito criminale con riguardo al quale soltanto si cumulano le previsioni del d.l. n. 93/2013, in punto di possibile adozione dell'ammonimento questorile per c.d. violenza domestica, e della legge n. 69/2019, introduttiva della sopra chiarita accelerazione del rito penale (c.d. codice rosso), occorre ora esaminare i riflessi di siffatta sovrapposizione normativa e dei connessi adempimenti procedurali per gli agenti ed ufficiali di polizia giudiziaria e di pubblica sicurezza coinvolti, segnatamente in ordine alla previsione del novellato art. 347 c.p.p.

Al riguardo, tuttavia, occorre rilevare che, sul piano formale, la novella del 2019 non pare avere insinuato alcuno stravolgimento nell'assetto discipli-

nare già tracciato ed esposto *supra* (nel capitolo 5), risolvendosi sul piano della mera accelerazione della tempistica degli adempimenti che, di per sé, rimangono invariati[85].

Così, l'operatore che, conoscendo – anche nella propria qualità di ufficiale o agente di pubblica sicurezza ed ai fini amministrativi-monitori – una vicenda di *violenza domestica*, vi ravvisi una notizia di reato sussumibile (alla stregua della valutazione qualificativa che compete alla polizia giudiziaria in quella fase) nei due casi di lesioni lievissime isolati sopra, sarà tenuto a curarne la rituale trasmissione all'autorità giudiziaria, rispettando la tempistica ora dettata dalla novellata disciplina procedurale.

Più in dettaglio, trattandosi, in entrambi i casi e per definizione, di reati perseguibili *a querela* della persona offesa, occorrerà distinguere a seconda che la condizione di procedibilità sussista o meno:

– se la querela non fosse stata sporta (o all'operatore di polizia non fosse noto), all'autorità giudiziaria dovrebbero essere trasmessi gli atti eventualmente assunti ai sensi dei già sopra esaminati artt. 346 c.p.p. e 112 disp. att. c.p.p., con la precisazione che (come già visto sopra per l'art. 612-*bis* c.p.), la legge n. 69/2019 non ha modificato l'art. 346 c.p. e non ha esteso il *codice rosso* e la conseguente accelerazione del rito anche a siffatte trasmissioni;

– se invece la querela risultasse sporta, la notizia di reato andrebbe trasmessa all'autorità giudiziaria con quella *immediatezza* ora prescritta dal novellato testo dell'art. 347 comma 3 c.p.p.

In tale ultimo caso, ferma restando la formale autonomia del procedimento monitorio preventivo, occorre prendere atto che, sul piano sostanziale, la funzione di tutela fortemente anticipata, tipicamente associata all'ammonimento questorile, rischi di apparire sminuita, se non superata, dalla fisiologica prospettiva dell'adozione di un eventuale provvedimento cautelare, sempreché tempestivamente richiesto dalla Procura, a seguito dell'immediato ricevimento della notizia di reato, dell'escussione della persona offesa nel termine di tre giorni dall'iscrizione ex art. 362 comma 1-*ter* c.p.p. e dal sollecito adempimento di eventuali deleghe di indagine da parte della polizia giudiziaria, il cui riscontro deve avvenire "senza ritardo" ex art. 370 comma commi 2-*bis* e 2-*ter* c.p.p. (come "senza ritardo" deve avvenire la trasmissione dei verbali e

85) In tal senso, le direttive emanate dalla Procura della Repubblica di Bologna il 26 luglio 2019 (prot. 2915/2019) e da quella di Mantova il 31 luglio 2019 (prot. 1068/2019) che parlano di deroga alla disciplina generale sulle sole modalità temporali di trasmissione della notizia di reato, ferme restando le attività di competenza della polizia giudiziaria, sia prima della trasmissione, che immediatamente dopo di essa (ex art. 348 c.p.p.).

della documentazione degli atti di polizia giudiziaria ex art. 357 c.p.p.).

Tuttavia, occorre ricordare che la tutela giudiziaria (anche cautelare) e quella preventivo-monitoria hanno presupposti ed effetti diversi (oltre a competere ad autorità diverse) e sono comunque contemplati dal legislatore come strumenti di tutela della vittima reciprocamente autonomi, e quindi potenzialmente cumulativi.

Conclusioni

La specifica questione tecnica

L'esame del problema sotteso al titolo del presente lavoro ed il tentativo di pervenire, per un verso, all'enucleazione di una soluzione interpretativa coerente con l'intrecciato insieme di norme giuridiche coinvolte e, per alto verso, all'indicazione di direttrici applicative utili ad orientare gli operatori, a fronte delle variegate opzioni offerte (od imposte) dall'ordinamento, nella materia della tutela della vittima di atti persecutori e violenza domestica, hanno postulato il confronto con aspetti disciplinari qualificati da marcato tecnicismo ed apparente settorialità.

Per contestualizzare la questione in esame, è parso opportuno muovere preliminarmente (capitolo 1) dalla ricostruzione della stessa figura istituzionale delle "*Autorità di pubblica sicurezza*", degli "*Ufficiali ed agenti di pubblica sicurezza*" di cui le prime si avvalgono per l'espletamento dei compiti della "*Amministrazione della pubblica sicurezza*", in cui tutte le predette figure sono inscritte, nonché dell'autorità provinciale di pubblica sicurezza sul piano tecnico-operativo, cioè il Questore.

Di quest'ultimo, in particolare, si è inteso declinare il poliedrico ruolo rivestito nell'attuale panorama ordinamentale (beninteso, a prescindere da quello di vertice provinciale della Polizia di Stato), e soprattutto le peculiari prerogative funzionali assegnategli dal legislatore, tra le quali figurano, per ciò che qui rileva, quelle in materia di *misure di prevenzione*.

Invero, anche in questo ambito (al pari di quello del governo tecnico dell'ordine e della sicurezza pubblica, in sede provinciale), il Questore emerge quale autorità qualificata da un'inequivoca centralità istituzionale: ciò è vero sul piano esecutivo delle misure preventive; sul piano della titolarità autonoma dell'iniziativa della proposta della sorveglianza speciale e delle attualissime misure patrimoniali; ma anche sul piano propriamente provvedimentale, siccome unica autorità amministrativa cui compete la stessa adozione di un numero (peraltro sempre più ampio, negli ultimi decenni) di misure di preven-

zione di natura personale: dall'avviso orale, ai fogli obbligatori di via, ai D.A.S.P.O., ai c.d. "Daspo urbani" o D.AC.UR ed infine agli "ammonimenti", introdotti dal d.l. n. 11/2009 per il contrasto del fenomeno dello *stalking* e poi estesi, dal d.l. n. 93/2013, alla tutela delle vittime dei fenomeni criminali di c.d. violenza domestica (oltre che, più recentemente, al fenomeno del cyberbullismo).

A questi due ultimi istituti monitori, esplicitamente evocati dal titolo del presente lavoro, è parso conseguentemente necessario (capitoli 2 e 3) riservare attenzione particolare, delineandone i diversi presupposti applicativi, i diversi effetti ma soprattutto la rispettiva disciplina, così difforme da insinuare il dubbio che, più opportunamente, dovrebbe parlarsi di istituti propriamente diversi: del resto, basti pensare che, in un caso (quello dell'ammonimento per *stalking*), si tratti di uno strumento connotato sia da marcata disponibilità in capo alla vittima, che da alternatività rispetto alla querela ed al conseguente procedimento penale; nell'altro caso (quello dell'ammonimento per c.d. violenza domestica), si tratta invece di uno strumento attivabile a prescindere dalla volontà della vittima e senza alcun rapporto di pregiudizialità rispetto alla tutela penale, con la quale può concorrere in un contesto di piena e reciproca autonomia.

L'adozione degli ammonimenti, in ogni caso, costituisce espressione di un potere "provvedimentale", che il Questore esercita all'esito di un procedimento amministrativo, il cui svolgimento prevede una rituale istruttoria. Essa, peraltro, pare connotata da peculiari profili, connessi sia all'orientamento teleologico verso l'eventuale adozione di un atto dell'*autorità di pubblica sicurezza*, dal contenuto cautelare, protettivo e di prevenzione, sia dai poteri autoritativi degli *agenti ed ufficiali di pubblica sicurezza*, cui è rimesso il suo concreto svolgimento, attraverso un'eventuale *investigazione di pubblica sicurezza*, alla quale pure è stata riservata specifica attenzione (nel capitolo 4). L'approfondimento ha costituito, del resto, occasione per rilevare e sottolineare una grave lacuna normativa (in punto di organica ed unitaria regolamentazione dei limiti contenutistici, della forma e dell'efficacia degli atti suscettibili di essere posti in essere dagli agenti ed ufficiali di p.s.) che si auspica sia legislativamente colmata quanto prima.

Una volta delineato il contesto in cui si inscrivono gli istituti degli ammonimenti questorili e tracciata la relativa disciplina, si è rilevato come, con tali strumenti di natura amministrativo-preventiva, il legislatore abbia voluto disegnare, nelle materie cennate, un dispositivo di tutela della vittima parallelo a quello rappresentato dallo strumento penale: si è così sottolineato come, accanto ad un tradizionale procedimento penale, di competenza dell'*autorità giudiziaria* che, attraverso gli *ufficiali ed agenti di polizia giudiziaria*, mira

ad accertare e reprimere i reati (previa applicazione, se del caso, di misure cautelari), esista un procedimento amministrativo di prevenzione, di competenza del *Questore*, che, attraverso gli *ufficiali ed agenti di pubblica sicurezza*, mira ad adottare un eventuale provvedimento cautelare anticipatorio e di tutela avanzata della vittima, che prevenga la stessa commissione della condotta pregiudizievole in danno di quest'ultima.

E si tratta di canali di tutela di pari dignità, da intendersi slegati da reciproci rapporti di pregiudizialità o *ancillarità*, all'insegna di un principio di assoluta autonomia dei procedimenti, espressione e corollario dell'autonomia istituzionale delle autorità giudiziaria e di pubblica sicurezza cui essi competono, nonché della volontà del legislatore di cumulare i predetti strumenti, onde potenziare lo statuto di tutela della vittima[86].

Tuttavia, se procedimento monitorio questorile e procedimento penale giudiziario sono autonomi e persino i rispettivi oggetti sono distinti (il primo essendo preordinato a rintracciare un sufficiente quadro "indiziario", ancorché basato su elementi di fatto legislativamente tipizzati, circa la pericolosità del soggetto; il secondo ricercando la "prova" della colpevolezza di un soggetto in ordine alla commissione di un reato), è altrettanto indubbio che essi finiscano col riguardare materie oggettivamente contigue, di tal ché esistono fisiologici rischi di sovrapposizioni e interferenze reciproche[87].

La delicatezza di siffatta interazione e delle possibili criticità che ne conseguono è acuita dalla notoria circostanza per cui gli ufficiali ed agenti di pubblica sicurezza (cui spetta il compito di supportare il Questore nell'esercizio delle sue prerogative provvedimentali in materia di misure preventive e segnatamente di quelle monitorie in esame) sono contestualmente – di fatto tutti

86) In tal senso, pare opportuno richiamare ancora il recente arresto del Consiglio di Stato, sezione III (sentenza 758 del 24-30 gennaio 2019 n. 758) che, pronunciandosi sui confini del diritto amministrativo di prevenzione (nello specifico campo delle interdittive antimafia), esclude esplicitamente ogni "rapporto di pregiudizialità, condizionalità o ancillarità tra il giudizio penale e quello amministrativo", che finirebbe peraltro per pregiudicare l'efficacia e tempestività dello strumento preventivo monitorio e quindi la ratio della sua stessa previsione legislativa quale strumento per scongiurare una condotta aggressiva che si abbia fondato motivo di ritenere possibile ed imminente.

87) Come sottolineato nel testo, ciò è ancor più vero ed evidente laddove la "fattispecie preventiva", da cui desumere elementi prognostici circa la futura pericolosità del soggetto, sia stata tipizzata dal legislatore essenzialmente con esplicito riferimento alla commissione di uno o più reati, come avviene appunto nel caso di cui all'art. 3 d.l. n. 93/2013 (che evoca la preventiva commissione da parte dell'ammonendo dei delitti ex artt. 581 e 582 cpv. c.p. sia pure con l'ulteriore contestualizzazione di essi in un ambito di violenza domestica).

– titolari anche della qualifica di ufficiali ed agenti di polizia giudiziaria, e come tali titolari di correlativi doveri verso l'autorità giudiziaria, funzionali ad assicurare l'esercizio dell'azione penale: in primo luogo quelli concernenti la trasmissione della notizia di reato ai sensi dell'art. 347 c.p.p.

Tale problematico rapporto tra i due procedimenti ed i relativi riflessi sui doveri degli operatori di polizia, ha così costituito oggetto di specifica riflessione (i cui termini sono compendiati nel capitolo 5) con l'avvertenza che, conformandosi esso in termini diversi, a seconda quantomeno del tipo di provvedimento questorile di cui si tratta, l'analisi è stata condotta con distinta attenzione al caso dell'ammonimento c.d. per *stalking* rispetto a quello per c.d. violenza domestica.

Nel primo caso, per la verità, non si sono ravvisati particolari problemi applicativi: la strutturale alternatività tra la presentazione di una richiesta di ammonimento ex art. 8 d.l. n. 11/2009 e la proposizione della querela, è sembrata escludere generalmente (salve talune eccezionali ipotesi, passate pure in rassegna) qualsivoglia dubbio circa i doveri degli operatori di polizia che ricevano l'uno o l'altro dei predetti atti di impulso, peraltro tutti necessariamente provenienti direttamente dalla vittima.

Nel secondo caso, invece, i rapporti tra procedimento penale e procedimento amministrativo finalizzato all'ammonimento per violenza domestica, ex art. 3 d.l. n. 93/2013, sottendono maggiori profili di fluidità ed incertezza, connessi alla non alternatività del procedimento monitorio rispetto a quello giudiziario ed alla possibilità di avvio del primo anche d'ufficio, senza alcuna richiesta della vittima.

Al riguardo, si è giunti a sostenere che l'autonomia delle reciproche funzioni assegnate alle autorità giudiziarie ed a quelle di pubblica sicurezza e la necessità di assicurare l'effettivo esercizio delle prerogative e dell'attribuzioni assegnate dal legislatore all'*Amministrazione della pubblica sicurezza*, vieppiù sul piano dell'implementazione della tutela della vittima, postulino la necessità di ravvisare, accanto ai pacifici obblighi (incombenti sugli ufficiali e agenti di p.s.) di riferire all'ufficio di Procura le notizie di reato apprese anche in contesti procedurali di natura amministrativo-preventiva, un parallelo obbligo (invocabile in capo agli ufficiali ed agenti di p.g.) di segnalare al Questore – con gli accorgimenti e nelle forme specificate *supra* – quei fatti che, pur appresi in contesti di polizia giudiziaria o comunque connessi alla ritenuta ricorrenza di un reato, appaiano anche integranti gli estremi del presupposto dell'ammonimento ex art. 3 d.l. n. 93/2013 (riassumibile nella ricorrenza di fatti *riconducibili* a lesioni o percosse in ambito di "violenza domestica" con ricorrenza degli estremi indiziari di una pericolosità del soggetto di cui si tratta).

Ciò, beninteso, sottolineando come la prudente e puntuale valorizzazione della specifica disciplina legislativa dell'ammonimento per violenza domestica (ad esempio laddove essa contempli l'anonimato del segnalante, una limitazione del diritto di accesso agli atti amministrativi o meccanismi di anticipazione in sede amministrativa delle garanzie processual-penalistiche dell'indagato, ai sensi dell'art. 220 disp. att. c.p.p.) paia poter scongiurare qualsivoglia compromissione del segreto investigativo nell'ambito delle indagini preliminari e, più genericamente, della giurisdizione penale e dell'autonomia dell'autorità giudiziaria, costituzionalmente tutelate.

Si è, infine, esaminato l'effetto dell'innesto, su tale assetto dei rapporti tra procedimento penale e preventivo-monitorio, dell'entrata in vigore della legge n. 69/2019, come noto introduttiva, tra l'altro, del c.d. *Codice rosso*, ossia di una corsia procedural-penalistica preferenziale, funzionale ad assicurare un'accelerazione nella trattazione (e prima ancora nella stessa conoscenza) giudiziaria di taluni reati, esplicitamente elencati dalla legge, siccome ritenuti sensibili o sintomaticamente connessi a fattispecie di elevato allarme sociale in materia di violenza di genere e violenza domestica: tra i quali ultimi, rientrano anche taluni dei fatti costituenti presupposto per l'esperibilità dell'ammonimento questorile.

Al riguardo, si è preliminarmente individuato l'esatto ambito di effettiva sovrapposizione del *codice rosso* rispetto ai presupposti degli istituti monitori

88) Come chiarito prima, atteso che la legge n. 69/2019 non ricomprende nel proprio ambito applicativo l'art. 581 c.p. (per il quale pure sarebbe possibile l'ammonimento per violenza domestica), il problema di possibili sovrapposizioni tra procedimento questorile monitorio ex art. 3 d.l. n. 93/2013 e procedimento penale da avviare secondo l'accelerazione del rito, connesso al c.d. codice rosso ex legge n. 69/2019, può porsi per i soli fatti di lesioni personali lievissime (procedibili a querela ex art. 582 comma 2), tentate o consumate – nell'ambito di un contesto di "violenza domestica" ex art. 3 legge 2013 – nei seguenti casi di contiguità familiare in senso ampio, attuale o cessata:
Caso ex art. 582 comma 2 c.p. aggravato ex art. 577 comma 1 n. 1: si tratta delle lesioni personali lievissime, procedibili a querela, tentate o consumate "contro l'ascendente o il discendente anche per effetto di adozione di minorenne o contro il coniuge, anche legalmente separato, contro l'altra parte dell'unione civile o contro la persona stabilmente convivente con il colpevole o ad esso legata da relazione affettiva";
Caso ex art. 582 comma 2 c.p. aggravato ex art. 577 comma 2: si tratta delle lesioni personali lievissime, procedibili a querela, tentate o consumate "contro il coniuge divorziato, l'altra parte dell'unione civile, ove cessata, la persona legata al colpevole da stabile convivenza o relazione affettiva, ove cessate, il fratello o la sorella, l'adottante o l'adottato nei casi regolati dal titolo VIII del libro primo del codice civile, il padre o la madre adottivi, o il figlio adottivo, o contro un affine in linea retta".

questorili, finendo col circoscriverlo ai soli casi di ricorrenza di un reato persecutorio ex art. 612-*bis* c.p. (in cui possono ricorrere i presupposti per adottare un ammonimento ex art. 8 d.l. 11/2009) e a due soli casi di condotte riconducibili a lesioni procedibili a querela, commesse in contesti di relazioni familiari o affettive, attuali o concluse (in cui possono ravvisarsi le condizioni per il parallelo ricorso all'ammonimento per c.d. violenza domestica, di cui all'art. 3 d.l. n. 93/2013)[88].

Per tali ultimi casi, in particolare, è stato isolato il complesso dei doveri incombenti sugli agenti ed ufficiali di pubblica sicurezza e polizia giudiziaria, in conseguenza delle novella recata dalla legge n. 69/2019 sulle norme del codice di rito e segnatamente sull'art. 347 c.p.p., in punto di trasmissione *immediata* della notizia di reato all'autorità giudiziaria, riassumendone la portata innovativa in termini di mera tempistica degli adempimenti, il cui contenuto si è ritenuto sostanzialmente immutato rispetto al quadro tracciato prima, con riguardo all'assetto previgente alla legge del 2019.

Le questioni sullo sfondo

Attraverso l'analisi della questione tecnica di cui alla traccia, e traguardando le intricate problematiche applicative ricadenti in materia sugli ufficiali ed agenti di pubblica sicurezza e di polizia giudiziaria, il presente lavoro ha permesso di approcciare il più ampio problema del rapporto intercorrente tra procedimento penale e procedimento amministrativo-preventivo, nonché sfiorare, ancora più sullo sfondo, il delicatissimo tema dei rapporti tra le diverse autorità cui essi competono e, segnatamente, l'autorità giudiziaria ed il Questore, quale autorità di pubblica sicurezza o di prevenzione.

Tali suggestivi temi sono stati affrontati, in questo lavoro, nella consapevolezza che il loro inquadramento sconti, ancora, diverse resistenze ideologiche, dogmatiche e pratiche.

Innanzitutto, mentre le regole ed il contenuto dei procedimenti giudiziari sono diffusamente e puntualmente noti, i procedimenti e le attività delle autorità di pubblica sicurezza costituiscono oggetto di una conoscenza molto più rara e spesso approssimativa, anche tra gli addetti ai lavori.

Ma vi è di più.

La declinazione dello stesso ambito istituzionale e delle attribuzioni dell'*Amministrazione della pubblica sicurezza* pare, spesso, ancora gravata da persistenti riserve ideologiche, incentrate su una collocazione ordinamentale di detta amministrazione come struttura orientata verso la tutela di un ordine pubblico concepito quale risultante di assetti di interessi pubblici, di volta in volta, politicamente connotati, piuttosto che quale presidio repubblicano di

una sicurezza dei cittadini, sempre più intesa (secondo il profondo ed autorevole insegnamento del Prefetto Carlo Mosca) nei pregnanti termini di "*diritto di libertà*" e "*di garanzia*"[89].

Nel campo specifico delle *misure di prevenzione*, poi, a siffatte riserve si sono affiancate quelle dottrinarie[90], incentrate sulla ritenuta deriva d'incostituzionalità, asseritamente insita nel sempre maggiore ricorso a pretese *pene del sospetto* o *praeter delictum.* E ciò, nonostante la Corte costituzionale abbia ribadito, sin dalla sentenza n. 2 del suo primo anno di vita (1956), la legittimità del sistema preventivo italiano[91] ed il legislatore stia sempre più spostando il baricentro del contrasto statuale ai fenomeni criminali dal livello giudiziario a quello amministrativo-preventivo, con la conseguente delineazione, accanto al diritto penale ed al diritto amministrativo, di un *diritto della prevenzione* non più liquidabile alla stregua di un settore *di confine* ma postulante, ormai, autonoma considerazione.

---

89) C. Mosca, *La sicurezza come diritto di libertà*, cit., e, da ultimo, C. Mosca, *La Sicurezza - Valori, modelli e prassi istituzionali*, cit., p. 97 ss., che ribadisce la costruzione della sicurezza come "diritto di libertà" o "di garanzia" (laddove essa si configura come "diritto alla libertà di essere sicuri" ovvero ancora "sicurezza di ogni diritto di libertà", a fronte del quale sussiste un correlativo "dovere dello Stato"): "il diritto alla sicurezza è, in termini di protezione preventiva delle persone dalle minacce concrete o potenziali, espressione di quel ragionevole bilanciamento, richiesto dalla Costituzione, di tutti i diritti, le libertà e gli interessi costituzionalmente protetti, in vista dell'effettiva affermazione della dignità e dell'uguaglianza sostanziale dell'essere umano".

90) Sul punto, cfr. F. Messina - G. Linares - G. Annichiarico, *La confisca di prevenzione: tra finalità preventive, effetti neutralizzatori ed esigenze ripristinatorie*, in *Sistema penale*, 9/2020, che stigmatizzano e contestano talune aspre critiche dottrinarie al sistema preventivo italiano, come quella di D. Petrini, *Le misure di prevenzione personali: espansioni e mutazioni*, in *Dir. pen. e processo*, 2019, 11, 1531 (commento alla normativa).

91) La Corte costituzionale è stata chiamata a pronunciarsi sulle misure di prevenzione, per riconoscerne sostanzialmente la compatibilità con la Costituzione (salve talune limature che hanno corretto profili attinenti la genericità delle norme circa l'individuazione dei soggetti destinatari delle misure o gli obblighi ad essi imposti), oltre che nella citata sentenza n. 2 del 1956, con le sentenze n. 27/1959, n. 45/1960, n. 126/1962; n. 23/1964; n. 68/1964, n. 32/1969, n. 76/1970 (che pure "dichiara l'illegittimità costituzionale dell'art. 4, secondo comma, della legge 27 dicembre 1956, n. 1423"), la n. 177/1980 e, da ultimo, dalle c.d. sentenze gemelle nn. 24 e 25 del 24 gennaio - 27 febbraio 2019, che riaffermano sostanzialmente la costituzionalità del sistema preventivo, pur dopo la celebre pronuncia della Corte EDU del 23 febbraio 2017 (ricorso n. 43395/09, causa De Tommaso c. Italia), che ha insinuato profili di rischio sotto tale aspetto. Per approfondimenti al riguardo, cfr. G. ALIQUÓ, *La violenza domestica. L'ammonimento del Questore*, *op. cit.*, p. 289 ss.

Infine, ma con rilievo pratico tutt'altro che trascurabile, occorre prendere atto che l'esistenza di una pluralità di strumenti statuali di tutela del cittadino, coinvolgenti organi e poteri diversi e tra loro autonomi, impone agli stessi (e a chi li rappresenta) un doveroso ampliamento degli orizzonti del proprio ambito di competenza ed uno sforzo differenziale di ricerca ed attuazione di intese e rapporti sempre più continui, per la definizione e l'applicazione dei quali la chiave di volta pare doversi riassumere – anche in questa dimensione interistituzionale – in quella cultura del "coordinamento" che, sul piano della pubblica sicurezza, è stata sancita e tradotta dalla legge n. 121/1981 e, da quaranta anni, informa proficuamente la vita e l'attività delle forze di polizia italiane.

La necessità di un approccio coordinato o raccordato

Invero, la strutturale contiguità (vieppiù dalla prospettiva degli agenti ed ufficiali di polizia giudiziaria e di pubblica sicurezza) tra la materia della prevenzione amministrativa e quella della repressione giudiziaria penale, sul campo che stiamo esaminando, insinua il costante rischio di sovrapposizioni istituzionali suscettibili di deleterie reciproche interferenze.

Detto diversamente, la previsione legislativa di due procedimenti (quello penale e quello amministrativo monitorio) che si avviano e sviluppano in piena autonomia reciproca, postula rischi di diseconomie, frizioni, possibili danni per gli stessi procedimenti ma soprattutto per le persone coinvolte nei fatti di cui si tratta.

Ad esempio, l'autonomo dispiegarsi dei due procedimenti può comportare rischi di duplicazioni procedurali in senso ampio, sottendenti talora inutili dispendi di risorse ma anche il rischio di c.d. vittimizzazione secondaria, attraverso l'esposizione della persona offesa o dei minori che abbiano assistito ai fatti a plurime escussioni e connesse deleterie ripercussioni psicologiche. Per non parlare dell'evidente rischio che iniziative provvedimentali, programmate o adottate in un procedimento (per esempio quelle giudiziarie, di tipo cautelare), siano compromesse o vanificate dalle conseguenze di atti posti in essere nell'altro.

Proprio per armonizzare l'esercizio concreto di siffatti distinti poteri dell'autorità giudiziaria e del Questore, onde consentire che gli stessi rafforzino effettivamente lo statuto di tutela della vittima di fenomeni di violenza domestica, piuttosto che finire con l'indebolirlo o comprometterlo, pare oltremodo auspicabile che, (anche) in questa materia, sia ricercato e praticato, per un verso, un proficuo coordinamento investigativo tra *polizia giudiziaria* e *ufficiali ed agenti di pubblica sicurezza* nonché, per altro verso, uno stretto raccordo

informativo ed operativo tra autorità giudiziaria ed autorità di pubblica sicurezza[92].

In questa auspicabile direzione di metodo, andranno quindi valorizzate ed incentivate tutte le prassi finalizzate ad assicurare uno stretto raccordo informativo ed operativo tra Questura e Procura circa le attività parallelamente avviate su temi così contigui e delicati.

Sarà oltremodo opportuno che la polizia giudiziaria che – secondo quanto sopra anticipato – "segnala" al Questore ex art. 3 legge 2013 una vicenda potenzialmente rilevante per un ammonimento per c.d. violenza domestica, di cui ha avuto contezza a seguito della ricezione di una querela o di un atto di delega giudiziaria, ne dia espressa contezza alla stessa a.g. (perché essa sappia del possibile avvio o della pendenza di parallelo procedimento amministrativo monitorio).

Analogamente, sarà opportuno che gli ufficiali o agenti di p.s. che abbiano segnalato al Questore una vicenda rilevante per l'eventuale adozione di un ammonimento per violenza domestica o quelli delegati all'istruttoria, gli segnalino altresì la trasmissione alla a.g. di atti (ex art. 346 c.p.p.) o la circostanza che sia sopravvenuta una querela destinata ad essere trasmessa agli uffici di Procura, onde consentire l'attivazione di un contatto con il magistrato titolare dell'eventuale successiva indagine.

Ancora in tale prospettiva, non solo parrebbe opportuno che l'ufficio delegato all'istruttoria del procedimento monitorio (in genere l'ufficio misure

92) Del resto, a titolo esemplificativo, l'esperienza di una proficua sinergia tra autorità di pubblica sicurezza e autorità giudiziaria, nell'esercizio di prerogative reciprocamente autonome ma potenzialmente interferenti, è stata già sperimentata con successo dal Servizio centrale anticrimine della Direzione centrale anticrimine della Polizia di Stato, negli ultimi tempi, sul piano diverso (ma non lontano da quello in esame) dei rapporti tra il potere di iniziativa del Questore in materia di misure di prevenzione patrimoniale e le prerogative degli uffici di Procura titolari di indagini, attraverso il modello della c.d "proposta congiunta" tra a.g ed autorità di p.s. Si tratta di un modello procedurale che ha conosciuto una forte implementazione: nel 2020 (alla stregua dei dati pubblicati il 10 aprile 2021, in occasione del 169° anniversario della fondazione della Polizia di Stato), i Questori hanno formulato n. 71 proposte di applicazione del sequestro finalizzato alla confisca, di cui 34 elaborate congiuntamente ai Procuratori competenti e inoltrato ai Tribunali una proposta di applicazione del controllo giudiziario, redatta in modalità congiunta con l'a.g. Sono stati, inoltre, eseguiti: 47 sequestri di beni, su altrettante proposte del Questore, formulate, in 15 casi, congiuntamente ai Procuratori competenti, per un valore complessivo di circa 85 milioni di euro; 35 confische, di cui 32 su proposta del Questore, formulate, in 9 casi, congiuntamente ai Procuratori competenti, per un valore complessivo di circa 227 milioni di euro.

di prevenzione della Divisione anticrimine della Questura) verificasse sempre l'eventuale presentazione di querele da parte della vittima dei fatti di cui si tratta, ma parrebbe auspicabile che si arrivasse anche alla definizione di protocolli operativi tra Procure della Repubblica e Questure, in virtù dei quali ciascuna autorità coinvolga immediatamente l'altra a fronte dell'avvio di un procedimento in ordine ad una vicenda che potrebbe sottendere la parallela pendenza di procedimenti.

Siffatto raccordo informativo (vieppiù laddove strutturalmente discendente da protocolli e connesse prassi consolidate nei rispettivi uffici) consentirebbe puntuali vantaggi sul piano operativo: ad esempio, si potrebbero scongiurare duplicazioni di atti istruttori, ricorrendo allo svolgimento congiunto di essi, da parte del personale di polizia giudiziaria delegato dall'a.g. unitamente a quello di p.s. delegato dal Questore (ove non si ritenga di concordare addirittura l'adozione di una delega congiunta ai medesimi operatori, come sarebbe opportuno ogni qualvolta essi abbiano stretto rapporti di particolare empatia con la vittima o abbiano una speciale formazione professionale al riguardo)[93].

Bibliografia

ALIQUÓ G., *Il Questore, autorità nel sistema della sicurezza complementare*, in *Quaderno della Rivista trimestrale della Scuola di perfezionamento per le forze di polizia*, II/2015

ALIQUÓ G., *La violenza domestica. L'ammonimento del Questore*, Pacini giuridica, 2019

ALPA G., *I principi generali*, Giuffré, ed. 2006

93) Come anticipato, l'istruzione dei procedimenti monitori e preventivi in genere è normalmente delegata dal Questore al personale della Divisione anticrimine - Ufficio misure di prevenzione della Questura, mentre gli accertamenti di polizia giudiziaria rientrano nella competenza della Squadra Mobile, costituente il "servizio di polizia giudiziaria" ex art. 55 c.p.p. che la Polizia di Stato, come forza di polizia, pone a disposizione dell'autorità giudiziaria in seno alle proprie questure. Per altro verso, siffatta destinazione funzionale non comporta, per il personale della Squadra mobile, né la perdita delle qualifiche di ufficiali o agenti di P.S né i vincoli di subordinazione gerarchica verso il Questore, che ben può continuare a disporne per finalità istituzionali connesse alle proprie prerogative (esulanti ovviamente da compiti di polizia giudiziaria). Analogamente, il personale della Polizia di Stato in servizio presso la Divisione Anticrimine è titolare di qualifiche di polizia giudiziaria.

Antonelli V., *Il diritto amministrativo preventivo a servizio della sicurezza pubblica*, in *Dir. pen. e processo*, 2019, 11
Basile F., *Le misure di prevenzione dopo il c.d. Codice Antimafia. Aspetti sostanziali e aspetti procedurali. Brevi considerazioni introduttive sulle misure di prevenzione*, in *Giur. it*., 2015, 6
De Paolis M., *Il fenomeno dello stalking occupazionale*, in *Azienditalia* - Il personale, 2014, 3
Fiandaca G. - Visconti C. *Il codice delle leggi antimafia: risultati, omissioni e prospettive*, in *La legislazione penale*, 2012, p. 183 ss
Licciardello S., *Il Questore*, Ed. Franco Angeli, 2016
Macri' F., *Le nuove norme penali sostanziali di contrasto al fenomeno della violenza di genere*, in *Dir. pen. e processo*, 2014, 1
Messina F. - Linares G. - Annichiarico G., *La confisca di prevenzione: tra finalità preventive, effetti neutralizzatori ed esigenze ripristinatorie,* in *Sistema penale*, 9/2020
Mosca C., *La Sicurezza - Valori, modelli e prassi istituzionali*, Editoriale scientifica, 2021
Mosca C., *La sicurezza come diritto di libertà*, Cedam, 2012
Mosca C., *Teoria generale del coordinamento delle Forze di polizia*, in Morcellini M. - Mosca C. (a cura di), *La sapienza della sicurezza*, Maggioli, 2014
Petrini D., *Le misure di prevenzione personali: espansioni e mutazioni*, in *Dir. pen. e processo*, 2019, 11, 1531
Pittaro F., *Il c.d. Codice Rosso sulla tutela delle vittime di violenza domestica e di genere*, in *Famiglia e diritto*, 2020, 7
Pittaro F., *La legge sul femminicidio: le disposizioni penali di una complessa normativa*, in *Famiglia e diritto*, 2014, 7
Rampioni M., *Le c.d. indagini "anfibie": linee di fondo sul controverso legame tra attività ispettive e processo penale*, nella rivista on-line *Processo penale e giustizia*, 1/2019
Roia F., *Crimini contro le donne. Politiche, leggi, buone pratiche*, Ed. Franco Angeli, 2017
Rombi N., *La circolazione delle prove penali*, Cedam, 2003.
Sono state inoltre consultate le *Linee guida in materia di misure di prevenzione personali* elaborate dal Servizio centrale anticrimine della Direzione centrale anticrimine della Polizia di Stato, ed. luglio 2020.

Parte III

Voci dall'Aula

Il traffico di stupefacenti e armi *on-line*: strumenti e metodologie di indagine nel *darkweb*. Le chat cifrate

di Vincenzo Pascale*

Abstract

Negli ultimi anni la rete Internet è diventata sempre più un fiorente mercato parallelo di scambio commerciale di beni e servizi di qualsiasi tipo, anche purtroppo di natura illecita.

Su tutti, il fenomeno del traffico di droga e di armi è riuscito a ritagliarsi uno "spazio virtuale" importante nella parte oscura del web, definita "dark web", generando un enorme volume d'affari che ha nel tempo consentito ad abili criminali di arricchirsi facendo leva sull'"anonimato" offerto dalla navigazione mediante specifiche dark net (Tor, la più nota) e dall'utilizzo di criptovalute (Bitcoin su tutte) come metodo di pagamento per mascherare il mittente e il destinatario della transazione economica.

Il dark web è cosi diventato "terreno fertile" per il proliferare di piattaforme di vendita illegale, i c.d. "black market", appositamente create per l'e-commerce di prodotti di diversa tipologia, dalla droga alle armi, al materiale pedopornografico, ai falsi documenti d'identità, alle carte di credito rubate, tanto per citarne alcuni.

Il funzionamento di un market in rete è simile a quello di un qualsiasi negozio di vendita. Un amministratore organizza lo shop e riserva ai vari venditori, dietro compenso, uno spazio espositivo virtuale dove pubblicizzare i propri prodotti con dovizia di particolari. Gli accordi di vendita vengono conclusi in forma privata (generalmente mediante chat cifrate) direttamente tra il venditore e l'acquirente, che paga con moneta digitale, parte della quale viene incassata dall'amministratore della piattaforma a titolo di commissione per il buon esito della trattativa.

La vendita di droga in rete, inizialmente limitata al mondo del web, si è nel tempo estesa dapprima ai social network (Facebook e Twitter su

(*) Colonnello dell'Arma dei Carabinieri, già frequentatore del XXXVI corso di Alta formazione presso la Scuola di perfezionamento per le forze di polizia.

tutti) e, successivamente, ai servizi di messaggistica istantanea (Telegram e Wickr in particolare), con questi ultimi in grado di offrire la riservatezza delle comunicazioni, tanto utile per chi con essi persegue scopi illeciti.

Anche per il fenomeno del traffico on-line di droga e armi, come per tutti quelli che si sviluppano mediante il web, vale la regola generale secondo cui nel cyberspace i concetti di tempo e di spazio sono totalmente stravolti; il primo è accelerato, mentre il secondo è del tutto azzerato.

Da ciò è facilmente comprensibile come le sue caratteristiche principali siano proprio la "globalità" (una piattaforma virtuale di vendita non ha confini potendo contare su server dislocati in varie parti del mondo) e la "mutabilità" (chi realizza uno shop in rete può aprirlo e chiuderlo con la stessa rapidità, così come può facilmente cambiarne l'indirizzo di accesso o la denominazione se si sente "osservato" dalle forze di polizia).

In uno scenario così complesso, l'attività di contrasto delle forze di polizia risulta non certo agevole. Per un investigatore che agisce in rete, è infatti necessario possedere un'elevata competenza informatica che gli consenta di utilizzare efficacemente gli strumenti di analisi oggi disponibili (software anche complessi) e, soprattutto, di saper interpretare al meglio e con abilità il proprio ruolo di "infiltrato" nello svolgimento di operazioni speciali che, nell'ambito di una irrinunciabile cornice di cooperazione internazionale giudiziaria e di polizia, rappresentano – nella maggior parte dei casi – l'unico mezzo per smantellarlo, cercando al contempo di individuarne gli ideatori\amministratori e di identificare il maggior numero di venditori.

Il presente elaborato, frutto semplicemente del confronto con gli operatori delle forze di polizia che si occupano delle investigazioni in rete, si prefigge lo scopo di fornire spunti di riflessione su un fenomeno certamente nuovo e in rapidissima espansione, sul quale è certamente indispensabile in futuro "investire", da un lato, implementando la tecnologia per renderla adeguata rispetto alla velocità con cui evolvono le dinamiche criminali nel web, dall'altro, puntando alla formazione specialistica di personale in un settore che negli ultimi anni, in termini di sicurezza, ha senza dubbio contribuito ad innalzare notevolmente il livello di allarme.

* * *

In the last few years, Internet has been increasingly transformed into a parallel market for the commercial exchange of any kinds of goods and services, unfortunately related, in some cases, to illegal activities.

The phenomenon of trafficking in drugs and weapons has become very important on the web, the so-called dark web, bringing about huge business opportunities arising in the course of the time and exploited by skilled criminals who have managed to gain money due to the possibility to remain anonymous. This possibility is offered by peculiar dark nets (Tor is the most popular) as well as by the use of cryptocurrency (above all bit coins), that is to say a payment method used to hide the identity of the buyers and sellers participating in the transaction.

Therefore, the dark web represents an opportunity for the spreading of illegal on-line trading platforms, the so-called black markets. These platforms have been deliberately created for the e-commerce, that is to say the purchase and sale of different kinds of products, such as for example drugs, weapons, child pornography material, forged identity documents, stolen credit cards.

The funcioning of an on-line market is similar to the activity of a shop. An administrator organizes the shop and provides, upon payment, the sellers with a virtual showroom where they can advertise in details their products. The terms of sale are privately agreed (generally by means of encrypted chats) between the seller and the buyer, who uses digital currency to make the payments. A part of this digital currency is collected by the administrator of the on-line platform by way of compensation for the success of the transaction.

The on-line sale of drugs, which originally took place only on the web space, has been spreading, in the course of the time, at first to social networks (above all Facebook and Twitter) and then to the cloud-based instant messaging system (Telegram and Wickr in particular) which are able to maintain confidentiality of communications for people who conduct illegal activities.

Moreover, taking into account on-line trafficking in drugs and weapons, as well as all the other illegal activities spreading over the web, we realize that the concepts of space and time are totally upset in the cyberspace: the first one is accelerated, the second one is cancelled.

In consideration of the above, it is evident that the characteristics of cyberspace are globality (an e-commerce platform has no bounderies since it can rely on servers located in different parts of the world) and flexibility (the person who creates an on-line shop is able to quickly open and close it, as well as to change the relevant login address or name when that person thinks to be under surveillance by police forces).

In such a complex scenario, the activity carried out by police forces is absolutely not easy. As a matter of fact, the investigators, who fight against on-line illegal activities, must be provided with high level digital competences allowing them to effectively use the current available tools of analysis (also complex softwares) and, above all, to play, in the best way, their role of undercover agent in the implementation of special operations. In the framework of an essential judicial and police international cooperation, these operations represent, in most cases, the only tool to counter this phenomenon and, at the same time, to detect the originators/administrators of on-line illegal activities and to identify most part of the sellers.

The content of this dissertation, which is the result of the contribution given by police forces' officers responsible for on-line investigations, is aimed at providing hints for reflection on a new phenomenon which is increasingly spreading. As a matter of fact, it will be fundamental in the future to focus the attention on the need to adjust technologies to the rapid development of criminal activities on the web, as well as to deliver special training to the staff working in a field which, in the last few years, has remarkably caused increased concerns in relation to security matters.

* * *

1. Il mondo sommerso del web tra anonimato e riservatezza

1.1. Internet e World Wide Web: brevi cenni storici

Prima di tracciare i confini delle aree virtuali in cui il web è suddiviso, occorre preliminarmente dirimere ogni dubbio sulla notevole differenza che esiste tra la rete Internet e appunto il web, due concetti che molto spesso ed erroneamente vengono ricondotti allo stesso significato.

Sinteticamente, la rete Internet è l'infrastruttura tecnologica sulla quale viaggiano i dati. Alcuni esperti la paragonano metaforicamente a una ferrovia digitale, composta da binari (canali), da stazioni (server) e da regole (protocolli).

Il web, invece, è uno dei servizi Internet che permette il trasferimento e la visualizzazione dei dati, sotto forma di ipertesto, al pari di altri servizi quali la posta elettronica, i newsgroups, i trasferimenti FTP, ecc.

Storicamente, la nascita della rete Internet viene fatta risalire al 1969, allorquando il DARPA (Defense Advanced Research Projects Agency), l'agenzia governativa del Dipartimento della Difesa degli Stati Uniti incaricata dello sviluppo di nuove tecnologie per uso militare, elaborò "ARPANET" (Advanced Research Projects Agency NETwork), una rete di nodi basata su una architettura client/server destinata ad un uso militare. Tale rete, pensata inizialmente per soli scopi militari durante la guerra fredda, agli inizi degli anni '80 perse la sua originaria connotazione, diventando un utile strumento utilizzato in ambito universitario per scambiare le conoscenze scientifiche e per comunicare.

Invece, il "World Wide Web" (WWW o abbreviato semplicemente in web), che come detto è il sistema che permette di usufruire della gran parte dei contenuti disponibili sulla rete Internet, fu descritto ufficialmente per la prima volta il 12 marzo del 1989 dal suo inventore, l'informatico britannico Tim Berners-Lee, in una sorta di memoria che presentò ai suoi capi al CERN[1] di Ginevra. Il "World Wide Web", inizialmente denominato MESH, in quel momento non era altro che un sistema che consentiva di gestire la grande mole di informazioni legata agli esperimenti scientifici svolti al CERN, rendendola fruibile ai circa 17.000 scienziati che ci lavoravano. Il suo stesso fondatore non avrebbe mai immaginato che quel sistema, apparentemente così semplice, sarebbe poi diventato il principale servizio di Internet, in grado addirittura di cambiare le quotidiane abitudini di vita in tutto il mondo. Nel 1990, Time Berners-Lee e i suoi collaboratori pubblicarono la prima pagina web, che consisteva nella descrizione del progetto che esemplificava e conteneva anche alcuni collegamenti ipertestuali per raggiungere altre pagine: si trattava di "link", il sistema principale su cui ancora oggi si basa l'architettura delle pagine web. Il primo server del web era quindi ospitato sul computer di Berners-Lee; suc-

1) Il CERN (Organizzazione Europea per la Ricerca Nucleare) è il più grande laboratorio al mondo di fisica delle particelle, ubicato al confine tra Svizzera e Francia, alla periferia ovest della città di Ginevra, nel comune di Meyrin.

cessivamente, nel marzo del 1991, i software necessari per usare il sistema del "World Wide Web" divennero disponibili anche per altre persone preso il CERN. Fu proprio nell'agosto di quell'anno che Berners-Lee annunciò pubblicamente la straordinaria invenzione del web.

1.2. La suddivisione del web, con un focus sul suo lato oscuro (il "dark web")

Dopo il breve inquadramento storico, passiamo ora a evidenziare le caratteristiche del web, concepito come un oceano di dati nel quale si possono fare una serie di distinzioni tra tutto ciò che c'è in superfice e quello che c'è sotto, in un "mondo virtuale sommerso".

Più in dettaglio, quella in superfice è la parte del web, denominata "*surface*" o "*clear*" web, che è scansionata e indicizzata[2] da motori di ricerca standard come Google, Bing, Yahoo o tramite altri normali browser. La quantità di informazioni contenute in tale "dimensione superficiale", benché sembri sconfinata, in realtà rappresenta solo il 4% dei contenuti che complessivamente girano sul *web*. Il restante 96% circola, infatti, nel c.d. "*deep web*", vale a dire in quella parte sommersa che ospita qualsiasi contenuto delle rete Internet che, per vari motivi, non può essere o non è indicizzato dai tradizionali motori di ricerca. Si tratta di un'area virtuale che include quindi pagine web dinamiche[3], siti bloccati (compresi quelli che chiedono per accedere di rispondere ad CAPTCHA[4]), siti non collegati, siti privati (come quelli che richiedono credenziali di accesso) e siti con contenuti in script[5]/ non in HTML. Non solo, ma anche quelle reti, ad accesso limitato, che coprono risorse e servizi che non sarebbero normalmente accessibili, ivi compresi tutti quei siti, con nomi di dominio registrati sul DNS (Domain

2) Vale a dire ricercabile.

3) Una pagina web dinamica è una pagina il cui contenuto, in tutto o in parte, è generato sul momento dal server, potendo dunque essere diversa ogni volta che viene richiamata e consentendo un'interattività con l'utente, secondo un paradigma di programmazione noto come "web dinamico".

4) Il "Completely Automated Public Turing-test-to-tell Computers and Humans Apart" è generalmente il test utilizzato quando si richiede all'utente di scrivere quali siano le lettere o i numeri presenti in una sequenza, che appare distorta o offuscata sullo schermo, ai fini di accedere ad una determinata pagina.

5) Pagine accessibili solo tramite link prodotti da JavaScript, con contenuti scaricabili in modo dinamico dai server web tramite Flash o Soluzioni AJAX.

Name System[6]), ma non gestiti dalla "Internet Corporation for Assigned Names and Numbers"[7] (ICANN). Conseguentemente per accedere alla pagina nella quale si vuole navigare è necessario conoscerne lo specifico URL[8].

Il vero boom nell'utilizzo del "*deep web*" è ascrivibile, temporalmente, al mese di giugno del 2003, allorquando l'informatico ed attivista statunitense Edward Snowden, ex tecnico della CIA, rivelò pubblicamente dettagli di diversi programmi di sorveglianza di massa del Governo statunitense e britannico, fino ad allora tenuti segreti.

All'epoca l'acquisita consapevolezza che la *privacy* di molti soggetti fosse stata violata per anni, indusse sempre più persone a cercare un modo per tutelarsi attraverso l'anonimato garantito dal "*deep web*": un ambito della rete amplissimo, nascosto dalla luce del sole, che costituiva terreno fertile per lo scambio di informazioni sensibili. Ed è per questo che iniziò ad essere usato dai giornalisti, specie quelli investigativi, mossi dalla necessità di confrontarsi su temi scottanti o da dissidenti politici per condividere informazioni sfuggendo ai controlli delle autorità di Governo.

Oggigiorno, la maggior parte di coloro che utilizzano la rete navigano inconsapevolmente in siti allocati nel "*deep web*", annoverandosi, tra questi, tutti quelli che richiedono un *login* e una *password* di accesso, come le pagine personali di home banking, le e-mail su web, le sezioni a pagamento dei siti di informazione, oppure le pagine che sono generate dinamicamente sulla base delle richieste degli utenti, come la risposta a un'interrogazione per la prenotazione di un viaggio aereo o di un soggiorno in un albergo.

Per immergersi nelle profondità della rete si possono utilizzare, a seconda degli obbiettivi, due principali metodi: utilizzare speciali motori di ricerca (come The WWW Virtual Library, Surfwax, IceRocket, ecc.), a cui si accede da browser regolari (come Internet Explorer, Firefox, Chrome, Safari, ecc.) conoscendo l'URL specifico oppure, in alternativa, sempre da motori di ricerca

---

6) In informatica e telecomunicazioni, il DNS ù un sistema utilizzato per assegnare nomi ai nodi della rete (in inglese host). Questi nomi sono utilizzabili, mediante una traduzione, di solito chiamata "risoluzione", al posto degli indirizzi IP originali.

7) L'"ICANN" è un ente di gestione internazionale (dal 2 ottobre 2016), istituito il 18 settembre 1998 per proseguire i numerosi incarichi di gestione relativi alla rete Internet che in precedenza erano demandati ad altri organismi. Tra i suoi compiti, figura quello di assegnare gli indirizzi IP.

8) Un "Uniform Resource Locator" (URL) è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa (che può essere un documento, un'immagine, un video), presente su un host server e resa accessibile a un client.

speciali (come Ahima o TorDi) ai quali si ha accesso però tramite browser che garantiscono l'anonimato quali TOR, I2P e Freenet (dei quali si parlerà più diffusamente nel paragrafo successivo).

Accade anche che, in alcuni casi, utenti che navigano sui normali motori di ricerca si trovino a interagire con una parte del "*deep web*", senza esserne a conoscenza. Proprio in quella parte del web, infatti, sono allocati database che sono disponibili al pubblico (come alcuni siti di librerie virtuali, quali ad esempio *findlaw.com*[9]), database a pagamento (come Westlaw[10] e LexisNexis[11]) o archivi di servizi di chat e servizi di sola sottoscrizione (presenti nella maggior parte delle biblioteche accademiche[12]).

Questo per dire che, contrariamente a quanto spesso ed erroneamente sostenuto, la parte nascosta della rete, il "*deep web*" appunto, non è il luogo della rete dove vige l'illegalità *sic et simpliciter*. Essa, infatti, è paragonabile a un vastissimo contenitore di dati al quale chiunque può accedere quotidianamente e lecitamente (come detto, anche per eseguire semplicemente operazioni di home banking).

Al suo interno, però, cela una porzione più "oscura" e "profonda", nella quale in effetti vengono condotte attività criminali di ogni genere; si tratta del "*dark web*" o delle "*darknet*": reti oscure criptate, vale a dire inaccessibili attraverso metodi di navigazione standard, in cui gli utenti possono scambiare in modo anonimo beni e servizi illeciti.

Si tratta, in altri termini, di un "*hidden space*", popolarmente noto come una piattaforma per attività di hosting illecite di vario genere (prima fra tutte, il commercio di droga e di armi, oggetto del presente elaborato), alla quale si accede principalmente (ma non solo) tramite il browser Tor (certa-

---

9) *FindLaw.com* è un sito web di informazioni legali gratuito che pubblica e rende consultabili gratuitamente alcune fonti della giurisprudenza statunitense, statuti statali e federali, un elenco di avvocati, notizie e analisi. Si rivolge ai consumatori, ai proprietari di piccole imprese, a studenti e professionisti del mondo giuridico relativamente ad aspetti di questioni legali quotidiane. Il servizio include un dizionario legale gratuito e "Writ", una rivista curata principalmente da accademici in materie giuridiche e aperta alla discussione con i lettori.

10) *Westlaw* è un servizio di ricerca legale *on-line* e un database per avvocati e professionisti legali disponibile in oltre 60 Paesi.

11) *LexisNexis* è una banca dati full-text in ambito giuridico e finanziario. La banca dati è strutturata come una biblioteca suddivisa in sezioni via via più specifiche.

12) Perfino l'elenco della biblioteca del Congresso degli Stati Uniti (*www.loc.gov*) è un database *on-line* che risiede nel "*deep web*".

mente il più noto), che attraverso la c.d. *onion routing* (del quale si parlerà più diffusamente in seguito) "crittografa" l'identità degli utenti in entrata e in uscita.

Figura 1 - "Surface", "Deep" e "Dark" web.

Il vasto mondo del web viene solitamente raffigurato come un iceberg: la punta visibile è solo il 4% (il "*surface web*"), mentre la parte sommersa è il restante 96% (il "*deep web*"). Della parte sommersa, una piccola porzione (la punta inferiore) ospita il "*dark web*".

Quanto sia grande il "*deep web*" è difficile se non addirittura impossibile saperlo; molti esperti ritengono che sia 400-500 volte più grande del "*surface web*"[13]. In realtà su questo argomento ci sono pareri contrastanti: non tutti sono d'accordo sul ritenere il "*deep web*" così ridondante rispetto al web di superficie.

Ciò su cui non sembrano esserci dubbi è, invece, che il "*dark web*" sia

13) Le pagine indicizzate da Google sono circa 30.000 miliardi (secondo un rilevamento riportato dal sito *ww.statisticbrain.com*, risalente all'anno 2014), per un totale di dati indicizzati di oltre 100.000.000 GB. Il volume di dati contenuti nel "*deep web*" ammonterebbe quindi a quest'ultimo numero moltiplicato per 400-500.

molto piccolo: si ritiene (ma è una stima molto approssimativa) che contenga non più di 100.000 siti, che rappresentano probabilmente meno dello 0,005% delle dimensioni dell'intero web.

Sempre con riferimento alla suddivisione del web, alcuni esperti fanno riferimento a *6 livelli*, vale a dire il:

– *web comune* (livello 0), cioè quello che utilizziamo tutti i giorni e che contiene siti totalmente accessibili come Facebook, Twitter, Youtube o sistemi di mail (Gmail, Libero, MSN, ecc.) o blog e forum;

– *surface web* (livello 1), dove operano i server informatici e siti come "*Reddit*"[14];

– *bergie web* (livello 2), ultimo accessibile senza particolari strumenti e conoscenze, che ospita risultati nascosti di Google e siti di video e immagini senza censure;

– *deep web* (livello 3), dove si entra solo usando software speciali e dove si trovano i canali di comunicazione degli hacker;

– *charter web* (livello 4), nei cui forum si muovono con disinvoltura hacker, trafficanti di armi e droga, jihadisti, estremisti e pornografi;

– *marianas web* (livello 5), che – secondo molti – comprenderebbe addirittura l'80% di Internet e dove sarebbe possibile trovare documenti storici di particolare rilevanza, oltre a piani segreti governativi[15].

Per concludere, volendo sintetizzare le caratteristiche delle varie aree del web, evidenziando gli aspetti tecnici di base da tenere presente nella conduzione di un'attività investigativa sui traffici in rete, si può affermare che:

– il "*clear web*":

- utilizza la tecnologia e i protocolli di comunicazione tipici di Internet, vale a dire l'IP (l'*Internet Protocol*[16], che – metaforicamente – è la

14) "*Reddit*" è un sito Internet di social news, intrattenimento e forum, dove gli utenti registrati (chiamati "*redditor*") possono pubblicare contenuti sotto forma di post testuali o di collegamenti ipertestuali (*link*). Gli utenti, inoltre, possono attribuire una valutazione, "*su*" o "*giù*" (comunemente chiamati in inglese "*upvote*" e "*downvote*"), ai contenuti pubblicati: tali valutazioni determinano, poi, posizione e visibilità dei vari contenuti sulle pagine del sito. I contenuti del sito sono organizzati in aree di interesse chiamate "*subreddit*".

15) Per accedere al "*marianas web*" si deve calcolare l'algoritmo "Polymeric Falcighol Derivation", operazione impossibile dai normali computer in uso, ma possibile solo con dispositivi potenti, in uso per esempio a strutture governative.

16) Un indirizzo IP è un'etichetta numerica che identifica univocamente un dispositivo detto *host* collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete.

targa dell'auto che tutti utilizziamo per navigare in rete), l'ISP (*Internet Service Provider*[17]) e il DNS (il *Domain Name System*[18], che è in pratica la "guida telefonica" di Internet che consente agli utenti di accedere alle informazioni *on-line* senza ricordare le stringhe degli indirizzi IP, ma semplicemente tramite dei nomi di dominio);

- è costituito da aree web pubbliche (liberamente accessibili);
- ospita un contenuto informatico indicizzato dai motori di ricerca;

– il "*deep web*":

- utilizza la stessa tecnologia e protocolli di comunicazione del "*clear web*" (quindi IP, ISP e DNS);
- ospita un contenuto informatico non indicizzato dai motori di ricerca;
- è costituito da aree web private, accessibili previa procedura di login e digitazione di password;

– il "*dark web*":

- utilizza tecnologia e protocolli di comunicazione diversi da quelli del "*clear*" e del "*deep web*" (in particolare, non utilizza il DNS);

Ci sono due versioni di indirizzi IP: IPv4 e IPv6. IPv4 è la versione standard attualmente utilizzata ed è composta da 4 serie di numeri separati da punti che vanno da 0 a 255. IPv6 è la versione più recente di un indirizzo IP ed è formata da 8 gruppi di 4 cifre esadecimali separati da due punti. Si parla, inoltre, di IP pubblico e privato: quello pubblico è un indirizzo visibile e raggiungibile da tutti gli *host* della rete Internet, mentre quello privato viene usato per identificare in modo univoco un dispositivo appartenente a una rete locale. Gli indirizzi IP privati quindi non possono essere utilizzati per l'accesso a Internet. Infine, gli indirizzi IP possono essere dinamici e statici.

I primi sono i più utilizzati e vengono impiegati per la normale navigazione on-line. Quando un utente si connette a Internet il suo Internet Service Provider gli assegna un indirizzo IP casuale che cambia dopo ogni sessione o a intervalli regolari (ogni 24 ore). Gli IP dinamici garantiscono una maggiore protezione della privacy degli utenti consentendo una navigazione più anonima.

Un indirizzo IP statico invece rimane invariato, tuttavia il proprietario può richiederne la modifica. Gli IP statici sono utilizzati principalmente nelle LAN (reti private) per comunicare, con una stampante o un altro computer della rete locale.

17) L'ISP è un fornitore di servizi Internet, vale a dire un'organizzazione o un'infrastruttura che offre agli utenti, dietro la stipulazione di un contratto di fornitura, servizi inerenti a Internet, i principali dei quali sono l'accesso al World Wide Web e la posta elettronica.

18) Il DNS è il sistema che regola la traduzione dei nomi dominio dei siti internet in indirizzi IP. Il suo compito è decodificare gli URL delle risorse web e metterle in relazione con i corrispondenti indirizzi IP.

- ospita contenuti non indicizzati dai motori di ricerca;
- è costituito da pagine accessibili tramite appositi software (tra questi, il più conosciuto è – come detto – il browser Tor).

1.3. La navigazione anonima con "TOR": la rete nascosta più nota

"Tor" è un protocollo e una rete di tunnel virtuali che permette a chiunque di nascondere la propria identità e migliorare la privacy e la sicurezza in Internet. Il progetto Tor (acronimo di "*The Onion Router*") è nato nel 1995 per merito della Marina militare degli Stati Uniti, allo scopo di garantire la riservatezza delle conversazioni governative (ordini e disposizioni d'impiego), sottraendole quindi all'eventuale intercettazione da parte di "entità nemiche" o da servizi d'intelligence stranieri. Il progetto, sviluppato dal 2002 dalla "*Electronic Frontier Foundation*" (quest'ultima sponsorizzata dalla "*US Naval Research Laboratory*"[19]) e reso di dominio pubblico nel 2006, è ora gestito da "*The Tor Project*", un'associazione senza scopo di lucro[20], che gode delle esenzioni fiscali che si applicano agli enti dedicati esclusivamente a fini religiosi, di beneficenza, scientifici, letterari o educativi. È inoltre finanziata da una pluralità di organizzazioni, tra le quali figurano anche istituzioni del Governo USA, quali "*DARPA*" ("*Defense Advanced Research Projects Agency*"[21]) e il "*Bureau of Democracy, Human Rights and Labor Affairs*"[22] del Dipartimento di Stato degli Stati Uniti, che – peraltro – è uno dei maggiori sostenitori del progetto.

Prima di approfondire il funzionamento della rete Tor da un punto di vista squisitamente informatico, è necessario precisare che il suo utilizzo non è di per sé illegale. In altri termini, le condotte illecite non derivano dalla semplice volontà di operare in rete mantenendo l'anonimato e la riservatezza delle

19) Lo "*United States Naval Research Laboratory*" (NRL, in italiano laboratorio di ricerche navali statunitense) è il laboratorio di ricerca della United States Navy e dello United States Marine Corps. Si trova a Washington e fu fondato nel 1923. Conduce programmi di ricerca scientifica e di sviluppo tecnologico avanzato.

20) È diretta da Bruce Schneier, crittografo e tecnologo della sicurezza di fama mondiale. Il suo blog "Schneier on Security" è tra i più noti e letti sui temi della Cybersecurity.

21) È un'agenzia governativa del Dipartimento della difesa degli Stati Uniti incaricata dello sviluppo di nuove tecnologie per uso militare.

22) L'Ufficio è sotto la competenza del Sottosegretario di Stato per la sicurezza civile, la democrazia e i diritti umani e si occupa sostanzialmente della promozione della democrazia in tutto il mondo, della formulazione di politiche sui diritti umani e del coordinamento delle politiche sulle questioni lavorative legate ai diritti umani.

comunicazioni (utilizzando quindi il browser Tor), ma scaturiscono dall'interazione con i mercati illegali (i c.d. "*black market*", il cui funzionamento verrà in seguito approfondito), che avviene nel "*dark web*" e proprio attraverso la navigazione con reti anonime, quali appunto Tor.

Nel sito del progetto Tor (liberamente accessibile[23]), i gestori – nel precisare che "*Tor è più di un semplice software: è il lavoro d'amore prodotto da una comunità internazionale di persone devote ai diritti umani*" – affermano che "*... tutte le persone che sono state coinvolte in Tor sono unite da un credo comune*… [vale a dire che]… *gli utenti di Internet dovrebbero avere un accesso privato ad un web senza censura*...". Sottolineano, a tal fine, di "*combattere ogni giorno perché tutti possano ottenere un accesso privato ad un Internet senza censure*"[24].

L'anonimizzazione delle comunicazioni garantita dalle *onion routing* non caratterizza, quindi, solo i mercati illegali e le attività criminali[25], ma anche quei siti in cui, ad esempio, la garanzia dell'anonimato è necessaria per poter usufruire in alcuni Paesi degli stessi servizi offerti dalla rete, altrimenti non accessibili poiché "*bannati*"[26]. Esistono, ad esempio, le versioni *.onion* (ospitate quindi nel dark web) di siti famosi, quali il "The New York Times"[27], la "BBC News"[28] e addirittura "Facebook"[29].

Inoltre, chiunque può navigare nel dark web mediante il browser Tor,

---

23) Sito: *www.torproject.org*.

24) Sul sito viene inoltre riportato, all'apertura della Homepage, lo *slogan*: "*Naviga in Privato. Esplora liberamente. Difenditi contro tracciamento e sorveglianza. Evita la censura"*. Vengono, inoltre, esplicitate le finalità di Tor, che consistono, in particolare, nel garantire l'anti-tracciamento ("*... isola ogni sito che visiti, così i tracciatori e gli ad di terze parti non possono seguirti. Qualunque cookie verrà automaticamente cancellato quando hai finito di navigare. Così come la cronologia*") e nella difesa contro la sorveglianza ("… *impedisce ad un estraneo di controllare la tua connessione per conoscere quali siti visiti*...").

25) In alcuni Paesi con regimi autoritari, viene utilizzata anche per permettere a gruppi di opinione, a dissidenti o ad attivisti politici di comunicare tra loro, senza rischiare di essere controllati ed intercettati dalle autorità di Governo e dalla polizia.

26) Il termine *ban* (derivato dalla lingua inglese, in italiano è traducibile con "*bandire*" o "*interdire*") viene utilizzato per riferirsi ad una serie di atti che consente di vietare l'accesso e/o l'interazione con gli altri ad un determinato utente tramite la sua username, il suo indirizzo IP o e-mail.

27) Con l'indirizzo *https://www.nytimes3xbfgragh.onion*, esiste dal 2017 e funziona esclusivamente con il browser Tor.

28) Presente nel dark web con l'indirizzo *https://www.bbcnewsv2vjtpsuy.onion*.

29) Nella versione mobile all'indirizo *https://m.facebookcorewwwi.onion*, esiste dal 2014 e sembra che sia il sito web più visitato dagli utenti di Tor.

scaricabile gratuitamente dal sito del progetto[30] (è disponibile in 30 lingue diverse e per tutti i sistemi operativi; da qualche anno, anche per gli smartphone[31]), tenendo presente che utilizzando Tor è possibile anche visitare siti dell'open web, ottenendo di fatto l'anonimato nella navigazione (viceversa, non è possibile navigare nel dark web – vale a dire accedere a siti *.onion* – attraverso browser classici, quali Chrome, Safari o Firefox).

1.3.1. Utilizzo nel mondo di Tor browser, con uno sguardo all'Italia

Come accennato, Tor è certamente la rete anonima più popolare e conosciuta, se si considera che è utilizzata – in tutto il mondo – da oltre 750.000 utenti Internet ogni giorno. Oltre la metà degli utenti Tor si trova in Europa, dove questo servizio è utilizzato da una media di 80 utenti ogni 100.000.

Analizzando il dato riferito all'Italia, in realtà il numero di utente Tor ha fatto registrare nel decennio 2010-2020 un costante decremento, partendo da un boom iniziale che risale agli anni 2012-2013.

Da un primo studio condotto dalla Oxford University ("*The anonymous internet*", sintetizzato nella figura sottostante), era infatti emerso che, tra agosto 2012 e luglio 2013, in Italia erano stati registrati oltre 76.000 utenti al giorno (circa un quinto dell'intera base di utenti giornalieri Tor europei; in pratica il nostro Paese era risultato secondo solamente agli Stati Uniti, che in quel periodo contava oltre 126.000 utenti al giorno).

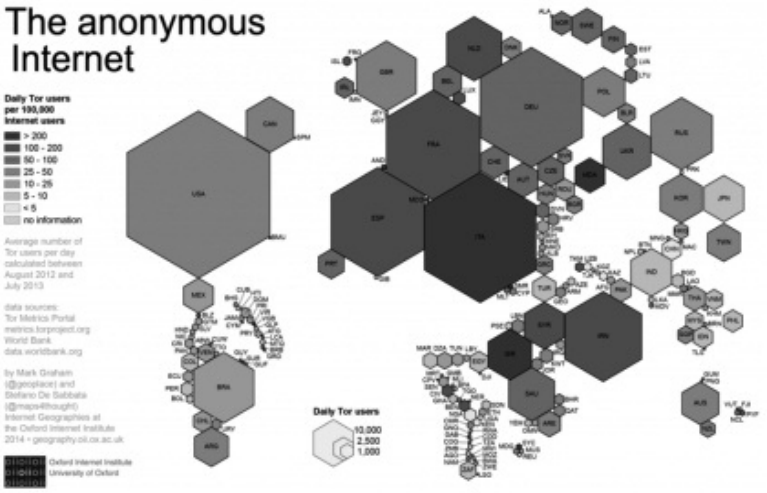
In realtà, il boom iniziale di utilizzo di Tor che ha riguardato l'Italia appare di dimensioni molto più vaste se si prendono in esame i dati che sono stati estrapolati dal sito "*Tor Metrics*"[32], dalla cui analisi (vds. grafico sottostante) emerge:

– un picco verso l'alto registrato negli ultimi mesi del 2013, con oltre 225.000 utenti al giorno. Il dato è compatibile con quello dello studio della

30) L'installazione del browser è molto semplice ed è assistita da un tutorial sul sito del progetto.

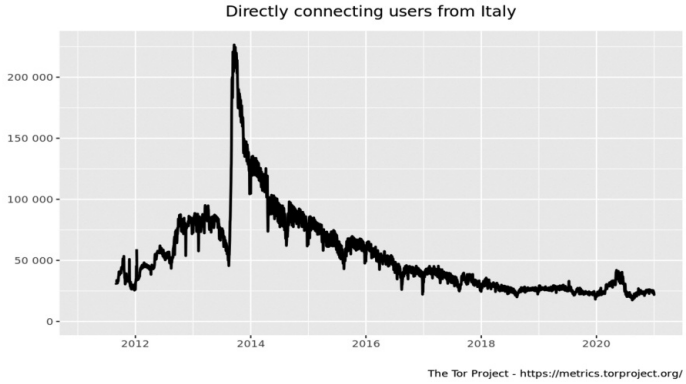
31) Per il sistema operativo Android esiste l'applicazione ufficiale Tor Browser, che è possibile scaricare dal sito Tor Project come file *.apk*, oppure più semplicemente dall'applicazione "Google Play Store". Non è invece presente una *app* ufficiale per iPhone, anche se sul sito Tor Project, nella pagina dedicata al sistema Android, viene consigliata l'applicazione "Onion Browser", che può essere scaricata direttamente dall'indirizzo *https://apps.apple.com/it/app/onion-browser/id519296448*.

32) Indirizzo: *https://metrics.torproject.org*. Il sito consente di verificare – in tempo reale – il traffico informatico sulla rete Tor.



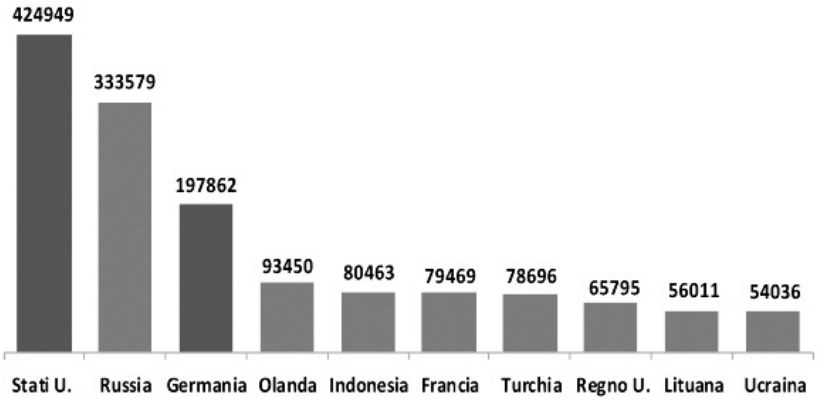
Oxford University (che segnalava oltre 76.000 utenti al giorno riferiti ad un arco temporale di poco antecedente, ovvero sino a luglio 2013), se si prende per buono il concetto che quest'ultimo studio fotografava solo l'inizio della diffusione in Italia del protocollo;

– un costante decremento negli anni successivi al 2014, sino a giungere ai circa 25.000 utenti al giorno rilevati nei primi mesi del 2021.



Inoltre, sempre analizzando il traffico su "*Tor Metrics*", emerge (vds. tabella sottostante) che, negli ultimi 3 mesi[33], tra i 10 Paesi con il numero maggiore di utenti giornalieri non figura l'Italia. In particolare, al primo posto figurano gli Stati Uniti (con oltre 400.000 utenti), seguiti dalla Russia e dalla Germania (primo Paese europeo con quasi 200.000 utenti).

33) Il periodo preso in esame va dal 27 novembre 2020 al 25 febbraio 2021.



In merito, occorre considerare come, se da un lato l'iniziale boom nell'utilizzo di Tor appaia facilmente comprensibile (si trattava, in quel periodo, di uno strumento informatico che consentiva, come d'altronde consente oggi, un approccio anonimo a un fenomeno all'epoca nuovo, quello della vendita di prodotti e servizi illeciti in rete, e in particolare droga e armi, mediante i c.d. *black market*), dall'altro, molto meno comprensibile risulti il costante decremento del numero di utenti Tor, soprattutto se letto in relazione alla contestuale crescita esponenziale del fenomeno degli *shops on-line* illegali. Unica spiegazione plausibile potrebbe essere lo sviluppo, nel corso degli anni, di altre reti anonime (si parlerà in seguito, ad esempio, della rete I2P), che offrirebbero maggiori garanzie di sicurezza anche rispetto alle modalità di contrasto nel frattempo messe a punto, in tutto il mondo, dalle forze di polizia.

1.3.2. Funzionamento del software. La "onion routing"

Passando ora al funzionamento della rete Tor, il primo aspetto squisitamente informatico da evidenziare è che si tratta di un network decentralizzato, costituito da migliaia di server chiamati "relay" (sempre dalla consultazione del sito "Tor Metrics", alla data del 25 febbraio 2021, risultavano complessivamente attivi nel mondo quasi 7000 relays[34].

34) Anche questo dato può essere estrapolato in tempo reale. Negli ultimi due anni, il numero di relays è oscillato tra i 6.000 e gli 8.000 con un solo calo al di sotto della citata media registrato verso la fine del 2019 (con poco più di 5.500 relays). Il numero dei server è invece aumentato in maniera costante, sempre nell'intervallo 6-8 mila, dai primi mesi del 2020, verosimilmente anche in conseguenza dell'emergenza pandemica che ha comportato l'utilizzo sempre più ampio di strumenti informatici, ivi comprese le reti anonime.

I dati di navigazione non transitano direttamente dal client al server, come accade per la navigazione normale, ma passano proprio attraverso i relays (chiamati anche "nodi"), che agiscono da router, realizzando un circuito virtuale crittografato a strati (come una "cipolla"; da qui il nome onion router e il motivo per cui gli URL[35] della rete Tor hanno il TLD[36] che non è il classico *.com* o *.it*, ma *.onion*).

Avviando la navigazione con Tor (che, come verrà in seguito illustrato, può essere ottenuto da chiunque, scaricandolo liberamente dal relativo sito), il browser sceglie dall'elenco "directory server" una lista di nodi e da questa lista ne individua almeno 3 in modo casuale, costituendo di fatto una catena di navigazione[37]. In ciascun passaggio la comunicazione viene crittografata e questo si ripete per ciascun nodo (a strati, proprio come la cipolla). Per di più, ogni nodo della rete può conoscere solo il nodo precedente e quello successivo, ma non gli altri, motivo per cui è pressoché impossibile (o comunque molto complicato) risalire al client di partenza.

I tre nodi che costituiscono la configurazione standard minima del sistema di navigazione Tor assumono la denominazione di "guard", "middle" ed "exit" relays.

Come detto, il traffico Tor, per ragioni di sicurezza, passa attraverso almeno 3 relays prima di raggiungere la sua destinazione. Il primo nodo, vale a dire il "guard" (o anche "entry") relay trasmette il traffico al secondo nodo, il "middle" relay (intermedio), che a sua volta lo trasmette all'"exit" relay. I relays intermedi sono visibili solo all'interno della rete Tor e, a differenza del relay d'uscita, non fanno apparire il proprietario del nodo che costituisce la fonte del traffico. Ciò significa che il relay intermedio è generalmente quello più sicuro. Il relay di uscita è l'ultimo nodo che il traffico Tor attraversa prima di raggiungere la sua destinazione. Pertanto, i servizi a cui i client Tor si connettono (sito web, servizio di chat, provider di posta elettronica, ecc.) visualizzano esclusivamente l'indirizzo IP del nodo di uscita e non quello del reale utente. In altri

35) Come già detto, l'"Uniform Resource Locator" (in acronimo URL) è la sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete di computer.

36) Il dominio di primo livello, in inglese top level domain (TLD), è l'ultima parte del nome di dominio Internet. Corrisponde alla sigla alfanumerica che segue il "punto" più a destra dell'URL.

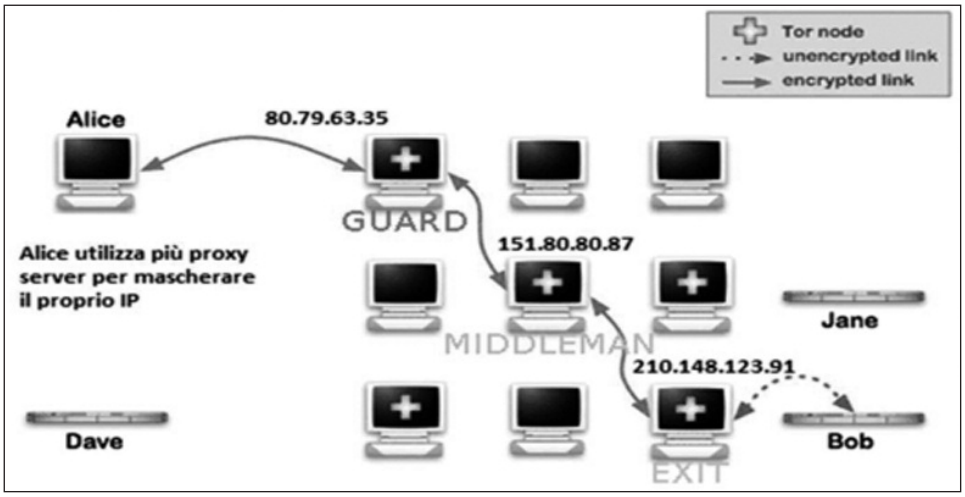
37) Nella pagina del browser si può vedere – in tempo reale – il percorso che viene fatto ed anche cambiarlo con il pulsante che si trova alla sinistra della barra dell'URL. Non è però possibile scegliere personalmente i relays, ma solo fare in modo che Tor ne individui altri tre differenti.

termini, nella catena di navigazione l'indirizzo IP del nodo di uscita (che non corrisponde al reale client) viene interpretato come la fonte del traffico.

Oltre all'*anonimato* dei soggetti che intervengono nella navigazione, la rete Tor si caratterizza anche per la *riservatezza* delle informazioni che veicola. Durante il percorso all'interno della rete, infatti, il traffico è completamente criptato. L'"entry" relay conosce l'indirizzo IP sorgente dell'informazione da trasmettere (in altri termini, il Tor client), ma non conosce il tenore dell'informazione che trasmette. L'"exit" relay, invece, può esclusivamente leggere il traffico in uscita (se non è criptato), ma non conosce chi glielo ha trasmesso (vale a dire il "middle" relay).

Sintetizzando, il funzionamento della rete Tor, pur apparentemente complesso, è in realtà concettualmente semplice: i dati che appartengono a una qualsiasi comunicazione non transitano direttamente dal client al server[38], ma passano attraverso i server Tor che agiscono da router costruendo un circuito virtuale crittografato a strati (a cipolla).

La figura sottostante, attraverso un percorso esemplificativo, aiuta a comprendere meglio il funzionamento della rete Tor, con particolare riferimento al requisito dell'*anonimato*.



Osservando la figura, supponiamo che Alice voglia inviare a Bob e a Jane dei messaggi. Normalmente il client provvede a dividere il messaggio in pacchetti, a numerarli e ad inserire in ognuno di essi il destinatario ed il ser-

38) In una rete informatica, il client è costituito da ogni computer collegato al server e in grado di scambiare dati con esso, mentre il server è un computer di elevate prestazioni che in una rete fornisce un servizio agli altri elaboratori collegati (detti appunto client).

vizio richiesto. In questo modo, però, chiunque riceve il pacchetto è perfettamente in grado di individuare subito il destinatario e quindi di decidere di non provvedere ad inviare a Bob e a Jane i pacchetti ad essi destinati, cestinandoli tutti. Per aggirare l'ostacolo Alice decide, quindi, di ricorrere alla rete TOR. Installa, pertanto, il browser Tor diventando di fatto un nodo della rete. A questo punto il client Tor di Alice contatta un particolare server di Tor, detto "directory server", per ottenere la lista di tutti i relays della rete Tor (nella figura indicati con il segno verde +). Il primo router della rete Tor che riceve i pacchetti di Alice è – come detto – il "guard node" (nodo di guardia), il secondo è il "middleman node" (nodo intermediario) e il terzo l'"exit node" (nodo di uscita)[39]. Tutti i relays Tor provvedono a registrarsi sul "Directory server" inviando ad esso il proprio indirizzo IP. L'"exit node", inoltre, deve dichiarare quali destinatari è in grado di raggiungere. Il client di Alice, analizzando la lista di tutti i relays della rete TOR inviatagli dal "Directory server", costruisce una catena di nodi che gli consentiranno di raggiungere il destinatario Bob. La rete di navigazione Tor a questo punto è configurata.

Sempre osservando la figura, si nota che i nodi sono collegati da frecce verdi, colore che indica una comunicazione crittata, realizzata per impedire a un attaccante di ricostruire il flusso intercettando un singolo messaggio. L'ultimo collegamento, invece, è di colore rosso perché, a questo punto della navigazione, si esce dalla rete Tor (si ipotizza, ad esempio, di aver richiesto una pagina web servita tramite protocollo http). In pratica, nell'ultimo tratto della navigazione si perde l'informazione che il pacchetto è transitato per la rete Tor: il destinatario Bob crede di aver ricevuto la richiesta dall'"exit node" e non dal mittente originario Alice, del quale – durante la navigazione – si è perso qualsiasi informazione.

Un altro metodo per comprendere come il protocollo Tor si sottragga ad eventuali analisi del traffico, consiste nell'utilizzare le immagini sottostanti di una cipolla "sbucciati a strati".

Strato 1

Strato 2

Strato 3

39) Vedendo la figura, si intuisce che i punti più vulnerabili della catena sono il nodo *guard* ed il nodo *exit*. Per tale motivo, tali nodi devono meritarsi questo status servendo la rete Tor per un lungo periodo come nodi *middleman*.

I pacchetti che Alice invia al primo router della rete Tor (il "guard node") può essere paragonato a una cipolla il cui contenuto è cifrato a strati. Per un provider che analizza il traffico, quei pacchetti hanno come destinazione l'indirizzo IP del "guard node" a cui viene chiesto un certo servizio il cui contenuto è crittografato. Non vi è traccia dell'effettivo destinatario Bob. "Guard", il primo router della rete TOR, è l'unico in grado di leggere il contenuto della buccia rossa (*strato 1*) disponendo, in via esclusiva, della chiave per decifrarlo. Leggendo le istruzioni contenute in questo primo strato, "Guard" sa di dover inoltrare tutto il resto del contenuto del pacchetto a "Middleman", router immediatamente successivo della rete TOR, unico in grado di leggere il contenuto della buccia verde (*strato 2*) e di individuare così il destinatario immediatamente successivo. È evidente che, già a questo livello, si è persa ogni informazione relativa ad Alice, reale proprietario del pacchetto. Il router "Middleman" della rete TOR, infatti, sa solo di aver ricevuto una richiesta dal router "Guard", ignorando l'effettivo mittente Alice. Infine, il router "Exit" riceve da "Middleman" le informazioni dello strato celeste della cipolla (*strato 3*). Decifrandola con la sua chiave privata, potrà leggerne il contenuto e provvedere a richiedere al server Bob una pagina web. Bob, ricevuta la richiesta, provvederà a sua volta a rispondere a "Exit", che a sua volta lo rigira a "Middleman", il quale la inoltra a "Guard", che chiuderà il circuito inviando la risposta al legittimo proprietario Alice.

In definitiva, il protocollo usato nella rete Tor, tenendo celati contenuto, mittente e destinatari dei pacchetti, impedisce l'analisi del traffico. Inoltre, per impedire che il contenuto della risposta possa essere letta da uno dei nodi del circuito, la comunicazione viene protetta da una chiave di sessione, modificata frequentemente, apribile solo ad opera del mittente Alice.

La topografia della rete Tor è infine completata dai c.d. "bridges" (ponti). Per comprendere a cosa servono i "bridges" è necessario evidenziare che la struttura della rete Tor prevede che gli indirizzi IP dei relays siano pubblici, requisito quest'ultimo che offre la possibilità di bloccarli inserendo in apposite blacklist gli indirizzi IP dei nodi[40]. Ed è proprio per eludere tale censura che si ricorre all'uso dei bridges, che non sono invece elencati pubblicamente e che consentono, bypassando i nodi bloccati, di non interrompere il flusso informatico.

Per come sinora descritta, la rete Tor può sembrare dal funzionamento complesso e difficilmente comprensibile. Proviamo, pertanto, tralasciando gli

40) L'uso dei *bridges* è diffuso in alcuni Paesi, quali la Cina, la Turchia e l'Iran, che bloccano sistematicamente gli indirizzi IP di tutti i relays Tor elencati pubblicamente.

aspetti squisitamente informatici che ne connotano l'utilizzo, a riassumerne in poche parole le caratteristiche che più interessano in relazione all'argomento del presente elaborato, vale a dire il traffico on-line di armi e droga.

Il browser Tor essenzialmente garantisce *connessioni anonime in uscita*, negoziando un circuito virtuale attraverso i nodi, fino alla destinazione finale. In tale circuito, la crittografia garantisce non solo l'impossibilità di conoscere l'origine o la destinazione della connessione, ma anche la riservatezza delle comunicazioni.

In pratica, un venditore – utilizzando la rete Tor – è certo che, in linea di massima, non è possibile risalire all'indirizzo IP della macchina che egli utilizza, né tantomeno risalire alle comunicazioni scambiate con l'acquirente, che rimangono inaccessibili.

1.4. Le altre reti nascoste più utilizzate: I2P, FREENET e VPN

Una seconda via di accesso al *dark web* è la rete anonima denominata I2P, più recente (è nata nel 2003), ma meno usata poiché più complicata da configurare, anche se garantisce un livello maggiore di sicurezza rispetto alla rete Tor.

Il modello usa comunicazioni P2P (Peer-to-Peer), basandosi quindi su un'architettura informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi ("clienti" e "serventi"), ma anche sotto forma di nodi equivalenti o paritari (peer), potendo fungere al contempo da client e da server verso gli altri nodi terminali (host) della rete.

Tutti i messaggi vengono trasmessi attraverso i cosiddetti "tunnel". Un tunnel è una connessione virtuale crittografata unidirezionale che utilizza in genere due, tre oppure quattro peer. A differenza di Tor, anche il router I2P che cerca di creare un tunnel fa parte del tunnel stesso. All'avvio ogni router I2P crea alcuni tunnel per il traffico in entrata, chiamati inbound tunnel e alcuni per il traffico in uscita, chiamati outbound tunnel. Il primo peer di un tunnel è chiamato gateway tunnel mentre l'ultimo è detto endpoint tunnel. Per i tunnel in uscita, il router I2P che ha istituito il tunnel è sempre il gateway tunnel. Invece, per i tunnel in entrata, il router I2P che ha istituito il tunnel è sempre l'endpoint tunnel. La quantità e la lunghezza predefinite dei tunnel possono essere specificate dall'utente nelle impostazioni I2P, tenendo presente che i tunnel più lunghi aumentano l'anonimato, diminuendo però le prestazioni e viceversa. Un'applicazione non è associata ad un tunnel specifico e può utilizzare tunnel diversi per inoltrare i messaggi. I messaggi crittografati inviati da un peer attraverseranno prima il proprio outbound tunnel e poi l'inbound

tunnel del destinatario. Per questo motivo ogni peer deve mantenere sia un tunnel in ingresso che un tunnel in uscita, non essendo tali tunnel bidirezionali.

All'interno della rete I2P, non vi sono limiti al modo in cui le applicazioni possono comunicare e i contenuti inviati sono criptati tramite 3 strati di crittografia: la "garlic" che verifica la consegna del messaggio al destinatario, la "crittografia tunnel" che interessa tutti i messaggi che passano attraverso un tunnel e la "crittografia del livello di trasporto" tra i router. Proprio in ragione di questa ampia funzione di crittografia, la rete è ritenuta molto affidabile e sicura per navigare anonimamente nei black markets.

Anche la rete I2P, che risulta comunque più veloce della rete Tor, è di libero accesso attraverso lo specifico browser scaricabile dal sito del progetto e gli hidden services hanno il suffisso *.i2p*.

Come la rete I2P, anche la darknet "Freenet" permette l'accesso al *dark web*. Si tratta di un'ulteriore rete pubblica, nata attorno all'anno 2000, il cui funzionamento è basato su un immagazzinamento di informazioni informatiche "a pezzi" che rende difficilissimo (quasi impossibile) capirne il contenuto. I file vengono inseriti in un database distribuito, per poi essere spezzettati e allocati in più computer (nodi) della rete, nonché salvati in diverse copie. Una chiave di cifratura, che viene consegnata al momento dell'inserimento nel database, permette il successivo recupero dei file che vengono scaricati attingendoli dai vari nodi in cui sono stati immagazzinati in maniera frammentata (ogni nodo permette di scaricare il pezzo di file che aveva precedentemente immagazzinato).

Per la rete Freenet, pertanto, la riservatezza è garantita dalla sua stessa configurazione; è infatti evidente che in una simile architettura di rete è impossibile controllare il contenuto di ciò che è stato immesso, come pure rimuoverlo (il file, di fatto, diventa "incensurabile").

Esiste, infine, anche un rete privata per la navigazione anonima, denominata VPN (Virtual Private Protocol), che costituisce un'alternativa per proteggere i propri dati e mantenere la privacy on-line. Senza entrare a fondo in dettagli tecnici, è sufficiente evidenziare che si tratta di una rete privata[41] che collega il PC in modalità remoto ad un server per mezzo di tunnel sicuri. Le

41) È nata per uso aziendale, per consentire al personale esterno di connettersi alla rete aziendale in sicurezza. Il suo uso è poi stato esteso anche ai privati. Le VPN hanno caratteristiche che possono variare da fornitore a fornitore: solitamente sono a pagamento, ma esistono anche VPN gratuite. Tuttavia, come spesso accade, sono i prodotti a pagamento ad offrire le prestazioni migliori. Inoltre, possono essere istallate su qualsiasi sistema operativo ed anche da su smartphone.

informazioni inviate sono sicure in quanto sono criptate e protette da un firewall che fa da scudo tra PC e server ed ha la funzione di bloccare un malware (software malevolo) ovvero qualsiasi altro tentativo di intercettazione.

Esistono, per concludere, tre diverse tipologie di VPN denominate:

– *trusted*, rete che offre la garanzia che nessun terzo non autorizzato possa usufruire del circuito del cliente. Per usare una VPN del genere è necessario che l'utente abbia un proprio indirizzo IP fisso e applichi una corretta politica di sicurezza delle informazioni;

– *secure*, rete più comune e costruita utilizzando la cifratura dei dati. Consente, quindi, di trasmettere dati su Internet senza che questi vengano intercettati;

– *hybrid*, particolare tipologia di rete privata in cui una Secure VPN viene utilizzata come parte di una Trusted VPN.

1.5. Il protocollo Bitcoin: la criptovaluta più conosciuta

Come accennato, nei portali di e-commerce, noti come "black market", attivi nel *dark web*, le transazioni avvengono nella maggior parte dei casi attraverso l'utilizzo delle criptovalute (valute digitali), che consentono pagamenti anonimi (o comunque "pseudo-anonimi", come verrà in seguito spiegato).

L'utilizzo delle criptovalute nelle dinamiche di criminalità organizzata e non è certamente argomento complesso, dalle molte sfaccettatura sia squisitamente tecnico-informatiche che economiche. Pertanto, nel presente elaborato, ci si limiterà a fornire alcune coordinate di riferimento, mettendo in relazione la valuta digitale con i traffici *on-line* di droga e armi. A tal fine, l'attenzione verrà immancabilmente rivolta al protocollo certamente più utilizzato in quegli ambiti criminali, ossia Bitcoin[42], al quale, come verrà evidenziato, ne sono seguiti altri, che ne hanno costituito semplicemente un'implementazione.

Inoltre, si focalizzerà l'attenzione solamente sulla strutturazione e sul funzionamento delle criptovalute (tralasciando quindi altri aspetti quali la regolamentazione giuridica dell'uso di tale strumento quale mezzo di pagamento o le attività criminali legate al riciclaggio), volendone in questa sede esaltare esclusivamente la caratteristica dell'anonimato nelle transazioni.

Il punto di partenza nella comprensione di tale strumento finanziario

42) Con l'iniziale maiuscola il termine descrive il protocollo (o la rete) sul quale si regge la moneta virtuale. Con l'iniziale minuscola, invece, il termine viene riferito alla moneta stessa, vale a dire all'unità di conto.

non può che essere la definizione wdi valuta digitale introdotta dal legislatore[43], che ne sintetizza le caratteristiche fondamentali: "… *rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*"[44].

Trattasi, dunque, di un genere di valuta esistente solo in forma digitale[45]: non viene immessa in circolazione da un ente erogatore, ma viene creata e sviluppata esclusivamente attraverso un protocollo informatico[46]. Il suo valore non è ancorato a un bene materiale di riferimento (come l'oro), ma viene determinato esclusivamente dal numero di monete in circolazione per il numero di relativi possessori.

Il termine criptovaluta è derivazione dell'inglese "cryptocurrency". È in pratica l'unione di "cryptography" (crittografia) e "currency" (valuta), vale a dire una rappresentazione digitale di valore basata sulla crittografia, in grado di offrire un ottimo livello di privacy, variabile a seconda del protocollo utilizzato[47].

L'idea della criptovaluta venne esposta per la prima volta nel 1998 da Wei Dai[48] nella mailing list cypherpunks[49]. La prima implementazione con-

---

43) D.lgs. 25 maggio 2017, n. 90, che ha modificato il d.lgs. 21 novembre 2007, n. 231.

44) La definizione permette di stabilire una netta e decisiva differenziazione con la moneta elettronica, descritta dal TUB (Testo Unico Bancario) come: "*il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento (...) e che sia accettato da persone fisiche e giuridiche diverse dall'emittente*".

45) Non hanno corso legale in quasi nessun angolo del pianeta e dunque l'accettazione come mezzo di pagamento è su base volontaria

46) Sono generalmente emesse e controllate dall'ente emittente secondo regole proprie, a cui i membri della comunità di riferimento accettano di aderire. In realtà, ci sono Stati che hanno deciso di sperimentare, sotto il proprio controllo, l'utilizzo di moneta virtuale nei propri Paesi (es. l'Uruguay con l'e-peso) o ne hanno annunciato il loro utilizzo senza che però si abbiano maggiori informazioni al riguardo (es. il Venezuela con il Petro) o, ancora, che abbiano in cantiere iniziative al riguardo (es. Estonia e Svezia).

47) È totale, per esempio, per quelle criptovalute che utilizzano il sistema di validazione "zero knowledge", grazie al quale non viene scambiata nessuna informazione delle parti ("Monero" e "Zcash" sono due criptovalute che possiedono tale tecnologia).

48) Wei Dai è un ingegnere informatico noto per i contributi alla crittografia e alle criptovalute. Ha sviluppato la libreria crittografica Crypto++, creato il sistema di criptovaluta b-money e co-proposto l'algoritmo di autenticazione dei messaggi VMAC.

49) Il "cypherpunk" era un gruppo ristretto ma tecnicamente attrezzato, che in quegli anni stava mettendo a punto le tecnologie necessarie proprio per creare denaro digitale, generato elettronicamente e protetto da crittografia.

creta di tale idea giunse, però, nel 2009 quando un utente noto con lo pseudonimo di Satoshi Nakamoto pubblicò, in un mailing list sulla crittografia, le prime specifiche di programmazione e la bozza del progetto Bitcoin[50]. Intorno alla fine del 2010, Satoshi lasciò il progetto (affermando di volersi dedicare ad altro), senza mai rivelare la sua identità, né le motivazioni che lo avevano indotto a rendere open source un protocollo di tale rilevanza[51].

Dal 27 settembre 2012 la standardizzazione del protocollo, la sua protezione e la sua promozione sono gestite dalla Bitcoin Foundation[52].

1.5.1. Gli elementi essenziali: il wallet, la blockchain e il "mining"

Passando alla strutturazione di Bitcoin, occorre subito evidenziare che il protocollo elimina la necessità di ricorrere a enti finanziari tradizionali per la produzione e per la gestione della valuta attraverso tre componenti: il "wallet", il "block chain" e il "mining".

Il "*wallet*" è un portafoglio virtuale indispensabile ai fini dell'utilizzo della valuta. Esso contiene *due chiavi*, una *pubblica*, che identifica univocamente il wallet e funge da indirizzo (è simile all'IBAN di un conto corrente bancario), e una *privata* (segreta), che consente al titolare del portafoglio di

---

In realtà, già nel 1996, Alan Greenspan, economista allora a capo della Federal Reserve, la banca centrale statunitense, aveva lanciato l'idea che il denaro, grazie alla rivoluzione di Internet, potesse venire sottratto al monopolio degli stati ed essere emesso anche da soggetti privati.

Successivamente, nel 1999, l'autore cyberpunk Neal Stephenson pubblicò Cryptonomicon, romanzo di grande successo nell'ambiente hacker, in cui veniva immaginato un mondo sotterraneo alimentato da una sorta di oro digitale, che permettesse alle persone di mantenere private le loro identità grazie a un complesso sistema di crittografia in grado di rendere un messaggio comprensibile solamente al suo destinatario.

50) L'emissione della moneta era data da un software creato appositamente da Nakamoto stesso. Questo software lavorava e funzionava solo in una rete P2P (peer-to-peer). Come già suggerisce il termine, che tradotto in inglese significa "da pari a pari", una rete di questo tipo è costituita da computer posti gerarchicamente sullo stesso livello. In una rete P2P non c'è un computer che comanda, ognuno assume lo stesso valore e lo stesso potere. In questo modo tutti i computer di questa rete, che utilizzavano il software di Nakamoto, di fatto, emettevano la moneta.

51) Le speculazioni economiche susseguitesi negli anni hanno fomentato le teorie secondo cui dietro lo pseudonimo Nakamoto si sarebbe in realtà celato un collettivo di *trader*.

52) La Bitcoin Foundation è una società senza scopo di lucro americana. È stata fondata nel settembre 2012 per cercare di ripristinare la reputazione di Bitcoin dopo diversi scandali e per cercare di promuoverne lo sviluppo e la diffusione.

disporre della criptovaluta che sullo stesso viene depositata o inviata. Il sistema della doppia chiave è denominata "crittografia asimmetrica" e merita alcune precisazioni per meglio comprenderne il funzionamento.

La coppia di chiavi (pubblica e privata) è legata matematicamente da una funzione che assicura che un messaggio criptato con una delle due chiavi possa essere decifrato solo dall'altra. A titolo esemplificativo, se il soggetto "A" vuole inviare un documento di testo (o, come interessa in questa sede, un certo quantitativo di criptovaluta) al soggetto "B", facendo in modo che solo quest'ultimo possa essere in grado di leggere il contenuto di tale documento, deve crittografare asimmetricamente il dato servendosi della chiave pubblica fornitagli dal soggetto "B" per criptare il suo messaggio. A questo punto, il documento così criptato non è più decifrabile da "A", poiché non è in possesso della chiave privata di "B", conosciuta solo da quest'ultimo.

Il soggetto ricevente il documento crittografato sarà in grado di decifrarlo unicamente utilizzando la sua chiave privata.

La figura sottostante sintetizza il percorso dell'informazione che da "A" raggiunge "B" utilizzando il sistema della crittografia asimettrica.

Viceversa, se il soggetto "B", una volta ricevuto e consultato il documento, intende rispondere al soggetto "A" garantendo lo stesso livello di riservatezza, per crittografare il dato utilizzerà la chiave pubblica di "A", che a sua volta utilizzerà la propria chiave privata per leggere il documento.

Dal funzionamento della crittografia asimmetrica così come brevemente descritto è facilmente intuibile come chiunque sia in possesso della chiave pubblica usata per criptare un messaggio non sarà in grado di decifrarlo a meno che non utilizzi, essendone a conoscenza, la chiave privata associata alla chiave pubblica utilizzata[53].

53) Nel caso contrario, invece, il sistema risulterebbe inefficace atteso che se si dovesse criptare un messaggio utilizzando la chiave privata, chiunque – in possesso della chiave pubblica associata – sarebbe in grado di decifrarlo.

Tornando ora al funzionamento del portafoglio digitale, occorre precisare che esistono due diverse tipologie di wallet: l'"hot wallet" e il "cold wallet".

L'"hot wallet" è un software messo a disposizione dell'utente nei modi più disparati (app per cellulare, pagina Internet o programma per computer) che permette di inviare/ricevere criptovaluta per mezzo di una connessione ad Internet, consentendo inoltre la custodia di entrambe le chiavi (sia pubblica che privata) relative al portafoglio digitale. Questo tipo di wallet è certamente più esposto a rischi soprattutto di matrice informatica. Infatti, qualora i server subissero una violazione dei dati in essi memorizzati, potrebbero essere trafugate le criptovalute detenute nei wallet, dei quali gli stessi server violati custodiscono i dati di accesso, ossia le chiavi pubblica e privata.

Il "cold wallet", invece, è un portafoglio digitale le cui chiavi (sia pubblica che privata) sono memorizzate e custodite in un luogo sicuro ma non connesso alla rete. Ciò che cambia rispetto all'"hot wallet", quindi, è che la chiave privata (indispensabile, come detto, per disporre del saldo del wallet) non è memorizzata sui sistemi di alcun software, ma viene "custodita" dal possessore secondo le modalità che egli stesso reputa opportuno adottare.

Il wallet, accessibile con password, è utilizzabile non solo come un consueto conto, dunque inserendo le proprie credenziali sui siti di e-commerce che accettano pagamenti in valuta digitale, ma altresì attraverso un pratico QR code scansionabile di cui è consigliata la conservazione in forma cartacea in luogo sicuro.

Il portafoglio, inoltre, può essere salvato su di un personal computer o altro genere di dispositivo, come supporti esterni (in questo caso si tratterà di un software wallet come Electrum) o sul web ad esempio in hidden server accessibili da remoto o ancora presso un wallet provider on-line (soluzione quest'ultima che da un lato risulta molto agevole sotto il profilo gestionale ma, dall'altro, richiede grande fiducia da parte dell'utente[54]). In ogni caso, trattandosi di un semplice file, qualora il wallet venga sottratto, ad esempio in seguito all'accesso abusivo al sistema, si perde tutto il credito in esso contenuto.

Chiarito il significato di "wallet", occorre illustrare come il protocollo digitale consenta di evitare che un utente malintenzionato possa utilizzare le stesse criptovalute del suo portafoglio per più di una volta. Entra in gioco a questo punto il secondo componente del protocollo, vale a dire la "*blockchain*"

54) Molte piattaforme di exchange offrono servizi di questo tipo.

("catena di blocchi"). Si tratta in sostanza di un vero e proprio "libro mastro" di Bitcoin, un database nel quale confluiscono tutte le transazioni eseguite dal 2009 ad oggi. Non è gestito a livello centralizzato, ma collettivamente (in maniera distribuita[55]) dai vari aderenti al network (chiamati "nodi"[56]), secondo la già descritta tecnologia "peer to peer".

La tecnologia utilizzata fa si che le operazioni si perfezionino solo nel caso in cui vengano validate da più del 50% della potenza computazionale presente nella rete che supporta Bitcoin. In pratica ogni nuovo utente della rete blockchain di Bitcoin (nodo) riceve tutti i blocchi di operazioni fino a quel momento validati[57] in copia e per intero cosicché, al momento di comprendere se un'operazione può essere o meno accettata come valida (procedimento di validazione delle operazioni), lo stesso invia in broadcast (indistintamente a tutti i componenti della rete) la possibile transazione nella quale è implicato, chiedendo agli altri utenti di verificarne la legittimità. Solo quando, da un lato, una quantità di partecipanti pari a più del 50% della potenza computazionale disponibile assicura che, dai dati in proprio possesso, effettivamente i Bitcoin appartengono all'indirizzo che dispone l'operazione, dall'altro, il destinatario della transazione accetta il pagamento, si procede all'aggiornamento della blockchain con la nuova transazione (operazione che diventa a questo punto valida per tutti gli utenti).

Per spiegare ancora meglio tale aspetto, si potrebbe paragonare ogni sin-

---

55) Un sistema distribuito è costituito da un insieme di applicazioni, logicamente indipendenti, che collaborano per il perseguimento di obiettivi comuni attraverso una infrastruttura di comunicazione hardware e software. Esso garantisce una maggiore flessibilità nell'organizzazione delle attività, permettendo ai client di essere configurati in modo da svolgere attività tra loro differenziate e di ridurre il carico operativo sul sistema centrale.

56) Con il termine "nodo" ci si riferisce ad ogni dispositivo hardware in grado di comunicare con altri dispositivi che fanno parte della rete Internet o di una sua sotto rete (vi rientrano dunque una molteplicità di strumenti informatici: computer, palmari, dispositivi mobili, web TV, ecc.).
I "nodi" vengono anche definiti host (dall'inglese "to host", ospitare), in quanto dotati di applicazioni che possono essere sia client (ad esempio browser web, reader di posta elettronica), sia server (ad esempio, web server). Un'applicazione assume il ruolo di client quando è utilizzatrice di servizi messi a disposizione da altre applicazioni. Assume, invece, il ruolo di server quando è fornitrice di servizi usati da altre applicazioni e, infine, si definisce actor, quando può fungere sia da client sia da server, a seconda dell'operazione richiestagli (è il caso del sistema "peer to peer").

57) Ognuno di questi blocchi viene sviluppato dalla comunità dei miner, che alla fine ottengono una Proof of Work facilmente verificabile senza necessità di particolare potenza computazionale da parte di qualsiasi utente della rete Blockchain.

gola unità di valore Bitcoin a un titolo al portatore, in calce al quale vengono riportate tutte le "girate" che lo stesso ha subito passando da un proprietario (magari originario) ad un altro. Così come per il titolo al portatore la coerenza delle "girate" conforta il proprietario sulla genuinità del titolo stesso, la coerenza dei dati memorizzati nella tecnologia Blockchain, posseduta indistintamente da tutti i nodi della rete, rassicura il proprietario sulla possibilità e legittimità di disporre di quell'unità di valore per futuri scambi.

L'ultimo componente del protocollo è costituito dal "*mining*" ("minare"), termine con cui si indica l'operazione di creazione delle criptovalute, condotta dai c.d. "miners".

A differenza delle classiche monete tradizionali che sono emesse da enti centrali governativi, l'emissione di moneta digitale avviene con una modalità molto differente e con l'uso di strumentazione tecnologica ed informatica di dimensioni imponenti. In particolare, l'attività di mining consiste nel prendere un blocco di transazioni come base per la soluzione di un complesso problema di calcolo che, una volta risolto, comporta la formazione di un nuovo blocco che viene aggregato alla blockchain, registrando in maniera perpetua le transazioni fino a quel momento avvenute e fungendo da base di calcolo per le successive. Essa dipende dal livello di difficoltà del codice da decriptare: i computer che svolgono mining, infatti, sono chiamati ad avere una notevole potenza di calcolo e di fatto è sempre più complesso minare criptovalute. Per quanto riguarda Bitcoin, ad esempio, se nel 2009 era considerato abbastanza semplice "minare" (quindi creare nuova moneta digitale), oggi è considerato abbastanza complesso e nei prossimi anni sarà quasi impossibile[58]. Tra l'altro, è questo il motivo per cui il valore di Bitcoin ha continuato a crescere (anche per la moneta digitale, vale la semplice regola di economia secondo cui la scarsità di una materia prima implica un apprezzamento).

Per il "miner" (attività che chiunque può svolgere scaricando liberamente il software) sono previste sia ricompense per la creazione di un nuovo blocco all'interno della rete blockchain, sia commissioni per la corretta inclusione di

58) Per semplificare, ipotizziamo che il "motore" che genera la moneta digitale sia un enorme cubo ricco di codici criptati, c.d. blocchi, e che questo enorme cubo contenga a sua volta altri cubi. Ogni cubo decriptato produce nuovi cubi e così via. Il compito del minatore di criptovaluta è quello di scovare i cubi e decriptarne i codici. L'algoritmo che genera i codici criptati è programmato per rendere sempre più difficile l'attività di decriptazione fino al giorno in cui verrà intensificata la difficoltà e non sarà più conveniente l'attività di mining (non sarà quindi prodotta altra moneta).

una transazione. Tuttavia, la possibilità di guadagnare attraverso questa attività è col tempo divenuta sempre più difficile, tenuto conto sia del limite imposto per la produzione di blocchi (1 ogni 10 minuti), sia per il numero massimo di Bitcoin che è stato fissato, al momento della loro creazione, in 21 milioni, prevedendone immissioni cadenzate nel tempo[59]. Inizialmente, nel 2009, la ricompensa era pari a 50 Bitcoin; da allora è stata però sistematicamente diminuita (nel 2014 è stata ridotta a 25 e nel 2018 è stata ulteriormente dimezzata) ed è destinata a giungere a zero in coincidenza con l'esaurimento della possibilità di conio, fissata – come detto – in 21 milioni.

Inoltre, al fine di mantenere costante l'inserimento di nuovi blocchi nonostante l'incremento di partecipanti al "mining" e, dunque, della potenza di calcolo collettiva, ogni 2016 blocchi viene ricalcolato il cd. "fattore di difficoltà", ossia viene incrementata la difficoltà di creazione di un ulteriore blocco.

Da ciò deriva anzitutto che l'abilità di minare Bitcoin non è direttamente proporzionale alla propria capacità di calcolo, bensì ad essa rispetto a quella degli altri minatori. Si consideri, infatti, che il "mining" viene effettuato in calcolo parallelo da tutti i computer deputati allo scopo, con un elaborato schema per risolvere incongruenze mediante un sistema di voti di maggioranza che sono ponderati in funzione della potenza di calcolo relativa offerta da ciascuno. In altri termini, maggiore è la potenza di calcolo relativa, maggiore è la possibilità di risolvere un blocco dunque di aggiudicarsi la ricompensa. Ne deriva che all'interno del network c'è una fortissima competizione fra i "miner" per garantirsi maggiori possibilità di introiti. Ciò ha condotto in primis ad una corsa all'acquisto di elaboratori dedicati al "mining" sempre più potenti ed efficienti sotto il profilo energetico, mentre – in un secondo momento – alla creazione di piattaforme per la condivisione della potenza di calcolo (cd. "mining pool"), con distribuzione dei guadagni fra i partecipanti[60]. In ultimo, si è addirittura passati all'inoculazione di malware all'interno

59) Nel 2013 era già stata immessa quasi metà della quantità complessiva e, nel 2018, sono stati raggiunti quasi i tre quarti. Il numero limitato di monete comporta un aumento esponenziale del loro valore all'aumentare del numero di possessori e, conseguenzialmente, anche una riduzione progressiva della capacità di scambio. Per ridurre la possibilità che si verifichi una cd. "crisi di liquidità", è stata prevista la divisibilità della moneta fino all'ottava cifra decimale, ottenendo approssimativamente 21×10 unità di moneta.

60) In questo modo, pur non essendo singolarmente competitivi, è possibile collettivamente contribuire alla generazione di un nuovo blocco, ricevendo una ricompensa proporzionata al contributo offerto.

di dispositivi di ignari utenti per sfruttarli surrettiziamente (anche nella forma di "botnet"[61]).

Ad oggi, è anche diffusa la pratica in base alla quale un gruppo di "miners" si avvalga di una "mining farm", vale a dire di una struttura ad alta tecnologia, equipaggiata per estrarre criptovalute (spesso si tratta di enormi capannoni industriali, che al loro interno hanno attive 24h su 24h delle macchine, ASIC[62], che effettuano l'attività di "mining").

Come accennato, il fattore di successo delle criptovalute è sicuramente rappresentato dall'anonimato delle transazioni, caratteristica che come detto induce i criminali a utilizzarle, tra l'altro, per i pagamenti di beni e servizi sui mercati illeciti della rete.

In realtà, sarebbe più appropriato parlare non di anonimato ma di "pseudo anonimato", tenuto conto che quando si parla di tracciamento dei Bitcoin ci si riferisce unicamente ad un'informazione relativa alla mera transazione finanziaria ed alla sua registrazione; non esiste e non è rilevabile, invece, alcun collegamento, quantomeno in via diretta, tra la moneta e i soggetti utilizzatore/detentore (l'operazione, infatti, pur se registrata, presenta quali unici elementi identificativi, una stringa di lunghezza compresa tra 25 e 34 caratteri frutto dell'algoritmo utilizzato e posto a base della blockchain).

Proprio in relazione alla problematica dell'attribuzione dell'indirizzo Bitcoin ad un utente verificato, molti Paesi hanno previsto (negli Stati Uniti e in Europa) o stanno prevedendo (in Russia, in India e in Cina) obblighi di adeguata verifica della clientela e il rispetto della normativa antiriciclaggio; ciò per far in modo che, al momento della conversione sul web della valuta ordinaria in valuta digitale presso una exchange platform, si sia in grado di far risalire il wallet utilizzato a un utente certo.

In realtà, anche per quanto riguarda le transazioni, Bitcoin non può ritenersi del tutto anonimo. Il processo di verifica descritto in precedenza, infatti, importa che nella blockchain vengano inseriti e resi pubblici tutti i movimenti di tutti i Bitcoin generati a partire dall'indirizzo del loro creatore fino all'ultimo proprietario, rendendo rintracciabili tutte le transazioni. Peraltro, va conside-

---

61) In questo caso la condivisione della potenza di calcolo può essere conseguita anche senza che il legittimo titolare del dispositivo ne sia consapevole. Ciò avviene attraverso l'infezione con un particolare tipo di software malevolo (c.d. "malware") finalizzato ad acquisire il controllo del dispositivo da remoto e innestarlo in una c.d. "botnet", una rete di elaboratori infetti.

62) L'acronimo ASIC, Application Specific Integrated Circuit, viene utilizzato per indicare un circuito progettato per un'applicazione di calcolo ben precisa.

rato che non solo la blockchain contiene lo storico di tutte le movimentazioni eseguite sin dalla nascita del protocollo, ma è anche possibile ottenerne una versione ridotta che abbia ad oggetto solo specifiche transazioni, mantenendone al contempo la totale verificabilità. Il ricorso, infine, a un nuovo indirizzo per ogni pagamento ricevuto o a differenti wallet, in base alle considerazioni fin qui espresse, non possono dunque ritenersi soluzioni efficaci per incrementare la privacy.

Per questo sono sorti all'interno del *dark web* numerosi service per l'occultamento dei Bitcoin che si prestano anche a finalità di riciclaggio digitale (cd. *cyberlaundering*), ossia per impedire il tracciamento di quelle monete che siano state utilizzate per transazioni illegali.

1.5.2. Le *exchange platforms*: uno dei modi per ottenere la moneta digitale

Per ottenere Bitcoin, oltre a svolgere l'attività di "miner", esistono due ulteriori modalità: l'acquisto presso le cc.dd. "exchange platforms" e l'accettazione della moneta digitale come metodo di pagamento in luogo della valuta ordinaria.

L'acquisto può semplicemente avvenire all'interno della piattaforma *Bitcoin.org*[63], che, tra le altre cose, offre una procedura guidata per poter configurare un wallet secondo le proprie esigenze e, se configurato sul proprio smartphone, anche in base al sistema operativo dell'apparecchio. Ottenuto un wallet, si avvia una seconda procedura guidata: dopo aver inserito alcune informazioni, tra le quali la nazione di riferimento e il metodo di pagamento che si intende utilizzare (in genere il bonifico SEPA), si viene reindirizzati a una serie di exchange da cui è possibile effettuare l'acquisto, previa registrazione e pagamento.

Esistono diverse piattaforme informatiche per lo scambio di criptovalute; le più note sono certamente Bitstamp[64], Coinbase[65] e The Rock Trading[66].

I Bitcoin sono accettati anche in alcune Università, come ad esempio quella di Nicosia a Cipro, dove viene utilizzato come mezzo di pagamento

63) Il sito in questione è il seguente: *https://Bitcoin.org/it.*

64) È un sito, con sede a Lussemburgo, che permette di scambiare Bitcoin, Litecoin, Ethereum, Ripple e Bitcoin cash.

65) È una società di scambio di beni digitali con sede a San Francisco in California e fondata a giugno 2012 da Brian Armstrong e Fred Ehrsam. Opera scambio di Bitcoin, Ripple, Ethereum, Bitcoin Cash, Ethereum Classic, Litecoin e altri beni digitali con valute di corso legale in 32 nazioni e con transazioni Bitcoin e di deposito in 190 nazioni.

66) La prima piattaforma europea per comprare criptovalute, attiva dal 2011.

per le tasse universitarie. A Zugo, capitale di uno dei Cantoni della Svizzera, è possibile pagare in Bitcoin alcuni servizi pubblici, tra cui la sanità e i trasporti.

Inoltre, moltissimi enti e associazioni accettano donazioni in Bitcoin; tra le tante si possono citare la Electronic Frontier Foundatione[67], la Free Software Foundation[68] e anche la Wikimedia Foundation[69].

1.5.3. Le caratteristiche di Bitcoin in estrema sintesi

Volendo sintetizzare, come già fatto per altri temi, le principali caratteristiche del protocollo le criptovalute sono:

– l'*assenza di autorità centrali* di gestione. Le transazioni, infatti, consistono in uno scambio di file crittografati tra privati;

– l'*anonimia*. Le transazioni avvengono in totale anonimato, tenuto conto che ogni operatore è identificato solamente da una stringa alfanumerica;

– la *sicurezza*. La valuta digitale è bloccata in un sistema di crittografia a chiavi pubbliche e private, memorizzate in un software denominato wallet. Le prime possono essere considerate l'IBAN di un conto corrente, le seconde il Pin di accesso;

– l'*irreversibilità*. Una transazione, una volta confermata, non può essere annullata;

– l'*attività di mining*. La valuta viene generata direttamente da soggetti privati, internauti, mediante l'utilizzo di specifici software (per i Bitcoin è denominato "*Bitcoin miner*") che risolve funzioni matematiche.

Per sintetizzare, invece, il funzionamento e le potenzialità della "blockchain", si evidenzia che essa:

– è la tecnologia che sta alla base delle criptovalute. Si tratta di un *raffinato sistema di certificazione* in un database distribuito e condiviso;

---

67) È un'organizzazione internazionale non profit di avvocati e legali rivolta alla tutela dei diritti digitali e della libertà di parola nel contesto dell'odierna era digitale. È stata fondata negli Stati Uniti nel 1990.

68) È un'organizzazione non a scopo di lucro, fondata il 4 ottobre 1985 da Richard Stallman (programmatore, informatico e attivista statunitense, tra i principali esponenti del movimento del software libero), che si occupa di eliminare le restrizioni sulla copia, redistribuzione, comprensione e modifica dei programmi per computer.

69) È una fondazione senza fini di lucro creata nel 2003 che ha sede a San Francisco. Si prefigge lo scopo di incoraggiare lo sviluppo e la diffusione di contenuti liberi, in tutte le lingue, e fornire gratuitamente al pubblico l'intero contenuto dei suoi progetti wiki, tra i quali il più noto è l'enciclopedia Wikipedia, che figura tra i 10 siti più consultati al mondo.

– è, in altri termini, un "*registro digitale*" (c.d. "*Distributed ledger*"), che non risiede su un unico server centralizzato ma è strutturato in blocchi in continua crescita, distribuiti su diversi nodi di una rete, sui quali sono memorizzati record di dati in modo sicuro, verificabile e permanente. Il registro digitale in cui sono raccolti e conservati i dati è definito "distribuito" in quanto copie identiche dello stesso vengono archiviate e aggiornate in tempo reale su tutti i computer (c.d. "*nodi*") della rete blockchain. Tutti i nodi hanno lo stesso ruolo e gli stessi diritti di accesso ai dati della blockchain. Non esiste in pratica un nodo centrale;

– *si serve*, per difendere i dati, *di tecniche crittografiche*, così da impedire l'accesso alle informazioni a chiunque non sia stato autorizzato dal proprietario dell'informazione stessa.

1.6. Le nuove criptovalute

Bitcoin è certamente la più importante criptovaluta presente sul mercato finanziario, ma non è l'unica. Sui vari *exchange* ne vengono, infatti, scambiate tante altre (secondo gli esperti, ne esisterebbero oggi 2677), tra le quali, le più utilizzate sono *Ethereum*, *Ripple*, *Bitcoin Cash* e soprattutto *Monero*.

Ethereum (ETH), rilasciata nel 2015, è la seconda criptovaluta per capitalizzazione azionaria, dietro al Bitcoin. Dato l'enorme successo, ad essa è stato spesso associato il termine "nuovo Bitcoin", anche se i progetti sono diversi fra loro. In particolare, Ethereum permette la creazione di "Smart Contracts"[70] tramite la rete peer-to-peer. Gli "Smart Contracts" sono realizzati mediante un linguaggio di programmazione, sono autonomi rispetto a qualsiasi eventuale intermediario e i dati contenuti al loro interno sono crittografati. Questi contratti "intelligenti" funzionano solo ed esclusivamente se trovano un riscontro sul piano reale. La potenza computazionale messa a disposizione sulla rete viene convertita nell'unità di conto denominata Ether. Senza quest'ultima, gli Smart Contracts non potrebbero funzionare. Ether è fondamento di Ethereum ed è essa stessa criptovaluta; viene acquistata dai partecipanti del-

70) Gli Smart Contract sono protocolli informatici che facilitano, verificano e fanno rispettare la negoziazione o l'esecuzione di un contratto, permettendo la parziale o la totale esclusione di una clausola contrattuale. Hanno anche un'interfaccia utente ed emulano la logica delle clausole contrattuali. Grazie agli Smart Contract è possibile rendere parzialmente o integralmente automatizzate le clausole. Inoltre, essi mirano a garantire maggiore sicurezza nella contrattualistica esistente e a ridurre i costi di transazione associati alla contrattazione.

la rete per pagare l'utilizzo della potenza di calcolo. Attenzione quindi a non confondere i due concetti. Anche se Ethereum è volgarmente concepita come crittografia, è in realtà una piattaforma pubblica blockchain che usa gli Ether come moneta digitale (token).

Ripple (XRP), nata nel 2013, si è subito inserita con forza nei mercati digitali finanziari. Si tratta di moneta protetta da misure di sicurezza tali da evitare la duplicazione e la falsificazione attraverso, ad esempio, funzioni di hash crittografico e meccanismi di convalida che, semplificando, tracciano la storia di ogni singolo conio digitale in modo da impedire frodi. Somiglia molto a Bitcoin, rispetto al quale però garantisce un'alta velocità sulle transazioni[71]. Una caratteristica peculiare della rete Ripple è la possibilità di scambiare e trasferire moneta senza continuità di forma. In pratica, si possono trasferire dollari ad un destinatario che poi riceverà in euro, grazie agli accordi esistenti con terzi esterni per la conversione in altre valute.

Bitcoin Cash (BCH) è un "hard fork" della criptovaluta Bitcoin. Il fork di un progetto avviene quando gli sviluppatori prendono una copia del codice sorgente da un pacchetto software e iniziano lo sviluppo indipendente su di esso, creando un separato e distinto pezzo di software. Il termine "fork" spesso implica non solo un ramo di sviluppo, ma anche una divisione nella comunità degli sviluppatori, una sorta di "scisma". Spesso un fork avviene quando ci sono delle dissonanze tra il team degli sviluppatori di un dato progetto (ed è proprio quanto avvenuto nel team di Bitcoin: una parte di esso non era d'accordo con alcune specifiche tecniche del progetto e ha deciso di dissociarsi creando – grazie al fork – una nuova criptovaluta più rispondente alle proprie esigenze e desideri). La nascita del Bitcoin Cash è avvenuta nel 2017. Ha quindi una storia molto breve, ma è prevedibile (secondo gli esperti) che possa godere di grande longevità. La sua caratteristica principale è la dimensioni di blocco a 8 MB, caratteristica che lo rende incompatibile con la blockchain del Bitcoin.

Waves (WAVES) risulta attualmente essere la criptovaluta con la blockchain decentralizzata più veloce. La sua caratteristica principale è quella di dare ai suoi utenti la possibilità di creare *token* monetari senza alcuna nozione di programmazione. In un futuro prossimo sarà prevista anche l'introduzione degli "Smart contracts".

Monero (XMR), introdotta nel mercato il 18 aprile 2014 con il nome di

71) Nel 2017, un calcolo aveva portato a quantificare in 1500 le transazioni completate al secondo, una cifra notevolmente superiore a quella del Bitcoin.

BitMonero, poi modificata in Monero solo 5 giorni dopo, è una criptovaluta che punta ad una maggior *privacy* degli utenti, non avendo una blockchain pubblica. Nelle sue transazioni non è possibile risalire né al mittente né all'importo, diversamente da quanto avviene nel caso dei Bitcoin, la cui blockchain garantisce solo l'anonimato della persona fisica, ma non degli importi. Nonostante non possa vantare i numeri di Bitcoin, l'interesse nei confronti di Monero ha registrato un costante incremento negli ultimi mesi, principalmente in ragione delle ottime performance messe a segno dalla quotazione (sembra che addirittura abbia sostituito Bitcoin per le transazioni nella maggior parte nei mercati illegali in rete). Il motivo di tale maggiore successo risiede sostanzialmente nella differenza che esiste con Bitcoin: l'implementazione di Monero si basa, infatti, sull'algoritmo CryptoNote e nelle sue transazioni non è possibile risalire né al mittente né all'importo, al contrario di quello che accade invece per Bitcoin e per altre criptovalute.

1.7. Le valute virtuali più utilizzate nel dark web

Nel marketing del *dark web* sicuramente Bitcoin occupa una posizione di primaria importanza, anche se sempre più spazio viene riconosciuto, negli ultimi anni, ad altre valute digitali per i motivi che verranno brevemente illustrati.

Tra le alternative a Bitcoin, un posto di primo piano occupano certamente Monero (del quale si è già sinteticamente parlato) e Zcash[72]. Si tratta di valute digitali più giovani, ma in grado di offrire maggiori garanzie di Bitcoin. La loro popolarità cresce a partire da agosto 2016, quando i principali mercati della *darknet*, accettano di integrare Monero come sistema di pagamento. La particolarità di Monero, come già detto, è che non ha una blockchain pubblica. Utilizza un protocollo chiamato Cryptonote che fa sì che le transazioni non possano essere rintracciate, garantendo una maggior *privacy* alla persona che ne fa uso. Nei Bitcoin invece, pur essendoci anonimato, la blockchain è pub-

72) Zcash (ZEC) è una criptovaluta che offre privacy e trasparenza selettiva delle transazioni (secondo molti esperti potrebbe diventare la valuta preferita per il riciclaggio di denaro sporco). I pagamenti Zcash sono pubblicati su una blockchain pubblica, ma il mittente, il ricevente e il valore della transazione possono rimanere privati. Il funzionamento di questa nuova moneta digitale è in gran parte simile a quello di BitCoin, ossia c'è una blockchain che tiene traccia delle transazioni che avvengono in questa valuta ma si differenzia per il fatto che è praticamente impossibile per utenti terzi sapere chi ha effettuato la singola operazione e verso quale portafoglio di arrivo. Sconosciuti sono quindi sia l'ordinante che il beneficiario: di tutta l'operazione si sa solo che è accaduta.

blica e quindi ogni utente può visualizzare su Internet tutte le transazioni dei singoli wallet, attraverso le chiavi pubbliche. Grazie alla diffusione veloce di Monero, si sono sviluppate tutta una serie di criptovalute dalle caratteristiche analoghe, come ad esempio proprio Zcash, che – lanciata nel gennaio 2016 – offre anch'essa la garanzia di riservatezza di ogni transazione, per mezzo di una tecnica di crittografia chiamata zk-Snark[73].

Un'ultima considerazione da fare è relativa alla tecnologia legata a Bitcoin, che pur essendo molto efficiente, presenta un difetto non trascurabile: la velocità.

Ad oggi si registrano talmente tante transazioni che per andare in porto ed essere completate a tutti gli effetti necessitano di lunghi tempi di attesa, per abbattere i quali si ricorre sempre più spesso a valute digitali meno efficienti, ma che garantiscono transazioni più veloci, come le già descritte Ripple e Waves, che fanno proprio della velocità di transazione la loro principale caratteristica.

2. Il traffico on-line di droga e armi

2.1. Aspetti generali di un fenomeno in costante crescita

Il crescente utilizzo della rete telematica per tutte le tipologie di attività di e-commerce ha di fatto creato le condizioni per la crescita di una nuova forma di imprenditorialità criminale "fai da te", anche nell'ambito del traffico della droga, favorendo notevolmente il mercato illecito dei diversi tipi di sostanze stupefacenti.

Si tratta di un fenomeno di proporzioni già vastissime, ma destinato ad espandersi ulteriormente e in materia molto veloce, anche per l'attrazione che

73) Si tratta di una nuova tecnologia di tipo "zero-knowledge proof" ("Dimostrazione a conoscenza zero") che richiede meno potenza computazionale di altre soluzioni simili. In informatica applicata per "zero-knowledge proof" si intende un sistema per cui un computer effettua una verifica su un'affermazione senza sapere altro che la dichiarazione di veridicità che gli viene trasmessa. È un concetto un po' complesso a livello teorico, ma più semplice se lo si applica. Un sistema del genere viene usato in diversi casi su Internet, ad esempio lo si può utilizzare per farsi autorizzare all'accesso in un sistema, inserendo una password ma senza dover necessariamente trasmetterla. Il protocollo ideato dai ricercatori di ZCash, nello specifico, permette agli utenti di provare che possiedono le monete che vogliono spendere senza rivelare però altre informazioni riguardo la provenienza o la destinazione, cioè senza indicare da quale portafoglio sono arrivate né in quale finiranno.

esercita in maniera sempre più forte nei confronti dei più giovani, ragazzi anche in età scolare, che nella duplice veste di spacciatore\consumatore colgono nei mercati della rete opportunità che non vengono loro offerte dallo smercio in strada "*vis a vis*", anche e soprattutto in termini di anonimato e riservatezza. È un metodo che non richiede particolari investimenti da parte dei fornitori e che consente ai consumatori di acquistare le sostanze direttamente da casa, senza dover entrare in contatto con lo spacciatore, ricevendole a domicilio in confezioni spesso spedite per posta aerea, con modalità che ne garantiscono il perfetto occultamento.

La diffusione del fenomeno è talmente veloce e ampia da aver addirittura ispirato la serie televisiva tedesca "*Come vendere droga on-line (in fretta)*", apparsa con grande successo su Netflix a maggio del 2019 e a luglio 2020. Vendere droga on-line, creando un sito sul quale si può acquistare la dose desiderata tramite Bitcoin e diventare ricchi in maniera impressionante: questa è stata la sceneggiatura di un prodotto che ha avuto un successo clamoroso; peccato che il copione della serie non era frutto dell'estro e dell'intuizione degli sceneggiatori, ma una storia realmente accaduta[74] e che accade sempre più spesso.

La nascita dei criptomercati on-line (così definiti anche per via dell'accesso tramite software crittografati che garantiscono l'anonimato) risale grosso modo agli anni 2010-2011 (il primo storico black market della storia, Silk Road, del quale si parlerà in seguito, è stato attivo tra il 2011 e il 2013). Sin dai primi anni, le transazioni illegali di droga in rete hanno fatto registrare un'inarrestabile escalation.

Si citano, in merito, due studi analitici che – seppur datati – si ritengono particolarmente significativi e utili a meglio comprendere la crescita esponenziale del fenomeno. Il primo è stato condotto dal settimanale d'informazione "The Economist"[75], che ha analizzato i dati di 360.000 vendite tra dicembre 2013 e luglio 2015 sui black markets Agorà, Evolution e Silk Road (3 piatta-

74) La serie ha raccontato la storia di due studenti delle scuole superiori che avevano creato un business di droga on-line in Europa per riconquistare l'amore di una ragazza. In particolare, il diciottenne Maximilian S. aveva lanciato un commercio di droga in rete dalla sua camera da letto, a Lipsia, alla fine del 2013, con il nome in codice "Shiny Flakes". Nel novembre 2015 è stato condannato a sette anni di carcere e la sentenza è diventata definitiva nel marzo 2016.

75) "The Economist" è un settimanale d'informazione politico-economica in lingua inglese, focalizzato su attualità globale, commercio internazionale, politica e tecnologia. Edita a Londra da The Economist Newspaper Limited, la rivista dispone di uffici editoriali nelle principali città del Nord America, dell'Europa, dell'Asia e del Medio Oriente. Nel 2019,

forme all'epoca tra le più attive nelle vendite), calcolando un volume d'affari complessivo di circa 50 milioni di dollari (i maggiori ricavi derivavano dalla vendita, in ordine, di MDMA con 7,7 milioni, di marijuana con 5,7 milioni e di cocaina con 5,2 milioni).

Il secondo studio, invece, è stato commissionato – nel 2016 – dall'Olanda all'istituto di ricerca "RAND Europe"[76]. Il report all'epoca predisposto evidenziava innanzitutto che in 3 anni (a partire dal 2013), il numero di transazioni era triplicato e i ricavi raddoppiati, toccando i 25 milioni di dollari di fatturato mensile. Si trattava, già all'epoca, di un giro d'affari enorme, pur rappresentando solo una piccola frazione del mercato della droga nella sua interezza, che secondo le stime fatturava circa 2 miliardi di dollari al mese. Nel report veniva segnalata, inoltre, l'esistenza di circa 50 criptomercati on-line, con i principali tre all'epoca attivi – Alphabay, Nucleus e Dreammarket – che coprivano il 65% dell'offerta. Sempre secondo lo studio, la cannabis generava la maggior parte (il 31%) dei ricavi complessivi, seguita dagli stimolanti (tra cui cocaina e anfetamine) che contribuivano per il 24% del fatturato totale. Al terzo posto si piazzavano ecstasy e affini (inclusa quindi l'MDMA), con una fetta del 16% delle vendite; a seguire le droghe psichedeliche con l'8% e gli oppiacei (tra cui l'eroina) con solamente il 6%. Altro aspetto significativo riportato nel report era che le richieste in rete si focalizzavano più sull'uso "ricreazionale" della droga (in particolare, di cannabis e di psichedelici) che non su quello legato alle dipendenze vere e proprie (di eroina, in particolare). Inoltre, nonostante le transazioni registrate erano per lo più di modesta entità (sotto i 100 dollari) e finalizzate all'uso randomico e personale, era emerso che circa un quarto del fatturato era costituito dalle cosiddette vendite "wholesale" (all'ingrosso), quelle che superavano i 1000 dollari l'una e che, presumibilmente, venivano effettuate da spacciatori che intendevano poi rivendere la merce off line. Il 46% di questi ordini supersize proveniva dalla Cina, il 20% dal Belgio, il 15% dal Canada e il 12% dall'Olanda. Infine, quanto a diversificazione geografica dei fornitori, il business spaziava dal mondo anglosassone all'Europa

---

la sua diffusione media globale combinata (tra copie stampate e versione digitale) è stata di oltre 1,6 milioni di lettori, più della metà dei quali in America settentrionale. Una rilevazione del 2017 dell'Università del Missouri ha appurato che "The Economist" è ritenuto in assoluto la fonte d'informazione più autorevole da parte del pubblico statunitense.

76) "RAND Europe" è un istituto di ricerca senza scopo di lucro la cui missione è aiutare a migliorare le politiche e il processo decisionale attraverso la ricerca e l'analisi condotte su argomenti rilevanti per le politiche (dalla difesa e sicurezza alla politica dell'innovazione e della tecnologia, dalla giustizia penale alle questioni sanitarie e sociali).

occidentale. In testa a tutti, anche per ragioni dimensionali, gli Stati Uniti, da cui operavano 850 venditori per un fatturato di 5,7 milioni di dollari al mese, vale a dire il 36% circa del totale. A seguire la Gran Bretagna, che deteneva il primato europeo con 338 venditori e 6,7 milioni di dollari mensili (pari al 16% del totale); terzo posto per l'Australia, con 185 venditori e 8 milioni di ricavi (ovvero il 10.6%). Seguivano la Germania e l'Olanda, entrambe con 225 venditori e un fatturato di circa 5 milioni al mese, corrispondente a circa l'8% dei ricavi complessivi.

2.2. I siti di vendita nell'"open web"

L'attività di monitoraggio delle compra-vendite di sostanze stupefacenti attraverso l'utilizzo della rete ha accertato che il fenomeno si sviluppa attraverso due differenti modalità virtuali. Gli acquisti, infatti, avvengono sia nell'*open web* che nel *deep web*, secondo dinamiche diverse, certamente più complesse e articolare nella parte oscura della rete.

Partiamo dall'*open web* (detto anche *surface web*).

L'osservazione delle dinamiche criminali nella parte del web liberamente accessibile (come detto, dai contenuti facilmente raggiungibili attraverso normali motori di ricerca) ha consentito di rilevare l'esistenza e l'intensa attività di due tipologie di siti, denominati "*siti proprietari*" e "*siti d'intermediazione*", ai quali è possibile accedere con connessioni in chiaro, attraverso l'utilizzo del semplice servizio di internet *www.*

Sempre dall'attività di monitoraggio è emerso che la maggior parte di tale tipologia di siti è ubicata in Olanda, in Cina e negli Stati Uniti, prevalentemente gestiti, specialmente nei Paesi Bassi (ovviamente anche in virtù della favorevole previsione legislativa rispetto alla vendita di droghe leggere), dai cc.dd. "smart shops" o "smart drug shop", ovvero piccoli negozi al dettaglio specializzati nella vendita di sostanze psicoattive legali e dei relativi accessori nonché di letteratura dedicata[77](ovviamente, parallelamente alla vendita legalizzata viaggia la vendita illegale di un'altra tipologia di prodotti, attuata proprio attraverso i canali informatici collegati a tali shops).

Le dinamiche relative all'acquisto di droga sui "siti proprietari" (nella

77) Il nome deriva dal tipo di prodotti venduti, chiamati smart drugs (cioè "droghe furbe"), una categoria di sostanze stupefacenti e psicoattive (tra cui rientrano caffeina, teofillina, taurina, ginseng, guaranà e varie altre) che non vengono considerate illegali dalle autorità, dal momento che esse contengono solo i principi attivi delle piante da cui derivano e non parti di esse, né tantomeno la pianta per intera, il che le rende automaticamente legali e

figura sottostante è riportata, a titolo esemplificativo, la homepage del sito Azarius, tuttora attivo sulla rete[78]) sono basate, come già accennato, sul rapporto venditore\acquirente. Quest'ultimo, con estrema facilità, sceglie il prodotto, completa l'ordine, effettua il pagamento (solitamente con carta di credito o prepagata, ma anche con bonifico bancario), dopodiché attende la ricezione del prodotto, che viene normalmente spedito con pacchi anonimi mediante gli ordinari canali di trasporto (per esempio, vettori DHL, SDA, FEDEX, ecc.).

Sul "sito d'intermediazione" (nella figura sottostante la homepage di uno dei tanti attivi in rete) il contatto tra venditore e acquirente avviene invece grazie alle funzionalità offerte dal sito stesso, che propone specifici spazi dove chiunque può inserire o leggere annunci pubblicitari di diversa natura.

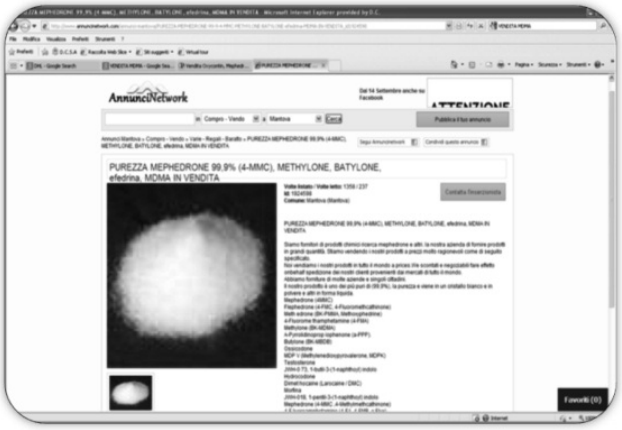
---

vendibili sia in Italia che nel resto d'Europa (gli smart shop sono infatti esercizi commerciali legali).

Le sostanze vendute possono essere di origine naturale come il Kratom o la Salvia divinorum o anche totalmente sintetiche come il mefedrone o il c.p. 47,497 che è un cannabinoide sintetico creato dalle case farmaceutiche. Negli smart shop vengono venduti inoltre tabacchi aromatizzati, accessori per fumatori, stimolanti sessuali, semi di cannabis ed attrezzature per la coltivazione.

78) Sul sito vengono descritte le sue finalità nel modo seguente: "*Nello smartshop on-line Azarius troverai tutto ciò che serve per aggiungere una scintilla di magia alla tua vita.Sia che tu cerchi estratti di erbe naturali o semi, erbe, tartufi e cactus psichedelici, Azarius è qui per esaudire i tuoi desideri. Inoltre offriamo kit di coltivazione per funghi magici e una vasta gamma di diversi tipi di semi: abbiamo tutto ciò di cui hai bisogno per dedicarti alla coltivazione. Sei novello al meraviglioso mondo degli integratori psicoattivi naturali? Sfoglia con curiosità e pazienza il nostro immenso assortiment, siamo sicuri che troverai la formula magica adatta a te*".

In pratica, l'inserzionista pubblica la sua "vantaggiosa" offerta, catturando l'attenzione dell'acquirente, che naviga in rete alla ricerca di "buone occasioni". A questo punto, il sito intermediario esce di scena, lasciando spazio al rapporto diretto tra le parti, che concludono la compra-vendita utilizzando altri canali di comunicazione quali Skype, Whatsapp, e-mail, ecc.



Le attività investigative sia sui siti "proprietari" che su quelli "di intermediazione" vengono generalmente svolte attraverso le ordinarie, tradizionali modalità, secondo un copione standard che comprende:

– l'*acquisizione della notizia di reato*, al quale si perviene generalmente attraverso il monitoraggio della rete;

– il *riscontro delle informazioni acquisite*, nella maggior parte dei casi mediante attività di polizia giudiziaria come l'acquisto simulato e/o la consegna controllata;

– la *localizzazione degli utenti*, in genere con l'acquisizione di file di log ovvero l'estrapolazione dell'indirizzo IP, che consente di identificare univocamente un pc, un server o altri dispositivi collegati alla rete in un dato momento;

– l'*identificazione degli utenti*, che può avvenire con la localizzazione geografica del "caller id", cioè della presa telefonica dalla quale è partita la connessione (spesso tale procedura non permette la reale identificazione dell'utente, che potrebbe per esempio utilizzare dispositivi collocati in esercizi pubblici) ovvero mediante il monitoraggio delle spedizioni e/o dei pagamenti.

Per i "siti d'intermediazione" valgono, però, alcune precisazioni. In primo luogo, il gestore del sito intermediario non è assoggettato all'obbligo generale di sorveglianza delle informazioni trasmesse o memorizzate (ex art. 17

del decreto legislativo 9 aprile 2003, n. 70, in tema di "*Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico*"[79]).

Inoltre, molto spesso gli annunci che pubblicizzano la vendita di stupefacenti sono solo "scamming", vale a dire inserzioni di compravendita che celano in realtà delle truffe.

Infine, nel corso delle indagini si può incappare nell'inconveniente di attivare uffici di polizia non territorialmente competenti, con l'inevitabile dispendio di risorse e di tempo. È il caso, ad esempio, di un annuncio che fa riferimento alla città di Roma, salvo poi scoprire – nel corso dei successivi approfondimenti – che in realtà l'inserzionista opera da Milano e che ha solamente attivato una procedura per sviare "geograficamente" le investigazioni.

2.3. I black markets del "dark web"

Nel *dark web*, alla luce dei vantaggi che l'uso di darknet (quali Tor o I2P) offre ai criminali in termini di anonimato delle comunicazioni e cifratura dei dati, risultano attive numerose piattaforme illecite di commercio elettronico, all'interno delle quali avvengono le transazioni e gli scambi più intensi e lucrosi per il mondo criminale. Si tratta dei citati "*black market*", che costituiscono "*… la nuova frontiera del crimine transnazionale, finanziario e informatico, su cui si concentra l'impegno delle forze di polizia di tutto il mondo*"[80].

Sono dei veri e propri "supermercati dell'illecito", da molti definiti "Amazon dell'illegalità", che offrono al loro interno una vasta gamma di pro-

---

79) L'art. 17 così recita: "*Nella prestazione dei servizi di cui agli articoli 14, 15 e 16* [responsabilità nell'attività di semplice trasporto - *mere conduit*, di memorizzazione temporanea - *caching* e di memorizzazione di informazioni - *hosting*], *il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite*".

80) Vds. "Relazione annuale 2019" della Direzione nazionale antimafia e antiterrorismo, nella quale viene richiamata – tra l'altro – l'azione denominata "OAP Carding Action 7.1", nell'ambito di un'importante azione EMPACT a leadeship italiana, che ha visto la partecipazione di investigatori di 9 Paesi europei ed esperti di Europol, coordinati dalla Polizia postale e delle comunicazioni. Tale azione ha condotto all'individuazione di numerosissimi account riconducibili a sodalizi criminali transnazionali attivi nel reperimento e nella commercializzazione illegale di dati personali e codici bancari.

dotti e servizi: dalle armi clandestine alle sostanze stupefacenti, dai documenti contraffatti al materiale pedopornografico, dalle carte di pagamento clonate a password e codici di accesso personali di migliaia di utenti, oltre a farmaci acquistabili solo tramite prescrizione medica (antidepressivi, stimolanti, antipsicotici, antidolorifici, sonniferi, ormoni, ecc.). In tali mercati virtuali, i pagamenti avvengono nella maggior parte dei casi mediante l'utilizzo di criptovalute, quali la più nota Bitcoin o la più recente Monero, che garantiscono (come già illustrato) l'anonimato delle transazioni.

L'attività di monitoraggio svolta dalle forze di polizia negli ultimi anni ha portato a stimare in circa 100 milioni di dollari il volume d'affari annuale degli shops illegali. Ad oggi, risulterebbero attivi circa 40 markets (il dato è comunque fluttuante, in ragione dei cambiamenti repentini e imprevedibili che connotano i fenomeni criminali in rete), per ciascuno dei quali è stata osservata la contemporanea presenza di almeno 300 venditori, con circa 21.500 annunci. Inoltre, è emerso che la merce venduta su tali piattaforme è costituita per il 62% da stupefacenti di ogni genere, per il 17% da false carte e documenti falsificati, per il 12% da servizi illeciti di vario genere, per il 6% da materiale pedopornografico, per il 2% da virus e il restante 1% da armi[81].

Altro interessante elemento, emerso sempre dall'attività svolta dalle forze di polizia, è costituito dal fatto che i black markets sembrerebbero suddivisi in due macro-aree: da un lato ci sono gli shops che trattano esclusivamente la vendita di materiale pedopornografico, dall'altro i rimanenti che invece sono attivi nella vendita di tutti o gran parte degli altri prodotti e servizi. La motivazione di una simile netta distinzione non è nota; tra gli investigatori pare comunque prevalere l'ipotesi che si sia trattata di una scelta operata dai primi organizzatori delle piattaforme illegali, che ritenevano "altamente immorale" dare spazio alla commercializzazione di materiale che riproducesse episodi di violenza/abusi su minori. Tale iniziale scelta è poi divenuta consuetudine per tutti gli altri.

2.3.1. La ricerca in rete di un illegal shop

Prima di illustrare il funzionamento di un black market, occorre evidenziare qualche aspetto relativo alla "ricerca" nel *deep web* (quindi anche nel dark web), cercando in particolare di capire come chi intenda acquistare online prodotti illeciti (droga e armi soprattutto) riesca a reperire le informazioni sui siti d'interesse. Non solo, ma anche provare a dare una chiave di lettura

81) La rilevazione, come detto, è frutto del monitoraggio delle forze di polizia.

sul perché molti prediligano a tal fine la rete, che comunque comporta l'inevitabile rischio della "truffa".

Eseguire una ricerca dati nel *deep web* non è semplice proprio alla luce delle sue caratteristiche, volte alla protezione dell'anonimato e della non tracciabilità. Come già detto, per la parte anonima della rete non esistono motori di ricerca evoluti, quali ad esempio Google e Bing per l'*open web*. Inoltre, i siti che realizzano attività illecite sulla rete, essendo costantemente nel mirino delle forze di polizia e molto spesso oggetto di continui attacchi anche da parte di "concorrenti" che tentano di distruggerli per guadagnare agli occhi degli acquirenti la primazia nel vasto panorama dei mercati esistenti, devono continuamente essere implementati con sofisticati sistemi di mascheramento per evitare di essere bloccati.

Sotto questo aspetto, lo scenario del mercato on-line è analogo a quello in cui si muove un comune spacciatore che, pur cercando di non farsi notare troppo, per svolgere la sua attività di scambio denaro-droga, deve accettare il rischio di esporsi, studiando nel tempo specifiche e diverse modalità di pubblicità per farsi trovare dai possibili acquirenti quanto più facilmente possibile. Allo stesso modo, un sito on-line di vendita di sostanze stupefacenti all'interno del *dark web* (protetto quindi dalla sua stessa struttura), per svolgere con continuità la propria attività commerciale, deve pianificare e realizzare un modo per permettere ai possibili acquirenti di:

– trovare il market con facilità dal web di superficie, preferibilmente tramite motori di ricerca intuitivi;

– farsi un'idea del funzionamento del market attraverso forum, blog o wiki che, oltre a illustrare i prodotti venduti, spieghino anche il funzionamento del mercato (in particolare, le regole di contrattazione e le modalità di spedizione\consegna della merce acquistata[82]);

– iscriversi al market facilmente e in modo anonimo.

Più in dettaglio, la ricerca di un market da parte di un acquirente, come accennato, parte generalmente dal web di superficie, attraverso alcuni siti che sono stati specificamente creati[83] oppure attraverso i numerosi forum, blog e wiki attivi[84]. In entrambi i casi, dall'*open web* si viene rimandati alle pagine

82) Uno dei fattori di successo di un market è il modo in cui accoglie l'acquirente. Ai suoi occhi il sito deve risultare accattivante, sicuro e professionale; deve inoltre infondergli la consapevolezza di poter concludere le trattative in totale sicurezza.

83) Ad oggi, i più noti accessibili da Google sono denominati *deepwebsiteslinks*, *thedarkweblinks* e *deepweb-sites*.

84) Tra i più diffusi, figurano quelli denominati *Thehiddenwiki*, *Deepdotweb* e *Reddit*.

corrispettive nel *deep web* ove sono pubblicati gli elenchi aggiornati dei black markets che risultano operativi.

A titolo esemplificativo, nella sottostante figura 1 viene riportata la homepage di un sito (*Onion.live*), accessibile liberamente dal *clear web*, che elenca i mercati indicandone lo stato con colore diverso (verde se disponibile, rosso se indisponibile).

In realtà, le informazioni veicolate da tali siti possono talvolta risultare scarsamente attendibili, soprattutto in termini di aggiornamento, tenuto conto – per esempio – dell'esigenza dei gestori di mascherare continuamente gli shops anche semplicemente modificandone il nome.

Dall'elenco, è poi possibile selezionare un market (tra questi, il "*white house market*" nella figura 2), del quale si possono acquisire speditivamente informazioni utili, relative principalmente alla tipologia di merci vendute.

Ultimata la ricerca, la successiva navigazione nel black market, come già illustrato, è consentita esclusivamente mediante una *dark net*, il cui utilizzo per l'utente segna di fatto il passaggio dal *clear* al *dark web*.

Figura 1

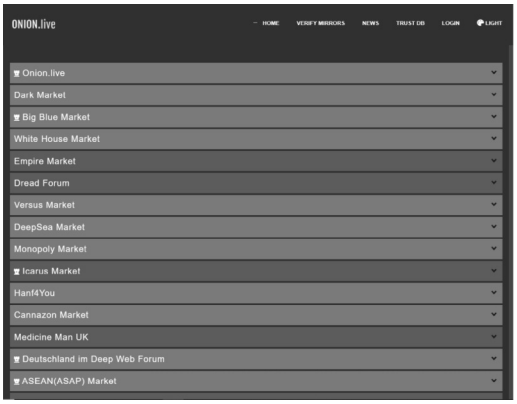
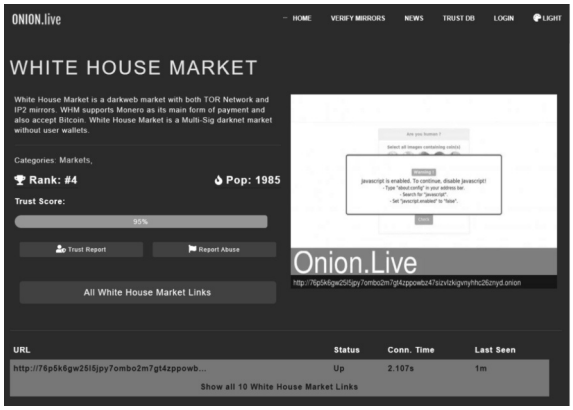


Figura 2



Nel provare invece a fornire risposta sul perché chi intende acquistare droga si rivolga al black market, piuttosto che ricorrere al tradizionale sistema dello spaccio con contatto diretto, ci viene in aiuto l'esito di una ricerca condotta dallo "*European monitoring centre for drugs and drug addiction*"[85].

Dalle analisi dei dati è emerso che i compratori sono principalmente giovani, tendenzialmente con un passato di abuso di droghe e con un età compresa tra i 21 e i 25. In termini di motivazioni, ciò che sembra spingere all'acquisto di droghe on-line è in primis la varietà dei prodotti disponibili. È emerso, per esempio, che chi era solito acquistare sul sito "Silk Road" (il black market più famoso della storia, del quale in seguito si parlerà in maniera più approfondita) lo faceva per poter sperimentare nuove sostanze proprio grazie alla ampia varietà offerta.

Oltre alla grande disponibilità di prodotti differenti, altri due elementi che incentiverebbero gli acquisti on-line riguarderebbero i costi, ritenuti più contenuti, e la qualità della droga. In particolare, con riferimento a quest'ultimo aspetto, dallo studio è emerso che l'acquirente si rivolge alla rete per poter selezionare il Paese di provenienza dello stupefacente, nella convinzione, per esempio, che l'MDMA approvvigionata in Olanda sia presumibilmente di più alta qualità[86].

È infine emerso che in molti preferiscono l'acquisto sul *dark web* per evitare incontri "faccia a faccia" con lo spacciatore, evitando così tutta una serie di "pericoli", quali il rischio di subire aggressioni o la possibilità di essere sottoposti a controlli di polizia.

Per quanto riguarda, invece, la vendita di armi, uno studio condotto nel 2017 dall'istituto di ricerca Rand Europe[87], in collaborazione con l'Università

---

85) Lo "European Monitoring Centre for Drugs and Drug Addiction" (EMCDDA) è il punto di riferimento sulle droghe in Europa. L'osservatorio, istituito nel 1993 e inaugurato a Lisbona nel 1995, è una delle agenzie decentrate dell'Unione europea (UE). Il suo principale obbiettivo consiste nel fornire all'UE e agli Stati membri una visione realistica dei problemi legati alla droga in Europa e una base solida di evidenze che supportino il dibattito sugli stupefacenti. Inoltre, offre ai responsabili politici i dati necessari per elaborare leggi e strategie in materia di droga e a professionisti e operatori del settore uno strumento per individuare le "best practices" e le nuove aree di ricerca.

86) Sul punto, altri studi hanno portato a conclusioni differenti. Infatti, da un'analisi su campioni di stupefacente acquistati on-line (nel 90% dei casi il prodotto ricevuto rispecchiava l'ordine effettuato), è emerso che – talvolta – la purezza del prodotto veniva sopravalutata. In un caso, ad esempio, in un 1 grammo di cocaina la cui purezza pubblicizzata era del 95%, dalle successive analisi era invece risultata tra il 30% e il 33%.

87) RAND Europe è un istituto di ricerca indipendente senza scopo di lucro la cui missione è aiutare a migliorare le politiche e il processo decisionale attraverso la ricerca e l'analisi.

di Manchester, è emerso che gli Stati Uniti sono la fonte principale di approvvigionamento di armi illegali con il 60% circa del totale (ovviamente, anche in ragione della normativa vigente nello specifico settore). L'Europa conta, invece, solo il 25% circa, ma risulta essere la principale piazza di acquisto, con volumi cinque volte maggiori rispetto agli Stati Uniti. Le armi vendute più frequentemente sono le pistole (84%), seguite dalle carabine (10%) e dalle armi automatiche (6%). È inoltre emerso che ogni mese, attraverso il *dark web*, vengono approvvigionate almeno 136 armi o prodotti correlati[88] e che, analizzando 12 mercati, il valore complessivo del fatturato legato alle armi è di circa 80 mila euro al mese.

Un secondo studio, condotto nel 2019 da un gruppo di ricercatori dell'Università del Michigan, oltre a confermare sostanzialmente i dati del primo con riferimento alla tipologia di armi vendute (pistole con il 64%, seguite dalle armi semi-automatiche con il 17%), ha fatto emergere un nuovo dato, vale a dire che solo il 4% degli oggetti messi in vendita rientra nella categoria "armi da guerra". Inoltre, la grossa fetta del mercato nero è composta da armi reperibili legalmente in molti Paesi, che vengono però acquistate attraverso il *dark web* da chi comunque mira a conservare l'anonimato garantito da Tor e dalle altre reti nascoste.

2.3.2. Il funzionamento e le principali caratteristiche

Passando, invece, al funzionamento di un black market, occorre preliminarmente indicare quali sono i soggetti coinvolti. Da un lato, il gestore (il c.d. admin), nella maggior parte dei casi unico soggetto; dall'altro, il "vendor" (venditore) e il "client" (cliente), che conducono invece la trattativa finalizzata alla compra vendita dei prodotti o dei servizi.

Il compito del gestore è quello di ideare e realizzare l'architettura informatica del market, dotandolo di almeno due caratteristiche fondamentali: la sua semplice individuazione in rete e un funzionamento intuitivo. In pratica, deve consentire al cliente di reperirlo nel *dark web* rapidamente e nella maniera più facile possibile, nonché di registrarsi allo stesso con altrettanta semplicità (in linea di massima, per consentire anche a chi non ha specifiche competenze informatiche di creare un proprio account, viene richiesto solamente di impo-

88) Esiste sul *dark web* la possibilità di comprare veri e propri "tutorial del crimine" relazionati alle armi stesse. Per fare degli esempi, si possono trovare istruzioni su come trasformare uno scacciacani in un'arma da fuoco o su come costruire da zero un esplosivo.

stare username e password). Inoltre, deve garantire al cliente una navigazione aderente alle sue esigenze, consentendogli di individuare con facilità il prodotto cercato e, soprattutto, di condurre la trattativa con il venditore in forma anonima e sicura. Infine, è necessario che preveda nell'architettura del market un'area dedicata ai forum, dalla cui consultazione l'acquirente deve trarre informazioni (riguardanti ad esempio l'organizzazione logistica del venditore, con particolare riferimento alle modalità di spedizione della merce) funzionali alla scelta del venditore "migliore".

Il ruolo dei forum e dei blog nella vita di un market merita un'ulteriore considerazione. Le trattative di acquisto su una piattaforma virtuale del web, connotata dalla totale assenza di qualsiasi forma di contatto personale, non possono che fondarsi sulla fiducia; in altri termini, sulla reputazione che il venditore è riuscito a costruirsi nel tempo e che si rileva dalle valutazioni espresse dagli utenti e dai feedback dagli stessi lasciati in relazione ad un acquisto effettuato. Per essere più chiari, un acquirente è chiamato a valutare la qualità del prodotto acquistato (viene in genere utilizzato un numero compreso tra uno e cinque, secondo la stessa procedura delle classificazioni "a cinque stelle" tradizionali) e a lasciare un breve commento sul tipo di servizio offerto; la qualità del prodotto (anche in termini di rispondenza di quanto ricevuto con quanto si era inteso comprare) e l'efficienza del servizio determinano il livello di affidabilità del venditore. Per quest'ultimo godere di buona reputazione è talmente importante da indurlo, talvolta, a comportamenti "truffaldini", che consistono nella creazione di numerosi account, fittiziamente riconducibili a soggetti differenti, per concludere operazioni di compra-vendita alle quali attribuire una valutazione alta.

Ma tornando al funzionamento del market, il cliente, una volta individuata la piattaforma d'interesse, procede alla creazione di un proprio account, solitamente scegliendo un nickname che lo associ immediatamente alla tipologia di merce che intende acquistare (stupefacenti, armi o altro). Dopodiché inizia la propria interazione con il market: consulta dapprima i blog e i forum per identificare il venditore migliore (sia in termini di affidabilità che di economicità); successivamente, avvia direttamente con quest'ultimo (senza alcuna intermediazione del gestore) la trattativa di acquisto, definendo tutti gli aspetti dell'"affare" (il prezzo e la modalità di spedizione). Per concludere l'ordine, l'acquirente deve procedere al pagamento depositando la moneta digitale su un "conto di deposito di garanzia" (il c.d. escrow), di cui necessariamente ogni piattaforma deve essere dotato; compete poi al gestore, una volta ricevuta dall'acquirente conferma della ricezione della merce, rilasciare al venditore la valuta digitale (nella quantità pattuita), trattenendo però una

commissione detta "fee", in genere pari al 4% del valore totale della transazione[89].

Il venditore, invece, allestisce lo spazio ("vetrina") che gli viene concesso dal gestore nello store, previo versamento di una quota di iscrizione "one time deposit"[90] (variabile a seconda del market). Anche l'allestimento della "vetrina" (come accade per un qualsiasi negozio) richiede la cura del particolare; lo scopo del venditore è infatti quello di attirare l'interesse del maggior numero di clienti. A tal fine, oltre alla semplicità di ricerca dei prodotti e alla loro varietà, un elemento vincente è certamente quello della "novità" su cui ricade inevitabilmente l'attenzione di coloro che, come detto, prediligono la rete soprattutto per poter sperimentare nuove sostanze.

Nel funzionamento del market e in particolare nella sua organizzazione logistica, un elemento vulnerabile (sul quale spesso si concentra l'attenzione investigativa delle forze di polizia) è certamente la spedizione della merce. Dal costante monitoraggio del fenomeno (svolto principalmente dalla Sezione dedicata della Direzione centrale per i servizi antidroga) emerge che spesso i plichi viaggiano per via aerea (talvolta vengono intercettati presso gli aeroporti), anche se i tradizionali servizi a mezzo posta o mediante vettori privati continuano a essere quelli ai quali si fa maggiormente ricorso.

Inoltre, lo stupefacente, principalmente di origine sintetica (quale amfetamina, MDMA, ecstasy, fentanyl e derivati), ma anche marijuana, hashish, eroina, cocaina, viene generalmente occultato all'interno di involucri nascosti nelle custodie di dvd e/o cd. musicali, posti a loro volta all'interno di buste argentate sottovuoto, modalità che impone chiaramente di limitare le trattative di compra vendita a piccole quantità, occultabili in plichi postali. Si registra, pertanto, un numero molto elevato di transazioni per l'acquisto di piccoli quantitativi, decisamente inferiori a quelli trafficati attraverso i metodi tradizionali.

I mittenti sono quasi sempre soggetti e/o società con indirizzo fittizio o ignoto e le spedizioni vengono effettuate soprattutto da aree geografiche medio-vaste del territorio tedesco, ai confini con l'Olanda, verosimilmente perché

89) Può accadere che il gestore decida, a un certo punto, di attuare una condotta truffaldina, nota con l'espressione "exit scam", che consiste semplicemente nell'uscire di scena dalla piattaforma impossessandosi di tutte le valute sino a quel momento versate dagli acquirenti.

90) Il guadagno del gestore del market, che come detto nella maggior parte dei casi non interviene nelle trattative di compra vendita lasciate invece al diretto rapporto tra venditore e acquirente, è quindi costituito dalla quota che il venditore versa per ottenere lo spazio espositivo virtuale e dalla commissione (il "fee") che trattiene per ogni transazione.

i mittenti, per lo più residenti nei Paesi Bassi, varcano il confine per effettuare spedizioni dagli uffici postali frontalieri. In alcuni casi, anche i destinatari utilizzano nomi di fantasia; in altri, è stato invece riscontrato l'utilizzo di servizi di domiciliazione della corrispondenza, offerto da alcune aziende come Indabox e Mail Boxes Etc., che consentono di ricevere i plichi direttamente presso le caselle postali noleggiate (si tratta di un'ulteriore escamotage per eludere i controlli di polizia).

2.3.3. Da Silk Road a Wall Street Market: la storia dei più famosi illegal shops

Silk Road (che tradotto significa "via della seta") è certamente il più conosciuto fra i black markets della storia: un vero e proprio centro commerciale on-line in cui gli users potevano acquistare ogni tipo di bene, in particolare sostanze stupefacenti (per varietà di prodotti disponibili veniva anche definito "Amazon delle droghe"), in assoluta sicurezza e totale anonimato, sfruttando le più volte richiamate potenzialità in tal senso offerte dal browser Tor e dal pagamento con moneta digitale (Bitcoin soprattutto).

Il sito ha avuto una vita breve (è stato attivo solamente per due anni, tra il 2011 e il 2013), ma molto intensa: basti considerare che il 3 ottobre 2013, data dell'arresto del suo gestore, il 29enne Ross William Ulbrich che lo dirigeva con lo pseudomino "Dread Pirate Roberts", sono stati sequestrati dal portafoglio digitale di quest'ultimo più di 26.000 Bitcoin, per un controvalore all'epoca stimato in circa 3,6 milioni di euro. Peraltro, dagli accertamenti esperiti dopo il suo arresto, avvenuto nell'ambito dell'operazione denominata "Onymous"[91], è emerso un volume d'affari di circa 100 milioni di dollari e soprattutto la presenza di oltre 10.000 prodotti diversi (si trattava di un sito che ricalcava la struttura di Ebay in termini di varietà di vendite e che prevedeva, in analogia, anche un deposito di garanzia, per ridurre il rischio di truffe).

Prima di illustrare il funzionamento di Silk Road, con particolare riferimento a quelle caratteristiche cha hanno poi fatto "scuola" per tutti i successivi markets, vale la pena soffermarsi brevemente sulla figura del suo fondatore, per comprendere le motivazioni che lo hanno spinto a ideare una simile, imponente struttura virtuale dell'illegalità.

Ross William Ulbricht è nato e cresciuto ad Austin, in Texas. Sin da pic-

91) Frutto della cooperazione tra diverse agenzie di polizia internazionali (FBI, Interpol e European Cybercrime Centre di Europol).

colo aveva dimostrato di essere molto capace negli studi, specialmente in materie come scienze dei materiali e fisica (conseguì infatti la Laurea in fisica presso l'Università del Texas). Si interessava, inoltre, anche all'economia, con un particolare interesse per le teorie del "libertarianismo americano"[92], fondate sulla libertà in ogni ambito (Ulbricht riteneva che tra i principi irrinunciabili ci fosse la libertà di ogni persona su se stessa e sul proprio corpo; in altre parole, ognuno poteva decidere liberamente se usare droghe o altro). Inoltre, era affascinato anche da una variante specifica di questo pensiero, l'"agorismo"[93], che sosteneva l'idea di una economia fatta di mercati liberi e volontari, come forma di resistenza al potere statale.

Fu proprio da queste idee che Ulbricht prese l'ispirazione per creare Silk Road; un sito che, da un lato, si atteneva a ferree regola di funzionamento (non era ammessa la vendita di materiale pedopornografico, di merci rubate, né di prodotti che potessero danneggiare altri, ma solamente di armi per autodifesa), ma dall'altro riconosceva la piena libertà di acquistare stupefacenti anonimamente e senza lasciare alcuna traccia della transazione economica (inizialmente vendeva, spedendoli per posta agli acquirenti, funghi allucinogeni che egli stesso coltivava).

Sulla sua pagina del social network Linkedin, Ulbricht, riferendosi a Silk Road e al suo desiderio "*di usare la teoria economica come mezzo per poter abolire l'uso della coercizione e dell'aggressività fra gli uomini*", così si esprimeva: "*Io sto creando una simulazione di un'economia affinché sia possibile dare alle persone un'esperienza di prima mano di come sarebbe poter vivere in un mondo dove non esista l'uso sistemico della forza*". Riteneva, in sintesi, che l'uso di stupefacenti fosse una questione di libertà, di scelta personale e che le politiche proibizioniste fossero un completo fallimento.

Su tali premesse, Silk Road divenne in breve il primo marketplace del web a offrire ai propri clienti una vasta ed economica selezione delle migliori sostanze stupefacenti reperibili al mondo, dall'hashish pakistano alle droghe sintetiche da laboratorio. Non solo, con il passare del tempo, la possibilità di

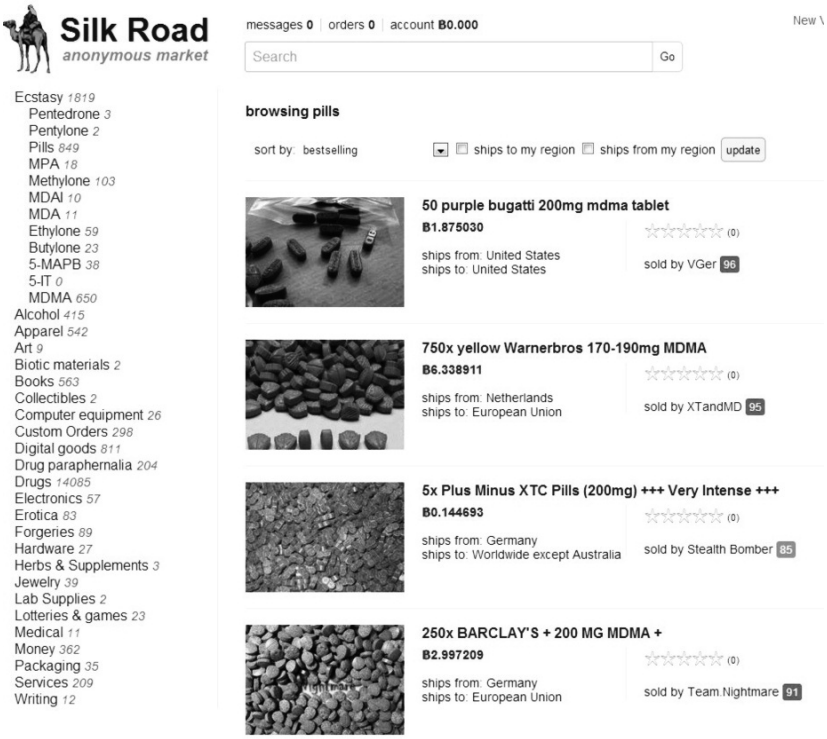
92) Il "libertarianismo" o "libertarismo" è un insieme di filosofie politiche tra loro correlate che considerano la libertà come il più alto fine politico. Ciò generalmente include la libertà individuale, la libertà politica e la libertà di associazione.

93) L'"agorismo" è una filosofia politica libertaria, fondata da Samuel Edward Konkin III come soluzione ideale per approdare ad una società dove tutte "le relazioni tra persone siano scambi volontari, un libero mercato". Il termine deriva dalla parola greca "agorà", la piazza aperta al libero scambio, alle assemblee e al mercato nelle città-stato greche.

acquisto venne estesa ai prodotti contraffatti, ai documenti falsi e, a partire dal marzo 2012, superando le regole iniziali che il fondatore si era imposto, anche a diverse tipologie di armi e al materiale pornografico.

L'accesso al sito Silk Road avveniva con una semplice registrazione: era infatti sufficiente fornire un nome utente, una password e un codice identificativo per le transazioni, nonché rispondere a un CAPTCHA per accedere all'homepage e usufruire di tutti i servizi offerti. Non tutte le pagine del sito erano pubbliche: esisteva, infatti, una "stealth listings", vale a dire una serie di pagine realizzate in modalità occultata, di cui potevano usufruire solo alcuni venditori, contattabili da una clientela selezionata solo attraverso messaggi privati in una specifica sezione (si faceva riferimento a "custom orders", vale a dire ordini personalizzati).

La droga costituiva una buona fetta dei prodotti disponibili: sul totale, la cannabis rappresentava il 18% dell'offerta, seguita dall'ecstasy e dagli stimolanti entrambi con il 17%. A seguire, si collocavano gli psichedelici (15%) e i farmaci (15%). Infine, gli steroidi con il 9% e, per finire, con il 4% sia i precursori che gli oppioidi (nella figura sottostante, la homepage del sito, con a sinistra il menu a tendina relativo agli stupefacenti).



La vendita di cannabis, con i suoi sottoprodotti e preparazioni (526 diversi articoli), rappresentava come detto il maggior introito di Silk Road (coinvolgeva ben 192 venditori, di cui 162 dagli Stati Uniti). La maggior parte di loro (152) vendeva al minuto, con quantità che andavano da un grammo fino al massimo di 100 grammi, per importi da 0,30 Bitcoin fino a 2 Bitcoin. 40 di loro, invece, vendevano anche all'ingrosso, offrendo quantità di merce anche da 5 kg., con transazioni che variavano dai 15 ai 300 Bitcoin. La maggior parte dei prodotti (131) era offerta al solo mercato statunitense; 28 prodotti dagli Stati Uniti raggiungevano tutto il resto del mondo (soprattutto le piante) e 9 dagli Stati Uniti venivano spediti in Canada.

Nel suo periodo più florido, Silk Road contava circa 277 venditori di sostanze stupefacenti; per ognuno era presente una pagina dedicata, che offriva, al pari di un qualsiasi altro market on-line ben organizzato, tutte quelle informazioni che ne formavano il profilo pubblico e che contribuivano ad aumentarne la reputazione (fondamentale, come già spiegato, per guadagnare la fiducia degli acquirenti e espandere conseguentemente la propria attività di vendita). Più in dettaglio, la pagina dedicata a ciascun venditore offriva informazioni dettagliate:

– oltre che sull'indice di gradimento ottenuto, sulle modalità di comunicazione con gli acquirenti e sulla disponibilità di nuovi prodotti e servizi;

– sulle modalità di pagamento e di spedizione della merce acquistata. In particolare, si faceva riferimento:

- al *Packaging*: confezioni non appariscenti (in "business style"), con busta a chiusura ermetica sottovuoto che garantiva l'assenza di odori e l'integrità della merce, oltre che la resistente all'umidità;
- allo *Shipping*: spedizioni in tutto il mondo entro quarantotto ore senza spese. Gli ordini superiori ai 200 dollari venivano spediti tramite i maggiori corrieri internazionali, come UPS, DHL, TNT e Fedex;
- al *Delivery time*: venivano indicati i tempi medi per il ricevimento della merce per ogni Paese (compresa Città del Vaticano);
- al *Refund* quale modalità di rimborso in caso di non ricezione della merce;
- alla *Privacy*: il venditore garantiva che tutte le informazioni sull'identità dei clienti sarebbero state cancellate subito dopo le transazioni e le spedizioni andate a buon fine;
- al *Support*: veniva fornito un indirizzo e-mail alternativo e una chat in caso di non funzionamento temporaneo del sito (veniva ovviamente raccomandato l'uso della crittografia in tutte le comunicazioni).

Una volta scelto il prodotto e inserito nel carrello personale, l'acquirente

poteva passare al pagamento, unicamente tramite Bitcoin. Anche Silk Road adottava il metodo del deposito di garanzia: il cliente non pagava direttamente al venditore, ma depositava la cifra stabilita presso l'operatore del mercato che in tal modo controllava tutte le transazioni, trattenendo la propria percentuale e risolvendo eventuali dispute. Non erano permessi pagamenti diretti, pena l'espulsione dal sito. Inoltre, sul sito veniva suggerito ai clienti di effettuare acquisti solo presso venditori con feedback positivi, oltre a essere segnalato che le commissioni sarebbero state utilizzate anche per ripagare i clienti truffati, a riprova del "comportamento corretto" di quella comunità.

Come per tutti i mercati on-line, anche il sito Silk Road, allo scopo di garantire e garantirsi il più completo anonimato, proteggeva tutte le comunicazioni, dai messaggi e-mail fino alle transazioni, tramite PGP (Pretty Good Privacy), il metodo crittografico a doppia chiave (pubblica e privata o segreta), il cui funzionamento è stato già illustrato con riferimento all'utilizzo della rete Tor.

Ma torniamo all'arresto del fondatore del sito, avvenuto il 1° ottobre 2013 in una biblioteca di San Francisco, per evidenziare alcuni aspetti che hanno caratterizzato le lunghe indagini condotte sotto copertura dagli agenti dell'FBI. Il primo passo delle investigazioni fu quello di estrapolare dalla rete un messaggio che menzionava l'esistenza di Silk Road. Si trattava di un messaggio, che risaliva al 27 gennaio 2011, pubblicato su un forum dedicato all'uso dei funghi allucinogeni chiamato "Shroomery". Un utente con il nickname "Altoid" linkò "Silk Road", scrivendo: "*Mi sono imbattuto in un sito che si chiama Silk Road, sto pensando di comprarci sopra… Fatemi sapere cosa ne pensate*". Solo dopo, gli investigatori capirono che si era trattato del primo errore commesso da Ulbricht, che aveva postato il commento per pubblicizzare il suo nuovo sito. Due giorni più tardi, un utente con lo stesso nickname scrisse un messaggio simile, sul forum "Bitcoin Talk", dedicato alla discussione su Bitcoin, sulla tecnologia blockchain e sulla criptovaluta, messaggio in cui definiva Silk Road un "Amazon.com anonimo" (si trattava del secondo errore commesso da Ulbricht). Otto mesi più tardi sempre "Altoid" scrisse nuovamente sul forum "Bitcoin Talk", segnalando l'esigenza di reperire un esperto di information technology che fosse pratico di Bitcoin per una startup. Nello stesso messaggio, Ulbricht commise il terzo errore: indicò che gli interessati potevano scrivere all'indirizzo di posta elettronica "rossulbricht@gmail.com" (corrispondente al suo vero nome), indirizzo che modificò immediatamente, senza però precludere all'FBI la possibilità di estrapolarlo.

Nel frattempo le indagini su "Dread Pirate Roberts", pseudomino uti-

lizzato dal gestore di Silk Road, permisero di risalire a un internet café di San Francisco (che si trovava vicino alla casa di un amico da cui si era trasferito), dal quale Dread Pirate Roberts accedeva alla piattaforma utilizzando una VPN (Virtual Private Network) per creare un falso indirizzo IP e nascondere così la propria posizione (peraltro, come poi scoperto dall'FBI, tramite lo stesso pc Ulbricht aveva più volte fatto accesso alla sua casella di posta Gmail).

Ma continuando con la ricostruzione delle fasi salienti delle indagini all'epoca svolte, un ulteriore e imperdonabile errore commesso da Ulbricht lo si rinviene allorquando, a marzo del 2012, su "StackOverflow", un sito per programmatori informatici, un utente pubblicò una domanda molto specifica. La domanda, che riportava anche alcune righe di codice, riguardava un "servizio nascosto su Tor". Il codice della domanda sul forum era identico in molte parti a quello utilizzato nella programmazione del server principale di Silk Road. L'errore plateale, in quest'occasione, fu il nickname con cui venne postata la domanda: Ross Ulbricht. Meno di un minuto dopo il nickname venne cambiato in "Frosty", ma ormai l'FBI aveva acquisito una prova importante che collegava Ulbricht alla gestione del sito Silk Road.

Ulbricht fu arrestato quando si trovava nella sezione "Glen Park" della biblioteca pubblica di San Francisco. Per evitare che egli crittografasse o eliminasse i dati riferiti al sito dal computer portatile che stava utilizzando nella biblioteca nel caso in cui si fosse accorto che stava per essere arrestato, due agenti finsero di litigare all'interno della biblioteca. Quando fu distratto dal litigio dei due, un altro agente prese il suo computer e vi inserì subito una chiavetta USB nella quale copiò tutti i dati presenti nell'hard disk del computer. Si trattò di un'operazione fondamentale per il prosieguo degli accertamenti sul market, parte dei quali investì anche l'Italia, come verrà in seguito evidenziato.

Il 30 maggio 2015, Ross Ulbricht è stato condannato in primo grado all'ergastolo, tra l'altro, per i reati di associazione per delinquere, frode informatica, distribuzione di false identità, riciclaggio di denaro e traffico di droga.

Nel corso delle indagini a carico del fondatore di Silk Road sono anche emersi alcuni particolari inquietanti. L'FBI, nel marzo del 2013, scriveva che "Dread Pirate Roberts" aveva perfino contattato un utente di "Silk Road" per commissionare un omicidio. La vittima designata era un altro utente, un canadese con il nickname "FriendlyChemist", che lo stava ricattando, chiedendogli 500 mila dollari per non rivelare l'identità di migliaia di utenti del market. Qualche tempo dopo, il presunto killer, contattato da Dread Pirate Roberts, mandò una foto per provare che l'omicidio (del quale le autorità canadesi non hanno comunque mai trovato traccia) era stato portato a termine, ottenendo

un compenso di 150 mila dollari in Bitcoin. Inoltre, Ulbricht è stato anche accusato di aver pagato 80 mila dollari a un agente dell'FBI (che stava operando sotto copertura) per torturare e uccidere un ex dipendente. Credeva che il dipendente fosse compromesso dopo che lo stesso agente sotto copertura aveva contattato Ulbricht, presentandosi come un trafficante di droga, per organizzare uno scambio di un chilo di cocaina. In quella circostanza, il dipendente sottrasse una grande somma in Bitcoin, inducendo Ulbricht, secondo la ricostruzione delle indagini, a intervenire per fare in modo che l'agente sotto copertura prima ottenesse la restituzione dei Bitcoin e poi uccidesse il dipendente infedele. All'epoca l'FBI inviò delle foto non veritiere dell'omicidio a Ulbricht, che rispose testualmente: "*Sono un pò scosso, ma va bene*".

Dopo l'arresto di Ulbricht, dall'analisi dei files rinvenuti nei server sequestrati, l'FBI è riuscita a estrapolare un'innumerevole quantità d'informazioni relative a migliaia di utenti collegati da ogni parte del mondo, tra i quali figuravano anche soggetti italiani. Per questo, nel 2014, la DCSA (Direzione Centrale per i Sevizi Antidroga) italiana, alla quale l'FBI aveva trasmesso alcuni supporti informatici d'interesse, ha avviato un'autonoma attività di analisi dei dati reperiti, concentrata in particolare su due utenti, con nickname "Boss" e "Bulldogistheboss", risultati poi essere venditori di stupefacenti collegati fra loro. In particolare, "Boss", secondo i dati forniti dall'FBI, aveva creato il proprio profilo sulla piattaforma di Silk Road il 10 ottobre 2012 (giorno in cui aveva anche concluso la sua prima vendita), profilo che non ebbe vita lunga, considerato che risulta essere stato chiuso il 17 gennaio 2013. Il periodo di operatività di "Boss", pur essendo stato relativamente breve, è stato comunque molto intenso; le transazioni all'epoca concluse, infatti, ammontano a 284[94], con un volume d'affari di circa 53.200 dollari, cifra che aveva portato gli inquirenti a posizionare lo stesso in una fascia di venditori medio alta. Con riferimento, invece, agli acquirenti di "Boss", dall'analisi dei dati informatici è emersa una fitta rete di conversazioni avvenute tra il venditore italiano e un soggetto svedese (con nickname "Widia"), interessato all'acquisto principalmente di eroina, probabilmente da rivendere al dettaglio su strada in quello Stato[95].

---

94) Le vendite riguardavano in 165 casi l'eroina, in 44 l'hashish, in 33 la cocaina, in 28 il metilenediossipirovalerone (MDVP) e in 13 la marijuana.

95) In una conversazione intercettata, "widia" così si esprime con "BOSS": "*controlla se la dogana svedese ha già trovato per caso qualcuna delle tue consegne, attendo 3-5 ore per ordinare 10 grammi di eroina e se i Bitcoin sono abbastanza anche cocaina. Sono deluso del campione di 0,6, era migliore l'ultima consegna, per il resto in Scandinavia l'eroina è molto richiesta*".

Ai primi di novembre del 2013, poco dopo l'arresto di Ulbricht, veniva annunciata la riapertura di Silk Road da parte dello pseudonimo "Dread Pirate Roberts", che accoglieva i visitatori del nuovo market, il "Silk Road 2.0", con un messaggio di benvenuto: "*È con grande gioia che vi annuncio un nuovo capitolo della nostra avventura. Silk Road è risorto dalle ceneri e ora è pronto ad accogliervi*". Anche Silk Road 2.0 non ebbe vita lunga: il 6 novembre 2014, infatti, venne chiuso dall'FBI che arrestò il suo amministratore identificato in tale Blake Benthall, 26enne di San Francisco, soprannominato "Defcon".

In realtà, nel frattempo, il sito "reddit.com"[96] aveva riportato, a gennaio del 2014, una nuova versione (la terza) di Silk Road, denominata Silk Road Reloaded, questa volta accessibile non da Tor ma dall'altra rete anonima I2P. Silk Road Reloaded presentava un catalogo di svariate sostanze stupefacenti, nonché di denaro falso, di false identità e di tools per condurre attacchi informatici. Inoltre, supportava transazioni con diverse criptovalute (gli Anoncoin, i Darkcoin, che a novembre sono stati ammessi come valuta su "Nucleas" - altro bazar di Tor, i Dogecoin, i Litecoin e tutti gli otto tipi di Altcoin) e i gestori del sito guadagnavano una percentuale non solo su ogni vendita, ma anche per ogni conversione di valuta in Bitcoin.

Il rilancio di Silk Road Reloaded aveva all'epoca evidenziato con forza un concetto importante, vale a dire che si potevano implementare con relativa facilità innumerevoli alternative a Tor e ai Bitcoin, azzerando in quel modo tutti gli sforzi sino ad allora compiuti dalle forze dell'ordine in termini di contrasto del fenomeno, in costante e pericolosa espansione.

Dopo le 3 versioni di Silk Road, è stata registrata in rete l'operatività di altri black markets, tra i quali, uno dei più floridi, è stato certamente AlphaBay, attivo tra la fine del 2014 e il luglio del 2017, sul quale, tanto per dare un'idea, operavano circa 40.000 venditori ed erano registrati oltre 200.000 utenti e 250.000 inserzionisti. Il volume d'affari, generato in gran parte dagli utenti che erano emigrati da un altro market chiamato Evolution (chiuso per exit scam), era stimato in circa 800.000 dollari giornalieri. Il market venne creato da un esperto di informatica, il 25enne Alexandre Cazes, il quale – grazie alla gestione del sito – era riuscito ad accumulare una fortuna di oltre 23 milioni di dollari, sparsi in paradisi bancari, da Cipro al Liechtenstein, alla Svizzera e alla Thailandia. Nel 2017, il suo arresto a Bangkok da parte dell'FBI fu conseguenza del suo ossessionante desiderio di mostrare la propria ricchezza ad

96) "Reddit" è un sito Internet di social news, intrattenimento e forum, dove gli utenti registrati possono pubblicare contenuti sotto forma di post testuali o di collegamenti ipertestuali.

amici e parenti. Di Cazes, infatti, gli inquirenti erano inizialmente in possesso soltanto di un indirizzo email (*Pimp_Alex91@hotmail.com*), utilizzato per dare il benvenuto ai nuovi utenti del sito. La sua localizzazione nel mondo avvenne però mediante una foto della Porsche Panamera che possedeva. In particolare, Cazes – mosso proprio da quella frustrazione di non poter mostrare in pubblico la sua ricchezza – su un forum denominato "RooshV", dedicato a come "conquistare le ragazze", di fronte alla sfida di un interlocutore, mostrò la sua Porsche raccontando come fosse "fondamentale" per attirare l'attenzione delle ragazze in Thailandia. Da quel momento, il suo arresto, operato dall'Interpol, fu solo questione di qualche ora. L'FBI, all'epoca, sequestrò 4 auto Lamborghini e tre case per un valore stimato di circa 11,8 milioni di dollari. Cazes, prima dell'estradizione chiesta dagli Stati Uniti, si suicidò strangolandosi in carcere.

La ricchezza di Cazes, oltre che dall'incasso delle commissioni sulle trattative di compra-vendite, derivava anche e soprattutto dall'investimento dei soldi che gli utenti depositavano sull'escrow del market a titolo di deposito di garanzia. "AlphaBay", infatti, agiva come una banca, per stessa ammissione dei suoi amministratori che così si esprimevano: "*… potete vedere Alphabay come una banca… I soldi depositati nei portafogli non restano lì freddi: investiamo in svariate cose in forma anonima, guadagniamo con quegli investimenti, assicurandoci sempre il 100 per cento della riserva*"[97].

Dopo la chiusura di Alphabay, gli utenti di quella piattaforma si spostarono su altri mercati, in particolare, su Hansa market, altro sito di vendita di beni e servizi illeciti, già attiva dal 2013 e chiuso definitivamente dalla polizia olandese nel luglio del 2017, dopo circa un mese di attività sotto copertura che aveva consentito agli investigatori di prendere il pieno controllo dei server del market.

In tale quadro generale, lo smantellamento della piattaforma denominata Berlusconi Market (considerato uno dei 25 principali black market sinora esistiti in rete) costituisce l'unico successo tutto italiano nel contrasto dei traffici on-line. Si tratta di un'operazione, denominata "Darknet.Drug", conclusa a novembre 2019 dal Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza di Roma, al termine di un'attività investigativa avviata a maggio 2019 e coordinata dalla Direzione distrettuale antimafia di Brescia.

97) Nel 2016, Cazes – a riprova delle sue capacità informatiche – introdusse anche un "cryptocurrencies tumbler", ovvero un meccanismo di mescolamento di fondi di criptovaluta potenzialmente identificabili o "contaminati" con altri, in modo da oscurare la traccia alla fonte originale del fondo.

L'organizzazione del market era interamente italiana, per la precisione pugliese, e il mercato era gestito da due utenze: "Vladimir Putin", con il ruolo di amministratore[98] ed "Emmanuel Macron", quale moderatore. A partire da gennaio 2019, Berlusconi Market ha certamente rappresentato il più importante mercato della darknet, sia per quantità di oggetti in vendita (è addirittura arrivato a pubblicizzare oltre 103.000 annunci di prodotti illegali[99]), sia per il volume degli scambi[100].

La modalità d'indagine che ha consentito di risalire all'identità degli ideatori e gestori del market rientra tra le più classiche. Gli investigatori hanno infatti acquistato (ricorrendo all'operazione speciale dell'acquisto simulato) alcune dosi di cocaina da un venditore[101], riuscendo a scoprire che tutti i pacchi venivano spediti da un ufficio postale di Barletta (BT). In seguito, grazie a una telecamera installata presso quella sede postale, hanno individuato l'attivissimo venditore, un 26enne, anch'egli di origine pugliese, successivamente tratto in arresto unitamente al gestore del market e ad un terzo soggetto italiano (dagli accertamenti svolti dopo l'arresto, è emerso che i tre avevano suddiviso tra loro i proventi illeciti maturati ammontanti a 41 Bitcoin – pari a circa 400.000,00 euro – a fronte di un volume complessivo di transazioni annue pari a circa 2 milioni di euro).

Nel corso dell'operazione sono stati sequestrati anche 2,2 kg. di sostanza stupefacente (cocaina, ketamina, MDMA) pronta per essere commercializzate in rete, 163 pasticche di ecstasy e 78 francobolli impregnati di LSD. Inoltre, è stato sottoposto a sequestro un locale commerciale, sito in Barletta (BT), in cui veniva esercitata l'attività di exchange di Bitcoin.

Dagli accertamenti eseguiti sui server e sui dispositivi informatici sequestrati nel corso dell'operazione, è emersa la reale portata del mercato, nel

---

98) Poi identificato in tale Luis Di Vittorio, 19 enne di origine pugliese, studente del Politecnico di Torino, il quale, in una conversazione telefonica con la fidanzata, così si esprimeva: "*Se mi devono condannare per tutti i crimini che ho fatto, devono prendere la chiave e la devono buttare! Sostituzione di persona! Documenti falsi! Spaccio internazionale! Tutto! Si spicciano prima a dire cosa non ho fatto*".

99) Dato rilevato alla data del 24 giugno 2019, durante il monitoraggio del market.

100) Vds. "Relazione annuale 2019" della DNA, nella parte in cui riporta testualmente: "*Si è accertato, ad esempio (a maggio 2019) che: (...) nell'ultimo mese, precedente alla cattura della schermata, sono stati effettuati ordini per 607.681,68 €; sul wallet escrow di Berlusconi Market sono presenti 2,46032162 Bitcoin (€ 23.263,00); sul wallet escrow di Berlusconi Market sono transitati 41,86789478 Bitcoin (€ 395.000,00)*".

101) Conosciuto nel giro con il nickname "G00d00", riceveva richieste di acquisti oltre cha da varie parti d'Europa, anche dagli Stati Uniti e perfino dall'Australia.

quale gli svariati prodotti in vendita erano organizzati nelle seguenti categorie:

– servizi relativi ai cosiddetti "Bank Drops", in virtù dei quali un intermediario si offre di effettuare una transazione su un conto corrente indicato dal cliente, dietro pagamento di una commissione pari ad una certa percentuale della transazione effettuata. Tale servizio viene generalmente richiesto quando si vuole celare la provenienza di una certa disponibilità finanziaria (anche in Bitcoin) che verrà inviata all'intermediario, il quale provvederà a recapitare la somma al destinatario finale tramite un tradizionale bonifico bancario da un conto corrente "pulito" a sua disposizione[102];

– annunci relativi a documenti di identità, nazionali ed esteri, riportanti i segni distintivi dei rispettivi Paesi (si trattava di documenti sia materiali che digitali. In particolare, con i documenti di identità digitali esiste la possibilità da parte dei clienti di acquistare il c.d. "template", ovvero veri e propri file editabili sui quali inserire dati anagrafici e fotografie a piacimento degli utilizzatori finali, per poi stampare un numero illimitato di documenti falsi);

– annunci (più di 30.000) di vendita relativi a farmaci\psicofarmaci (quali, Benzos) e sostanze stupefacenti, con la suddivisione in: "cannabis & hashish", "dissociatives" (allucinogeni dissociativi), "ecstasy" (MDMA o ecstasy), "opioids" (oppioidi), Prescription (medicinali soggetti a prescrizione medica), "steroids" (steroidi), "stimulants" (stimolanti), "psychedelics" (sostanze pischedeliche), oltre ovviamente alla cocaina e all'eroina. Erano inoltre presenti le voci "pharaphernalia" (strumenti per l'alterazione e prodotti per il trattamento delle sostanze stupefacenti) e "other" (riferita a sostanze e farmaci non categorizzati);

– annunci (circa 600) riguardanti la vendita di oro, argento e altri prodotti di gioielleria, verosimilmente di provenienza illecita o contraffatti;

– annunci (circa 5.000) relativi alla vendita di armi (anche da guerra tipo Kalashnikov), esplosivi e munizionamento;

– software comprendenti diverse categorie di applicativi di carattere dannoso (virus informatici), tra cui Botnet, Malware ed Exploits;

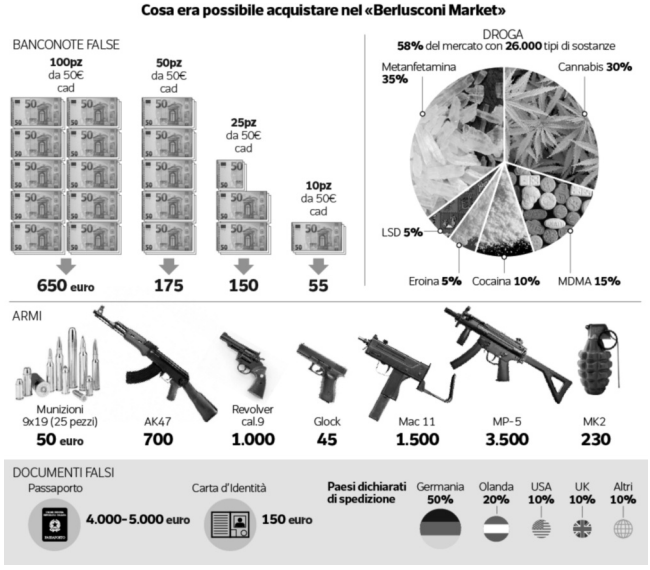
– servizi di "Security & Hosting", tra cui utilità di controllo remoto e VPN utili a celare il proprio indirizzo IP (tutti strumenti volti ad incrementare le misure di sicurezza in termini di anonimato).

---

102) Uno dei servizi di "bank drop" offerto era quello di un venditore apparentemente operante in territorio italiano, che si offriva come intermediario per il riciclaggio di disponibilità illecitamente acquisite, con un compenso pari al 35% della somma "da ripulire".

Tanto per dare un'idea delle varie offerte disponibili, basti pensare che su Berlusconi Market era possibile acquistare, a meno di 5.000 euro, un passaporto Usa e a un prezzo leggermente inferiore un passaporto italiano, tedesco, olandese o francese. Un Ak 47 costava 700 euro e 230 euro erano sufficienti per ottenere una bomba a mano (risultavano disponibili anche revolver e pistole di vario tipo, oltre a fucili e mitragliatrici). La droga più trattata era la metanfetamina, seguita da cannabis, MDMA e cocaina[103].

Nella figura sottostante sono indicati alcuni dei prodotti in vendita, con il relativo costo.



Concludendo su Berlusconi Market[104], da un punto di vista organizzativo, il sito ripercorreva l'architettura delle altre piattaforme in rete. La creazione di un account era estremamente semplice; bastava, infatti, impostare username

103) Un sesto del fatturato era inoltre costituito da dati bancari e banconote false, che si acquistavano a pacchetti: 650 euro per 100 pezzi da 50 euro. Gli acquirenti, invece, provenivano in gran parte da Olanda e Germania.

104) Uno studio dell'Università di Oxford dell'aprile 2018, posizionava Berlusconi Market al quarto posto dopo il più antico Dream Market e dopo Tochka e Wall Street (del quale si parlerà in seguito). Peraltro, quando Dream Market, all'inizio del 2019, chiuse per motivi ignoti, "Putin" e "Macron" commentarono non sapendo di essere intercettati: "*Dream Market sta per chiudere, serve una full immersion*". E infatti, nei mesi successivi, i venditori di Dream Market transitarono in gran parte nella piattaforma dello studente italiano, facendo schizzare in alto, in maniera esponenziale, il numero degli annunci.

e password (il criterio era sempre lo stesso: consentire una facile navigazione anche a chi non possedeva elevate conoscenze informatiche). Come detto, l'operazione della Guardia di finanza è unica nel suo genere in Italia ed è considerata importante a livello mondiale; analogamente alle due che hanno portato all'arresto, rispettivamente, nel 2013, dell'americano Ross Ulbricht (fondatore e gestore di Silk Road) e nel 2017 del canadese Alexandre Cazes (gestore di AlphaBay e Hansa Market), rappresenta certamente uno dei maggiori successi investigativi nel panorama delle attività sinora svolte con riferimento al contrasto dello specifico fenomeno.

Oltre a quelli sinora descritti, in rete è stata registrata, più o meno contemporaneamente, l'intensa attività di altri black markets, quali Samsara Market, Silkroad 3.0, Empire Market, Bitcoinpharma, Olympus e, soprattutto, Wall Street Market, uno dei più recenti, chiuso nel mese di maggio del 2019, nel corso di un'operazione condotta da Europol e dalla polizia criminale federale tedesca (Bundeskriminalamt), con la collaborazione delle agenzie statunitensi DEA ed FBI.

Il Wall Street Market, sul quale si commercializzavano principalmente narcotici, armi e dati rubati, al momento della chiusura contava oltre 5.000 venditori (con circa 63.000 registrazioni di vendita) e oltre 1 milione di clienti.

L'operazione, che ha inizialmente portato all'arresto di tre cittadini tedeschi, considerati gli amministratori del sito, e di altri due soggetti (risultati essere i venditori di droga più attivi), si è protratta nel tempo, concentrandosi sull'analisi dei dati informatici riguardanti in particolare la "exit scam" (la truffa informatica) attraverso la quale i suoi amministratori, subodorando le indagini a loro carico, avevano dirottato numerosi Bitcoin su conti a loro riferibili.

A distanza di poco più di un anno (nel settembre del 2020), in tutto il mondo, nell'ambito dell'operazione denominata "DisrupTor"[105], sono stati arrestati ben 179 venditori del market[106], responsabili di decine di migliaia di vendite di beni illeciti in tutta Europa e negli Stati Uniti. Nella circostanza,

105) L'importanza di tale operazione risiede nella proficua forma di collaborazione instaurata tra le forze di polizia e le autorità giudiziarie di diversi Paesi (Austria, Cipro, Germania, Paesi Bassi, Svezia, Regno Unito, Australia, Canada e Stati Uniti). Gli approfondimenti investigativi svolti sui server sequestrati e il costante, reciproco scambio di informazioni sono risultanti determinanti ai fini dell'identificazione dei venditori e alla loro localizzazione in ogni parte del mondo.

106) 121 negli Stati Uniti, 42 in Germania, 8 nei Paesi Bassi, 4 nel Regno Unito, 3 in Austria e 1 in Svezia.

sono stati sequestrati oltre 6,5 milioni di dollari, sia in contanti che in valuta digitale, oltre a circa 500 chilogrammi di droghe (tra cui fentanyl, ossicodone, idrocodone, metanfetamina, eroina, cocaina, ecstasy, MDMA) e a svariate armi da fuoco.

2.4. I traffici e le reti sociali

Il fenomeno del traffico on-line di droga e armi, oltre al mondo del web, ha via via interessato altri ambiti informatici che nel tempo e con andamento differenziato (come verrà in seguito evidenziato) hanno "fatto irruzione" nella vita di ogni individuo, tanto da diventare oggi elementi imprescindibili della quotidianità di ciascuno di noi. Il riferimento è alle tantissime "reti sociali" esistenti: da un lato, i social network (in particolare Facebook, Instagram e Twitter), dall'altro, i servizi di messaggistica istantanea (fra tutti, Telegram e Wickr).

2.4.1. Le vendite sui social network: un fenomeno in calo

Le attività criminali legate al commercio di droga che si sviluppano sui social network, dopo una iniziale, rapida diffusione, hanno fatto registrare un andamento decisamente calante, soprattutto da quanto tali piattaforme, in ragione della necessità di contrastare le cc.dd. "fake news" e nel contempo rispettare il GDPR[107], hanno notevolmente innalzato il livello di controllo relativo all'identificazione dei propri clienti (c.d. "Know Your Customer" - KYC[108]). Basti pensare che per aprire un profilo bisogna fornire un'utenza te-

---

107) Il Regolamento Generale sulla Protezione dei Dati (GDPR in inglese General Data Protection Regulation) è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno (operativo a partire dal 25 maggio 2018). Con questo regolamento, la Commissione europea si prefigge l'obiettivo di rafforzare la protezione dei dati personali di cittadini dell'Unione europea e dei residenti nell'UE, sia all'interno che all'esterno dei confini dell'UE, restituendo ai cittadini il controllo dei propri dati personali, semplificando il contesto normativo che riguarda gli affari internazionali, unificando e rendendo omogenea la normativa privacy dentro l'UE.

108) *Know Your Customer* ("Conosci il Tuo Cliente", talvolta indicata come *Know Your Client* e spesso abbreviata in KYC) è un'espressione con cui si indica un processo di riconoscimento utilizzato dalle aziende per verificare l'identità dei propri clienti e per valutare potenziali rischi o intenzioni illegali nel rapporto con il cliente. Il termine fa spesso riferimento alle regolamentazioni bancarie e alle normative anti-riciclaggio che regolano queste attività.

lefonica e un'e-mail, che vengono poi verificate tramite l'invio di codici di sicurezza; in alcune circostanze, viene perfino richiesto all'utente, per garantire una sorta di "Adeguata verifica" della propria identità, di inviare una foto in cui compaia anche un suo documento di riconoscimento e la data della foto.

Ciò non vuol dire che le attività criminali legate principalmente agli stupefacenti non trovino più alcuno spazio sui social network, ma certamente che in quell'ambito hanno subito un forte ridimensionamento. Peraltro, nella maggior parte dei casi, esse si concretizzano all'interno di gruppi privati con accesso su invito, i cui membri ovviamente non hanno alcun interesse a segnalarne l'esistenza.

2.4.2. La messaggistica istantanea: le chat cifrate e i c.d. "criptofonini"

Discorso completamente diverso vale per i servizi di messaggistica istantanea, la cui diffusione è sempre più ampia e veloce, soprattutto tra i giovani (nell'attuale periodo di restrizioni alla mobilità imposte con le norme di contenimento del coronavirus il ricorso a tali servizi per acquistare droga è esponenzialmente cresciuto).

In termini generali, si può dire che le *app* di messaggistica criptata si collocano a metà strada tra il mercato delle droghe on-line[109] e quello di strada, in quanto offrono un metodo rapido, conveniente e sicuro per entrare in contatto con gli spacciatori, senza troppa fatica, non essendo neanche richiesta una particolare competenza informatica.

Rispetto ai traffici nel *dark web*, attraverso i servizi di messaggistica vengono tendenzialmente acquistate quantità inferiori di stupefacenti, con trattative tra venditore e cliente che però avvengono con maggiore dinamicità e velocità.

Anche utilizzando le *app*, il meccanismo di acquisto è molto semplice e viene ampiamente pubblicizzato dai venditori. Il pagamento viene generalmente effettuato con valuta digitale (per garantire l'anonimato), ma alcuni consentono anche pagamento tramite PayPal (con la raccomandazione, però, di utilizzare amici e familiari in modo da sviare la sorveglianza sulle transazione). La spedizione avviene di massima con plichi confezionati "a prova di controlli", spesso con pacchetti con doppio vuoto sigillati per evitare la pro-

109) I due "servizi" (siti web e *app*) non sono in antagonismo, ma si completano. Molti venditori presenti nel *dark web* sono attivi anche su Telegram, WhatsApp o Instagram e/o, comunque, spesso rimandano la fase della contrattazione proprio su tali applicazioni.

pagazione dell'odore o con l'utilizzo di carta carbone per neutralizzare le scansioni. La consegna, infine, avviene in modo discreto, all'indirizzo che viene pattuito (mai corrispondente al reale destinatario). Si tratta, quindi, di un servizio completo, con tanto di consigli su dove acquistare criptovaluta con pochi e semplici passaggi.

Il motivo per cui l'utilizzo delle *app* di messaggistica istantanea per la commercializzazione di stupefacenti è in continua crescita è facilmente comprensibile; si tratta di sistemi che garantiscono la sicurezza e la privacy delle comunicazioni tra gli utenti, grazie a una crittografia forte e avanzata.

Tra le tante, Wickr è certamente considerata una delle più sicure[110]; non richiede per la registrazione né il numero di telefono, né un'email, ma è sufficiente impostare un nickname.

Inoltre, Wickr è stata una delle prime *app* ad aver implementato i messaggi a scomparsa. Si può impostare un arco temporale (da 6 ore a 6 giorni), trascorso il quale i messaggi inviati si autodistruggono, senza lasciare alcuna traccia. In aggiunta all'Expiration Timer (tempo di scomparsa), esiste un'ulteriore opzione definita Burn-On-Read Timer. Quest'ultima, se impostata prima dell'invio del messaggio, serve a cancellarlo dopo che il ricevente l'ha letto.

Wickr è' considerata una delle più sicure[111] perché è dotata di una crittografia molto forte, il Wickr Secure Messaging Protocol[112], che in pratica impedisce a chi dovesse rubare o sequestrare il dispositivo di leggere i messaggi.

Inoltre, crea un database di archiviazione crittografato su ogni dispositivo per memorizzare i dati sensibili come le chiavi d'identità, i messaggi e i dati dell'account. Questo database viene decriptato durante le sessioni di accesso attive e il suo contenuto viene utilizzato per le normali operazioni. Quando l'utente si disconnette, il database viene nuovamente criptato con una chia-

110) È utilizzata anche dal Dipartimento della difesa degli Stati Uniti ed è ritenuta dalla National Security Agency lo "*strumento di collaborazione più sicuro al mondo*". Chris Howell (cofondatore di Wickr) afferma che "*i clienti governativi e aziendali la scelgono perché è la piattaforma di comunicazione con la crittografia end-to-end più sicura al mondo*". È disponibile per iPhone e Android e ha l'applicazione desktop anche per Linux.

111) Implementa la crittografia *end-to-end* anche sulle chiamate, sulle videochiamate e sulla messaggistica vocale.

112) Più in dettaglio, usa sia la crittografia simmetrica AES, sia quella asimmetrica a curve ellittiche. In crittografia, l'Advanced Encryption Standard (AES), conosciuto anche come Rijndael, di cui più propriamente è una specifica implementazione, è un algoritmo di cifratura a blocchi utilizzato come standard dal Governo degli Stati Uniti d'America.

ve che viene rimossa dalla memoria locale. In questo modo, il materiale sensibile è sempre criptato anche quando l'*app* non è attiva[113].

Infine, utilizza la crittografia anche nelle chat di gruppo[114] e implementa l'opzione Secure Shredder, per impedire il recupero dei file cancellati anche con strumenti o tecnologie particolari.

Le caratteristiche tecniche sopra descritte, riferite a Wickr, ma che possono in gran parte valere anche per le altre chat, aiutano a capire l'elevato livello di privacy che garantisce un'*app* cifrata (ed è proprio questo il motivo per cui il suo uso è destinato a crescere ulteriormente).

Sempre con riferimento ai servizi di messaggistica istantanea, a titolo meramente esemplificativo, è possibile consultare il contenuto del gruppo Telegram "Dark Web Ita Market"[115]. Si tratta di un gruppo che, analogamente a un qualsiasi dark market presente nella rete Tor, si è dotato di una sorta di deposito in garanzia per i pagamenti (escrow). In pratica, in forza di un accordo (scritto) fra due soggetti, le somme di denaro o i titoli di proprietà oggetto del "contratto" vengono depositate presso una terza parte (intermediario) a titolo di garanzia e rilasciate successivamente solo al verificarsi di determinate condizioni espressamente stabilite dalle parti su un gruppo creato appositamente.

L'occasione di illustrare le caratteristiche delle chat cifrate è propizia per evidenziare un ulteriore, importante aspetto legato all'utilizzo di tale tecnologia.

Le risultanze di investigazioni delle forze di polizia hanno fatto emergere come il ricorso ai servizi di messaggistica istantanea a fini illeciti non sia limitato al "commercio al dettaglio", nel cui ambito ha consentito di "dematerializzare" le tradizionali "piazze di spaccio" (soprattutto nel periodo di emergenza sanitaria, è stato per gli acquirenti uno dei principali strumenti per entrare in contatto con gli spacciatori).

---

113) I messaggi e le chiavi di crittografia sono disponibili solo nelle applicazioni Wickr e non vengono rivelati in rete o nei server di Wickr. I messaggi sono cifrati con crittografia simmetrica usando chiavi generate casualmente. Le chiavi simmetriche casuali del messaggio vengono trasmesse ai destinatari usando una crittografia asimmetrica. Perciò, per decifrare i messaggi, i riceventi invertono il processo, usando la crittografia asimmetrica per estrarre le chiavi casuali e poi le chiavi casuali per decifrare il testo cifrato.

114) La messaggistica di gruppo è supportata nello stesso modo, criptando un messaggio, criptando la chiave di quel messaggio più volte (per più nodi), impacchettando e inviando un singolo messaggio a più nodi.

115) *Https://t.me/darkwebita1*.

Si tratta, infatti, di una modalità che caratterizza anche la "grande distribuzione" di stupefacenti, in relazione al quale – sin dal 2017[116] – è stato accertato l'utilizzo da parte delle organizzazioni criminali, specie quelle dedite al traffico internazionale di stupefacenti, dei c.d. "criptofonini", vale a dire sistemi informatici mobili (es. smartphone *BQ Aquaris*)[117] in grado di eludere le intercettazioni, essendo dotati di un doppio sistema operativo: uno Android accessibile all'utente terzo ed un secondo latente, denominato EncroChat OS[118], totalmente cifrato ed inaccessibile alla luce delle moderne tecnologie informatiche impiegate nell'ambito della *mobile forensics*.

Prima però di illustrare le caratteristiche tecniche dei criptofonini, è necessario fare una preliminare considerazione che concerne lo sviluppo sociale dell'ultimo decennio, caratterizzato dall'ampia diffusione dell'elettronica di largo consumo (l'uso degli smartphone), dal cloud computing, dall'anonimato in rete, dalle nuove piattaforme di e-commerce (Amazon, eBay, Alibaba), dall'impiego delle criptovalute (es. i bitcoin), dall'uso sempre maggiore dei sistemi di messaggistica istantanea (WhatsApp, Telegram, ecc.) e dai social network.

In tale contesto, le organizzazioni criminali sono andate a rinnovare sia la propria natura, mutando da realtà territoriali a realtà transnazionali, che i propri metodi e tecniche attraverso le quali perpetrare i propri interessi, "arruolando" esperti informatici in grado di offrire servizi (sempre più virtualizzati ed esternalizzati) con finalità cyber criminali pronte all'uso (c.d. CaaS - "Crime-as-a-Service")[119].

Questa "industrializzazione" del cybercrime ha fatto nascere una filiera produttiva in grado di offrire un ampio portafoglio di servizi, con una diver-

---

116) A febbraio 2018, i servizi infra-provinciali di polizia giudiziaria italiani (ROS, SCO e GICO) e della DCSA hanno partecipato ad un meeting nel corso del quale la polizia olandese ha mostrato ben 95.452 messaggi di posta elettronica cifrata con sistema PGP (risalenti al periodo marzo 2015 - maggio 2017), che avevano coinvolto 3.080 account riconducibili a soggetti, per lo più albanesi, che avevano comunicato tra loro sul territorio nazionale olandese in merito ad attività connesse al traffico internazionale di droga da quel Paese.

117) *Https://www.bq.com/en/smartphones*.

118) *Https://encrophone.com/en*.

119) CaaS offre accesso a tutti le risorse digitali necessarie per commettere reati informatici, come l'uso di software malevoli (malware) da eseguire anche all'interno di apposite reti di calcolatori (botnet) ovvero il furto di database di informazioni personali (data breach). Le modalità di diffusione/commercializzazione di tali servizi sono le stesse utilizzate nel mondo del business legittimo.

sificazione dei ruoli tali da permettere, da un lato, anche a persone poco esperte, ma spregiudicate, di compiere azioni criminali in danno o per mezzo del cyberspace; dall'altro, di ampliare il business dei veri cybercriminali in modo da aumentare la penetrazione del mercato creando una rete capillare di "rivenditori" (c.d. "reseller") del loro prodotto. Ed è proprio su questo nuovo modello di business che si basa il fenomeno criminale dell'impiego dei sistemi di comunicazione anonima "Encrochat".

Tali sistemi sono stati inizialmente utilizzati nelle attività di narcotraffico, organizzate e gestite dalla *'ndrangheta* tramite l'impiego di clan albanesi, che si occupavano e continuano ad occuparsi preliminarmente del trasporto dai porti olandesi all'Italia. Successivamente, il loro impiego si è esteso anche a sodalizi di più "basso rango criminale", in ragione della conclamata impermeabilità alle attività intercettive, dei costi contenuti di acquisto e di manutenzione della piattaforma, nonché della diffusione della conoscenza di tale metodologia (avvenuta semplicemente mediante il passa parola tra le varie organizzazioni).

In realtà, da un punto di vista strategico-informatico, i sodalizi criminali – per garantirsi la riservatezza nelle comunicazioni – hanno nel tempo preferito noleggiare, tramite dei reseller olandesi della società EncroChat[120], i c.d. "server enterprice", piuttosto che impiegare gli smartphone EncroChat (c.d. "EncroPhone").

In particolare, le attività info-investigative condotte hanno consentito di appurare che:

– i predetti server sono dislocati in vari punti nel mondo (attualmente sono stati individuati in Francia, Olanda, Canada e Romania);

– le comunicazioni tra i sodali avvengono mediante l'impiego di versioni appositamente personalizzate dei telefoni BQ Acquaris, acquistati tra la Spagna e l'Olanda e dotati, come detto, di un doppio sistema operativo, di cui uno latente denominato EncroOS;

– la distribuzione dei dispositivi viene realizzata mediante la consegna del dispositivo BQ Acquaris corredato da apposito "pizzino" dove vengono annotati i codici di sblocco, ossia quello del sistema operativo Android e quello del sistema EncroOS, nonché – in alcune circostanze – anche il c.d. "panic code", che consente di azzerare l'intero contenuto del dispositivo;

– i sistemi EncroChat sembrano stranamente non funzionare nel conti-

120) Uno dei tanti è Spycity Amsterdam, Moezelhavenweg 61 1043 AM Amsterdam, T: +31 (0) 203375444

nente americano. Per tale motivo le organizzazioni criminali per comunicare con i narcos locali stanno impiegando dispositivi Nokia, Apple iPhone 6 e 6S ed alcuni Samsung dotati dell'app di messaggistica cifrata Sky ECC[121].

Inoltre, i sistemi "BQ Acquaris & EncroChat" (o loro similari) risultano particolarmente appetibili alle organizzazioni criminali per le seguenti funzionalità:

– cifratura ECDHE[122] sia dei dati ivi memorizzati che del canale di comunicazione;

– volatilità dei messaggi attesa la possibilità, anche da parte di un soggetto terzo, di effettuare da remoto sul dispositivo l'auto distruzione del contenuto dei messaggi;

– dissimulazione dei codici IMEI e l'IMSI[123] tramite apposite applicazioni;

– possibilità di inserire il citato "panic code"[124];

– impermeabilità per quanto concerne l'accesso[125] e la modifica[126] della "partizione nascosta e cifrata" da parte delle forze dell'ordine;

– possibilità di impiego, almeno da un punto di vista teorico, dei dispositivi su tutto il globo terrestre, in quanto dotati di sistema Quad-band (GSM, UMTS e CDMA).

Infine, la configurazione tipo di EncroOS prevede l'installazione dei seguenti applicativi:

– "EncroChat" per la messaggistica cifrata;

---

121) *Https://www.skyecc.store*.

122) Elliptical Curve Diffie-Hellman Ephemeral.

123) IMSI è la sigla di International Mobile Subscriber Identity ("Identità internazionale di utente di telefonia mobile"). Si tratta di un unico numero che viene associato a tutti gli utenti di telefonia mobile di reti GSM o UMTS. Il numero viene memorizzato nella SIM. Viene inviato dal dispositivo mobile alla rete ed è utilizzato per controllare gli altri dettagli del terminale mobile nel HLR (Home Location Register) o come copiato localmente nel VLR (Visitor Location Register).

124) Tale evento può risultare particolarmente critico specie quanto il sospettato si presenti collaborativo con le FF.PP., vanificando di fatto l'attività di isolamento del dispositivo da connessioni esterne.

125) Il sistema impedisce l'interfacciamento con il servizio ADB (Android Debug Bridge) e la possibilità di impostarlo in "recovery mode".

126) Il sistema effettua dei controlli di ridondanza ciclica sull'integrità del file system, tali da rilevare la presenza di file non autorizzati o noti, come ad esempio un "captatore informatico". Oltre a ciò impedisce l'impiego della fotocamera, del microfono, del sistema di localizzazione GPS e della porta dati USB, rendendo così potenzialmente vana ogni tentativo di inoculazione pur avendo la materiale disponibilità dello smartphone.

– "EncroTalk" per la realizzazione di chiamate VoIP cifrate;
– "EncroMail" per il servizio di posta elettronica con crittografia PGP;
– "EncroNotes" per il salvataggio di note/appunti in formato cifrato;
– "EncroSnap" per l'invio di foto cifrate.

2.4.3. Le condotte dei "singoli" e la configurabilità del reato associativo

Con riferimento ai traffici che interessano la rete, uno degli aspetti sui quali si è maggiormente focalizzata l'attenzione sia delle forze dell'ordine che della magistratura (inquirente e giudicante) è la configurabilità del reato associativo rispetto alle condotte dei soggetti, che con ruoli differenti, interagiscono nelle piattaforme di vendita.

In altre parole, se si tratta di un fenomeno caratterizzato dalla compresenza di più identità virtuali che operano separatamente o se, quantomeno in relazione alla ideazione e gestione di un market, più soggetti possano dar vita a veri e propri gruppi organizzati.

In questo, la storia dei più grandi market (Silk Road e AphaBay su tutti) porterebbe a ricondurre la loro operatività all'ingegno informatico e all'intuizione criminale di singoli soggetti (Ross Ulbricht per Silk Road e Alexander Cazes per AlphaBay), i quali erano riusciti a dar vita a una sofisticata forma di "impresa virtuale individuale" con lo scopo di perseguire esclusivamente il proprio personale arricchimento.

In realtà, lo "European monitoring centre for drugs and drug addiction", in un report del 2017[127], nel premettere che inizialmente "*la maggior parte dei fornitori sui mercati darknet erano venditori individuali, che distribuivano quantità limitate di sostanze diverse in base alla loro disponibilità*", ha sottolineato come, successivamente, il volume complessivo delle droghe scambiate on-line indicasse "*il coinvolgimento dei gruppi criminali organizzati, che sono in grado di procurarsi maggiori quantità di stupefacenti e distribuirli a singoli acquirenti*". Ha inoltre segnalato che "*indagini* [evidenziano] *lo spostamento dei gruppi criminali organizzati coinvolti nella produzione su larga scala di cannabis a base di erbe nell'UE ai mercati darknet per la distribuzione della loro produzione*".

Sul punto, per quanto riguarda l'Italia, è interessante richiamare anche la giurisprudenza della Suprema Corte di Cassazione, che – negli ultimi anni

127) EMCDDA, *Drugs and the darknet: perspectives for enforcement, research and policy*, Europol, Lisbon, November 2017.

– con alcune sentenze (una delle quali del 2020), ha di fatto confermato la configurabilità del reato di associazione per delinquere in relazione a condotte criminali in rete, mettendo in risalto diversi, significativi aspetti.

Più in dettaglio, nel 2013 (con la sentenza 16 dicembre 2013, n. 50620), ha confermato la legittimità della custodia agli arresti domiciliari a carico dell'ingegnere informatico Gianluca Preite, arrestato nel corso dell'operazione "Tango Down" della Polizia di Stato, il quale – in nome dei valori espressi dall'organizzazione Anonymous – aveva effettuato – insieme ad altri soggetti – accessi abusivi a sistemi informatici. In tale sentenza, la Suprema Corte ha evidenziato come Anonymous potesse "*assimilarsi a un'organizzazione non statica, operante in una dimensione di per sé aperta e non individuabile su una base meramente territoriale*", in cui cellule diverse potevano aver pianificato diverse iniziative illecite. Si è certamente trattato di un'interpretazione evolutiva della nozione classica di associazione per delinquere, in cui viene superato il concetto della "territorialità" riferita alle organizzazioni operanti nel cyberspace, ambito in cui predomina invece una "dimensione aperta" e in cui il concetto di "distanza" è di fatto inesistente.

Sempre nel 2013, la Suprema Corte di Cassazione (con la sentenza della sezione III del 15 maggio 2013, n. 20921), pronunciandosi questa volta su un caso di pornografia minorile, ha riconosciuto la configurabilità del reato di associazione per delinquere nei confronti dei *net users*, osservando come nel mondo del *dark web*, prima di poter entrare a far parte di una comunità virtuale, l'utente dovesse sottoporsi a una "prova di iniziazione", al fine di creare il necessario vincolo fiduciario con gli altri membri. Secondo i giudici di legittimità, la deliberata sottoposizione a questo esame preliminare dimostrava come l'utente fosse indefettibilmente al corrente del fine illecito perseguito dal gruppo e, pertanto, dovesse considerarsi un associato del sodalizio criminoso a tutti gli effetti[128].

Infine, nel 2020, con la sentenza della sezione III n. 10485, ha ribadito come "*l'allestimento di un sito di black market e la sua gestione* [siano] *indicativi dell'esistenza di un programma criminoso finalizzato alla commissione*

128) Nel caso di specie una complicata indagine della Polizia Postale aveva portato alla luce la presenza nel *dark web* di una comunità virtuale riunita allo scopo di scambiare e diffondere materiale pedopornografico. Si trattava di una struttura informatica molto simile a quella di un social network denominato "PedoBook". Gli utenti una volta registrati, dopo aver superato una prova iniziale, venivano ammessi dalla comunità ad accedere ad un archivio che contava oltre un milione di files che ritraevano minori, anche in tenerissima età, in condizioni di nudità e intimità sessuale.

di una serie indeterminata di reati e, di conseguenza, della sussistenza di un sodalizio ex art. 416 cod. pen.".

Si tratta di una sentenza, oltre che recente (del 21 febbraio 2020), molto importante poiché pronunciata sui ricorsi presentati dai tre giovani italiani, gestori del Berlusconi Market (arrestati a novembre 2019 nel corso dell'operazione denominata "Darknet.Drug" della Guardia di finanza), avverso l'ordinanza con cui il Tribunale del Riesame di Brescia aveva confermato l'applicazione della misura cautelare della custodia in carcere per associazione per delinquere disposta con provvedimento del Giudice per le indagini preliminari.

Al riguardo, è interessante segnalare come la Corte di Cassazione abbia preliminarmente riportato la ricostruzione delle condotte dei tre giovani fatta dal Giudice per le Indagini Preliminari, evidenziando che l'art. 416 del Codice penale era stato loro contestato poiché "… *con la partecipazione di altri soggetti non identificati, con i nickname di Vladimir Putin di Emmanuel Macron (in qualità, rispettivamente, di amministratore e moderatore), mediante: l'apertura della piattaforma denominata Berlusconi Market, attiva nel cd. Dark Web; la gestione di un market on-line attraverso la fornitura del servizio e-commerce per l'offerta in vendita… di sostanza stupefacente, dati finanziari abusivamente sottratti, documenti di identità contraffatti, prodotti industriali contraffatti, armi da sparo anche da guerra ed esplosivi; la cura nella programmazione dell'interfaccia grafica della Home e della bacheche dei cd. vendor, la gestione delle iscrizioni dei vendor, la pubblicazione e cancellazione dal pannello dedicato agli annunci di vendita, la gestione e il controllo contabile del wallet Bitcoin e dei depositi a garanzia cd. escrow…, l'offerta di supporto tecnico sistematico ai vendor mediante la gestione delle richieste di apertura di tickets, la gestione delle dispute tra i vendor; si* [erano associati] *fra loro allo scopo di consumare una serie indeterminata di delitti in concorso, quali il contrabbando di armi, lo spaccio di sostanza stupefacente, la vendita di monete contraffatte, la ricettazione… tutti delitti aggravati dalla transnazionalità della condotta…*".

Peraltro, la Corte di Cassazione, sempre nel caso in esame, ha anche osservato, decidendo su un ulteriore censura mossa in relazione al giudizio di adeguatezza della misura applicata (la custodia in carcere era ritenuta troppo afflittiva), come il Tribunale cautelare avesse correttamente ritenuto che "… *in considerazione della natura e delle modalità del reato come concretamente contestato, una misura meno affittiva non sarebbe* [stata] *idonea a preservare il pericolo di reiterazione di analoghe condotte criminose, tenuto conto… che… la piattaforma Berlusconi Market* [era] *ancora attiva e che i ricorrenti,*

dotati di specifiche competenze informatiche, non [avessero] *voluto rivelare agli inquirenti le credenziali di accesso a detta piattaforma, credenziali che, quindi,* [avrebbero potuto] *continuare ad utilizzare anche in regime di arresti domiciliari mediante computer o anche smartphone, strumenti facilmente reperibili anche in ambiente domestico*".

A carico dei tre giovani, il 17 novembre 2020, è anche arrivata la sentenza di condanna del Tribunale di Brescia, che – al termine di un processo celebrato con rito abbreviato – li ha condannati a 4 anni di reclusione. Si tratta certamente di un primo, importantissimo passo in Italia verso una generale, maggiore sensibilità rispetto a un fenomeno che, nell'ultimo decennio, sembra aver sinora avuto vita troppo facile.

Discorso diverso vale invece per la configurabilità dell'associazione di tipo mafioso. Sul punto, nel premettere che – ad oggi – con riferimento all'ideazione\gestione di piattaforme on-line di vendita di droga e armi non risultano sentenze di condanna ex art. 416-*bis*, è da considerare che, nell'eventuale ricostruzione delle dinamiche criminali in rete di un gruppo organizzato di matrice mafiosa, sarebbe certamente difficile, se non impossibile, dimostrare "la condizione di assoggettamento e di omertà" del popolo di Internet. La comunità virtuale di un market illegale, infatti, è costituita da un numero indeterminato di "identità fittizie" (pertanto, del tutto anonime), che possono in qualsiasi momento interrompere l'interazione con gli altri utenti, senza per questo dover temere azioni ritorsive.

Tutt'altra considerazione è da sostenere circa il "concorso esterno in associazione mafiosa", rispetto al quale appare invece possibile dimostrare il sostegno logistico che i cybercriminali potrebbero fornire all'associazione mediante il loro rilevante contributo di natura squisitamente informatica. Si pensi, ad esempio, alla fornitura ai narcotrafficanti o ai latitanti dei criptofonini (dei quali si è precedentemente parlato) per eludere le intercettazione da parte delle forze di polizia ovvero al riciclaggio di denaro provento/frutto di illeciti attraverso l'utilizzo di criptovalute, attività quest'ultima sempre più devoluta a informatici competenti[129].

La questione resta comunque aperta e merita certamente ulteriori appro-

129) Nella Relazione annuale della DNA relativa al 2018, nel far riferimento ai paradisi finanziari virtuali del web, si poneva l'attenzione proprio sull'"*utilizzo massiccio delle criptovalute da parte delle organizzazioni delinquenziali, anche di matrice mafiosa, per ripulire somme consistenti di proventi illeciti, anche mediante lo spacchettamento delle somme da riciclare e\o l'utilizzo di più soggetti riciclatori, ovvero il ricorso a più monete virtuali*".

fondimenti, tenuto conto che – a fronte della mancanza ad oggi di specifiche risultanze investigative – appare singolare (per non dire improbabile) che le organizzazioni criminali di tipo mafioso non abbiano ancora risposto alcun interesse economico nella gestione dei traffici illeciti attraverso la rete, che – come detto – è un business in grado di assicurare un lucroso giro di affari.

2.4.4. L'impatto del COVID-19 sull'*e-commerce* della droga

In base alle risultati di alcune ricerche di settore, nel periodo dell'emergenza pandemica, la mancanza di un mercato regolato e le misure di social distancing imposte non hanno impedito ai consumatori europei di fare scorte di stupefacenti, soprattutto di cannabis, costringendoli solamente a cambiare le modalità di acquisto.

In Canada e in molti Stati Americani, nello scorso mese di marzo, vale a dire all'inizio del primo, severo lockdown, molte persone si sono accalcate presso i rivenditori locali (legali) di cannabis per farne incetta. Anche in Europa, nello stesso periodo, secondo il report[130] dello European Monitoring Center for Drugs and Drug Addiction[131] (EMCDDA), è accaduta la stessa cosa, con la sola differenza che i canali maggiormente sfruttati per interagire con i "rivenditori non regolamentati" erano ad appannaggio del *deep web*[132] (proprio in ragione dell'anonimato garantito dalla navigazione con browser specifici, quale Tor, e dal pagamento in criptovalute).

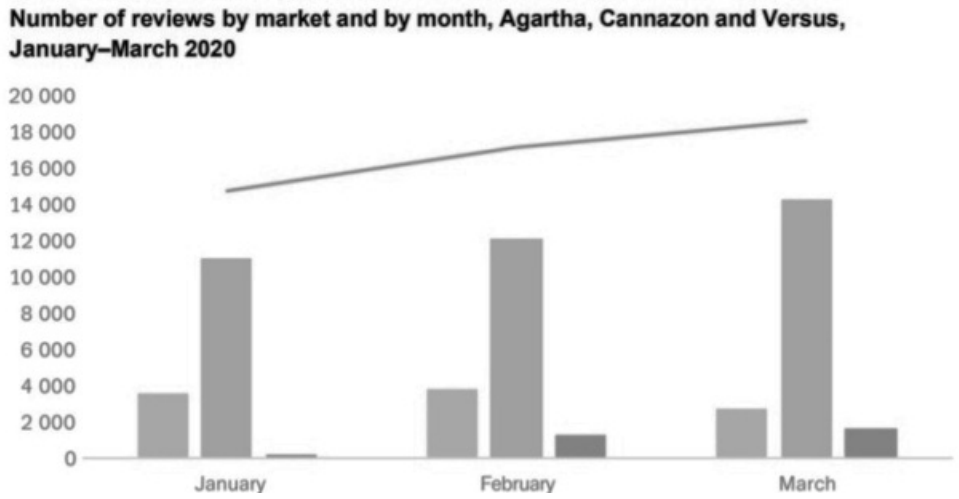
---

130) Pubblicato nel mese di maggio del 2020.

131) L'Osservatorio europeo delle droghe e delle tossicodipendenze di Lisbona, istituito nel 1993, è l'Agenzia tecnica della Commissione europea in materia di droga. L'obiettivo principale dell'EMCDDA è quello di fornire un supporto informativo obiettivo, affidabile e comparabile a livello europeo sul fenomeno delle droghe e delle tossicodipendenze e sulle loro conseguenze alla Comunità europea e agli Stati membri. L'Osservatorio raccoglie le informazioni essenzialmente attraverso la "rete REITOX", un gruppo di punti focali situati in ciascuno dei 28 Stati membri dell'UE, in Norvegia, nei Paesi candidati e presso la Commissione europea. Il Punto focale italiano è parte integrante dell'Ufficio tecnico-scientifico del Dipartimento politiche antidroga della Presidenza del Consiglio dei Ministri. Tra i destinatari delle attività dell'Osservatorio, che pubblica annualmente una relazione sull'evoluzione del fenomeno della droga nell'Unione europea, figurano i responsabili politici che usano queste informazioni per formulare strategie coerenti in materia di droga a livello nazionale ed europeo, i professionisti e i ricercatori che lavorano nel settore delle droghe e, più in generale, i mezzi di comunicazione e l'opinione pubblica.

132) In occasione della pubblicazione del report, il Direttore pro-tempore dell'EMCDDA, Alexis Goosdeel, aveva evidenziato come "… *il commercio on-line e l'espansione dei sistemi di comunicazione criptata* [avessero dato] *filo da torcere alle forze dell'ordine...*".

Il rapporto dell'EMCDDA ha monitorato tre dei principali mercati di cannabis sul *deep web* dell'Unione europea, Agartha, Cannazon e Versus, per valutare come la pandemia abbia influenzato le loro vendite dal 1° gennaio al 31 marzo 2020[133]. Dal monitoraggio è emerso che le attività di mercato sono aumentate, nel periodo preso in esame, di più del 25%, trainate principalmente dalle vendite del mercato Cannazon (nel grafico sottostante in verde le colonne relative alla citata piattaforma).



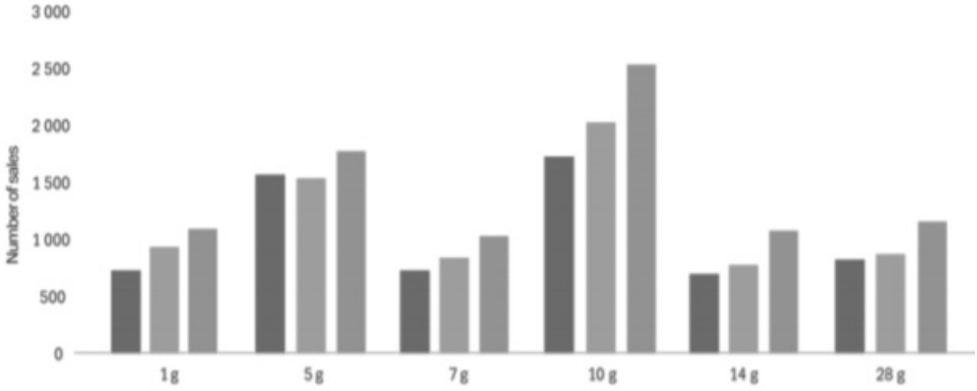
Inoltre, nel corso dei primi tre mesi del 2020, i rivenditori hanno acquistato meno prodotti a base di cannabis a scopo di redistribuzione al dettaglio, probabilmente perché i protocolli di social distancing renderebbero difficile venderla di persona.

Aumentato, invece, il numero di acquirenti di cannabis per uso personale, anche se è emersa la diminuzione del numero di persone che hanno ordinato sul *deep web* sostanze generalmente utilizzate in occasioni "sociali" e di gruppo (in particolare, l'MDMA).

Sul mercato Cannazon, sempre secondo il report, è stata venduta – nell'arco dei tre mesi considerati – cannabis per circa 4.3 milioni di euro, pari a circa 1,6 tonnellate di prodotti (il quantitativo più comunemente acquistato si è aggirato sui 10 grammi, per un costo medio di 125 euro - vds. grafico sottostante).

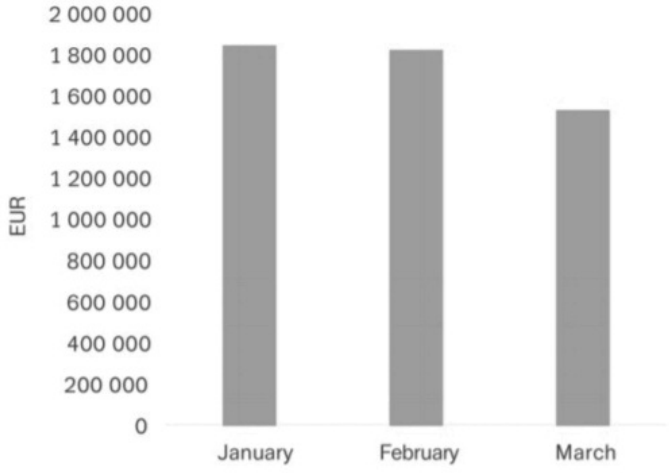
133) L'Osservatorio ha escluso dal monitoraggio il mercato Hydra (considerato uno dei più grandi mercati illeciti di stupefacenti in rete), poiché serve principalmente la Russia e i Paesi dell'Europa orientale.

Number of sales for common retail-level weight categories by month, Cannazon, January–March 2020

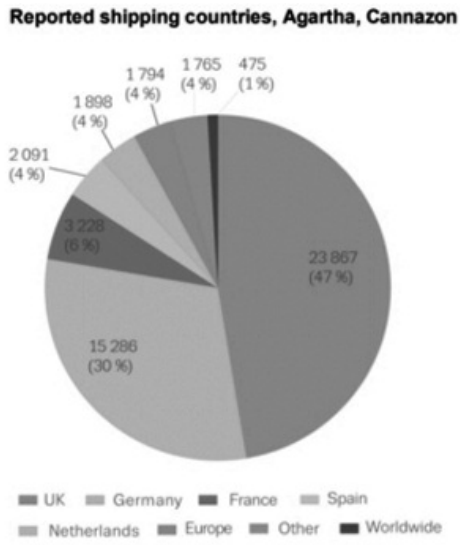


Inoltre, nonostante l'aumento delle vendite, sempre nel periodo preso in esame, è stata osservata la diminuzione degli introiti totali (vds. grafico sottostante), presumibilmente a significare che le persone hanno iniziato ad acquistare quantitativi inferiori e prodotti meno costosi (anche in ragione della crisi economica indotta dall'emergenza pandemica, che ha comunque impoverito molte famiglie).

Monthly value of cannabis products, Cannazon, January–March 2020



L'Osservatorio ha infine evidenziato che la maggior parte delle sostanze vendute sul *deep web* proveniva dal Regno Unito con il 47%, dalla Germania con il 30% e dalla Spagna con il 6% (vds. grafico sottostante).



Alcuni esperti hanno infine evidenziato un ulteriore aspetto legato alle criticità registrate in periodo di pandemia nell'organizzazione delle attività di produzione e commercializzazione di droga, in ragione della fragilità delle catene di approvvigionamento nelle industrie di tutto il mondo. In particolare, l'aumento dei prezzi degli stupefacenti presenti sul *deep web* sarebbe da ricondurre alla carenza di prodotti chimici utilizzati per la produzione di droghe sintetiche, dovuta proprio al loro difficile approvvigionamento, principalmente dalla Cina (duramente colpito, almeno nella fase iniziale, dall'emergenza sanitaria poi divenuta di portata mondiale), Paese dal quale provengano la maggior parte degli ingredienti chimici ("precursori") usati per la produzione di metanfetamina e di fentanil.

3. Metodologia e strumenti di contrasto dei traffici in rete

3.1. I fattori di successo di un'investigazione complessa e complicata

Il traffico di droga, di armi e di altri prodotti e servizi illeciti sul *dark web* è, come detto, un fenomeno in veloce espansione. Basti pensare che, secondo i sondaggi di *Global Drug Survey*[134], il numero di persone in Europa che utilizzano le piattaforme della rete come canale per l'approvvigionamento

134) La *Global Drug Survey* (GDS) è un'istituzione britannica indipendente costituita da una rete di esperti internazionali nel campo delle droghe, della salute, dell'epidemiologia e delle politiche pubbliche. Tale istituzione mappa annualmente i *trend* del consumo di

di sostanze stupefacenti è più che raddoppiato negli ultimi cinque anni, in ragione principalmente della vasta gamma di prodotti offerti e del sistema di recensioni dei fornitori e dei prodotti (che garantisce una certa affidabilità degli acquisti), nonché della facilità di conduzione delle trattative di compra-vendita, che non comportano alcuna forma di esposizione a pericolo (a differenza dell'acquisto per strada).

Si tratta, quindi, nel panorama globale del traffico illecito di droga e di altri prodotti e servizi, non solo del presente, ma soprattutto del futuro, avuto proprio riguardo alla veloce diffusione del fenomeno su scala mondiale.

Conseguente, per le forze di polizia, esso costituisce e lo sarà sempre di più una avvincente sfida, resa ardua proprio dalle sue principali caratteristiche: il *sofisticato contenuto tecnologico* (i gestori\ideatori di un black market sono generalmente in possesso di vaste conoscenze informatiche), la *globalizzazione* (la compra-vendita di prodotti non ha limiti geografici, ma avviene contemporaneamente in varie parti del mondo) e la *costante innovazione* dei e nei mercati (i cambiamenti nelle modalità organizzative di uno shop in rete sono all'ordine del giorno; i siti dedicati alle vendita sono, infatti, caratterizzati da una spiccata *volatilità* e dalla *mutabilità* con riferimento sia alla loro denominazione, sia agli indirizzi di accesso).

In tale quadro, i fattori di successo di un'investigazioni nello specifico ambito sono riconducibili, in linea di massima, alla:

1) rispondenza di dati informatici acquisiti nel *dark web* (quali ad esempio, il nickname, l'e-mail o la chiave pubblica di un vendor del black market) con quelli rilevati nell'*open web.* Si tratta di una circostanza fortunata che si concretizza solitamente a seguito di un errore grossolano commesso dal criminale. Uno degli esempi emblematici di errore è stato quello commesso da Ross Ulbricht, ideatore e gestore di Silk Road, a marzo del 2012, allorquando utilizzò il suo nickname (corrispondente al nome) per postare una domanda specifica riguardante un servizio nascosto del browser Tor. Il nickname venne cambiato in meno di un minuto, in un tempo però troppo lungo per evitare che l'FBI captasse l'importantissimo dato informatico;

---

stupefacenti rivolgendosi direttamente ai consumatori. L'obiettivo dell'indagine, alla quale aderisce attualmente anche l'Italia, è capire le nuove tendenze nel campo delle droghe chiedendo a chi fa uso di sostanze – in modo rigorosamente anonimo – quantità e modalità di assunzione. I promotori della GDS ritengono che la conoscenza e l'esperienza delle persone che usano alcol e altre droghe, legali e illegali, possano essere utilizzate per promuovere politiche più adeguate a gestire il fenomeno dell'uso di sostanze.
Negli ultimi 8 anni più di 750.000 persone hanno partecipato ai sondaggi (nel 2019 il sondaggio è stato tradotto in 18 lingue e ha coinvolto numerosi partner in oltre 30 Paesi.

2) materializzazione nel mondo reale di ciò che è virtuale nel mondo del web, con particolare riferimento alla delicata e vulnerabile fase della spedizione dei prodotti acquistati in rete. Anche in questo caso, l'esempio più lampante è legato allo smantellamento di un'altra importante piattaforma, il Berlusconi Market. L'arresto di alcuni dei soggetti che gestivano la piattaforma avvenne, infatti, grazie all'individuazione dell'ufficio postale (in Puglia) dal quale venivano spediti i prodotti e alla sua successiva sorveglianza da parte degli operatori di polizia mediante le tradizioni tecniche d'indagine.

Le investigazioni in rete, sempre molto complesse e articolate per le forze di polizia, si fondano generalmente sull'utilizzo di alcune tecniche (a loro volte attuate mediante specifici strumenti informatici), tra le quali:

1) l'attività di OSINT riferita alle fonti aperte e di SOCMINT riguardante invece i social media;

2) il monitoraggio dei black market attivi nel *dark web*;

3) le operazioni *undercover*;

4) l'utilizzo di strumenti basati sui software, come *malware* e NIT (*Network Investigative Technique*) e i c.d. "attacchi informatici".

Tutti gli strumenti e tutte le tecniche disponibili non possono comunque prescindere da due condizioni fondamentali: il possesso di elevate competenze informatiche da parte degli operatori di polizia che le utilizzano e l'attivazione di efficaci forme di cooperazione internazionale, intesa principalmente come costante e immediato scambio di informazioni tra gli investigatori dei diversi Paesi interessati (il fenomeno è come detto connotato dalla globalità; pertanto, molto spesso ci si imbatte in una rete di server, facenti capo ai vari venditori, che sono allocati in svariate parti del mondo).

3.2. L'importanza dell'OSINT e della SOCMINT

Per "Open Source Intelligence" (OSINT) si intende il ciclo di raccolta, elaborazione, analisi, produzione, classificazione e diffusione delle informazioni derivate da fonti apertamente disponibili, legalmente accessibili e utilizzabili dal pubblico (fonti quindi non segrete o coperte)[135]. In altri termini, è un'attività che consente il reperimento di contenuti (potenzialmente) informativi senza metodi coercitivi.

135) Non esiste una nozione giuridica univoca di "Open source intelligence". In campo militare la NATO la definisce come "*un processo di raccolta, selezione, distillazione e diffusione di informazioni non classificate ad una comunità ristretta di operatori ed in relazione a specifici argomenti*".

Questo è ciò che lo distingue dalle altre attività di intelligence basate su altre fonti, quali l'HUMINT, che si concentra sugli informatori, la SIGINT sulle intercettazioni, l'IMINT sulle immagini satellitari e il MASINT sugli strumenti di indagine scientifica. Inoltre, se si fa riferimento alle investigazioni, la connotazione "aperta" delle fonti consente a chi le conduce di non oltrepassare il confine della legalità nella ricerca delle informazioni e di non dover coinvolgere altri soggetti.

In sintesi, l'OSINT è un processo che mira a creare una specifica conoscenza in supporto di una specifica decisione di un individuo o di un gruppo, basandosi su due concetti cardine:

1) l'*informazione*, intesa quale entità (anche astratta) di varia natura – più o meno organizzata, più o meno strutturata – che si caratterizza per il fatto di essere portatrice di un certo contenuto informativo;

2) la *fonte*[136], intesa quale risorsa che ha la particolare attitudine di poter mettere in qualche modo l'analista in relazione con l'informazione di cui necessita. Con riferimento alle fonti on-line il primo aspetto da tenere presente è quello di valutare l'attendibilità delle stesse, tenuto conto che attualmente il problema della ricerca nel web non consiste nel trovare semplicemente le informazione, ma nel reperire quelle giuste in un oceano di dati in continuo e incontrollabile mutamento[137]. La delicata fase della valutazione della fonte si basa pertanto sui seguenti requisiti:

- accuratezza delle informazioni;
- capacità di mantenere le informazioni aggiornate;
- attendibilità e autorità del sito stesso;
- rilevanza delle informazioni contenute.

Applicando un processo di valutazione secondo i citati criteri, l'analista – tramite il confronto delle informazioni offerte – riesce a selezionare una serie di siti considerati "attendibili" a cui fare riferimento, senza però mai dimenti-

136) Le *fonti* prese in esame in un'attività di OSINT sono i *mezzi di comunicazione* (giornali, riviste, televisione, radio, ecc…), i *dati pubblici* (rapporti, piani finanziari, dati demografici, dibattiti, conferenze stampa, discorsi, avvisi aeronautici e marittimi), le *osservazioni dirette* (fotografie di piloti amatoriali, ascolto di conversazioni radio e osservazione di geoferenziate satellitari e non mediante Google Earth o Google Street), i *professionisti* e gli *studiosi* (conferenze, simposi, lezioni universitarie, associazioni professionali e pubblicazioni scientifiche).

137) Secondo alcuni studi statistici, in rete ogni 60 secondi – citando solo alcuni dei dati rilevati – vengono creati 571 nuovi siti, inviate 204 milioni di mail, eseguite 2 milioni di ricerche su "Google", caricati 72 ore di video su "Youtube" (su Facebook sono addirittura 41.000 i post al secondo).

care che nel web nascono nuove fonti e, soprattutto, che – a differenza delle fonti canoniche, facilmente inquadrabili – nel web sono disponibili solo testi e immagini non sicuramente riconducibili a un preciso autore.

Il ciclo di intelligence applicato al web si compone di 4 fasi: "*planning and decision*", "*collection*", "*processing and exploitation*", "*analysis and production*". Si tratta di un percorso chiuso che si compone delle citate attività, che in realtà non devono necessariamente essere tutte espletate (se un'informazione è già disponibile, si salta la "ricerca" per passare direttamente all'"analisi"). Inoltre, la procedura si svolge per raffinamenti successivi, ripetendo il ciclo ogni qualvolta si presentano nuovi dati o nuove informazioni.

Andando più in dettaglio, la fase di "*planning and decision*" consiste nella pianificazione dell'obbiettivo. Essa include l'identificazione e la determinazione delle esigenze di informazione e la decisione su come le informazioni devono essere raccolte, nonché l'elaborazione del calendario dei successivi step di raccolta e analisi delle stesse. In questa fase, il responsabile del processo, oltre a fissare le priorità, individua le tecnologie da utilizzare e il personale da impiegare, attribuendo a ciascuno un ruolo e delle responsabilità chiare.

La fase di "*collection*" consiste nella ricerca di specifiche pagine web e nella raccolta di dati coerenti. La raccolta può essere effettuata tramite mezzi tecnici o umani e comporta la necessità di sottoporre i dati grezzi rilevati a un esame attento e critico volto ad appurarne la rilevanza, il significato e l'accuratezza. Inoltre, proprio questa fase include la verifica della fonte in termini di affidabilità e la ponderazione dei dati, che – una volta raccolti – vengono correlati e inoltrati agli analisti per la loro elaborazione.

La fase di "*processing and exploitation*" consiste nella selezione e valutazione dei dati rilevanti (indicatori). In pratica, i dati grezzi diventano informazioni, vale a dire vengono interpretati, tradotti e convertiti in forme utilizzabili. A loro volte le informazioni vengono "organizzate" in modo tale da poter essere analizzate per rilevanza e priorità (a tal fine, alcuni dei metodi utilizzati sono la decrittografia, la traduzione in lingua o l'organizzazione e l'indicizzazione dei dati per la standardizzazione in campi).

La fase di "*analysis and production*" consiste, infine, nell'estrapolazione e interpretazione delle informazioni in relazione all'obiettivo prefissato. Essa si compone di 3 sotto fasi: 1) l'*analisi*, durante la quale l'analista continua a studiare e a valutare i fatti e a metterli in relazione con altre fonti delle informazioni raccolte. Significa in pratica separare un'informazione in segmenti al fine di studiarne le caratteristiche essenziali (è un'attività che può essere considerata come la prosecuzione della valutazione delle informazioni); 2) l'*integrazione*, che consiste nell'assemblare le informazioni analizzate. È come

comporre un puzzle i cui pezzi sono rappresentati dalle varie informazioni, per realizzare un prodotto informativo fruibile in relazione agli obiettivi fissati; 3) la *disseminazione* che consiste nella divulgazione del prodotto dell'attività di intelligence svolta, nel formato richiesto. Le peculiarità di un report funzionale allo svolgimento di un'investigazione sono la celerità (deve essere ultimato nei tempi prestabiliti; non è utile se tardivo), la comprensibilità (non deve essere connotato da eccessivo tecnicismo e dall'uso di terminologia troppo specifica; in caso contrario risulterebbe comprensibile solo agli esperti del settore) e la fruibilità (le informazioni acquisite in maniera confidenziale non sarebbero producibili in alcuna sede; è necessario quindi richiamare le fonti in modo che queste siano verificabili in qualunque momento). Il report, inoltre, deve essere prodotto nel format ritenuto più idoneo.

Quando il ciclo d'intelligence riguarda i social media, si parla, invece, di SOC.M.INT. ("SOCial Media INTelligence"), branca della disciplina dell'OSINT che ormai da tempo viene impiegata sempre più frequentemente anche in diversi ambiti di contrasto alla criminalità in genere.

In merito, un'importante precisazione da fare preliminarmente all'illustrazione delle principali caratteristiche di tale attività è la differente accezione – spesso confusa – fra social network e social media. I social network sono solo una piccola componente dei social media, che includono anche blog, forum, siti social, audio, foto, immagini varie, video, chat, livecasting, virtual words, ecc.

Tutti questi siti e queste applicazioni hanno lo scopo di facilitare la creazione e lo sviluppo dei rapporti sociali e la comunicazione fra individui. Ed è proprio questo il motivo principale per cui i social network sono la fonte primaria, ma non esclusiva, della SOC.M.INT. Esiste un social per tutto: Twitter per le comunicazioni brevi ed istantanee, Facebook per esprimere emozioni e stati d'essere, Foursquare per condividere luoghi, Instagram per le foto, Youtube per i video, LinkedIn per l'ambito professionale, Badoo e Meetic per le relazioni affettive[138].

La natura social di tali network facilita la condivisione e la visibilità di stati psicologici, di opinioni politiche o della fede religiosa; non solo, ma anche l'appartenenza a gruppi connotati dalla passione per un determinato argomento\attività o da una specifica condizione di vita sul piano economica.

Pertanto, su un piano squisitamente investigativo, sfruttare queste fonti

138) Sono considerate fonti aperte alle quali attingere anche i c.d. "User generated content", ossia i file multimediali postati liberamente sui social network e sui forum; si pensi a Wikipedia, oppure ai post con hasthtag condiviso o ai video su Youtube.

informative consente di acquisire utili notizie non riscontrabili ad esempio nelle banche dati istituzionali o nel corso delle tradizionali attività d'indagine.

Peraltro, l'uso dei social è così largamente diffuso che non è improbabile che il "soggetto monitorato" proprio in tali network possa lasciare le proprie "impronte digitali" (è questo un "passo falso" che ha segnato le sorti di tanti ideatori\amministratori di black markets). Per un investigatore è però indispensabile affidarsi a più canali, senza imbattersi nell'errore di dare credito ad un unico social network, tenuto conto che le informazioni ivi presenti sono state postate dallo stesso "soggetto monitorato", motivo per cui potrebbero non essere veritiere. Risulta, pertanto, indispensabile mettere insieme più fonti e verificare l'esito delle informazioni incrociate: a tal fine l'attività di SOC.M.INT. significa ricavare da ogni social network, ma non solamente, specifiche informazioni con diversa intensità e significatività.

È da tenere presente che i social media sono tipicamente caratterizzati da *proprietà* (alto livello di pertinenza), *immediatezza*, *usabilità* (sono tutti essenziali ed intuitivi, si apprendono con nozioni basiche), *volatilità* (difficile reperire post eliminati), *dialogo* ed *interazione* (offrono la possibilità di interagire e di condividere elementi). Inoltre, amplificano voci e azioni, promuovono trasparenza e si connotato per una inconsueta *immersività*. Tutte queste caratteristiche devono indurre un investigatore competente a saper circoscrivere l'obiettivo investigativo, selezionando e creando una lista di priorità che servono allo scopo (deve a tal fine tenersi sempre aggiornato sugli strumenti più adatti e tipici per ogni nazione, fascia d'età, cultura, religione, interessi dell'individuo o del gruppo). È indispensabile, inoltre, che egli incroci, dapprima, i risultati ottenuti dal ciclo di intelligence applicato ai diversi canali interni alla SOC.M.INT. e, successivamente, gli ulteriori esiti così "raffinati" con quelli relativi al resto delle analisi e delle indagini svolte sfruttando altri, tradizionali strumenti; solo in questo modo avrà a disposizione un supporto informativo totale e concreto, utile alla prosecuzione delle investigazioni.

Solitamente, ai risultati della SOC.M.INT., si associa la SNA (Social Network Analysis[139]), efficace nell'individuare i "nodi" più importanti all'interno delle reti sociali; si tratta di una tecnica che analizza le strutture, le funzioni e il contenuto delle reti sociali e che negli ultimi anni ha visto incremen-

139) È l'analisi delle reti sociali, intendendo per esse un qualsiasi gruppo di individui connessi tra loro da diversi legami, che vanno dalla conoscenza casuale, ai rapporti di lavoro, ai vincoli familiari. Tale analisi guarda alle relazioni sociali dal punto di vista della teoria delle reti, sulla base della quale le relazioni sono rappresentabili da collegamenti (archi) tra individui (nodi) che possono essere mostrati attraverso grafi.

tare il suo utilizzo in prospettiva investigativa e nello studio della criminalità organizzata.

Per concludere, proprio con riferimento all'attività di OSINT riferita ai social network, uno degli indicatori nei quali gli investigatori ripongono notevoli aspettative di successo è quello della "*somiglianza culturale*" in rete tra identità solo in apparenza diverse. Si tratta, in pratica, di ricercare tra le numerosissime informazioni disponibili, quelle che possano far convergere comportamenti\atteggiamenti rilevati su piattaforme differenti verso la stessa identità. È il caso, ad esempio, del contributo determinante ai fini della successiva identificazione di Ross Ulbricht, fondatore di Silk Road, ottenuto dall'analisi da parte degli investigatori dei suoi profili pubblici sui social network, analisi dalla quale è emersa proprio la "somiglianza culturale" tra il soggetto al quale facevano capo i profili e Dread Pirate Roberts, pseudonimo con cui era noto Ulbricht. Entrambi facevano infatti riferimento (in post o in discorsi resi pubblici sulla rete) alla convinta adesione alle teorie libertarie del noto economista di origini austriache, Ludwing von Mises[140] (in particolare, Dread Pirate Roberts aveva più volte sostenuto che le teorie dell'economista avevano fornito "*le basi filosofiche di Silk Road*").

3.3. Gli strumenti di analisi

Ovviamente per poter sfruttare le fonti aperte occorre avere dimestichezza con le tecniche avanzate concesse dai motori di ricerca ed occorre sapersi districare tra i database istituzionali.

Le possibilità offerte dall'OSINT, con l'aumento dei grandi collettori di informazioni (in primis i social network) e la diffusione degli strumenti di sorveglianza, sono direttamente proporzionali alla repentina diffusione delle nuove tecnologie.

In questa sovrabbondanza di informazioni, spesso imprecise e incomplete (si parla di "infodemia"[141]), diventa fondamentale saper passare da dati grezzi e generici a notizie validamente filtrate. Pertanto, l'esigenza dell'analista OSINT è quella di effettuare ricerche secondo rigidi criteri utilizzando

140) Ludwig von Mises, morto nel 1973, è stato un economista austriaco naturalizzato statunitense, tra i più influenti della scuola austriaca e del pensiero liberale, nonché uno dei padri del moderno libertarianismo. È considerato il decano della scuola economica austriaca.

141) L'infodemia è una combinazione di "informazione" ed "epidemia" che si riferisce tipicamente a una diffusione rapida e di vasta portata di informazioni accurate e imprecise su qualcosa, come una malattia.

best practices che non riguardano la mera interrogazione sui motori di ricerca di una certa keyword, ma il ricorso ad una procedura complessa, in grado di filtrare a monte le notizie "non utili", restringendo il campo di ricerca a poche decine di risultanze.

A tal fine, esistono diversi aggregatori finalizzati all'OSINT (il più diffuso è senza dubbio *https://osintframework.com*[142]) e alcuni tools specifici per la ricerca di immagini (come *tineye.com*[143]) o per la ricerca di forum (*boardreader.com*[144]).

3.3.1. I software più utilizzati

Per l'attività di analisi, vengono utilizzati numerosi software, ognuno dei quali è in grado di fornire risultati preziosi per il successivo sviluppo di un'investigazione. In particolare, con riferimento al contrasto del fenomeno del traffico di droga in rete, gli strumenti informatici più utilizzati sono certamente:

– "*Maltego*"[145], che può essere considerato un buon supporto nel caso si voglia conoscere l'analisi delle relazioni esistenti nel mondo reale fra persone, gruppi, siti web, domini Internet, reti di appartenenza a social network (pur tenendo presente che non esiste nessun *software* in grado di soddisfare tutte le necessità dell'analista OSINT). Con riferimento a Maltego, uno dei

142) Il framework OSINT è un sito web che classifica i migliori strumenti per trovare e raccogliere informazioni open source. È un repository on-line (letteralmente deposito o ripostiglio; è un ambiente di un sistema informativo in cui vengono gestiti i metadati, attraverso tabelle relazionali), che contiene una moltitudine di risorse per la ricerca di informazioni open source. È simile a un archivio, la cui gestione è semplice e intuitiva, in cui si possono trovare fonti classificate per argomento; raccoglie più di 30 categorie. Se, per esempio, si è in possesso di un indirizzo e-mail, è possibile verificarne la validità utilizzando un percorso guidato che consente l'accesso ai migliori servizi di validazione esistenti.

143) "TinEye" è il primo motore di ricerca d'immagini nel web che utilizza una tecnologia d'identificazione dell'immagine. In pratica, è possibile sottoporre un'immagine a TinEye per scoprire dove e come l'immagine appare nel web oppure per trovare versioni modificate o elaborate della stessa.

144) È un motore di ricerca specializzato nel trovare informazioni all'interno delle community. Indicando la propria query il sito permette di estrapolare le informazioni dai forum di discussione attivi sul web.

145) Realizzato dall'azienda Paterva, viene definito come "il prodotto per eccellenza nel campo dell'OSINT".

fattori importanti è la possibilità di integrarlo con altri servizi gratuiti o a pagamento di aziende partner e leader nel mercato della sicurezza informatica e dell'intelligence che ne implementano le possibili attività. L'impatto grafico del network di relazioni esistenti (che il sistema è in grado di ricostruire) e la possibilità di generare in automatico un report finale con la descrizione di ogni singola entità sono alcuni dei punti di forza del software, che – di contro – presenta notevoli limitazioni nel caso in cui si svolgano delle attività OSINT in merito ad entità situate al di fuori dell'area europea e del Nord America. I dati forniti, inoltre, necessitano sempre di un lavoro dell'analista per convalidarne la reale affidabilità. Interessante, infine, l'opzione "Maltego CaseFile", che permette di realizzare un report di dati in modalità off line (sempre con supporto grafico), andando a indicare le diverse entità che fanno parte di un network, al fine di analizzarne le attività;

– "*Whois*", che consente di risalire, oltre all'identità del titolare di un dominio[146], anche a numerosi informazioni riguardanti un sito web, quali l'amministratore, la data di creazione e l'ultimo aggiornamento;

– "*Waybackmachine*"[147], che consiste in una vera e propria "libreria digitale", oggi contenente oltre 330 miliardi di pagine web, raccolte a partire dal 1996 per mano dell'organizzazione non-profit "Internet Archive"[148]. Alla stessa stregua di Google, anche "Internet Archive" ha i suoi instancabili crawler[149] che scandagliano il web catturando delle istantanee (snapshot) delle pagine web incontrate. Queste vengono poi archiviate e inserite all'interno di una linea temporale. In pratica, grazie alla "macchina dei ricordi" è possibile curiosare su come è cambiato un sito nel corso del tempo e, volendo, anche resu-

146) *Whois* è un protocollo di rete che consente, mediante l'interrogazione di appositi database server da parte di un client, di stabilire a quale provider Internet appartenga un determinato indirizzo IP.

147) Pare che il suo nome sia stato ispirato dall'omonima macchina del tempo del cartone americano *Rocky & Bullwinkle*.

148) Come recita lo statuto dell'organizzazione, lo scopo della stessa è quello di fornire l'accesso universale a tutte le conoscenze. Costruire dunque un patrimonio informativo da mettere a disposizione di storici, ricercatori e studenti.

149) Un crawler (detto anche web crawler, spider o robot), è un software che analizza i contenuti di una rete (o di un database) in un modo metodico e automatizzato, in genere per conto di un motore di ricerca. Nello specifico, è un tipo di bot (programma o script che automatizza delle operazioni), che solitamente acquisisce una copia testuale di tutti i documenti presenti in una o più pagine web creando un indice che ne permetta, successivamente, la ricerca e la visualizzazione.

scitare non solo gli URL[150] eliminati, ma anche molti siti che non sono più online;

– "*HTTrack*"[151], che consente il download di un intero sito e di conservarne una copia da analizzare off line, oltre che utilizzarlo come fonte di prova;

– "*Geosetter*"[152], che – attraverso una comoda interfaccia dotata di una mappa interattiva – permette di aggiungere a qualsiasi foto presente sul PC le informazioni relative alla posizione geografica. In questo modo, è possibile applicare i cosiddetti "geotag" anche alle foto scansionate o scattate con fotocamere/telefonini non molto recenti e salvare in esse i dati relativi alla posizione geografica in cui sono state realizzate[153].

Infine, molto utilizzati per l'analisi dei social media sono i tolls denominati "Facebook Investigative Toll" e "TwitterForencis", che sono analizzatori, rispettivamente, di profili Facebook e Twitter.

3.3.2. Il sistema di analisi italiano "D.O.L. - DCSA"

In Italia, la sezione "*Drug@ on line*" della DCSA[154], nell'attività di monitoraggio della rete Internet finalizzata all'individuazione e localizzazione di siti web dediti o legati al traffico di droga[155], utilizza il software denominato D.O.L. ("Droga on line").

---

150) Un Uniform Resource Locator (in acronimo URL) è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete di computer, come ad esempio un documento, un'immagine, un video, tipicamente presente su un host server e resa accessibile a un client.

151) È tradotto in numerose lingue e risulta, anche per questo motivo, di facile utilizzo.

152) Giunto alla versione 3.3.60, è distribuito con licenza freeware.

153) Le fotocamere digitali e i telefonini di ultima generazione salvano all'interno delle foto le informazioni relative al luogo in cui sono state scattate. Grazie a questi dati, si possono sfogliare le proprie foto sul pc sapendo subito quando e, soprattutto, dove sono state realizzate.

154) La Sezione è stata istituita con circolare del Capo della Polizia il 20.9.2014, proprio in ragione dell'esponenziale crescita dei fenomeni criminali connessi con i traffici di stupefacenti in rete.

155) Attività che rientra tra i compiti della Sezione, oltre all'analisi ed elaborazione dei dati catturati sul web e, soprattutto, all'attivazione degli uffici e dei reparti territoriali delle forze di polizia per lo sviluppo delle successive investigazioni. Proprio da un'attivazione della DCSA è nata, per esempio, l'indagine condotta dalla Guardia di finanza che ha portato allo smantellamento del "Berlusconi Market" (del quale si è già parlato in maniera più approfondita) e all'arresto dei suoi gestori, tutti italiani.

Si tratta di un sistema informativo realizzato nell'ambito del Progetto "Save Our Net (S.O.N.) Support"[156] e impiegato per la ricerca dei siti in chiaro (quindi nell'*open web*) che favoriscono le attività illecite relative alla compravendita di droga.

L'architettura del software è strutturata in 3 fasi: 1) la *ricerca*; 2) l'*archiviazione*; 3) l'*elaborazione.*

In particolare, nella fase di *ricerca*, il sistema – utilizzando parole chiave – effettua il monitoraggio automatizzato di tutti i siti web presenti sulla rete Internet che consentono l'acquisto di stupefacenti, attuando però una ricerca:

– "*filtrata*": dai risultati del monitoraggio vengono esclusi automaticamente tutti i siti web contenenti informazioni di tipo scientifico o testate giornalistiche, oltre agli elementi poco rilevanti per le investigazioni;

– "*intelligente*": il *software* dispone di una funzione di "autoapprendimento", per cui i risultati del monitoraggio, una volta archiviati, non vengono più ricercati, evitando così duplicazioni.

Le informazioni trovate vengono salvate automaticamente dal sistema in un'area denominata "limbo", dove vengono elencate in una griglia; cliccando sulla stringa corrispondente a uno dei siti web rilevati, si possono ottenere ulteriori informazioni riguardanti il sito stesso, quali la data di creazione e di ultimo aggiornamento, il tipo di sito (se proprietario, ad esempio), l'indirizzo IP e il dominio.

Nella seconda fase, il software – una volta analizzati i dati salienti dei siti rilevati – ne consente l'*archiviazione* nelle seguenti 4 macro aree:

– "siti web proprietari", intesi – come già illustrato – quali piattaforme virtuali in cui il contatto tra venditore e acquirente avviene in maniera diretta;

– "siti web di intermediazione", dove il contatto tra venditore e acquirente avviene con l'intermediazione del sito, che mette a disposizione dei venditori delle aree virtuali (per similitudine, basti pensare alle vetrine di un ne-

156) Il progetto, che nasce nell'ambito del "Prevention and Fight Programme" della Commissione europea, è realizzato dall'Istituto di istruzione superiore Carlo Urbani e promosso dal Dipartimento per le politiche antidroga e dal Ministero dell'istruzione, dell'università e della ricerca. L'intervento risponde all'esigenza di tutelare la categoria dei minori, la più facilmente esposta al fenomeno della vendita on-line di droga e si rivolge, in particolar modo, ai genitori, agli educatori e agli insegnanti che avvertono la necessità di tutelarli maggiormente rispetto alla navigazione e all'accesso a siti web (attivi principalmente nel *dark web*) che commercializzano sostanze stupefacenti.

gozio) nelle quali è possibile inserire messaggi\promozioni di vendita di droga (le trattative avvengono successivamente e in forma privata tra le parti, principalmente attraverso chat cifrate);

– "aree web dedicate a forum", nelle quali è consentito agli utenti di dialogare e discutere su determinati argomenti (i forum di maggiore interesse riguardano, oltre l'affidabilità del venditore, la varietà delle sostanze offerte e la sicurezza\riservatezza della spedizione dei prodotti acquistati);

– "siti web scartati", vale a dire catturati dal software erroneamente, poiché non contengono informazioni rilevanti ai fini dell'investigazione.

Infine, la fase di elaborazione dei dati che avviene attraverso l'incrocio di tutte le informazioni immagazzinate nel sistema e che consente di:

– effettuare un'analisi generale sulle dinamiche del traffico di droga, per quanto emerge dal monitoraggio dei siti rilevati;

– cercare possibili convergenze di informazioni utili all'avvio di nuove indagini o al prosieguo di investigazioni in corso (spesso si ricerca se più siti siano stati registrati dal medesimo soggetto o se più siti siano locati su server "residenti" nello stesso Paese);

– stilare statistiche dettagliate riguardanti i siti (con particolare riferimento al Paese in cui risultano ubicati i server), le sostanze vendute (con indicazione della Nazione di provenienza) e le forme di pagamento maggiormente utilizzate.

3.3.3. Il "web profiling" e la riproduzione *off-line* di un market

Altri importanti strumenti di cui l'investigatore può avvalersi per ricostruire l'organizzazione "virtuale" di un traffico in rete di stupefacenti e di altri beni e servizi illeciti sono la creazione del *website profiling* (relativo ovviamente alle piattaforme monitorate) e all'*analisi di un market* (con particolare riferimento alla sua architettura informatica e alle modalità operative adottate).

In entrambi i casi, si tratta di raccogliere on-line il maggior numero di informazioni riguardanti la "vita in rete" di un sito o di un market, per poterne creare una "copia off line" sul quale approfondire successivamente l'analisi, sempre con lo stesso obbiettivo: cercare di "materializzare" ciò che è puramente virtuale fino a quando rimane nel web. Per l'operatore di polizia che "osserva" le dinamiche del web, il risultato ottimale è acquisire un elemento informativo (che può essere, per esempio, la geolocalizzazione di un server o l'individuazione di uno dei luoghi di spedizione dei prodotti) che consenta di spostare lo sforzo investigativo dal mondo virtuale del web (ostico e comples-

so) ad un ambito reale e materiale, nel quale proseguire più agevolmente le indagini secondo le tradizionali tecniche.

Ma torniamo alla descrizione dei citati strumenti.

La *creazione del profilo di un sito web* si compone di più fasi: 1) la profilazione dei dati; 2) l'estrazione di informazioni caratterizzanti da chat, forum o blog; 3) l'analisi della strutturazione del codice[157] (analisi dei listati) e delle funzioni implementate.

Più in dettaglio, la *fase di profilazione dei dati* (procedura squisitamente tecnico-informatica) avviene mediante:

– la modellazione e classificazione, intesa quale identificazione e distribuzione dei comportamenti simili in aree omogenee, con successiva classificazione per caratteristica;

– l'associazione, che consiste nell'identificazione di azioni, eventi, comportamenti tra loro associati;

– la deviazione, vale a dire la rilevazione dello scostamento di alcuni dati dalla massa in analisi;

– l'identificazione delle ricorrenze (in altri termini, dei dati che si ripetono);

– l'analisi dei path[158], con la generazione di grafi che illustrano le relazioni tra le pagine web;

– la modellazione sequenziale, che consiste nella rilevazione della frequenza di occorrenze in sequenze di dati;

– la comparazione di stringhe, vale a dire il confronto dei campi di testo nei record di coppie di database e il calcolo delle similitudini.

Invece, *l'estrazione di informazioni caratterizzanti* da chat, forum o blog mira a rilevare elementi d'interesse da comparare successivamente con altri dati acquisiti in rete per cercare di ottenere la convergenza verso una precisa identità. A tal fine, risulta particolarmente utile:

---

157) I programmi e le pagine web che vengono utilizzate quotidianamente si basano su lunghe istruzioni, a volte molto complicate, indirizzate al computer. Questo testo di comando è chiamato codice sorgente o più semplicemente sorgente (ma anche codice o listato). I programmatori stabiliscono tutte le regole per l'azione che deve eseguire il computer servendosi di un determinato linguaggio di programmazione. Se il redattore dovesse involontariamente inserire un errore nel testo che va contro le direttive del linguaggio di programmazione, il programma non funzionerà oppure crasherà durante l'esecuzione di determinati processi.

158) In informatica, indica la sequenza delle cartelle a cui bisogna accedere per raggiungere la posizione di un determinato file.

– rilevare il nickname utilizzato dal gestore del sito o le espressioni idiomatiche alle quali quest'ultimo fa ricorso (interessante anche l'approfondimento sugli errori di ortografia e di battitura);

– analizzare la timeline delle conversazioni e la frequenza delle stesse;

– estrapolare le interconnessioni tra utenti diversi;

– tentare di geolocalizzare le foto;

– estrapolare dai testi delle conversazioni ulteriori informazioni caratterizzanti, quali ad esempio il riferimento a cose, a persone o a luoghi.

L'*analisi della strutturazione del codice e delle funzioni implementate*, infine, è finalizzata a rilevare eventuali commenti o firme che possano celare indicazioni utili a "far luce" sulla figura del programmatore (che spesso coincide con il gestore del sito o con l'ideatore\amministratore del market).

Anche l'analisi di un market si compone di diverse fasi, che mirano sostanzialmente a riprodurne una "fedele copia". Essa avviene, infatti, mediante:

– il login al sito. Come già illustrato, la navigazione nel *dark web* (come detto, area del web che ospita gli illegal shops) può avvenire esclusivamente utilizzando specifici software, tra i quali quello più noto è certamente Tor browser;

– la ricognizione visiva della piattaforma, al fine di cercare di comprenderne, in linea di massima e in maniera speditiva, la strutturazione e il funzionamento;

– la creazione di una cartella con la medesima struttura del sito. In particolare, la riproduzione deve contenere, oltre alla "homepage" del sito, informazioni estrapolate dai forum riguardanti i venditori, gli ordini effettuati o in gestione, i prodotti e i servizi offerti, l'organizzazione di vendita, le modalità di spedizione (con particolare riferimento alle modalità di occultamento dei prodotti e al Paese dal quale i prodotti vengono spediti o comunque dal quale è presumibile che vengano spediti, tenuto conto che spesso i venditori – per sviare eventuali indagini – indicano località non esatte). Utile, infine, verificare l'eventuale collegamento a link esterni;

– il salvataggio di tutte le pagine di interesse nelle rispettive sotto-cartelle per la successiva analisi off line.

Per l'attività di analisi di un sito di vendita di sostanze stupefacenti, viene in supporto dell'investigatore perfino la semplice *regola delle 5W*[159], la cui

159) La cosiddetta regola delle 5 W (iniziali di Who, What, Where, When, Why) è considerata la regola principale dello stile giornalistico anglosassone. In inglese è nota sia come Five

applicazione consente di realizzare uno "schema informativo" che aiuta a focalizzare l'attenzione su quei dati che risultano indispensabili per la conduzione di un'indagine nello specifico ambito. Il risultato di una raccolta informativa basata su tale regola si concretizza nella conoscenza della:

– tipologia di utente a cui il sito vuole rivolgersi (*WHO*);

– la sua struttura e le funzionalità offerte (blog, chat, forum, archivi documentali, transazioni, ecc… - *WHAT*);

– la struttura dei link interni e soprattutto di quelli esterni (*WHERE*);

– la timeline della vita del sito e la sua evoluzione (*WHEN*);

– gli scopi che il sito si prefigge (*WHY*).

Infine, nell'analisi della pagina web di un venditore che opera nell'ambito di un market, oltre all'estrapolazione di informazioni che risultano utili a ricostruire le modalità con cui vengono condotte e concluse le trattative di compra-vendita (analizzando principalmente il contenuto dei forum), risulta di particolare interesse la c.d. "chiave pubblica".

Come già illustrato parlando del funzionamento di Tor, il protocollo PGP (Pretty Good Privacy) è un software per la crittografia, che si fonda su un sistema – tra i più sicuri in assoluto – che consente di criptare messaggi di testo, file e cartelle garantendo un altissimo livello di privacy. Tale sistema – giova ripeterlo – usa un metodo di crittografia "asimmetrico" basato su una "coppia di chiavi": una pubblica, che viene fornita agli altri per poter comunicare in modo anonimo (è in pratica la "casetta della posta" nel quale possono essere lasciati messaggi); una privata, strettamente personale (non dovrebbe essere mai divulgata), che consente di aprire la "cassetta della posta" e leggere i messaggi contenuti (la riservatezza di tale chiave consente esclusivamente al proprietario di poter decifrare i messaggi che gli vengono inviati).

L'importanza dell'analisi della "chiave pubblica" è riconducibile al fatto che, talvolta, i venditori – pur utilizzando i più sofisticati sistemi informatici per garantirsi l'anonimato e per garantire la riservatezza dei messaggi che si scambiano con gli acquirenti – sono superficiali proprio nella procedura di creazione di tale chiave, che richiede l'abbinamento della stessa a un indirizzo e-mail. È il caso, per esempio, dei venditori "Area51" e "Darkapollo" del black market Alphabay, i quali – nel crearla – avevano ingenuamente inserito l'indirizzo *Adashc31@gmail.com*, senza però considerare che Adashc31 era il nickname utilizzato da un soggetto americano per il proprio profilo Facebook

---

Ws che come W-h questions e fa parte delle regole di buona formazione del discorso (altro non sono che le domande che ogni giornalista dovrebbe porsi per comprendere bene la situazione ed elaborarla).

(si è trattato in quel caso, di un errore grossolano che ha consentito agli investigatori americani[160] di identificare il soggetto che aveva attivato su Alphabay due differenti canali di vendita utilizzando due diversi pseudonimi).

3.4. Le operazioni speciali antidroga in rete: l'infiltrazione e l'acquisto simulato

Nell'attività di contrasto al fenomeno dei traffici on-line di droga particolare importanza riveste il ricorso alle operazioni speciali secondo un copione che prevede generalmente:

– la preliminare raccolta informativa circa l'operatività in rete di un market o di un sito di vendita, raccolta svolta mediante l'attività di OSINT\SOC.M.INT. nell'*open web* o dal monitoraggio nel dark web (che avviene, invece, tramite gli specifici strumenti di navigazione);

– l'"infiltrazione" nella "piattaforma di spaccio" monitorata[161], allo scopo di incrementare il bagaglio informativo sulla funzionalità della stessa;

– l'"acquisto simulato" di prodotti, grazie al quale l'attenzione investigativa si concentra sulla fase della loro spedizione con lo scopo di provare ad addivenire, attraverso le tradizionali tecniche d'indagine, all'identificazione del mittente (come detto, la maggiore criticità per i trafficanti in rete ricade proprio nella procedura di consegna della merce agli acquirenti, unica fase in cui si "materializza" ciò che sino ad allora è solo "virtuale").

Lo svolgimento di operazioni sotto copertura in rete non può essere in alcun modo connotata dall'improvvisazione, nella considerazione che il web sembra anonimo, ma in realtà non sempre lo è; senza le opportune precauzioni, infatti, ogni connessione è tracciabile e identificabile. Inoltre, non è da trascurare il rischio che può derivare per un investigatore che interagisce con altri utenti di una piattaforma dall'essere a propria volta oggetto di attacchi infor-

160) Il dato emerge dalla deposizione dell'agente della DEA sotto copertura che ha svolto gli approfondimenti investigativi che hanno all'epoca consentito l'identificazione del venditore.

161) Lo strumento è normativamente previsto dalla legge 16 marzo 2006, n. 146, che – all'art. 9 – prevede, tra l'altro, la possibilità per gli ufficiali e gli agenti di polizia giudiziaria che conducono operazioni speciali di "… *utilizzare documenti, identità o indicazioni di copertura anche per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione*…", oltre che di essere autorizzati all'"… *utilizzazione temporanea di beni mobili ed immobili, di documenti di copertura, l'attivazione di siti nelle reti, la realizzazione e la gestione di aree di comunicazione o scambio su reti o sistemi informatici*…".

matici (attraverso, per esempio, l'invio di malware) o di tentativi di intrusione finalizzati a rilevarne l'identità.

Pertanto, nello svolgimento di attività undercover, allo scopo di preservare il proprio anonimato, è indispensabile usare precauzioni quali:

– non utilizzare il proprio personal computer o quello collegato alla rete interna dell'ufficio, né connessioni WIFI condivise o pubbliche;

– scollegare sempre la webcam e il microfono del pc utilizzato;

– utilizzare un programma di wiping sulla macchina utilizzata per "ripulirla" periodicamente da eventuali malware;

– avviare sempre una VPN (Virtual Private Network[162]) per nascondere il proprio IP;

– navigare utilizzando il browser Tor (da aggiornare costantemente);

– utilizzare un account e-mail anonimo (*.onion*[163]) e una chiave PGP (per la crittografia delle comunicazioni);

– costruire e utilizzare una (o più) false identità sui social network e\o forum nei quali si ritiene di indagare (è importante utilizzare sia nickname che avatar[164] differenti, così come è necessario fare attenzione alla configurazione della lingua nell'attivazione di un falso profilo per non insospettire gli altri utenti).

Inoltre, di fondamentale importanza è l'attività propedeutica all'infiltrazione; prima di interagire con altri utenti di una piattaforma virtuale è indispensabile imparare la "lingua scritta" del web, studiando le conversazioni nei forum dei black markets per imparare, per esempio, le espressioni che vengono maggiormente utilizzate o il significato di alcune immagini che spesso sostituiscono le parole. In altri termini, è necessario "immergersi completamente" nella vita della comunità virtuale che si intende infiltrare per far percepire agli altri utenti di essere "uno di loro e come loro".

Come accennato, l'infiltrazione in una piattaforma serve a completare il quadro informativo riguardante la sua strutturazione e il suo funzionamento;

---

162) Il servizio VPN permette di "nascondere" il vero indirizzo IP della macchina da cui ci si connette ad Internet dietro l'indirizzo IP di numerosi altri *server* in tuto il mondo, rendendo quindi irrintracciabile l'autore della connessione in corso. Inoltre, allo scopo di raggiungere una buona garanzia di non-tracciabilità, la connessione va configurata in modo tale da poterla spostare, a brevi intervalli di tempo, a rotazione e in modalità casuale, su *server* differenti.

163) Spesso vengono utilizzati gli *account* MAIL2TOR (*mail2tor2zyjdctd.onion*), SIGAINT (*sigaintevyh2rzvw.onion*) e ONIONMAIL (*I3xzz25unf54s7ii.onion*).

164) L'avatar è un'immagine scelta per rappresentare la propria utenza in comunità virtuali, luoghi di aggregazione e di discussione o di gioco on-line.

non solo, ma anche ad "accreditarsi" agli occhi della comunità virtuale. Si tratta, da un lato, di acquisire in itinere tutte quelle notizie indispensabile al prosieguo delle indagini, dall'altro, di attivare un proprio "falso profilo" credibile e affidabile[165]. La piena conoscenza del market e la fiducia acquisita costituiscono la base essenziale per l'attuazione della seconda fase dell'operazione undercover, vale a dire l'acquisto simulato di prodotti. Lo scopo di questo secondo step investigativo è quello di ricostruire l'iter di spedizione della merce, con particolare riferimento al punto di partenza, inteso sia come località dalla quale la merce parte (si tratta spesso di società di trasporto, ma talvolta anche di uffici postali, come di fatto accertato nell'indagine condotta sul Berlusconi Market), sia come soggetto mittente. Con riferimento a quest'ultimo, è facilmente intuibile come l'acquisto simulato, nella quasi totalità dei casi, porti all'identificazione di un soggetto terzo, assoldato dai venditori dietro compenso economico (talvolta vengono utilizzati minorenni o anziani, in ragione del minore sospetto che destano; in altre circostanze, la spedizione viene affidata a tossicodipendenti, disposti a esporsi al rischio pur di ottenere in cambio una dose di stupefacente). È pertanto necessario considerare tale identificazione quale punto di partenza di un'ulteriore step investigativo, che – attraverso il monitoraggio dell'intermediario eseguito con le normali tecniche d'indagini (pedinamenti, intercettazioni telefoniche o ambientali) – miri a risalire alla reale identità del venditore.

Le attività undercover in rete sono spesso associate anche all'utilizzo di strumenti informatici basati sui software, come malware e NIT (Network Investigative Technique), che generalmente sfruttano gli errori di configurazione dei siti nascosti nelle darknet[166].

---

165) Dalla lettura di alcuni articoli reperiti su fonti aperte, emerge che in altri Paesi (in particolare negli Stati Uniti, in ragione di una normativa più ampia e di una maggiore "spregiudicatezza" investigativa), l'attività sotto copertura condotta nel black market non è limitata all'attivazione di un "falso profilo" da acquirente, ma va ben oltre. In alcuni casi (il più emblematico è quello dello smantellamento di Hansa Market), gli agenti sotto copertura si sono addirittura sostituiti agli amministratori (una volta identificati e arrestati), subentrando di fatto nelle loro "identità on-line" (peraltro, se il soggetto "sostituito" nella piattaforma gode, nell'ambito della stessa, di una posizione di privilegio, potrebbe aver facilmente accesso a importanti dati amministrativi).

166) Secondo gli esperti, le vulnerabilità dovute ad errori di configurazione sono molto diffuse. Circa il 6% dei siti presenta errori di configurazione che permettono di risalire al loro reale indirizzo IP. Inoltre, il 25% dei siti contiene errori di configurazione che consentono di ottenere utili informazioni (ad esempio la riconducibilità di siti diversi alla stessa persona).

Come in precedenza illustrato, i punti vulnerabili del protocollo TOR sono rappresentati dai c.d. "nodi" di accesso. Infatti, prima di accedere alla rete TOR i pacchetti presentano ancora l'header[167] in chiaro e quindi anche l'IP se lo stesso non viene opportunamente nascosto tramite l'utilizzo di un server proxy, che funga da intermediario per le richieste da parte dei client alla ricerca di risorse su altri server. Approfittando di una simile vulnerabilità provocata da un errore di configurazione, è possibile inserire nella rete Tor il server gestito dall'investigatore, al quale il software del computer del target invia il suo vero indirizzo IP.

Uno degli esempi più eclatanti di utilizzo con successo di strumenti informatici è quello che ha consentito all'FBI di smantellare, nel 2015, uno dei maggiori siti pedopornografici del *dark web*, denominato "PlayPen"[168], nonché di identificare e arrestare i suoi due amministratori e un moderatore.

L'indagine era nata nel 2014, allorquando la polizia di un altro Stato non americano aveva segnalato all'FBI non solo l'esistenza di questo sito nascosto, ma anche il suo vero indirizzo IP (visibile a causa di un errore di configurazione), associato a un server localizzato negli Stati Uniti. Una volta individuato il server, in North Carolina, l'FBI decise di non oscurarlo, bensì di gestirlo direttamente per analizzarne gli accessi. L'attività sotto copertura dell'FBI portò, non solo all'identificazione degli amministratori del sito, ma anche di altri 1300 utenti che usufruivano dell'illecito servizio. In quella circostanza, venne utilizzata la tecnica investigativa di rete, nota come NIT (Network Investigative Technique), attuata iniettando nei pc degli internauti monitorati un malware (codice malevolo) in grado di ottenerne il vero indirizzo IP, anche in caso di navigazione con il browser Tor (che, come detto, in condizioni normali, nasconde l'IP del suo utilizzatore).

Un ultimo aspetto da evidenziare nella conduzione delle attività sotto copertura in rete è di natura procedurale e consiste nell'opportunità di registrare lo scherma del pc utilizzato, mediante l'utilizzo di software quali, ad esempio, "OBS Studio"[169]. Si tratta di una procedura, applicabile in realtà an-

---

167) Intestazione di un messaggio di posta elettronica, che indica il mittente, il luogo, l'ora di spedizione e altre informazioni per l'instradamento del messaggio fra i server Internet.

168) All'epoca contava ben 150.000 membri che pubblicavano e accedevano a immagini e video di abusi sessuali su minori.

169) "Open Broadcaster Software" è un programma di streaming e registrazione video gratuito e open source, gestito dal Progetto OBS. Il programma dispone di supporto per Windows 7, OS X 10.8 e Linux Ubuntu 14.04 (comprese le successive versioni).

che all'attività di OSINT o di monitoraggio di un black market (quindi ad operazioni informatiche da eseguire non necessariamente sotto copertura), che – consentendo di ricostruire fedelmente tutti i passaggi dell'attività svolta – risulta molto utile anche per produrre fonti di prova in fase processuale.

3.5. La cooperazione internazionale: uno strumento irrinunciabile

Come illustrato, una delle caratteristiche principali del traffico on-line di droga e degli altri prodotti\servizi illeciti è la globalità. Si tratta di un fenomeno che interessa contestualmente le varie parti del mondo dove sono allocati i server dei venditori o dove risiedono gli acquirenti, ai quali la merce potrebbe essere peraltro spedita da un'altra parte ancora. Inoltre, una piattaforma dedita ad attività illecite in rete rappresenta una vera e propria "comunità virtuale", in cui interagiscono culture differenti, lingue differenti e addirittura abitudini di vita differenti.

Con tali premesse, un'azione di contrasto per essere efficace non può che essere altrettanto globalizzante; in altri termini, non può che fondarsi, oltre che sulle competenze specifiche maturate dalle forze di polizia di ciascun Paese, su una concreta cooperazione internazionale, ritenuta – come detto – una dei fattori di maggiore successo nell'azione di contrasto dei fenomeni che interessano la rete.

Proprio con riferimento ai traffici on-line, alcune recenti interventi di polizia che hanno portato allo smantellamento, nel maggio del 2019, del Wall Street Market (sul quale erano registrati oltre 5000 venditori ed erano presenti circa 63.000 annunci di vendita) e, nel settembre 2020 (con l'operazione denominata "DistrupTor"), all'arresto di 179 venditori attivi nel *dark web* (identificati grazie all'analisi dei dati informatici contenuti nei server sequestrati nel corso dell'operazione di chiusura del citato market), hanno ancora una volta evidenziato la fondamentale importanza della cooperazione a livello mondiale tra le varie forze di polizia. Basti considerare che dei 179 soggetti, 121 sono stati arrestati negli Stati Uniti, 42 in Germania, 8 nei Paesi Bassi, 4 nel Regno Unito, 3 in Austria, 1 in Svezia e che allo svolgimento dell'operazione hanno contribuito ben 9 Paesi (oltre ai sei interessati dall'esecuzione degli arresti, anche Cipro, Australia e Canada).

A livello europeo, sono stati nel tempo adottati alcuni strumenti di raccordo informativo che si prefiggono lo scopo di garantire maggiore efficacia al contrasto dei fenomeni criminali in rete esaltando proprio il criterio della cooperazione e della collaborazione tra Stati.

In particolare, nel 2013, avendo rilevato che oltre al terrorismo, al traf-

fico internazionale di droga e al riciclaggio di denaro, alla frode organizzata e alla falsificazione di euro, anche la criminalità informatica già rappresentava una grave minaccia alla sicurezza interna dell'UE, è stato fondato – all'interno di Europol – lo "European Cybercrime Centre" (EC3) per rafforzare la risposta delle forze dell'ordine al cyber crimine[170].

L'EC3 riserva particolare attenzione ai mercati criminali presenti nel *dark web*, nel cui ambito la strategia di Europol è quella di creare un approccio coordinato di contrasto con la partecipazione delle forze di polizia di tutti gli Stati membri e di altri partner, tra i quali – per esempio – Eurojust. Proprio per raggiungere l'obiettivo di ridurre le dimensioni dell'economia illegale generata dai traffici nella parte oscura del web, all'interno dell'EC3 opera il "Dark Web Team", che fornisce un approccio completo e coordinato, in termini di condivisione di informazioni, di supporto operativo e di sviluppo di strumenti, tattiche e tecniche per condurre indagini sul *dark web*[171].

Anche sotto l'aspetto giudiziario, esistono strumenti che si fondono sulla cooperazione per la raccolta delle prove in materia penale, ivi compresi i reati commessi mediante l'utilizzo della rete.

In particolare, l'"*ordine europeo di indagine*"[172] è una decisione emessa

---

170) L'attività dell'EC3 si concentra principalmente su tre aree: 1) reati informatici commessi da gruppi della criminalità organizzata; 2) crimini informatici che causano gravi danni alle loro vittime (come lo sfruttamento sessuale dei minori); 3) crimini informatici (compresi gli attacchi informatici) che colpiscono infrastrutture critiche e sistemi informativi nell'Unione. In merito a queste tre aree di monitoraggio, il Centro si pone come collettore di varie funzioni come: fungere da hub centrale per informazioni e *intelligence* criminali; sostenere le operazioni e le indagini degli Stati membri mediante analisi operative, coordinamento e competenze; fornire una varietà di prodotti di analisi strategica che consentano di prendere decisioni informate a livello tattico; stabilire una funzione di sensibilizzazione completa che colleghi le forze dell'ordine relative alla criminalità informatica; sostenere la formazione e il rafforzamento delle capacità, in particolare delle autorità competenti degli stati membri; fornire capacità di supporto tecnico forense digitale altamente specializzate alle indagini e alle operazioni di polizia giudiziaria.

171) Il team mira inoltre a potenziare azioni tecniche ed investigative congiunte, organizzando iniziative di formazione e rafforzamento delle capacità, insieme a campagne di prevenzione e sensibilizzazione all'interno di una strategia a 360° contro la criminalità informatica.

172) La direttiva relativa all'ordine europeo di indagine penale è stata adottata il 3 aprile 2014 ed è stata recepita in Italia con il decreto legislativo n. 108 del 21 giugno 2017 (la Danimarca e l'Irlanda non sono vincolate da detto strumento). L'ordine europeo di indagine è basato sul riconoscimento reciproco, ossia sul fatto che l'autorità di esecuzione è tenuta a riconoscere e a garantire l'esecuzione della richiesta formulata dall'altro Paese. L'ese-

o convalidata dall'autorità giudiziaria di un Paese dell'UE per ottenere atti di indagine[173] effettuati in un altro Paese dell'UE al fine di raccogliere elementi di prova, anche di natura elettronica, quali informazioni in merito al titolare di un conto di posta elettronica o data/ora e contenuto di messaggi scambiati attraverso Facebook messenger (tutti dati che possono essere conservati in un Paese UE diverso da quello che sta conducendo le indagini).

Infine, sempre con riferimento alla cooperazione giudiziaria e di polizia in materia penale, l'attivazione di "*Squadre investigative comuni*"[174] costituisce certamente una efficace modalità operativa di contrasto dello specifico fenomeno.

Più in dettaglio, per l'Italia, il d.lgs. 34/2016 prevede la costituzione di una SIC su iniziativa di un'autorità requirente italiana oppure la partecipazione del nostro Paese a una SIC su invito della competente autorità di un altro Stato membro per indagare su una determinata fattispecie criminosa di interesse comune. Più in dettaglio, quanto alla prima delle due ipotesi, il legislatore ha individuato, quale autorità competente ad esercitare tale iniziativa, il Procuratore della Repubblica nei casi in cui:

– "*… procede a indagini relative ai delitti di cui agli articoli 51, commi 3-bis, 3-quater e 3-quinquies, e 407, comma 2, lettera a), del Codice di procedura penale o a delitti per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni*" (si tratta, quindi, di condotte criminose gravi e sovente caratterizzate da portata transnazionale);

– "*… vi è l'esigenza di compiere indagini particolarmente complesse sul territorio di più Stati membri o di assicurarne il coordinamento*"[175].

---

cuzione, inoltre, deve essere eseguita con le stesse modalità che si seguirebbero se l'atto investigativo in questione fosse stato ordinato da un'autorità dello Stato di esecuzione. Infine, l'autorità di emissione può utilizzare un ordine europeo di indagine nel caso in cui l'atto d'indagine sia necessario, proporzionato e consentito in casi nazionali analoghi. I termini stabiliti sono 30 giorni per decidere di riconoscere ed eseguire la richiesta; 90 giorni per dare esecuzione alla richiesta in maniera efficace, in seguito all'adozione della predetta decisione.

173) Possono includere, a titolo di esempio, l'escussione di testimoni, le intercettazioni telefoniche, le operazioni d'infiltrazione e informazioni su operazioni bancarie.

174) Il quadro di riferimento giuridico dell'UE contempla la possibilità di istituire Squadre investigative comuni fra Stati membri all'articolo 13 della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea e nella decisione quadro 2002/465/GAI del Consiglio, decisione attuata in Italia con il decreto legislativo 15 febbraio 2016, n. 34.

175) Con questa seconda previsione, il legislatore ha allargato il novero di reati per combattere i quali è consentita l'istituzione delle SIC, coerentemente con quanto previsto dalla de-

Uno degli aspetti certamente più delicati e complessi della disciplina delle SIC concerne la redazione dell'accordo costitutivo da parte dei rappresentanti degli Stati partecipanti. Mediante tale accordo, infatti, vengono disciplinati aspetti essenziali della loro composizione e del loro funzionamento, quali – ad esempio – i poteri dei partecipanti, l'oggetto e le finalità delle indagini.

Con riferimento alla composizione, le scelte del legislatore italiano meritano qualche riflessione in quanto si distaccano parzialmente dalle indicazioni contenute nella decisione quadro 2002/465/GAI. Il d.lgs. 34/2016 prevede, infatti, che l'atto costitutivo debba indicare i componenti della SIC, i quali vengono distinti in due categorie: *i membri nazionali*, cioè agenti e ufficiali di polizia giudiziaria dello Stato membro di intervento, nonché uno o più magistrati dell'ufficio del pubblico ministero che ha sottoscritto l'atto costitutivo; i *membri distaccati*, cioè i "componenti della squadra appartenenti ad altri Stati membri". Fin qui, la disciplina italiana coincide perfettamente con quanto previsto dalla decisione quadro, dal quale però il legislatore italiano si è discostato nella parte in cui non ha contemplato la partecipazione alla SIC di "persone diverse dai rappresentanti delle autorità competenti degli Stati membri" che la costituiscono, espressione che si riferisce a funzionari di organismi istituiti ai sensi del TUE, tra cui, certamente, membri di Europol e di Eurojust, dell'OLAF o rappresentanti di altri organismi internazionali. L'esclusione di tali soggetti dalle SIC, giustificata con l'obbligo di mantenere il segreto sugli atti di indagine del pubblico ministero e della polizia giudiziaria, non può che indurre a una riflessione sull'opportunità di aver operato tale scelta, tenuto conto che l'eventuale partecipazione di organismi quali Europol ed Eurojust potrebbe di contro risultare determinante al fine di risolvere eventuali difficoltà di coordinamento tra i membri della squadra e di acquisire eventuali informazioni supplementari, senza in alcun modo mettere a rischio il buon esito delle indagini.

Un altro aspetto poco chiaro, circa la composizione della SIC, riguarda la determinazione del soggetto preposto a dirigerla. La decisione quadro 2002/465/GAI si è in questo mostrata coerente al principio della *lex loci* (secondo cui, la squadra opera conformemente al diritto nazionale dello Stato membro in cui interviene), stabilendo che la sua direzione debba spettare al rappresentante dello Stato membro nel quale di volta in volta essa interviene.

---

cisione quadro 2002/465/GAI che non contempla alcuna limitazione quanto alla tipologia di reato perseguito. Inoltre, ha eliminato il riferimento – contenuto nell'art. 1 lett. a) della decisione quadro 2002/465/GAI – al requisito del "collegamento tra le indagini", così da rendere possibile costituire la squadra anche qualora vi sia una sola indagine complessa, che richiede un'azione investigativa coordinata in più Stati membri.

Una soluzione di questo tipo, tuttavia, denota criticità che discendono dalla circostanza che il capo della squadra debba mutare ogni volta in cui l'indagine si sposti da uno Stato membro ad un altro, con possibili ricadute negative sull'efficienza organizzativa della squadra. Sul punto, il legislatore italiano sembra aver considerato questa circostanza laddove ha previsto che la designazione del direttore della squadra avvenga in via convenzionale in sede di redazione dell'atto costitutivo. Tuttavia, ha disposto perentoriamente che sia il pubblico ministero italiano a dirigere la SIC, quando questa operi in territorio italiano, nel rispetto dell'art. 327 c.p.p. Ne discende che, qualora il direttore della squadra, nominato nell'accordo costitutivo, non appartenga all'autorità giudiziaria italiana e le indagini si spostino nel nostro Paese, la guida della squadra dovrà necessariamente mutare in favore del membro italiano.

Un ultimo cenno merita infine l'accordo costitutivo nella parte in cui deve contenere l'indicazione dell'oggetto e della finalità delle indagini, nonché della loro durata. Ciò non dovrebbe comportare un'eccessiva rigidità nello svolgimento delle attività della SIC, in quanto è comunque consentito modificare in corso di svolgimento obiettivi ed oggetto dell'indagine, coerentemente con le sopravvenute esigenze investigative ed organizzative[176].

Tutti gli strumenti di cooperazione sin qui descritti risultano certamente funzionali allo svolgimento di incisive attività di contrasto di fenomeni che interessano contestualmente più Stati, quali appunto l'illecito traffico in rete. Il loro utilizzo, pur se validissimo in termini di efficacia, non può però che essere complementare all'attuazione di una forma di cooperazione, molto più semplice, ma di fondamentale importanza: lo scambio di informazioni tra le forze di polizia. Sul punto, occorre considerare come tale scambio informativo, nelle forme in cui è attualmente congeniato (vale a dire per il tramite di Europol o di Interpol), avvenga con una procedura che si completa in tempi troppo

176) Quanto alla delicata questione della durata delle indagini svolte dalla SIC, la soluzione prescelta dal legislatore italiano consiste nel non limitarne rigorosamente la durata. Si prevede, infatti, che i membri della SIC – in sede di redazione dell'accordo costitutivo – stabiliscano in via convenzionale un termine entro cui ragionevolmente le attività investigative dovrebbero concludersi, salva possibilità di proroga. Tale proroga non necessita di autorizzazione da parte di un'autorità giudiziaria ma, benché non espressamente indicato, dovrà rispettare i termini massimi di durata delle indagini ex art. 405 e ss. del nostro codice di procedura penale. In pratica, il legislatore mostra di ritenere implicito il rispetto delle norme procedurali del nostro ordinamento. Pertanto, essendo le SIC nient'altro che uno strumento di indagine, esse dovranno soggiacere al termine generale di durata stabilito dal nostro ordinamento per gli atti compiuti in fase di indagini preliminari.

lunghi se messi in relazione alla velocità con cui evolvono le dinamiche criminali nel web, rispetto alle quali un'informazione risulta utile se celermente condivisa. A tal fine, parrebbe pertanto molto più conveniente ricorrere alle interlocuzioni dirette tra le forze di polizia, secondo una procedura più snella e immediata che consenta agli investigatori di "stare al passo del web".

In tale direzione, per l'Italia, un ruolo di primaria importanza può certamente essere ricoperto dagli Esperti per la Sicurezza[177], che – per la DCSA (in materia quindi di stupefacenti) – coincide con l'Esperto antidroga, figura già prevista dall'art. 11 del Testo unico sugli stupefacenti. L'Esperto per la sicurezza, che opera presso la rappresentanza diplomatica o presso l'ufficio consolare di destinazione, acquista temporaneamente lo status di agente diplomatico e, nel rispetto della sua autonomia operativa e senza pregiudizio per il proprio rapporto di servizio con l'Amministrazione di appartenenza, è posto alle dipendenze funzionali del Capo missione[178]. Esplica la sua attività nell'acquisizione di dati informativi relativi ai vari fenomeni criminosi, tra i quali ovviamente il traffico di stupefacenti. Inoltre, nel quadro di specifici Accordi di cooperazione internazionale stipulati con i Governi interessati, l'Esperto per la sicurezza provvede ad organizzare training specifici nel settore del narcotraffico e del terrorismo internazionale, che prevedono la formazione e lo scambio di informazioni tra le forze di polizia del Paese straniero e l'Italia[179].

Conclusioni

Negli ultimi anni la rete Internet è diventata sempre più un fiorente mercato parallelo di scambio commerciale di beni e servizi di qualsiasi tipo, anche

177) È un appartenente alle forze dell'ordine individuato tra i Dirigenti e i Commissari della Polizia di Stato, gli ufficiali dell'Arma dei Carabinieri e della Guardia di finanza, in servizio ovvero assegnati temporaneamente presso la Direzione centrale della polizia criminale - Servizio per la cooperazione internazionale di polizia, ovvero presso la Direzione centrale per i servizi antidroga (il numero degli Esperti per la sicurezza è determinato nel limite massimo di cinquanta unità).

178) Per la DCSA, sono attualmente schierati in Spagna (Madrid e Barcellona), Marocco, Iran, Senegal, Ghana, Uzbekistan, Canada, Repubblica Dominicana, Venezuela, Brasile, Colombia e Perù.

179) La legge del 26 febbraio del 2011 n.10 ha ampliato le competenze di tale figura estendendole ad altri come per esempio il terrorismo internazionale, il traffico d'armi, l'immigrazione clandestina, la tratta di esseri umani, i sequestri di persona e le ricerche di latitanti.

purtroppo di natura illecita. Su tutti, il fenomeno del traffico di droga e armi è riuscito a ritagliarsi uno "spazio virtuale" importante, generando un enorme volume d'affari che ha nel tempo consentito ad abili criminali, esperti d'informatica, di arricchirsi, facendo leva sulle potenzialità che il web offre in termini di "anonimato" sia nella navigazione che nelle procedure di pagamento per gli illeciti acquisti effettuati.

Ma andiamo per ordine, sintetizzando gli aspetti salienti dell'elaborato, prima di concludere con alcune personali considerazioni sull'attività di contrasto delle forze di polizia, frutto anche del confronto con "addetti ai lavori".

Utilizzando una nota metafora, si può paragonare l'intera rete di Internet a un iceberg, del quale solo la minima parte che affiora (circa il 4%), denominata "*open*" o "*surface web*", è costituita dai contenuti quotidianamente fruiti dagli utenti. Si tratta, in altre parole, di quella piccola porzione del web agevolmente navigabile utilizzando comuni *tools*, quali ad esempio Google o Bing.

La parte sommersa dell'iceberg si compone, invece, in gran parte (circa il 90%) del "*deep web*", cioè di quella ampia porzione del World Wide Web "invisibile", contenente risorse informatiche (siti internet di recente costituzione e non ancora indicizzati, pagine web a contenuto dinamico, forum di conversazione chiusi, chat di messaggistica private), il cui accesso – da parte di un utente generico – appare progressivamente più difficoltoso man mano che si cerca di penetrare in quei livelli che sono maggiormente nascosti.

Fino a questo punto, quindi, nulla di strano. Il discorso inizia, tuttavia, a complicarsi quando ci si immerge in profondità sino a raggiungere – per proseguire con la metafora – la punta inferiore dell'iceberg dove trova spazio, seppur minimo (il restante 6% circa), il c.d. "*dark web*", un piccolo mondo virtuale non accessibile utilizzando una normale connessione Internet, ma solamente mediante particolari software in grado di anonimizzare l'utente e la sua navigazione.

Lo strumento di accesso al *dark web* più diffuso è certamente "TOR" (acronimo di "The Onion Router"); si tratta di un software, liberamente scaricabile, che permette di occultare l'indirizzo IP del computer utilizzato (e quindi di rendere anonima l'identità dell'utente), facendo rimbalzare l'accesso alla connessione Internet tra una molteplicità di computer sparsi in tutto il mondo. In altre parole, a differenza di un sistema tradizionale in cui le informazioni transitano direttamente da un client al server finale, in questo caso i dati informatici attraversano vari server TOR, che si comportano a loro volta come router realizzando una sorta di percorso virtuale crittografato e a strati (a cipolla).

L'accesso da parte di un generico utente al "*deep web*" e alla sua parte più nascosta, il "*dark w*eb", non presenterebbe di per sé profili di rilievo giuridico, ovviamente nella misura in cui la condotta dell'utente rimanga entro i confini di ciò che non è giuridicamente vietato.

Basti pensare che, nei primi anni successivi al suo esordio, proprio quella porzione sommersa del web, nei Paesi lacerati dalle dittature militari e sottostanti a rigide politiche di censura della libera manifestazione del pensiero, era diventata per giornalisti, associazioni di tutela dei diritti umani e dissidenti perseguitati dai governi l'unico spazio di comunicazione sicuro con il resto del mondo.

Non solo, ma era stata concepita anche come uno dei pochi luoghi sicuro di scambio di informazioni in ambito commerciale ed industriale, tenuto conto che la possibilità di crittografare la trasmissione dei dati consentiva di ridurre drasticamente il rischio di fuga dei segreti industriali.

I problemi sono tuttavia sorti quando – addentrandosi nel *dark web* – si è scoperto che quella stessa parte sommersa della rete nata per fini leciti veniva utilizzata anche per la realizzazione di svariate attività illegali da parte di cybercriminali che beneficiavano del fatto di potervi navigare in totale anonimato. Ed ecco che oggi, in essa, trovano terreno fertile i c.d. "black markets", vale a dire piattaforme virtuali appositamente create per l'e-commerce di prodotti illeciti di diversa tipologia (droga e armi soprattutto, ma anche materiale pedopornografico, carte di credito rubate, falsi documenti d'identità, dati e codici bancari sottratti e tanto altro ancora).

Il funzionamento di un market in rete è simile a quello di un qualsiasi negozio di vendita; un amministratore organizza lo shop e riserva ai vari venditori uno spazio espositivo virtuale dove pubblicizzare i propri prodotti, con dovizia di particolari, e rendere note le condizioni di vendita, in particolare le modalità di pagamento e quelle di spedizione. Ogni market è dotato di specifici forum, dove gli acquirenti possono lasciare recensioni, sulla base delle quali i nuovi utenti della piattaforma operano generalmente la scelta del venditore ritenuto "più affidabile". Le trattative di compravendita avvengono, in linea di massima, in forma privata, mediante l'utilizzo di chat cifrate. Una volta raggiunto l'accordo, l'acquirente procede al pagamento utilizzando criptovalute (Bitcoin, in particolare), sfruttando anche in questo caso l'anonimato offerto dalle transazioni con moneta digitale (il possessore viene identificato solo mediante un indirizzo che non contiene alcuna informazione che possa consentire di risalire al legittimo proprietario). Il passaggio della moneta tra acquirente e venditore non è però diretto, ma avviene attraverso un deposito di garanzia (il c.d. *escrow*), gestito dall'amministratore, il quale rilascia in favore del vendi-

tore la quantità di moneta digitale pattuita, solo dopo aver ricevuto dall'acquirente conferma dell'avvenuta ricezione della merce ordinata e dopo averne trattenuto una percentuale (solitamente il 4%) a titolo di commissione.

Il "valore aggiunto" di un black market è, per il venditore, la facilità con cui un esperto informatico riesce ad architettare una piattaforma di e-commerce capace di generare un enorme volume d'affari; per l'acquirente è, invece, la possibilità di acquistare con una fittizia "identità virtuale" qualsiasi tipo di prodotto senza correre il pericolo di dover contrattare di persona con lo spacciatore, oltre che di sperimentare nuove sostanze stupefacenti, reperendole agevolmente e anche a buon prezzo.

La vendita di droga in rete, inizialmente limitata al mondo del web, si è nel tempo estesa, dapprima, ai social network (Facebook e Twitter su tutti) e, successivamente, ai servizi di messaggistica istantanea (Telegram e Wickr in particolare), con questi ultimi in grado di offrire la riservatezza delle comunicazioni, tanto utile per chi con essi persegue scopi illeciti.

L'utilizzo delle chat cifrate merita un'ulteriore approfondimento tenuto conto che si tratta di uno strumento di comunicazione riservata che si è diffuso in un duplice ambito criminale; da un lato, quello della "vendita al dettaglio", rispetto alla quale hanno di fatto contribuito alla "dematerializzazione" delle tradizionali "piazze di spaccio", consentendo soprattutto ai più giovani di acquistare droga comodamente da casa (si tratta di un servizio molto utilizzato anche in questo periodo di emergenza sanitaria che ha comportato notevoli limitazioni in termini di mobilità); dall'altro, quello della "commercializzazione all'ingrosso" da parte dei narcotrafficanti, che per mantenersi in contatto, ormai da qualche anno, ricorrono all'uso dei c.d. "criptofonini", basati proprio su un sistema di comunicazione anonima non intercettabile.

Sempre con riferimento al traffico on-line di droga e armi, un ultimo aspetto da evidenziare è che per tale fenomeno, come per tutti quelli che si sviluppano mediante il web, vale la regola generale secondo cui nel *cyberspace* i concetti di tempo e di spazio sono totalmente stravolti; il primo è accelerato, mentre il secondo è del tutto azzerato. Da ciò è facilmente comprensibile come le sue caratteristiche principali siano proprio la "globalità" e la "mutabilità". Una piattaforma virtuale di vendita non ha confini potendo contare su server collocabili in qualsiasi punto del mondo, che consentono la conclusione simultanea di trattative tra utenti che, a loro volta, si trovano in Paesi o addirittura continenti differenti (globalità). Inoltre, così come è facile ideare e realizzare uno shop in rete, è altrettanto facile chiuderlo rapidamente (magari per aprirne un altro, più sicuro, se ci si sente "osservati" dalle forze di polizia) o semplicemente cambiarne l'indirizzo di acceso o la denominazione (mutabilità).

In uno scenario criminale così articolato, l'attività di contrasto delle forze di polizia risulta non certo agevole. Per un investigatore che agisce in rete, è infatti necessario possedere un'elevata competenza informatica che gli consenta di utilizzare efficacemente gli strumenti di analisi oggi disponibili (software anche complessi) e, soprattutto, di saper interpretare al meglio e con abilità il proprio ruolo di "infiltrato" in un market nello svolgimento di operazioni speciali, che – come detto – rappresentano nella maggior parte dei casi l'unico mezzo per smantellarlo, cercando al contempo di individuarne gli ideatori\amministratori e di identificare il maggior numero di venditori.

Peraltro, la consapevolezza della pericolosità di un fenomeno tanto "sommerso" quanto "dilagante" ha indotto a ricorrere sempre più spesso a preziose forme di cooperazione internazionale in materia penale, sia giudiziaria che di polizia (tra tutte, si citano l'"ordine di indagine europeo" e le "squadre investigative comuni"), oltre che a rafforzare, in Europa, lo scambio informativo tra le forze di polizia degli Stati membri mediante l'istituzione, all'interno dello "European Cybercrime Centre" (EC3) di Europol del "Dark Web Team", deputato al supporto informativo ed operativo per le indagini condotte in rete.

In Italia, un primo importante passo avanti in materia è stato fatto con la creazione, nel 2014, nell'ambito della Direzione centrale per i servizi antidroga del Dipartimento della pubblica sicurezza, della sezione "Drug@online", cui è demandato, in via esclusiva, il compito di "… *monitorare la rete in funzione di prevenzione e di coordinamento delle relative attività di repressione da svolgere in ambito territoriale*".

Inoltre, nel 2019, il Dipartimento delle politiche antidroga della Presidenza del Consiglio dei Ministri ha siglato tre importanti accordi di collaborazione interistituzionale: uno con l'Arma dei Carabinieri, denominato "NPS - Online", il cui principale obiettivo è quello di monitorare costantemente i siti web e i social network per contrastare il traffico illegale di Nuove Sostanze Psicoattive (NPS)[180]; il secondo, denominato "Hermes", con la DCSA, volto al potenziamento delle attività di prevenzione e di contrasto della diffusione delle sostanze stupefacenti, principalmente di sintesi chimica, attraverso il monitoraggio e il controllo delle spedizioni postali operate dai principali corrieri; il terzo, infine, denominato "Kriptoval", con il Comando generale della Guardia di finanza, finalizzato al monitoraggio dei flussi finanziari connessi al nar-

180) Il progetto, in particolare, ha consentito di sviluppare e testare innovativi sistemi informatici – software e hardware – idonei ad implementare le capacità investigative nel monitoraggio del deep e del dark web.

cotraffico, realizzati anche attraverso criptovalute o altri strumenti di pagamento elettronico.

Anche sul piano normativo, la legge 18 dicembre 2020, n. 173[181], ha previsto – quale ulteriore modalità di contrasto alle piazze di spaccio virtuali – l'"oscuramento"[182] dei siti di vendita in rete inseriti in un'apposita lista, analogamente a quanto già praticato con riferimento al fenomeno della pedopornografia. In particolare, la DCSA ha il compito di fornire l'elenco dei siti di cui viene chiesta l'inibizione all'accesso all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione[183], che provvede a interessare gli Internet Provider sui quali ricade l'onere di procedere al loro oscuramento entro sette giorni[184], "*avvalendosi degli strumenti di filtraggio e delle relative soluzioni tecnologiche*"[185].

Tutte le iniziative sinora intraprese denotano un indiscutibile atteggiamento positivo e propositivo da parte di tutte le istituzioni chiamate a contrastare un fenomeno certamente nuovo, del tutto "invisibile", ma non per questo meno allarmante soprattutto in relazione alla velocità con cui si sta diffondendo in tutto il mondo.

Occorre pertanto fare di più, partendo innanzitutto dall'adozione di alcuni accorgimenti in relazione alle attuali procedure di contrasto che ricondu-

---

181) Legge di conversione, con modificazioni, del d.l. 21 ottobre 2020, n. 130, recante "*Disposizioni urgenti in materia di immigrazione, protezione internazionale e complementare, modifiche agli articoli 131-bis, 391-bis, 391-ter e 588 del codice penale, nonché' misure in materia di divieto di accesso agli esercizi pubblici ed ai locali di pubblico trattenimento, di contrasto all'utilizzo distorto del web e di disciplina del Garante nazionale dei diritti delle persone private della libertà personale*".

182) L'oscuramento è possibile solo per i siti attivi nell'*open web*.

183) Con la legge nr. 249 del 1997, che istituisce l'Autorità per le garanzie nelle comunicazioni, e con il decreto interministeriale del 19 gennaio 1999, è stato previsto che l'Organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni sia il Servizio polizia postale e delle comunicazioni, che nell'assolvere i propri compiti si avvale delle articolazioni periferiche dei Compartimenti di polizia postale e delle comunicazioni.

184) Gli Internet Provider che non ottemperano a tale obbligo incorrono in una una sanzione amministrativa pecuniaria da euro 50.000 a euro 250.000, non applicabile se il fatto costituisce reato (nel caso, per esempio, in cui venga ipotizzato il concorso nell'attività illecita svolta da un sito di cui è stato ordinato l'oscuramento).

185) Il decreto del Ministro delle comunicazioni 8 gennaio 2007 aveva previsto i requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet avrebbero dovuto utilizzare, al fine di impedire, con le modalità previste dalle leggi vigenti, l'accesso ai siti segnalati dal Centro nazionale per il contrasto alla pedopornografia.

cono, in linea di massima (non è una regola, ma sembra essere ad oggi l'unica strada seguita), alle strutture centrali (DCSA in primis, per quanto riguarda le sostanze stupefacenti) il compito di effettuare il "monitoraggio" della rete, primo e fondamentalo *step* di un complesso percorso investigativo. Gli esiti di tale monitoraggio[186] vengono poi riversati agli uffici\reparti territorialmente competenti[187], che sviluppano conseguentemente le indagini utilizzando gli strumenti attualmente disponibili[188].

Un sistema così congeniato, da un lato, certamente garantisce la possibilità di avere una visione unitaria dell'andamento del fenomeno grazie al ruolo delle strutture centrali che fungono sia da "volano" per le attività di contrasto a livello nazionale che da qualificato interlocutore a livello internazionale (con Europol e Interpol innanzitutto); dall'altro lato, sembra però essere inadeguato se si considera che oggi il monitoraggio, di fatto affidato a poche persone (anche in ragione dei volumi di forza delle strutture centrali che lo effettuano), genera una quantità di informazioni assolutamente insufficienti rispetto alla velocità con cui il fenomeno si sta diffondendo.

Pertanto, al fine di migliorare lo strumento di contrasto dei traffici illeciti on-line, si potrebbe ipotizzare, sul piano operativo, la creazione – non solo a livello centrale (in seno ai Servizi centrali delle tre forze di polizia), ma anche

---

186) Il monitoraggio è finalizzato all'acquisizione di un bagaglio informativo il più completo possibile in ordine ad un market place, con particolare riferimento alla tipologia di prodotti commercializzati, alle modalità di pagamento, al luogo di spedizione da parte dei venditori, alle modalità di occultamento, al tipo di messaggistica criptata utilizzata per i dettagli della contrattazione, all'affidabilità dei venditori, desumibile dai giudizi e dai commenti espressi nelle chat e nei forum. Inoltre, mira alla geolocalizzazione dei dispositivi informatici attivi nell'ambito del market, con la precisazione che tale attività è possibile in maniera diretta solo per i siti di vendita operanti nell'*open web*; nel dark web, invece, è necessario procedere per indagini deduttive partendo dai luoghi di spedizioni, dalla lingua utilizzata oppure dagli esiti dell'attività di OSINT\SOCMINT che possano far emergere "somiglianze culturali" delle identità virtuali che operano nel web sommerso con profili attivi nell'*open web* o sui social network.

187) Per la DCSA l'attivazione avviene a rotazione tra Carabinieri, Polizia e Guardia di finanza e in direzione dei servizi centrali, che – a loro volta – valutano autonomamente la strategia investigativa da attuare.

188) Tra gli strumenti disponibili, come già evidenziato, particolare importanza rivestono le operazioni speciali. In linea di massima, gli investigatori undercover dapprima si infiltrano nella "piattaforma di spaccio" individuata, incrementando il bagaglio informativo sulla stessa e, successivamente, procedono ad acquisti simulati per focalizzare l'attenzione sulle spedizioni allo scopo di tentare di addivenire all'individuazione del mittente e del destinatario.

a livello periferico (preferibilmente provinciale) – di *team* specializzati composti da personale adeguatamente formato nello specifico settore, ai quali affidare un duplice compito:

– condurre le indagini su attivazione delle strutture centrali, potendo contare su personale in possesso di un'adeguata capacità tecnica, soprattutto con riferimento alle attività sotto copertura in rete che richiedono un'elevata competenza informatica;

– svolgere un'autonoma attività di monitoraggio delle piattaforma di vendita, i cui esiti potrebbero confluire in un unico database centralizzato dal quale ogni comando\reparto centrale o periferico (dove ovviamente esiste il *team*) potrebbe poi estrapolare gli elementi d'informazione utili allo sviluppo di proprie investigazioni. Si tratterebbe, in sostanza, di una sorta di "raccoglitore informatico", alimentato e consultabile da tutti i team, la cui gestione ricadrebbe su strutture a livello centrale (per le sostanze stupefacenti, per esempio, potrebbe essere attribuita alla DCSA, come peraltro già avviene per ogni comunicazione afferente i traffici con metodologie tradizionali).

Operare adeguatamente in rete comporta ovviamente la necessità di implementare continuamente la propria dotazione tecnologica. Solo disponendo di mezzi informatici (hardware, notebook, periferiche USB, Hard Disk, traduttori elettronici vocali) all'avanguardia, si è in grado, infatti, di contrastare con maggiore efficacia l'operatività dei cybercriminali che si basa prima di tutto su tecnologie molto sofisticate e costantemente aggiornate; non solo, ma anche di poter garantire la dovuta efficienza a livello internazionale, nel caso in cui – per esempio – si venga chiamati ad operare nell'ambito di "squadre investigative comuni".

Si tratta certamente di buoni propositi, ma perseguibili solo se si decidesse di investire concretamente nello specifico settore, puntando prima di tutto sulla formazione del personale, dalla iniziale specializzazione al successivo aggiornamento. A tal fine, risulterebbe particolarmente utile organizzare, oltre a specifici corsi, anche frequenti incontri con le forze di polizia di altri Paesi, al fine di poter attuare un concreto scambio di "best practices", utili a meglio orientare e sviluppare le proprie attività investigative.

Un'ulteriore considerazione inerisce agli strumenti normativi attualmente a disposizione. Un fenomeno tanto sommerso quanto dilagante, che fa della globalità e della mutabilità le sue caratteristiche principali, non può che far aumentare – giorno dopo giorno – la consapevolezza che si tratta di un fenomeno "allarmante" che va in qualche modo infrenato o quanto meno limitato. A tal fine, uno dei fattori di successo sarebbe certamente la possibilità di poter contare su una legislazione che individui nella creazione e gestione di un mar-

ket in rete una specifica fattispecie di reato da sanzionare con pene certamente più severe di quella (4 anni di reclusione) inflitta, in primo grado, dal Tribunale di Brescia, ai tre giovani pugliesi, ideatori di un negozio virtuale di vendita di prodotti illegali nel *dark web* (il Berlusconi Market) in grado di generare un giro d'affari semplicemente milionario.

Per concludere, il fenomeno "sommerso" e "invisibile" dei traffici in rete di droga e armi è certamente in preoccupante crescita e richiede l'adozione di strumenti di contrasto ulteriori rispetto a quelli disponibili, oltre che l'affinamento delle metodologie d'indagine. Sotto quest'ultimo aspetto, in particolare, occorre dare una risposta concreta alla domanda che viene naturale porsi, vale a dire quale sia, ad oggi, la posizione della criminalità organizzata italiana di tipo tradizionale (soprattutto della *'ndrangheta*, particolarmente attiva a livello internazionale nel narcotraffico) rispetto a tali dinamiche criminali che si sviluppano mediante la rete. Ad oggi, non esistono risultanze investigative che consentano di ricostruire una stretta connessione tra gli "attori" (ideatori e venditori) di un mercato illegale in rete e le organizzazioni di matrice mafiosa[189]; basti considerare che i tre gestori del Berlusconi Market (ora detenuti) non erano legati ad alcun ambiente criminale, ma solamente abili conoscitori di informatica. La questione è chiaramente da approfondire, tenuto conto che appare quantomeno singolare che le mafie tradizionali, sempre così attente a intercettare le nuove possibilità di illecito arricchimento, non abbiano ancora allungato le mani sulla gestione di tale fruttuosissimo business.

Un aspetto da chiarire di non poco conto, che porta inevitabilmente a considerare come il vasto mondo del web costituisca per le forze di polizia una sfida che si fa sempre più avvincente.

Bibliografia

Colombini M.C. (Consulente informatico), *La ricerca e l'analisi nel deep web: i black market*, in *Sicurezza e giustizia*, numero IV del MMXV, 26 gennaio 2016

Direzione Centrale Per i Servizi Antidroga, *Relazione annuale 2020 su dati 2019*

Direzione Nazionale Antimafia, *Relazione sulle attività svolte dal Procu-*

189) È emerso, di contro, l'interesse delle mafie tradizionali ad "assoldare" esperti d'informatica per il riciclaggio del denaro sporco mediante le criptovalute.

ratore nazionale e dalla Direzione nazionale antimafia e antiterrorismo nonché sulle dinamiche e strategie della criminalità organizzata di tipo mafioso nel periodo 1° luglio 2018 - 31 dicembre 2019, 24 novembre 2020
European Monitoring Centre for Drugs and Drug Addiction, *EU Drug Markets. Impact of COVID-19*, maggio 2020
European Monitoring Centre for Drugs and Drug Addiction, *The Internet and drug markets*, 2016
Europol, *How COVID-19-related crime infected Europe during 2020*, 11 novembre 2020
Europol, *Internet organised crime threat assessment 2020*
Fontana F., approfondimento su *Criptovalute e rischi di riciclaggio*, in *Antiriciclaggio & compliance - Rivista italiana dell'antiriciclaggio*, n. 2\2020 (Aprile/Giugno)
Razzante R., *Bitcoin e criptovalute. Aspetti giuridici e finanziari*, Maggioli, 2018
United Nations Office on Drugs and Crime, *Report 2020*

Sitografia

http://politicheantidroga.gov.it
http://rivista.eurojus.it
https://antidroga.interno.gov.it
https://bitcoin.org
https://cortedicassazione.it
https://cybersecurity360.it
https://e-justice.europa.eu
https://emcdda.europa.eu
https://europol.europa.eu
https://metrics.torproject.org
https://sicurezza.net
https://torproject.org

Parte IV

Documenti, Normativa e Giurisprudenza di interesse

Hate crime e *hate speech*: strategia di prevenzione e di contrasto del Dipartimento della Pubblica Sicurezza

di Francesca Romana Capaldo*

Abstract

Nel presente lavoro ho analizzato il fenomeno degli hate crimes, nella loro dimensione internazionale ed unionale, nonchè attraverso la tutela apprestata dall'ordinamento italiano nel contrastarli, recependo convenzioni e direttive internazionali.

In particolare i crimini d'odio sono stati approfonditi attraverso l'analisi delle caratteristiche criminologiche dell'under-reporting, under-recording e del rischio di escalation, nonché tratteggiandone i principali markers di pregiudizio, i cd. "bias indicators".

Partendo da una disamina del concetto di odio nella sua dimensione ontologica, filosofica e sociologica, da funzionario di polizia ho tratteggiato i contorni tecnico giuridici dell'odio nella sua dimensione criminologica, quale discriminazione razziale, nazionale, etnica e religiosa, consapevole che la sensibilità del legislatore è strettamente legata alla maturità e alla coscienza che una comunità sviluppa in un determinato momento storico.

E proprio sul tema della discriminazione religiosa nei confronti degli ebrei e sulla rilevanza della recentissima adesione dell'Italia alla definizione internazionale di antisemitismo dell'IHRA, ho realizzato un'intervista con il Presidente dell'Unione delle Comunità ebraiche italiane (UCEI), dott.ssa Noemi Di Segni.

Particolare attenzione è stata prestata, inoltre, nel tratteggiare i contorni dell'odio on-line, soffermandosi sulle peculiarità e caratteristiche dello stesso, nonché sulla necessità di un'azione di contrasto sinergica, multidisciplinare, ma soprattutto condivisa a livello sovranazionale.

Anche nel panorama internazionale, inoltre, l'odio, così come riportato dalle parole del neo Presidente degli Stati Uniti Joe Biden, rappresenta "un nemico da combattere che non può e non deve avere un porto sicuro negli Stati Uniti e nel mondo intero". Un nemico che non rimane confinato nel web, ma è in grado di generare violenza e disordine nel mondo reale.

(*) Vice Questore della Polizia di Stato, già frequentatrice del XXXVI corso di Alta formazione presso la Scuola di perfezionamento per le forze di polizia.

Ed infatti, negli Stati Uniti i cd. movimenti suprematisti di estrema destra, che fanno dell'odio verso gli stranieri, le persone afroamericane, gli ebrei, gli islamici, le persone LGBTIQ+, parte integrante delle loro ideologie, hanno fortemente messo in pericolo la stabilità delle istituzioni democratiche. Questi gruppi (tra cui Proud Boy, Qanon, Boogaloo), che nell'ultimo anno hanno avuto un'enorme diffusione on-line, sono passati all'azione in numerose occasioni, sino ad arrivare all'assalto a Capitol Hill del gennaio 2021.

Le Agenzie di intelligence statunitensi ritengono che il suprematismo negli Stati Uniti rappresenti, per la stabilità delle istituzioni democratiche, una minaccia persino più pericolosa di quella sinora costituita dal terrorismo islamico.

Alla luce dell'esperienza statunitense il tema degli hate crimes assume, dunque, una dimensione assolutamente strategica nella valutazione delle minacce globali per la democrazia e per la pace delle comunità.

Ed ancor di più, all'indomani della morte di George Floyd, avvenuta nel corso di un controllo di polizia a Minneapolis (Minnesota) il 25 maggio 2020, la condivisione della tematica dell'odio, la necessità di conoscere e riconoscerne le cause e di fornire adeguata accoglienza alle vittime di hate crimes, divengono tematiche di strategica rilevanza proprio per le forze di polizia, quale know how e patrimonio culturale imprescindibile dell'agire quotidiano, in grado di incidere sulla reputazione di un'istituzione che tutela, ma prima di tutto rispetta i diritti umani.

In questo ambito sicuramente l'Osservatorio per la Sicurezza Contro gli Atti Discriminatori (Oscad), istituito presso la Direzione Centrale della Polizia Criminale, rappresenta un unicum nel panorama europeo ed internazionale, ma soprattutto l'impegno del sistema di law enforcement italiano per poter sviluppare una cultura del rispetto e della non discriminazione. Nato 11 anni fa da una geniale intuizione del Prefetto Manganelli, l'Oscad oggi più che mai conferma la sua attualità, in un momento storico in cui il tema dell'odio è diventato trasversale nelle dinamiche sociali e le forze di polizia costituiscono un argine ad ogni forma di discriminazione. Il tema è centrale e nevralgico, non esiste consenso sociale e rispetto delle forze dell'ordine se queste non godono di reputazione e se "l'esercizio legittimo della forza" da parte di uno Stato non si coniuga con l'etica del rispetto delle regole e dei diritti umani.

* * *

In this dissertation I have analyzed the phenomenon of hate crimes at international and EU dimension, as well as the measures provided for by the

Italian legislation to fight against these kinds of crimes, making reference to international agreements and guidelines.

In particular, hate crimes have been analyzed in details taking into account the criminological characteristics of under-reporting, under-recording, the risk of escalation, as well as the main markers of prejudice-motivated crimes, the so-called "bias indicators".

In my capacity as Senior Police Officer, starting from the analysis of the concept of hate in its ontological, philosophical and sociological dimension, I have described the technical-legal aspects of hate from a criminological perspective, and specified that it is a kind of discrimination on the grounds of racial, national, ethnic and religious characteristics. Moreover, I have underlined that the laws issued in this field are strictly linked to the level of awareness and development of society in a certain historical context.

Taking into account the religious discrimination against the Jews and stressing the importance of the participation of Italy in the adoption of the international definition of antisemitism by IHRA, I have interviewed the President of the Union of the Italian Jewish Communities (UCEI), Mrs. Noemi De Segni.

Moreover, a special attention has been focused on the description of online hate crimes, examining, above all, their peculiarities and characteristics, as well as the need to carry out a synergic, multidisciplinary and shared activity against this kind of crimes at supranational level.

Taking into account the international context, the President of the United States of America Joe Biden declared that hate crime represents "an enemy to be countered who cannot be accepted neither in the United States nor in the other countries worldwide". This kind of enemy doesn't operate only on the web, but he is able to provoke violence and riots also in the real world.

As a matter of fact, in the United States the so-called extreme right wing movements based on suprematism, the ideology of which is based on the hate against foreigners, Afro-American citizens, Jews, Islamic people, as well as lesbian, gay, bisexual, transgender and questioning groups, have remarkably jeopardise the stability of democratic institutions. These movements (such as Proud Boy, Qanon, Boogaloo), which, in the course of last year, have been considerably spreading online, carried out a lot of actions, such as for example the attack against Capitol Hill perpetrated in January 2021.

The US Intelligence Agencies believe that suprematist ideology in the United States represents a more dangerous threat to democratic institutions than the one represented by Islamic terrorism.

Therefore, in the light of US experience, the topic of hate crimes acquires

a strategic meaning in the assessment of global threats to democracy and peace in the world.

After the death of George Floyd, caused during a police check conducted in Minneapolis (Minnesota) on May 25 2020, the shared committment to counter hate crimes, the need to know and detect the motivations and to provide for a proper protection to the victims of hate crimes, acquire a strategic importance for police forces, who should be able to count on a useful know how and cultural heritage to carry out their daily activity, thus increasing the good standing of police forces that represent an institution devoted to protect, but above all to respect human rights.

In this framework, the Observatory for security against acts of discrimination - OSCAD, which was established at the Central Directorate of Criminial Police, is the only institution of this kind at European and international level and represents, above all, the committment of Italian Police Forces in developing and promoting a culture based on respect and rejection of any forms of discrimination. OSCAD, which was created 11 years ago on the successful initiative of Prefetto Manganelli, is nowadays very important to counter this kind of phenomenon in many different fields of society, since police forces represent an institution engaged in countering any forms of discrimination. This is a key and major topic and it is to be pointed out that social appraisal and respect for police forces can be gained only when they enjoy a well deserved reputation and when "the lawful use of force" by a State is associated with the principle of respect for laws and human rights.

* * *

Introduzione

Il tema della non discriminazione rappresenta oggi una priorità nell'agenda delle Agenzie europee ed internazionali.

Le manifestazioni di odio sono all'ordine del giorno sia nel panorama nazionale che internazionale.

La Direzione Centrale della Polizia Criminale costituisce il punto di raccolta delle informazioni provenienti da numerosi Osservatori interforze, primo tra tutti l'Oscad (Osservatorio per la Sicurezza contro gli atti discriminatori), specificamente dedicato al tema dell'odio, ma anche dagli Osservatori sugli atti di intimidazione nei confronti dei giornalisti e degli amministratori locali, che registrano un sempre maggiore incremento di condotte minatorie che, di fatto, sono manifestazioni di odio ed avvengono prevalentemente via web.

Anche nel panorama internazionale, l'odio, così come riportato dalle parole del neo Presidente degli Stati Uniti Joe Biden, rappresenta "un nemico da combattere che non può e non deve avere un porto sicuro negli Stati Uniti e nel mondo intero". Un nemico che non rimane confinato però soltanto nel web, ma è in grado di generare violenza e disordine nel mondo reale.

Negli Stati Uniti i cd. movimenti suprematisti di estrema destra, che fanno dell'odio verso gli stranieri, le persone afroamericane, gli ebrei, gli islamici, le persone LGBTIQ+, parte integrante delle loro ideologie, hanno fortemente messo in pericolo la stabilità delle istituzioni democratiche. Questi gruppi (tra cui Proud Boy, Qanon, Boogaloo), che nell'ultimo anno hanno avuto un'enorme diffusione on-line, sono passati all'azione in numerose occasioni, organizzando l'assalto a Capitol Hill del gennaio 2021, ma ancora prima nell'ottobre 2020, realizzando il tentato sequestro di persona del Governatore del Michigan, Gretchen Whitmer, rea di aver limitato la libertà di movimento dei cittadini per contrastare la diffusione della pandemia!

Le Agenzie di intelligence statunitensi ritengono che il suprematismo negli Stati Uniti rappresenti la più grave delle minacce per la stabilità delle istituzioni democratiche, persino più pericolosa di quella sinora costituita dal terrorismo islamico.

Alla luce dell'esperienza statunitense il tema degli *hate crimes* e della strategia di prevenzione e contrasto alla loro diffusione assume una dimensione assolutamente strategica nella valutazione delle minacce globali per la democrazia e per la pace delle comunità.

All'indomani della morte di George Floyd, avvenuta nel corso di un controllo di polizia a Minneapolis (Minnesota) il 25 maggio 2020, la condivisione della tematica dell'odio, la necessità di conoscere e riconoscerne le cause e di fornire adeguata accoglienza alle vittime di *hate crimes*, assume ancora più rilevanza per le forze di polizia, quale *know how* e patrimonio culturale imprescindibile dell'agire quotidiano, in grado di incidere sulla reputazione di un'istituzione che tutela, ma prima di tutto rispetta i diritti umani.

In questo ambito sicuramente l'Osservatorio per la sicurezza contro gli atti discriminatori (Oscad) rappresenta un elemento distintivo del sistema di *law enforcement* italiano e un unicum nel panorama europeo ed internazionale.

Nato 11 anni fa da una geniale intuizione del Prefetto Manganelli, l'Oscad oggi più che mai conferma la sua attualità, in un momento storico in cui il tema dell'odio è diventato trasversale nelle dinamiche sociali e le forze di polizia costituiscono un argine ad ogni forma di discriminazione. Il tema è centrale e nevralgico, non esiste consenso sociale e rispetto delle forze del-

l'ordine se queste non godono di reputazione e se "l'esercizio legittimo della forza" da parte di uno Stato non si coniuga con l'etica del rispetto delle regole e dei diritti umani. Una democrazia matura deve poter contare su Forze di polizia autenticamente educate al rispetto della dignità umana che, oltre a rappresentare il fondamento stesso del vivere civile, è anche il bene giuridico protetto dalle norme dell'ordinamento che puniscono l'odio e le discriminazioni.

Non sempre ciò che è giusto in natura è giusto anche per legge, certamente contrastare l'odio in tutte le sue manifestazioni significa garantire il rispetto della dignità umana.

Straordinario momento di sintesi tra etica del rispetto dei valori e etica del rispetto delle regole.

1. Il quadro normativo di contrasto all'*hate crime* e *hate speech*

1.1. Agenzia dell'UE per i diritti fondamentali (FRA): la situazione *on the ground*

"*Dobbiamo parlare di razzismo, ma dobbiamo anche agire. Cambiare direzione è sempre possibile se ve ne è la volontà. Sono felice di vivere in una società che condanna il razzismo, ma non dovremmo limitarci alla semplice condanna. Il motto della nostra Unione europea è "Uniti nella diversità" e il nostro compito è essere all'altezza di queste parole e dare ad esse un significato concreto*". Queste le parole del Presidente della Commissione europea Ursula von der Leyen nel discorso pronunciato dinanzi al Parlamento europeo il 17 giugno 2020.

La Carta dei diritti fondamentali dell'Unione europea vieta la discriminazione, vincolando gli Stati membri dell'UE a combattere l'odio e con esso i reati motivati da razzismo, xenofobia, intolleranza religiosa, discriminazione verso la disabilità, orientamento sessuale o identità di genere di una persona.

Nonostante ciò, ancora troppe persone in tutta l'UE sono bersaglio di abusi semplicemente a causa della loro provenienza, delle loro credenze, delle loro scelte di vita o dell'aspetto fisico, siano essi percepiti e/o reali.

L'Agenzia dell'UE per i diritti fondamentali (FRA) ha pubblicato due rapporti sui reati generati dall'odio che forniscono un'analisi comparata del quadro giuridico esistente, delle esperienze individuali delle vittime di reati motivati dal pregiudizio e dello stato della raccolta di dati ufficiali nei 27 Stati membri dell'UE.

Nonostante gli sforzi compiuti dagli Stati membri dell'UE per combat-

tere la discriminazione e l'intolleranza, la strada da percorrere è ancora molto lunga.

Dall'indagine condotta dalla FRA su "minoranze e discriminazione" nell'Unione europea (EU-MIDIS) del 2008, che ha coinvolto 23.500 intervistati migranti o appartenenti a una minoranza etnica, è emerso che più di uno su quattro intervistati riteneva di essere stato vittima di reati contro la persona di "matrice razzista" (aggressione, minaccia o molestie gravi) nei 12 mesi precedenti l'indagine.

Nella "Seconda indagine su minoranze e discriminazioni nell'Unione europea - principali risultati (2017)", oltre ad essere stata evidenziata la presenza di elevati livelli di discriminazione all'interno dell'UE, sono stati identificati anche gli ambiti di vita in cui la discriminazione razziale si manifesta maggiormente. Ad esempio la discriminazione nel mercato del lavoro è un problema non solo nella ricerca di un impiego, ma anche quando lo si è già trovato: il 22% degli intervistati dichiara, infatti, di essersi sentito discriminato sul posto di lavoro per via della propria origine etnica o per la provenienza da un particolare contesto migratorio. Quando si cerca di prendere in affitto o di comprare un appartamento o una casa, il fattore scatenante alla base della discriminazione è il nome (44%), seguito dal colore della pelle o dall'aspetto fisico (40%) e dalla cittadinanza (22%). Per quanto riguarda l'accesso ai beni e ai servizi (pubblica amministrazione, trasporti pubblici, negozi, ristoranti, ecc.), i rom (28%) e le persone di origine nordafricana (27%) subiscono le discriminazioni maggiori. La discriminazione razziale risulta meno diffusa nell'assistenza sanitaria (3%), anche se con notevoli differenze tra i vari gruppi, in quanto è percepita in maniera molto forte da parte delle persone di etnia rom (8%), che, peraltro, hanno anche una minore aspettativa di vita rispetto al resto della popolazione.

I dati dell'indagine mostrano, inoltre, che le considerazioni di carattere razziale influiscono anche sulla probabilità di essere fermati dalla polizia. Del 14% delle persone intervistate che nell'ultimo anno hanno dichiarato di essere state fermate, il 40% collega l'ultimo fermo alla propria origine etnica o alla propria provenienza da un contesto migratorio. Al riguardo la stessa Agenzia FRA ha realizzato una guida per evitare la cd. "profilazione illecita", con uno specifico focus rivolto alle forze di polizia e alle autorità di gestione delle frontiere[1].

Nel complesso, il 3% degli intervistati dichiara di aver vissuto esperienze

1) European Union Agency for Fundamental Rights (FRA), *Evitare la profilazione illecita oggi e in futuro: una guida*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2019.

di violenza razzista nell'ultimo anno, mentre un altro 24% dichiara di aver subito, nello stesso periodo, molestie di stampo razzista. Quasi la metà (47%) degli ebrei intervistati teme di diventare bersaglio di insulti verbali o molestie di matrice antisemita, mentre oltre un terzo (40%) ha paura di essere aggredito fisicamente in spazi pubblici[2]. Spesso, tuttavia, le violenze e le molestie motivate dall'odio non vengono denunciate. I dati dell'indagine FRA sulle persone di origine africana, ad esempio, mostrano che quasi due terzi (64%) delle vittime di violenza razzista non hanno denunciato alla polizia, né a qualsiasi altra organizzazione o servizio, l'episodio più recente che hanno subito[3]. In tale panorama emerge chiaramente, sotto un duplice profilo, la rilevanza della formazione sui temi dell'anti-discriminazione delle forze di polizia: da un lato per evitare il fenomeno della profilazione illecita, dall'altro per evitare il fenomeno dell'*undereporting*, sostenendo le persone nella denuncia e facilitando così l'emersione del sommerso.

La Corte europea dei diritti dell'uomo (Cedu) ha, inoltre, sottolineato che i Paesi devono indicare chiaramente la motivazione alla base di reati di matrice razzista o di quelli commessi a causa del credo religioso della vittima. Ignorare il pregiudizio all'origine di un reato costituisce una violazione dell'articolo 14 della Convenzione europea dei diritti dell'uomo (CEDU).

La Corte europea ha posto l'accento sulla necessità di far emergere il pregiudizio alla base dei reati generati dall'odio, in quanto gli autori di questi reati, prendendo di mira le persone per quello che sono o per come sono percepite, trasmettono un messaggio particolarmente umiliante: la vittima non viene infatti percepita come un individuo con personalità, abilità ed esperienze proprie, ma soltanto come un membro senza volto di un gruppo contraddistinto da un'unica etichetta caratterizzante. L'autore del reato in tal modo lascia intendere che i diritti di quel gruppo possano – o addirittura debbano – essere ignorati, in palese violazione dei principi fondamentali di democrazia e uguaglianza dell'UE. Da alcune ricerche condotte sull'argomento emerge, infatti, che le vittime e i testimoni di reati generati dall'odio sono riluttanti a denunciarli, sia alle forze dell'ordine, che al sistema di giustizia penale, ad organizzazioni non governative o ad associazioni. Di conseguenza, molti reati non vengono denunciati né perseguiti, restando quindi invisibili.

---

2) European Union Agency for Fundamental Rights (FRA), *Esperienze e percezioni di antisemitismo. Seconda indagine sulla discriminazione e i reati generati dall'odio subiti dagli ebrei nella UE*, 2018.

3) European Union Agency for Fundamental Rights (FRA), *Essere di colore nell'UE*, 2018.

1.2. Standard di rispetto dei diritti fondamentali nelle organizzazioni internazionali e nel Consiglio d'Europa

In un sistema gerarchico e multilivello delle fonti del diritto, l'acquisizione di diritti, e la sussistenza dei correlati doveri, si fonda sul riconoscimento e l'affermazione di principi fondamentali all'interno di trattati internazionali e Carte costituzionali.

Il principio di non discriminazione – che sancisce, in termini generali, il godimento pieno ed eguale dei diritti, vietando illegittimi fattori di discriminazione – trova il suo fondamento giuridico in fonti costituzionali di livello internazionale, europeo e nazionale.

La fine della seconda guerra mondiale, e la scoperta delle aberrazioni del nazismo, nel 1945 rappresentano il punto di svolta e di partenza delle attività internazionali per la protezione dei diritti dell'uomo, in quanto segnano l'inizio della creazione di un sistema di norme internazionali teso a vincolare gli Stati al rispetto di un catalogo di diritti umani. Questo è un esempio di quello che viene definito il potere salvifico dell'odio cioè la forza e la capacità di riscatto che nasce proprio all'indomani di momenti di profonda avversione o grande violenza nella storia dell'umanità.

Nella Dichiarazione universale dei diritti umani, il principio di non discriminazione è indicato come uno dei principi generali per il godimento dei diritti umani. In questo senso, il divieto di discriminazione appartiene a quello zoccolo duro del Diritto Internazionale generale che costituisce lo *ius cogens*, che tutti incondizionatamente sono obbligati a rispettare.

I principi enunciati nei primi 2 articoli della menzionata Dichiarazione sono in tal senso paradigmatici: tutti gli esseri umani nascono liberi ed eguali in dignità e diritti (art. 1); ad ogni individuo spettano tutti i diritti e tutte le libertà enunciati nella presente Dichiarazione, senza distinzione alcuna, per ragioni di razza, di colore, di sesso, di lingua, di religione, di opinione politica o di altro genere, di origine nazionale o sociale, di ricchezza, di nascita o di altra condizione (art. 2). Inoltre, l'art. 3 inserisce un principio innovativo di straordinaria importanza, perché oltre a riconoscere il diritto alla vita ed alla libertà, introduce anche il diritto alla sicurezza della propria persona come precondizione per l'esercizio di ogni altra libertà.

Pochi anni dopo, nel 1950, nel contesto del Consiglio d'Europa, la "Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali" (Cedu), ha enunciato il diritto alla vita (art. 2) e alla libertà e sicurezza (art. 5), nonchè esplicitato la protezione dall'odio e dalla violenza con il diritto al rispetto della vita privata e familiare (art. 8).

Ma sicuramente è l'art. 14 Cedu che ha introdotto esplicitamente il "Divieto di discriminazione"[4], la cui portata, dapprima limitata ai diritti ed alle libertà riconosciute nella Convenzione, verrà generalizzata ad ogni altro diritto previsto da qualsivoglia legge attraverso il Protocollo addizionale n. 12[5] (Roma, 4 novembre 2000).

Dal punto di vista internazionale, però, la prima definizione di discriminazione è contenuta nella Icerd, Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale (Ris. Assemblea generale N.U. del 21 dicembre 1965). La Convenzione definisce, all'art.1, la discriminazione razziale come «*ogni distinzione, esclusione, limitazione o preferenza basata sulla razza, il colore della pelle, la discendenza o l'origine nazionale o etnica, che abbia lo scopo o l'effetto di annullare o compromettere il riconoscimento, il godimento o l'esercizio, in condizioni di parità, dei diritti umani e delle libertà fondamentali in campo politico, economico, sociale e culturale o in ogni altro ambito della vita pubblica*».

La Convenzione ha previsto, inoltre, l'istituzione di un Comitato sull'eliminazione della discriminazione razziale con compiti di tutelare l'applicazione della Convenzione attraverso lo studio dei rapporti degli Stati parte della stessa.

Il diritto a non essere discriminati per la propria origine è ormai riconosciuto ampiamente, riportato in tutti i documenti internazionali di tutela dei diritti umani, a conferma che in ambito NU la lotta contro il razzismo e la discriminazione razziale ha rappresentato fin dalla costituzione dell'organizzazione un obiettivo primario. In questo senso, l'Assemblea generale ha ribadito il suo impegno nel corso degli anni convocando tre Conferenze mondiali (1978, 1983 e 2001), e proclamando tre decenni dedicati alla lotta contro il razzismo e la discriminazione razziale (1973-1982, 1983-1992 e 1994-2003).

L'Italia ha ratificato tale Convenzione con la l. 654/1975 (detta "Legge Reale") che, come si vedrà in seguito, costituisce il primo atto normativo interno specificamente rivolto a criminalizzare condotte discriminatorie. È, inol-

---

4) Il godimento dei diritti e delle libertà riconosciuti nella presente Convenzione deve essere assicurato senza nessuna discriminazione, in particolare quelle fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o quelle di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione. La sede dell'Onu è a New York.

5) Il godimento di ogni diritto disposto da una legge sarà garantito senza alcuna discriminazione per motivi di sesso, razza, colore, lingua, religione, opinione politica o altra opinione, origine nazionale o sociale, associazione ad una minoranza nazionale, proprietà, nascita o ogni altra condizione.

tre, interessante osservare che la definizione di discriminazione razziale di cui all'art. 1 della Icerd è stata recepita, quasi integralmente, nell'ordinamento italiano con l'art. 43 del d.lgs. 286/98 (T.U. Immigrazione).

1.3. La normativa dell'Unione europea in materia di diritti fondamentali

Nel quadro del diritto dell'Unione europea esistono molte norme concernenti il divieto di discriminazione calate in diversi contesti, sia a livello di normativa originaria (trattati, accordi, convenzioni) che a livello di diritto derivato (regolamenti, direttive, decisioni).

Il rispetto della dignità e dei diritti umani è posto tra i valori fondanti dell'Unione europea dall'art. 2 del "Trattato sull'Unione europea" (TUE)[6]; mentre il "Trattato sul funzionamento dell'Unione europea" (TFUE), all'art. 10[7], pone la lotta alle discriminazioni tra gli obiettivi prioritari dell'Unione.

La Carta dei diritti fondamentali dell'Unione europea cosiddetta "Carta di Nizza", del 7 dicembre 2000, che con l'entrata in vigore del trattato di Lisbona nel 2009, ha acquisito lo stesso effetto giuridico vincolante dei trattati dell'Unione europea, riconosce una serie di diritti personali, civili, politici, economici e sociali dei cittadini e dei residenti dell'UE. Essa rappresenta il testo normativo che più di ogni altro si apre alla più ampia gamma di categorie criminologiche, infatti, all'art. 21 pone un divieto generale di discriminazione fondata sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, gli handicap, l'età o le tendenze sessuali e anche sulla cittadinanza.

Nel 2000, l'Unione europea ha adottato due direttive specificamente finalizzate alla tutela del principio di non discriminazione, recepite anche in Italia.

---

6) Art. 2 Tue: *L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini.*

7) Art. 10 Tfue: *Nella definizione e nell'attuazione delle sue politiche e azioni, l'Unione mira a combattere le discriminazioni fondate sul sesso, la razza o l'origine etnica, la religione o le convinzioni personali, la disabilità, l'età o l'orientamento sessuale.*

La direttiva 2000/43/CE del 29 giugno 2000 attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica. L'obiettivo della direttiva è quello di stabilire un quadro per la lotta alle discriminazioni fondate sulla razza o l'origine etnica, al fine di rendere effettivo negli Stati membri il principio della parità di trattamento. In particolare l'art. 2 definisce le fattispecie ascrivibili alle discriminazioni ai sensi della direttiva, distinguendo tra discriminazione diretta, indiretta e molestie[8].

La direttiva 2000/78/CE del Consiglio del 27 novembre 2000 stabilisce un quadro generale per la parità di trattamento in materia di occupazione e delle condizioni di lavoro. L'obiettivo principale della direttiva è sancito all'art. 1 che definisce un quadro generale per la lotta alle discriminazioni fondate sulla religione o le convinzioni personali, gli handicap, l'età o le tendenze sessuali, nonché per quanto concerne l'occupazione e le condizioni di lavoro, al fine di rendere effettivo negli Stati membri il principio della parità di trattamento.

Di particolare rilievo, inoltre, la "Decisione quadro 2008/913/GAI del Consiglio sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale". Tale decisione rappresenta la normativa principale che definisce un approccio unitario di contrasto al razzismo e xenofobia basato sul diritto penale riproponendosi di assicurare che le stesse condotte siano considerate reati in tutti gli Stati membri.

Attualmente nel nostro Paese la tutela è ristretta a razza, religione, origine nazionale o etnica, ma nell'adozione a livello internazionale della decisione, alcuni Stati hanno esteso tale protezione anche alle vittime di discriminazione sulla base di altri fattori, come orientamento sessuale e identità di genere[9].

Da ultimo, con riferimento al fenomeno dei cosiddetti "discorsi d'odio" la raccomandazione n. R (97) 20 del 1997 contiene una serie di principi per il

---

8) Sussiste *discriminazione diretta* quando, a causa della sua razza od origine etnica, una persona è trattata meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga; si parla di *discriminazione indiretta* quando una disposizione, un criterio o una prassi apparentemente neutri possono mettere persone di una determinata razza od origine etnica in una posizione di particolare svantaggio rispetto ad altre persone, a meno che tale disposizione, criterio o prassi siano oggettivamente giustificati da una finalità legittima e i mezzi impiegati per il suo conseguimento siano appropriati e necessari; le *molestie*, invece, sono da considerarsi una discriminazione in caso di comportamento indesiderato adottato per motivi di razza o di origine etnica e avente lo scopo o l'effetto di violare la dignità di una persona e di creare un clima intimidatorio, ostile, degradante, umiliante od offensivo. In questo contesto, il concetto di molestia può essere definito conformemente alle leggi e prassi nazionali degli Stati membri.

9) Nel nostro ordinamento il ddl Zan contro l'omotransfobia ha cercato di estendere la tutela anche a tale *ground*.

contrasto ai discorsi di odio, specificando che possono essere talmente offensivi nei confronti di individui o gruppi, in quanto finalizzati all'annientamento o ingiustificata limitazione dei diritti e delle libertà previste dalla Convenzione, da non rientrare nella legittima tutela alla libertà di espressione garantita dall'art. 10 Cedu.

Sui discorsi di odio on-line, inoltre, è necessario richiamare il Protocollo addizionale[10] alla "Convenzione di Budapest sulla criminalità informatica", che impegna gli Stati a considerare reati, quando vengano realizzati attraverso mezzi informatici: la disseminazione di materiale razzista e xenofobo, almeno nei casi in cui il materiale promuova o inciti alla violenza (art. 3); minacce e insulti di matrice razzista e xenofoba (artt. 4 e 5); la negazione, grave minimizzazione, approvazione o giustificazione del genocidio o di crimini contro l'umanità (art. 6). L'Italia ha sottoscritto, nel 2011, ma non ancora ratificato il Protocollo. Infine, nel maggio 2016 è stato sottoscritto, da parte della Commissione europea e di Facebook, Microsoft, Twitter e You Tube, il "Codice di condotta per lottare contro le forme illegali di incitamento all'odio on-line", nel cui contesto viene riconosciuta la pericolosità virale di forme illegali di incitamento all'odio on-line.

1.4. Il contrasto all'*hate crime* nell'ordinamento italiano

Con riguardo alla normativa interna, un riferimento, seppur indiretto, alla non discriminazione si ritrova nella Costituzione Italiana all'art. 3, che postula il principio di eguaglianza in senso formale (comma 1) e sostanziale (comma 2).

Inoltre, la prima norma che, nel nostro ordinamento, ha stigmatizzato sotto il profilo penale la discriminazione razziale, sia pure incidentalmente, è stata la l. 645/1952 (cosiddetta "Legge Scelba"). Essa – in quanto attuazione della XII disposizione transitoria e finale, comma primo, della Costituzione – ha quale fine prioritario il divieto di riorganizzazione, sotto qualsiasi forma, del disciolto partito fascista; tuttavia, sin dalla originaria formulazione, contemplava la propaganda razzista tra le modalità di perseguimento delle finalità antidemocratiche proprie del partito fascista (art. 1)[11]. Inoltre, nella attuale versione dell'art. 4, co. 2 (modificato dalla

10) Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici.

11) Art. 1 l. 645/52: "... si ha riorganizzazione del disciolto partito fascista quando una associazione, un movimento o comunque un gruppo di persone non inferiore a cinque persegue finalità antidemocratiche proprie del partito fascista... svolgendo propaganda razzista...".

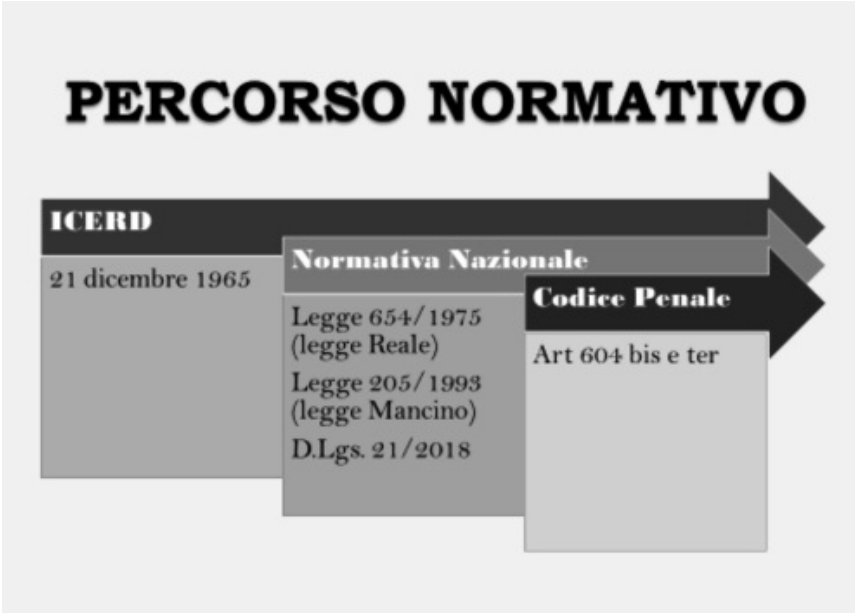
cosiddetta "Legge Mancino", di cui si dirà più avanti) è stata prevista una ipotesi aggravata di apologia del fascismo per chiunque ne esalti pubblicamente le idee o i metodi razzisti[12].

È utile fornire alcune precisazioni allo scopo di superare le difficoltà interpretative che possono porsi rispetto alla applicabilità di talune tra le fattispecie criminose disciplinate dalla l. 645/52 e l'impianto Reale-Mancino. La giurisprudenza di Cassazione (Cass. I 3791/93; Cass. I 7812/99) ha chiarito che la legge Scelba e l'impianto Reale-Mancino presentano una oggettività giuridica sostanzialmente coincidente (la lettera e la ratio delle due leggi si identificano) e che esse sono in rapporto di sussidiarietà. Nei casi di incertezza circa l'applicabilità delle norme in parola, laddove si riscontri la condizione costituita da un pericolo per le istituzioni democratiche – circostanza che si verifica allorquando la condotta ponga in pericolo la tenuta dell'ordine democratico e dei valori allo stesso sottesi (cfr. Cass. I 8108/2018) – si applicano le disposizioni della legge Scelba, in caso contrario quelle di cui al "Sistema Reale/Mancino" (Cass. III 37390/2007).

Successivamente la legge 654/1975 (c.d. Legge Reale), ha ratificato e dato esecuzione alla Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale, adottata dalle Nazioni Unite a New York nel 1966, dando inizio ad un percorso normativo che ha portato attraverso le modifiche successivamente introdotte dalla Legge Mancino (Legge 205/1993) e dal d.lgs. 21/2018 all'attuale disposto degli articoli 604-*bis* e 604-*ter* c.p.

---

12) Chiunque fa propaganda per la costituzione di una associazione, di un movimento o di un gruppo avente le caratteristiche e perseguente le finalità indicate nell'articolo 1 è punto con la reclusione da sei mesi a due anni e con la multa da lire 400.000 a lire 1.000.000 (1). Alla stessa pena di cui al primo comma soggiace chi pubblicamente esalta esponenti, princìpi, fatti o metodi del fascismo, oppure le sue finalità antidemocratiche**.** Se il fatto riguarda idee o metodi razzisti, la pena è della reclusione da uno a tre anni e della multa da uno a due milioni (4). La pena è della reclusione da due a cinque anni e della multa da 1.000.000 a 4.000.000 di lire se alcuno dei fatti previsti nei commi precedenti è commesso con il mezzo della stampa (1). La condanna comporta la privazione dei diritti previsti nell'articolo 28, comma secondo, numeri 1 e 2, del c.p., per un periodo di cinque anni (5). (1) La misura della multa è stata così elevata dall'art. 113, quarto comma, l. 24 novembre 1981, n. 689. La sanzione è esclusa dalla depenalizzazione in virtù dell'art. 32, secondo comma, della legge sopracitata. (4) Comma così sostituito dall'art. 4, d.l. 26 aprile 1993, n. 122. (5) Così sostituito dall'art. 10, l. 22 maggio 1975, n. 152.



Tale percorso normativo ha portato nel tempo a modificare tanto le tipologie di condotte discriminatorie, laddove inizialmente erano punite soltanto le discriminazioni per motivi razziali etnici e nazionali, a cui si è aggiunta con la Legge Mancino anche la discriminazione per motivi religiosi, tanto il quantum delle pene previste per le singole condotte.

L'attuale impianto normativo, basato sulle richiamate norme del Codice penale all'art. 604-*bis* c.p., punisce, salvo che il fatto costituisca più grave reato:

– chiunque propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi (comma 1, lett. a): reclusione fino ad un anno e 6 mesi o multa fino a 6.000 euro)[13];

13) La giurisprudenza ha chiarito che la fattispecie consistente nel propagandare idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero nell'istigare a commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi configura un *reato di pura condotta* e di *pericolo astratto* che si perfeziona indipendentemente dalla circostanza che la propaganda o l'istigazione siano raccolte dai destinatari; si tratta inoltre di ipotesi di reato a dolo generico (Cass., sez. I, sent. n. 724 del 21-01-1998; sez. III, sent. n. 37581 del 07-05-2008).

– chiunque, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi (comma 1, lett. b): reclusione da 6 mesi a 4 anni)[14];

– chiunque partecipa o presta assistenza ad organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi (comma 3: reclusione da 6 mesi a 4 anni);

– chiunque promuove o dirige organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi (comma 3: reclusione da 1 a 6 anni).

Tale norma[15] ("Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa"), criminalizza tutte le condotte previste all'art. 4 della Icerd:

– propaganda della superiorità o dell'odio razziale;

– istigazione o commissione di atti discriminazione o di violenza di natura razziale (primo comma);

– promozione/direzione/partecipazione/assistenza ad organizzazioni o gruppi razzisti (secondo comma).

Infine, al terzo comma, vengono stigmatizzate le condotte negazioniste[16] contemplate dalla decisione quadro 2008/913/GAI. L'aver introdotto il negazionismo e la minimizzazione nel nostro ordinamento rappresenta un ulteriore passo in avanti dal punto di vista culturale. La norma, inoltre, nel fare specifico riferimento alla Shoah e dunque allo sterminio degli ebrei vittime del genocidio nazista, ha voluto sottolineare l'autonoma rilevanza delle condotte antisemite rispetto al genus più ampio delle discriminazioni religiose.

---

14) La fattispecie che sanziona la violenza commessa per motivi razziali, etnici, nazionali o religiosi, configura invece un delitto a dolo specifico, ove l'agente operi con coscienza e volontà di offendere la dignità e l'incolumità della vittima in considerazione di fattori etnici, religiosi o razziali (Cass., sez. III, sent. n. 7421 del 26-02-2002).

15) Che, unitamente all'art. 604ter, costituisce il contenuto della sezione I-*bis* (Dei delitti contro l'eguaglianza) introdotta dal più volte citato d.lgs. 21/2018 nell'ambito del capo III - titolo XII - libro II del codice penale.

16) Negazione, minimizzazione in modo grave o apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra. La dottrina è discorde nel considerare tale norma, introdotta nell'ordinamento interno dalla l. 115/2016 e modificata dalla l. 167/2017, circostanza aggravante o fattispecie autonoma di reato e, manca, al momento, giurisprudenza chiarificatrice sul punto.

Inoltre, l'articolo 2 della Legge Mancino (Disposizioni di prevenzione) ha altresì previsto sanzioni penali per:

– chiunque, in pubbliche riunioni, compia manifestazioni esteriori od ostenti emblemi o simboli di tipo razzista, o basati sull'odio etnico, nazionale o religioso propri o usuali delle organizzazioni di cui all'art. 3 della legge n. 654/1975 (art. 2, comma 1: reclusione fino a 3 anni e multa da 103 a 258 euro);

– chiunque acceda ai luoghi ove si svolgono competizioni agonistiche con gli emblemi o i simboli sopra citati (art. 2, comma 2: arresto da 3 mesi ad un anno).

Infine, la Legge Mancino ha introdotto (articolo 3) la circostanza aggravante della finalità di discriminazione o di odio etnico, oggi recepita dall'art. 604-*ter* c.p., prevedendo per qualsiasi reato – ad eccezione di quelli per i quali è previsto l'ergastolo – commesso per le finalità di discriminazione di cui alla legge n. 654/75, che la pena venga aumentata fino alla metà[17]. In caso di concorso di circostanze, il comma 2 stabilisce che il giudice non possa ritenere le attenuanti equivalenti o prevalenti rispetto all'aggravante della finalità di discriminazione e che le eventuali diminuzioni di pena devono essere calcolate sulla pena risultante dall'aumento conseguente alla predetta aggravante. Tale principio non opera rispetto all'attenuante della minore età (di cui all'art. 98 del Codice penale)[18].

Le norme penali sinora menzionate sanzionano la commissione di reati

17) La giurisprudenza della Cassazione ha stabilito che al fine della configurazione dell'aggravante della finalità di discriminazione o di odio etnico, nazionale, razziale o religioso, non è necessario che la condotta incriminata sia destinata o, quanto meno, potenzialmente idonea a rendere percepibile all'esterno ed a suscitare il riprovevole sentimento o, comunque, il pericolo di comportamenti discriminatori o di atti emulatori, giacché ciò varrebbe ad escludere l'aggravante in questione in tutti i casi in cui l'azione lesiva si svolga in assenza di terze persone (Sez. V, sent. n. 37609 del 11-07-2006).

18) Dunque è con il d.l. 122/1993 (convertito con modificazioni dalla l. 205/ 1993, cosiddetta "Legge Mancino") che viene predisposto dal legislatore penale un compiuto sistema di contrasto del razzismo che, tra l'altro: criminalizza le manifestazioni esteriori[18] e l'esibizione di emblemi e simboli razzisti (art. 2); contempla una severa disciplina per perquisizioni e sequestri quando si proceda per reati di tale natura (art. 5); prevede la sospensione cautelativa e lo scioglimento di associazioni/gruppi razzisti (art. 7) nonché sanzioni accessorie per i soggetti condannati (art. 1); e, in particolare, una *circostanza aggravante ad effetto speciale (aumento della pena fino alla metà*) (art. 3) per tutti i reati[18] commessi con finalità razziste o per agevolare le attività di associazioni/gruppi razzisti. Tale aggravante si sottrae al cosiddetto "bilanciamento" con le circostanze attenuanti eventualmente concorrenti (salvo quella relativa alla minore età del reo) e, soprattutto, determina sempre la procedibilità d'ufficio (art. 6).

di matrice discriminatoria su base razziale, etnica, nazionale e religiosa, ma vi sono ulteriori "caratteristiche protette" della vittima che si ricollegano ad altrettanti ambiti discriminatori.

In merito alla "disabilità" – in aggiunta alle varie fattispecie criminose nelle quali la disabilità della vittima è prevista quale elemento costitutivo o circostanza aggravante speciale del reato – va menzionata la norma di cui all'art. 36 della l. 104/ 1992, in virtù della quale quando i reati di cui all'art. 527 del c.p. (atti osceni), i delitti non colposi di cui ai titoli XII (contro la persona) e XIII (contro il patrimonio) del libro II del Codice penale, nonché i reati di cui alla l. 75/1958 (cosiddetta "Legge Merlin": reclutamento, induzione, favoreggiamento, sfruttamento della prostituzione), sono commessi in danno di persona portatrice di minorazione fisica, psichica o sensoriale, la pena è aumentata da un terzo alla metà. In proposito, è necessario evidenziare che, per l'applicazione dell'aggravante in parola, non è richiesta la motivazione discriminatoria, ossia che l'autore provi odio o pregiudizio nei confronti della vittima, ma esclusivamente che la stessa sia portatrice di minorazione fisica, psichica o sensoriale, come definite dall'art. 3 della medesima legge.

Per quel che concerne i crimini basati sull'orientamento sessuale o l'identità di genere della vittima, l'attuale impianto normativo penale non prevede una specifica copertura. La matrice omotransfobica del reato è stata, talvolta, stigmatizzata attraverso l'applicazione dell'aggravante comune dei motivi abietti (art. 61, comma 1, n. 1)[19].

È opportuno, infine, evidenziare che il citato d.lgs. 212/2015, di attuazione della cosiddetta "Direttiva vittime" Ue, ha introdotto l'art. 90-*quater* c.p.p. codificando, in modo strutturale, la "condizione di particolare vulnerabilità" della persona offesa dal reato che, ai sensi della norma in esame, oltre a dover essere desunta, tra l'altro, dalla disabilità della vittima, può essere riconosciuta in caso di reati commessi con odio razziale o per finalità di discriminazione. È dunque importante evidenziare che siffatta formulazione consente di includere, tra le vittime in condizione di particolare vulnerabilità, in linea di principio, tutte le vittime di crimini d'odio, incluse quelle fatte oggetto di crimini di matrice omotransfobica.

19) Un interessante precedente in materia può essere rinvenuto nella sentenza del Tribunale di Napoli, VII sez. pen., n. 17573/2014 nella quale, appunto, la matrice omofobica di un'aggressione è stata stigmatizzata attraverso la condanna con applicazione dell'aggravante dei motivi abietti.

Dal riconoscimento di tale status derivano una serie di importanti diritti per la vittima del reato e specifiche incombenze in capo all'autorità giudiziaria e alla polizia giudiziaria. In proposito, per la polizia giudiziaria rivestono particolare importanza gli articoli 90-*bis* c.p.p.[20], 90-*ter* c.p.p.[21], 134, co. 4 c.p.p.[22] e 351 co. 1-*ter* c.p.p.[23], su cui ci si soffermerà più diffusamente in seguito.

1.5. Risoluzione del Parlamento europeo del 24 novembre 2020 sulla situazione dei diritti fondamentali nell'Unione europea - Relazione Annuale 2018-2019

La recente Risoluzione del Parlamento europeo del 24 novembre 2020 sulla situazione dei diritti fondamentali condanna i reati generati dall'odio e incitamento all'odio, nonché la discriminazione basata su qualsiasi motivazione, come la razza, il colore della pelle, l'origine etnica o sociale, la lingua, la religione o le convinzioni personali, le opinioni politiche, l'appartenenza a una minoranza, la disabilità, l'orientamento sessuale, l'identità di genere, l'espressione del genere o le caratteristiche sessuali.

Inoltre, viene ribadita la preoccupazione relativa al fatto che l'incitamento dell'odio on-line continui a rappresentare un problematica diffusa ed urgente.

---

20) Art. 90-*bis* c.p.p. ("Informazioni alla persona offesa"). *La vittima ha diritto ad ottenere, in una lingua a lei comprensibile, informazioni in merito a: modalità di presentazione della denuncia/querela; il suo ruolo nelle indagini e nel processo; stato del procedimento; possibilità di ottenere consulenza legale e patrocinio a spese dello Stato; diritto ad interpretazione/traduzione; eventuali misure di protezione; modalità per procedere alla contestazione di violazioni di propri diritti e per ottenere il rimborso delle spese*.

21) Art. 90-*ter* c.p.p. ("Comunicazioni dell'evasione e della scarcerazione"). *In caso di delitti commessi con violenza contro la persona, la vittima può far richiesta di ottenere informazioni in merito ai provvedimenti di scarcerazione e di cessazione della misura di sicurezza detentiva; le deve essere data tempestiva notizia dell'evasione dell'imputato o del condannato, nonché della volontaria sottrazione dell'internato all'esecuzione della misura di sicurezza detentiva*.

22) Art. 134 comma 4 c.p.p. ("Modalità di documentazione"). *Quando il verbale, in forma integrale o riassuntiva, è ritenuto insufficiente, è sempre consentita la riproduzione audiovisiva delle dichiarazioni della vittima particolarmente vulnerabile*.

23) Art. 351 co. 1-*ter* c.p.p. ("Altre sommarie informazioni"). *La polizia giudiziaria, quando deve verbalizzare una vittima particolarmente vulnerabile, si avvale dell'ausilio di un esperto in psicologia o in psichiatria, nominato dal pubblico ministero. In ogni caso, dovrà fare in modo che la vittima particolarmente vulnerabile, in occasione della verbalizzazione, non abbia contatti con l'indagato e che non sia verbalizzata più volte, salvo l'assoluta necessità per le indagini*.

La Risoluzione mette in guardia contro la crescente diffusione e normalizzazione dell'incitamento all'odio e delle diverse forme di razzismo come l'islamofobia, l'antiziganismo, l'antisemitismo e il razzismo contro le persone di colore. Tale fenomeno in numerosi Stati membri ha favorito l'ascesa di movimenti estremisti e politici o di Governo che ricorrono alla retorica dell'odio, diffondendo l'incitamento al razzismo e alla xenofobia.

Nel testo approvato viene inoltre sottolineata la necessità di superare la riluttanza delle vittime a denunciare reati generati dall'odio a causa delle garanzie insufficienti e dell'incapacità delle autorità di condurre indagini adeguate e ottenere condanne per reati generati dall'odio.

Di fondamentale importanza dunque la necessità di incoraggiare le vittime a denunciare i crimini generati dall'odio e le discriminazioni, nonché agevolare tale processo e fornire loro la protezione e sostegno adeguati.

Infine, la Commissione e l'Agenzia dell'Unione europea per i diritti fondamentali sono state sollecitate a proseguire l'attività di monitoraggio e la raccolta dei dati sulla specifica tematica.

2. Crimini e discorsi d'odio

2.1. Crimini d'odio. Definizione e caratteristiche

In Italia non esiste una definizione giuridica di crimine d'odio. La definizione che oggi trova maggiore consenso è quella fornita dall'Ufficio per le istituzioni democratiche e i diritti Umani (Odihr) dell'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), secondo la quale gli *hate crimes* costituiscono «*violente manifestazioni di intolleranza dotate di un profondo impatto non solo sulla vittima diretta bensì anche sul gruppo con cui la vittima si identifica. Essi colpiscono la coesione della comunità e la stabilità sociale. Pertanto, una risposta vigorosa è importante sia per la sicurezza individuale che per quella comune*»[24].

In altre parole, il crimine d'odio è un reato (contro la persona o contro

24) Osce, *Hate Crime Laws. A Practical Guide*, Odihr, Varsavia, 2009, 11: «*Hate crimes are violent manifestations of intolerance and have a deep impact on not only the immediate victim but the group with which that victim identifies him or herself. They affect community cohesion and social stability. A vigorous response is therefore, important both for individual and communal security*».

il patrimonio), commesso contro un individuo e/o beni ad esso associati, motivato da un pregiudizio che l'autore nutre nei confronti della vittima, in ragione di una "caratteristica protetta" di quest'ultima.

Il crimine d'odio, quindi, presenta due elementi caratterizzanti: un fatto previsto dalla legge penale come reato, la "*criminal offence*" (cosiddetto reato base) e la motivazione di pregiudizio, il c.d. "*bias motive*", cioè un motivo di pregiudizio in ragione del quale l'aggressore sceglie il proprio "bersaglio".

Da questa definizione possono tracciarsi alcune caratteristiche di questi reati. Innanzitutto, la bidirezionalità o plurioffensività del crimine: esso mira, cioè, a danneggiare non soltanto il singolo, ma anche il gruppo cui lo stesso appartiene. La vittima del crimine d'odio viene scelta non in base alle proprie caratteristiche personali quanto, piuttosto, in base a ciò che rappresenta ed alla sua appartenenza ad una certa categoria. Colpendo il singolo, l'autore della condotta intende mandare un messaggio discriminatorio all'intero gruppo di appartenenza[25]: la vittima prescelta costituisce mero veicolo di questo messaggio; non è un caso, infatti, che tali crimini siano stati altresì definiti, proprio dall'OSCE, come "simbolici".

Gli effetti di tale caratteristica si rinvengono nell'analisi delle conseguenze di tali crimini: il gruppo avverte la minaccia veicolata attraverso l'*hate crime* ed ogni appartenente ad esso patisce l'ansia di poter subire a sua volta crimini discriminatori, in ragione di una propria caratteristica personale, spesso immutabile e palese (come, ad esempio, il colore della pelle). Le conseguenze, dirette e indirette, di tale genere di crimini li rendono differenti da qualsiasi altro genere di illecito. L'*hate crime* è capace di innescare un processo di vittimizzazione delle minoranze, tale per cui la vittima e il gruppo di appartenenza patiscono effetti pregiudizievoli sia a livello psicologico che sociale.

La definizione fornita dall'OSCE evidenzia, infatti, anche l'impatto che tali crimini possono avere sulla coesione e sulla stabilità di una società. Non è un caso, infatti, che i primi studi concernenti l'individuazione del bene giuridico protetto da siffatto genere di norme collocassero i delitti d'odio nell'ambito della tutela dell'ordine pubblico[26]. La Cassazione ha successivamente

25) Per tale ragione i crimini d'odio vengono anche definiti *target crimes* o *message crimes* per evidenziare che si tratta di reati con uno specifico bersaglio, attraverso i quali l'autore intende lanciare un messaggio di non accettazione di quella persona e della relativa comunità di appartenenza.

26) Per una puntuale ricostruzione dell'evoluzione del bene giuridico oggetto di tutela delle norme antidiscriminatorie, cfr. G. Puglisi, *La parola acuminata. Contributo allo studio dei delitti contro l'eguaglianza, tra aporie strutturali ed alternative alla pena detentiva*, in *RIDPP*, 2018.

individuato nella dignità umana il bene giuridico tutelato da questi reati. Tali crimini posseggono la capacità di minare alcuni dei valori fondamentali su cui si basano le moderne società democratiche, tra cui la sicurezza dei membri che ivi convivono e la loro uguaglianza e pari dignità, ingenerando comuni sentimenti di ansia e paura.

Rispetto ai crimini d'odio quando si parla di caratteristiche protette si fa riferimento ai tratti distintivi fondamentali, condivisi da un gruppo di persone, che riflettono un aspetto profondo dell'identità di un individuo e creano un'identità tipica del gruppo, la cd. "dimensione identitaria". Non appare possibile fornire una elencazione definitiva delle categorie meritevoli di protezione proprio in ragione della costante evoluzione cui tale materia è esposta. In dottrina si rifiuta l'idea del "*numerus clausus*" delle categorie bisognose di protezione[27]. Nel tentativo di delineare quali caratteristiche personali meritino di essere oggetto di tutela da parte dell'ordinamento, l'OSCE evidenzia come i tratti esistenziali fatti oggetto di discriminazione debbano connotarsi per la loro immutabilità e per l'irrinunciabilità rispetto alla persona offesa. Dovrebbe trattarsi di note comuni (possibilmente subito percepibili) che costituiscano il c.d. «*marker of group identity*»: non basta che i membri del gruppo abbiano un certo elemento in comune, ma è, inoltre, fondamentale che questo dato connoti la categoria e consenta a tutti coloro che risultano accomunati da quella caratteristica di considerarsi come parte del "gruppo".

Comunque tra le caratteristiche più diffusamente protette dagli ordinamenti giuridici democratici vi sono: la "razza" (o, più correttamente, l'origine etnica), il credo religioso, la nazionalità, l'orientamento sessuale, l'identità di genere, la disabilità. Queste caratteristiche possono essere reali, quando la vittima (o un bene, come ad esempio un luogo di culto, in qualche modo collegato al gruppo) possiede, appunto, la caratteristica che la identifica come appartenente ad una determinata minoranza o presunte, quando l'autore del reato sceglie la vittima ritenendo erroneamente che sia legata al gruppo di minoranza. Si parla di "discriminazione per associazione" quando la vittima, sebbene non appartenente a una specifica "comunità di minoranza" viene colpita, perché in qualche modo ad essa legata (ad esempio un individuo può essere aggredito in quanto coniugato con una persona di colore). Nel caso in cui la vittima venga colpita perché espressione di più caratteri-

27) L. Goisis, *Crimini d'odio. Discriminazioni e giustizia penale*, Napoli, 2019.

stiche protette (ad esempio in quanto persona di colore e musulmana oppure omosessuale e disabile), si parla di "discriminazione multipla".

I crimini d'odio si caratterizzano, inoltre, anche per l'*under-reporting*, l'*under-recording* e il rischio di *escalation*.

L'under-reporting è il fenomeno per il quale le vittime e i testimoni di crimini d'odio tendono, per varie e complesse motivazioni (soprattutto di carattere psicologico), a non denunciarli. Tra le principali ragioni per le quali vittime e testimoni hanno difficoltà a denunciare vi sono:

– non aver cognizione o rifiutare il fatto che l'aggressione sia motivata dal pregiudizio nei confronti di quella caratteristica protetta;

– mancanza di fiducia nelle forze di polizia in quanto si teme che non vengano attivate indagini accurate;

– paura di compromettere la propria privacy (è il caso di molti reati commessi contro appartenenti alla comunità LGBTIQ+);

– timore di ritorsioni;

– non conoscenza della lingua e del sistema giuridico nazionale.

L'under-recording è, invece, il fenomeno per il quale sono proprio le forze di polizia a non riconoscere la matrice discriminatoria del reato denunciato e, conseguentemente, non lo registrano né lo investigano come tale. Questo può accadere per diverse motivazioni:

– mancato riconoscimento dei cosiddetti indicatori di pregiudizio (o "*bias indicators*") ossia degli elementi indiziari che consentono di rilevare la motivazione discriminatoria del reato (dei quali si dirà diffusamente più avanti);

– scarsa sensibilità/mancanza di formazione adeguata sul fenomeno;

– carenza di risorse.

Infine, il rischio di escalation deriva dall'accettazione sociale della discriminazione contro taluni gruppi di minoranza (fenomeno della cosiddetta normalizzazione dell'odio) che favorisce l'aumento dei crimini d'odio. Infatti, laddove comportamenti discriminatori a bassa intensità vengano accettati dalla società perché non percepiti come offensivi – ma, magari, interpretati, come battute o episodi di goliardia – e quindi non adeguatamente contrastati, vi è un forte rischio di escalation. Da atteggiamenti o comportamenti basati sul pregiudizio si può passare ad atti di discriminazione (nell'accesso a pubblici servizi, al lavoro, ecc.), fino a giungere a veri e propri reati: vandalismi, profanazioni di luoghi sacri, minacce, aggressioni. Tale concetto è rappresentato dalla cosiddetta Piramide dell'odio *dell'Anti Defamation League* (Adl).

"Piramide dell'odio" elaborata dall'AntiDefamation League (https://www.adl.org/sites/default/files/documents/pyramid-of-hate.pdf)

2.2. Contrasto ai discorsi d'odio e sua evoluzione

Hate speech – l'espressione tradotta normalmente in italiano come "discorsi d'odio" o "espressioni d'odio" o "linguaggio d'odio" – consiste in una specifica forma di discriminazione che si estrinseca non attraverso azioni o omissioni, ma mediante modalità di manifestazione del pensiero. Queste forme espressive, assai diffuse e reiterate anche attraverso Internet, hanno l'effetto di alimentare i pregiudizi, consolidare gli stereotipi e rafforzare l'ostilità di taluni gruppi di persone**,** solitamente in maggioranza o in posizione di dominanza in un determinato contesto sociale, nei confronti di altri gruppi, in genere minoritari, che presentano diverse caratteristiche[28].

Gli "*hate speeches*" costituiscono una *species* del *genus* "*hate crimes*", ma non esiste una norma giuridica che definisca con precisione e completezza in cosa consista l'*hate speech*.

Nel contesto europeo l'*hate speech* può essere ricondotto a una di quelle forme di discriminazione vietate dall'art. 14 della *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* (Cedu), in quanto consistente proprio in una violenza, realizzata attraverso modalità espressive verbali o audiovisive, atta a discriminare particolare categorie di individui. L'art. 14 della Cedu vieta, infatti, le discriminazioni «fondate sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o quelle

28) M. Mensi - P. Falletta, *Il diritto del web. Casi e materiali*, Padova, 2015.

di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione».

Per quanto in Italia non esista ancora una puntuale definizione di tali condotte, in base alla Raccomandazione n. 20 del 1997 del Comitato dei Ministri del Consiglio d'Europa con tale espressione ci si riferisce a «discorsi suscettibili di produrre l'effetto di legittimare, diffondere o promuovere l'odio razziale, la xenofobia, l'antisemitismo o altre forme di discriminazione o odio basate sull'intolleranza incluse l'intolleranza espressa attraverso il nazionalismo aggressivo e l'etnocentrismo, la discriminazione e l'ostilità contro le minoranze, i migranti e le persone di origine migrante».

Sul punto nell'ambito del Consiglio d'Europa, il protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica firmato a Strasburgo il 28 gennaio 2003, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici, obbliga gli Stati aderenti ad adottare sanzioni penali per punire la diffusione, attraverso i sistemi informatici, di materiale razzista e xenofobo, le minacce e gli insulti razzisti e xenofobi, la negazione, la minimizzazione, l'approvazione o la giustificazione di crimini di genocidio o contro l'umanità.

Una più recente definizione di *hate speech* si rinviene nella decisione-quadro 2008/913/GAI del Consiglio del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale. Tale decisione impegna gli Stati membri dell'Unione europea a rendere punibili i comportamenti di stampo razzista e xenofobo, in particolare «l'istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica», nonché «l'apologia, la negazione o la minimizzazione grossolana dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra». Anche in questo caso, soltanto alcune fra le possibili categorie potenzialmente vulnerabili vengono indicate nella definizione, tralasciandone altre altrettanto rilevanti.

Per tale motivo il Parlamento europeo, con una Risoluzione approvata il 14 marzo 2013, ha evidenziato l'esigenza di una revisione della decisione-quadro 2008/913/GAI, in modo da includervi anche le manifestazioni di antisemitismo, intolleranza religiosa, antiziganismo, omofobia e transfobia.

Per quel che concerne gli elementi costitutivi, gli *hate speeches* difettano del primo degli elementi che compongono in genere i crimini d'odio, ossia la commissione di un reato: ove il discorso incriminato venisse depauperato del motivo di pregiudizio e dell'odio che muove le dichiarazioni esternate si tratterebbe di una condotta assolutamente lecita. Di fondamentale importanza è

comprendere il confine tra critica e odio. Uno dei principali rischi connaturati nell'incriminazione dei c.d. discorsi d'odio si individua, infatti, nella possibile creazione di nuovi reati di opinione. In materia di "discorso d'odio", dunque, assume fondamentale rilievo l'esigenza di bilanciare i principi che, nel sistema giuridico nazionale, sono statuiti agli articoli 2 (riconoscimento dei diritti inviolabili) e 3 (pari dignità ed uguaglianza davanti alla legge) della Costituzione con il principio di libera manifestazione del pensiero ex art. 21 della stessa Carta. Al riguardo, va considerato il principio stabilito dalla Corte di Cassazione, in armonia con le indicazioni della Corte europea dei diritti umani, secondo il quale: "nel possibile contrasto fra la libertà di manifestazione del pensiero e la pari dignità dei cittadini, va data preminenza a quest'ultima solo in presenza di condotte che disvelino una concreta pericolosità per il bene giuridico tutelato" (Cass. pen. 36906/2015).

In ogni caso, lo strumento normativo utilizzato per contrastare penalmente il discorso d'odio è l'art. 604-*bis* c.p. (ex art. 3 l. 654/75) "Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa".

Nonostante le molte sfaccettature di interpretazione che riguardano l'*hate speech* possiamo giungere alla conclusione che siano necessari almeno tre requisiti affinchè un'espressione possa considerarsi *hate speech*: la volontà e l'intenzione di incitare l'odio con ogni mezzo di comunicazione; l'esortazione vera e propria idonea a causare atti di odio e violenza sui soggetti presi di mira; la concretezza del rischio che gli atti di violenza o di discriminazione si verifichino.

2.2.1. Il ruolo di web e social nella diffusione dell'*hate speech*

Le espressioni di odio si sono sempre realizzate anche in passato, verbalmente o attraverso l'uso dei *media* tradizionali. Oggi però, tramite Internet e in particolare i *social network*, tali espressioni possono circolare con estrema rapidità, diffondersi su larghissima scala e raggiungere una enorme *audience*, con l'effetto di stimolare la proliferazione di ulteriori espressioni di tipo analogo. L'ambiente digitale – e in particolare quello dei *social network* – ha un potere di diffusione e di pubblicità dell'odio ben maggiore rispetto ai media tradizionali, inoltre, l'odio, una volta immesso in rete, ha una notevole capacità di persistenza e di resistenza ai tentativi di occultamento dei messaggi offensivi[29]. Internet rappresenta uno strumento facilitatore della diffusione e della potenzialità dell'odio, anche per il senso di impunità che deriva, per molti

29) G. Ziccardi, *L'odio on-line. Violenza verbale e ossessione in rete*, Milano, 2016.

utenti di Internet, dalla falsa percezione di essere protetti dall'anonimato. Ciò impone un nuovo approccio multidisciplinare che obblighi tutti gli attori coinvolti – le istituzioni pubbliche, tra le quali le forze di polizia, le organizzazioni della società civile ed i singoli utenti – a confrontarsi con nuove sfide, per contrastare l'odio *on-line*.

Secondo un documento pubblicato dall'Unesco nel 2015, intitolato *Countering on-line hate speech*, i caratteri distintivi dell'odio espresso attraverso Internet rispetto a quello *offline* sono i seguenti:

– la permanenza nel tempo della manifestazione di odio: il discorso d'odio tende a restare on-line per molto tempo; più a lungo rimane accessibile, più elevato è il rischio che produca effetti dannosi;

– il suo "ritorno imprevedibile", per via dello sfruttamento del medesimo contenuto da parte di utenti di varie piattaforme in tempi diversi. La dinamica della diffusione del contenuto d'odio può essere itinerante e ricorrente in quanto un contenuto rimosso, infatti, può apparire sotto un altro nome e/o titolo sulla stessa piattaforma o altrove (non a caso si dice che il Web non dimentica);

– la percezione che sovente hanno gli autori dell'*hate speech* di essere protetti dall'anonimato;

– la diffusione transnazionale dei contenuti e, conseguentemente, il loro maggiore impatto sociale rispetto ai contenuti *offline*.

Gli autori di *hate speech* spesso non riflettono sulle possibili conseguenze dei propri atti e non percepiscono il potenziale impatto dei loro messaggi d'odio sulla vita reale delle persone. Diversi studi hanno dimostrato che i cosiddetti "leoni da tastiera" non manifestano in quei termini il loro odio quando sono *offline*. Infatti un'ulteriore ragione della facilità di diffusione dell'odio *on-line* riguarda gli effetti provocati dalle interazioni fra persone attraverso Internet in termini di estremizzazione e quindi maggiore offensività delle opinioni espresse. È stato, infatti, evidenziato che i gruppi di persone che partecipano a dibattiti via Internet hanno la tendenza ad orientarsi ideologicamente verso posizioni più estreme, tale tendenza di "polarizzazione di gruppo", comporta che al termine di un dibattito le persone tenderanno a mantenere ferme le proprie iniziali convinzioni, ma in forma più estremistica[30]. Da questo punto di vista, i *social network*, favorendo l'interazione e lo scambio di opinioni fra persone, non avrebbero un ruolo neutrale, ma agevolerebbero e am-

30) C. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni?*, Il Mulino, Bologna, 2003.

plificherebbero la diffusione di questo tipo di espressioni e la loro gravità.

Dunque la natura stessa del Web rende evidente il fatto che il contrasto *all'hate speech on-line* non possa essere affrontato dai Paesi singolarmente, ma necessiti, come detto, invece, di un approccio su base internazionale.

Sul punto, va menzionato l'approccio nordamericano, fondato sul primo emendamento della Costituzione, che non tollera alcuna interferenza dei poteri pubblici nell'esercizio della "*freedom of speech*" e non prevede limitazioni con riguardo ai contenuti espressi o alle modalità con cui l'espressione avviene. Anche i messaggi più discutibili, impopolari e scabrosi, dunque, possono essere diffusi liberamente nel *free marketplace of ideas*, nel quale si presuppone che la corretta informazione emerga attraverso il libero confronto fra idee contrastanti. Per queste ragioni negli Stati Uniti ogni forma di responsabilizzazione degli intermediari digitali, soprattutto nel caso in cui preveda il ricorso a tecniche di filtraggio preventivo dei contenuti, è guardata con sospetto, perché potrebbe dare luogo a forme di *collateral censorship*[31].

A livello UE sono stati recentemente compiuti importanti passi in avanti, a partire dalla sottoscrizione, nel maggio 2016, del "Codice di condotta per lottare contro le forme illegali di incitamento all'odio on-line" da parte della Commissione europea e di *Facebook*, *Microsoft*, *Twitter e You Tube*. La sottoscrizione impegna le "aziende informatiche" a reagire con maggiore prontezza per contrastare i contenuti di incitamento all'odio razziale e xenofobo che vengono loro segnalati. L'obiettivo è quello di dare una risposta più adeguata agli utenti che segnalano tali contenuti e garantire maggior trasparenza sulle notifiche e sulle cancellazioni effettuate, grazie anche alla creazione di una rete di "relatori di fiducia" (*trusted flaggers*) che trasmettano segnalazioni di qualità.

Come anticipato, il Codice definisce il discorso d'odio ("*Illegal hate speech*"), richiamando la decisione quadro 2008/913/GAI. A giugno 2016, la Commissione europea ha, poi, istituito il "Gruppo di alto livello sulla lotta contro il razzismo, la xenofobia e altre forme di intolleranza", nel cui contesto è stato, tra l'altro, attivato un tavolo di lavoro in materia di *hate speech on-line* che prevede un meccanismo di monitoraggio dell'applicazione del Codice di condotta, con particolare riferimento alle percentuali e alle tempistiche di rimozione dei contenuti illeciti segnalati, che in tre anni, dal 2016 al 2019, ha fatto registrare un costante miglioramento dei dati. A livello nazionale, esistono notevoli difficoltà nel perseguire quei contenuti che, ai sensi della normativa citata

31) J.M. Balkin, *Old School/New School Speech Regulation*, 2014.

(art. 604-*bis* c.p.), configurano una condotta penalmente illecita. In molti casi, infatti, i server dei social network o dei siti sui quali sono presenti contenuti illegali sono allocati in Paesi, come gli Stati Uniti d'America, che non criminalizzano i cosiddetti "reati d'opinione", tra i quali vengono annoverati i discorsi d'odio. Ciò scoraggia l'attivazione delle lunghe e costose procedure di "rogatoria internazionale" finalizzate all'acquisizione all'estero dei necessari elementi di prova, atteso che l'esperienza operativa ha fatto ripetutamente riscontrare il rigetto della richiesta, da parte delle autorità giudiziarie di quei Paesi.

2.2.2. Progetto CO.N.T.R.O (*COunter Narratives againsT Racism Online*)

Il progetto CO.N.T.R.O., promosso e finanziato dalla Commissione europea, è ideato e coordinato dall'UNAR (Ufficio Nazionale Antidiscriminazioni Razziali), in partenariato con IRS (Istituto per la Ricerca Sociale).

Il Ministero dell'Interno partecipa attivamente a tale progetto attraverso l'Osservatorio per la sicurezza contro gli atti discriminatori, partner stabile dell'UNAR anche in virtù del protocollo di intesa siglato nel 2011 ed attualmente in fase di revisione allo scopo di ottimizzare il meccanismo di collaborazione tra i due organismi.

Nell'iniziativa sono, altresì, coinvolti: Ministero della Giustizia; MIUR; AGCOM; Amnesty International - Italia; Arcigay; ARCI; COSPE; Lunaria.

Il progetto CO.N.T.R.O. ha avuto una durata di due anni (2018-2020) ed è stato finalizzato ad arginare i discorsi di odio on-line, attraverso la diffusione di un'intensa e mirata campagna di sensibilizzazione e comunicazione sul fenomeno.

L'hate speech on-line è un fenomeno in forte crescita che sfrutta la rete per diffondere i propri messaggi in maniera veloce e pervasiva. Nel tentativo di fornire risposte sempre più adeguate ed efficaci, alle varie forme di discriminazione presenti in rete, sono nate molte iniziative di contrasto, prevenzione ed informazione sui discorsi di odio. CO.N.T.R.O. si inserisce proprio in questo contesto, ponendosi come obiettivo generale quello di contribuire al contrasto del razzismo, della xenofobia e di altre forme di intolleranza diffuse attraverso discorsi di incitamento all'odio on-line. Attraverso una prima fase di studio e ricerca sui discorsi di odio on-line e sulle migliori strategie in uso per contrastarli (mappatura delle maggiori esperienze di individuazione e analisi dei discorsi di odio on-line e delle pratiche più efficaci di contro-narrativa), seguita da una mirata campagna di comunicazione e sensibilizzazione sul fenomeno, il progetto ha avuto, altresì, l'obiettivo di raggiungere una metodologia comune ed efficace contro i discorsi di odio on-line.

2.3. L'accoglienza alle vittime di crimini d'odio alla luce della più recente normativa europea

Se l'era della investigazione digitale vuol dire un nuovo approccio ai reati, nuove tecniche investigative, tecnologie sofisticate, anche il nostro modo di interagire con la vittima deve cambiare.

In passato l'attenzione nella consumazione del reato è stata tutta focalizzata sulla figura del reo di cui sono state analizzate caratteristiche, personalità, background ambientale. La vittima è stata per anni marginalizzata. Un protagonista dimenticato, di cui nello stesso c.p.p. non si parla che in una sola occasione, rivestendo il ruolo di mera circostanza dell'azione delittuosa e processualmente quello di persona offesa dal reato.

In quell'offesa non c'è traccia però del vissuto di sofferenza, del dolore, dei bisogni della sua condizione e della sua vulnerabilità.

Se l'obiettivo dello Stato è la tutela dei diritti dei cittadini allora è proprio in quest'offesa che si può ricucire lo strappo con la società, è qui che si può e si deve riparare il torto, nel riconsegnare alla vittima quell'indennità morale di cui ha diritto.

Ma il pieno riconoscimento dello status giuridico della vittima è stato un percorso lento. Il salto culturale si è avuto con la direttiva europea 29/2012 che conferisce al termine vittima un significato più profondo.

È necessario offrire assistenza, tutela, protezione, informazione, assicurare la possibilità di esercitare un'attiva partecipazione al procedimento penale.

Tutto ciò porta ad una nuova concezione di reato i cui contorni sono tratteggiati, non soltanto come violazione dei diritti individuali, ma come torto subito dall'intera società. Vittime non sono più considerati solo i minori, le donne sottoposte a violenza di genere, ma anche le vittime di crimini d'odio e tutte le persone in condizione di particolare vulnerabilità.

L'art. 90-*quater* c.p.p. sancisce, infatti, che la particolare vulnerabilità si desume oltre che dall'età e dal sesso, dallo stato di infermità, anche dalla disabilità, dalle modalità e circostanze del fatto, dalla violenza subita, dall'odio razziale, dalla discriminazione, dall'essere vittima di terrorismo, di criminalità organizzata, di tratta di esseri umani.

Ed è in questa concezione olistica che dà spazio a tante voci per troppo tempo inascoltate, nella loro particolare fragilità che trovano accoglienza e sostegno le vittime di discriminazione e di crimini d'odio e cioè le persone disabili, le vittime di crimini di matrice etnico/razziale e, più in generale, tutte le vittime di reati di natura discriminatoria, che non trovano altra copertura o

un specifico *ius puniendi* nel nostro ordinamento, come per le vittime ad esempio di omotransfobia.

A tutte queste vittime viene oggi riconosciuta una tutela rafforzata; ad esse infatti sono riconosciuti precisi diritti, ai quali corrispondono altrettanti obblighi che danno voce ai loro bisogni: di essere informate, di avere un ruolo attivo, di veder riconosciuto rispetto, protezione, ascolto, aiuto nell'accesso alla giustizia, rimborsi economici e supporto psicologico. In particolare, per gli aspetti d'interesse della polizia giudiziaria, la vittima ha diritto ad ottenere, in una lingua a lei comprensibile, informazioni in merito alle modalità di presentazione della denuncia/querela, al suo ruolo nelle indagini e nel processo, allo stato del procedimento, alla possibilità di ottenere consulenza legale e patrocinio a spese dello Stato, al diritto ad un'interpretazione/traduzione nella sua lingua, ad eventuali misure di protezione, alle modalità di contestazione di eventuali violazioni di propri diritti e alle procedure per ottenere il rimborso delle spese (art. 90-*bis* c.p.p.). In caso di delitti commessi con violenza contro la persona, la vittima può far richiesta di ottenere informazioni in merito ai provvedimenti di scarcerazione e di cessazione della misura di sicurezza detentiva, le deve essere data tempestiva notizia dell'evasione dell'imputato o del condannato, nonché della volontaria sottrazione dell'internato all'esecuzione della misura di sicurezza detentiva (art. 90-*ter* c.p.p.). Nell'audizione nel corso dell'incidente probatorio, in dibattimento ma anche prima, nella fase delle indagini preliminari, è sempre consentita la riproduzione audiovisiva delle dichiarazioni della vittima particolarmente vulnerabile (art. 134 c.p.p.) e la polizia giudiziaria può avvalersi dell'ausilio dello psicologo indipendentemente dall'età della vittima, che non deve essere chiamata più volte a deporre, salva l'assoluta necessità, e non deve aver contatti con l'indagato mentre viene sentita (art. 351 comma 1-*ter* c.p.p.).

Prendere coscienza della sofferenza che c'è dietro e proteggere significa allora assicurare loro:

– informazione completa ed analitica;
– garantire priorità nella trattazione dei casi;
– rimanere in contatto con i bisogni e le necessità anche successivamente;
– ma soprattutto ascoltare e proteggere.

Come Polizia di Stato realizzare un adeguato approccio vittimologico vuol dire dare una risposta al senso di profonda insicurezza che i crimini, soprattutto quelli violenti, determinano non soltanto su chi li subisce ma sulla società che assiste da spettatore inerme.

Il dolore dei singoli e la paura della gente chiedono attenzione ed un se-

rio riconoscimento da parte delle istituzioni per il superamento del trauma individuale e collettivo generato dal crimine, restituendo fiducia alle vittime e migliorando il livello e la percezione di sicurezza.

L'accoglienza e attenzione alla vittima diventano, dunque, strumento per misurare il livello di democrazia, di rispetto dei diritti umani, di crescita culturale di una società.

Come istituzione pubblica realizzare questi obiettivi è passaggio obbligato ed imprescindibile per guadagnarsi quella rispettabilità sociale ponendosi agli occhi dei cittadini come polizia civile e moderna improntata a valori etici in grado di entrare in sintonia e fornire una risposta adeguata ai singoli bisogni ed alle sofferenze degli individui.

2.4. Gli indicatori di pregiudizio nei crimini d'odio

Gli indicatori o *markers* del pregiudizio (conosciuti a livello internazionale con il termine "*Bias indicators*") sono fatti e circostanze che consentono di supporre di essere in presenza di un crimine d'odio, ossia di un reato commesso in ragione del pregiudizio che l'autore nutre nei confronti della vittima, a causa di una o più caratteristiche protette (reali o solo presunte dall'autore) che la contraddistinguono.

L'ODIHR, l'Ufficio per le istituzioni democratiche ed i diritti umani dell'OSCE, li definisce come: "*fatti obiettivi, circostanze, modalità relative ad un reato che, da soli o in connessione con altri fatti o circostanze, suggeriscono che le azioni dell'autore sono motivate, in tutto o in parte, da una qualche forma di pregiudizio*". Questi elementi sono assai rilevanti ai fini investigativi in quanto consentono all'investigatore di far emergere le motivazioni di natura discriminatoria che hanno spinto l'autore a commettere il reato scegliendo proprio quella vittima. La trascrizione degli stessi nella redazione degli atti destinati all'autorità giudiziaria consentirà alla stessa di disporre di tutti gli elementi informativi necessari per trattare il reato come crimine d'odio (ad esempio, contestando – e applicando – l'aggravante di cui all'art. 604-*ter* c.p.).

La Corte di Cassazione (Cass. 434/99 e Cass. 16328/12) in alcune pronunce ha sottolineato l'importanza degli indicatori di pregiudizio e la necessità di una lettura coordinata del contesto in cui si inquadra il fatto reato, di conseguenza la presenza o l'assenza di un singolo indicatore non è di per sé decisiva per stabilire la motivazione discriminatoria di un reato. I principali indicatori di pregiudizio sono i seguenti:

– percezione della vittima/del testimone: la percezione della vittima (o

degli eventuali testimoni) rispetto a quanto accaduto è un importante indicatore che dovrebbe dare, all'operatore di polizia, un ulteriore impulso nella ricerca di elementi oggettivi per determinare la possibile motivazione discriminatoria del reato;

– commenti denigratori, gesti, dichiarazioni scritte, disegni, simboli e graffiti: spesso l'autore di un crimine d'odio intende evidenziare la motivazione di pregiudizio, non accettazione o, addirittura, di vero e proprio odio alla base del reato (non a caso gli *hate crimes* vengono anche definiti *message crimes*, ossia reati che inviano un messaggio);

– differenze tra autore e vittima per motivi etnici, religiosi o di altro tipo (ad esempio per orientamento sessuale): sono un indicatore significativo, soprattutto – ma non necessariamente – se la vittima appartiene (o è percepita come appartenente) a un cosiddetto gruppo di minoranza;

– coinvolgimento di cosiddetti gruppi organizzati dell'odio (ossia, dediti a crimini d'odio o all'incitamento all'odio) o dei loro componenti: l'autore può anche non essere strutturalmente organico ad alcun gruppo del genere, ma condividerne l'ideologia ed i metodi violenti;

– luogo: il reato è stato commesso nei pressi di un luogo di culto (sinagoga, moschea, chiesa cristiana) o di un locale prevalentemente frequentato da persone a rischio di discriminazione (persone LGBTIQ+, migranti);

– data, timing; il reato ha avuto luogo in occasione di una particolare ricorrenza, festa religiosa o altro evento di particolare significato per una comunità;

– modelli/frequenza di crimini o incidenti avvenuti precedentemente: l'episodio è simile ad altri di analoga natura che si sono verificati in un dato periodo; ricorre un certo schema delittuoso, una serialità;

– natura della violenza: nei crimini d'odio il livello di violenza può essere particolarmente elevato ed è spesso accompagnato da gravi offese fisiche o umiliazioni non di rado rese pubbliche, dallo stesso autore, attraverso il web;

– mancanza di altre motivazioni: alcune volte non vi sono motivi evidenti che possano giustificare la commissione del reato: la vittima e il sospettato non si conoscono, un eventuale litigio che possa aver innescato l'aggressione appare chiaramente pretestuoso, non vi è un movente economico, in tali casi quella discriminatoria potrebbe essere l'unica motivazione plausibile.

3. *Hate Crime* e *hate speech* strategia di prevenzione e contrasto del Dipartimento della Pubblica Sicurezza

3.1. L'Osservatorio per la Sicurezza contro gli Atti Discriminatori (OSCAD)

L'Osservatorio per la Sicurezza Contro gli Atti Discriminatori (OSCAD) è un organismo interforze istituito, con decreto del Capo della Polizia, nel settembre del 2010, per rispondere operativamente alla domanda di sicurezza delle persone appartenenti a "categorie vulnerabili", mettendo a sistema e dando ulteriore impulso alle attività svolte dalla Polizia di Stato e dall'Arma dei Carabinieri in materia di prevenzione e contrasto dei crimini d'odio.

L'OSCAD, incardinato nell'ambito del Dipartimento della P.S. - Direzione Centrale della Polizia Criminale, è presieduto dal Vice Direttore Generale della P.S. - Direttore Centrale della Polizia Criminale ed è composto da rappresentanti della Polizia di Stato, dell'Arma dei Carabinieri e delle articolazioni dipartimentali competenti per materia.

Alla luce della *mission* istitutiva dell'Osservatorio e tenuto conto delle caratteristiche peculiari dei crimini d'odio, gli obiettivi prioritari dell'OSCAD sono: agevolare le denunce dei crimini d'odio (in modo da contrastare il fenomeno dell'*under-reporting*); migliorare costantemente il monitoraggio del fenomeno (per misurarne con sempre maggiore precisione la portata e l'impatto); sensibilizzare/formare/aggiornare costantemente gli operatori delle forze di polizia (per combattere il fenomeno dell'*under-recording*).

Nello specifico, sono componenti dell'OSCAD: il direttore dell'Ufficio affari generali; il direttore dell'Ufficio tecnico-giuridico e contenzioso; il direttore del Servizio analisi criminale; il direttore dell'Ufficio di staff del Vice Direttore Generale della P.S. (Direzione Centrale dellaPolizia Criminale); il direttore del Servizio per il contrasto dell'estremismo e del terrorismo interno (Direzione Centrale della Polizia di Prevenzione); il direttore del Servizio immigrazione (Direzione centrale dell'immigrazione e della polizia delle frontiere); il direttore del Servizio polizia postale e delle comunicazioni (Direzione centrale per la polizia stradale, ferroviaria, delle comunicazioni e per i reparti speciali della Polizia di Stato); il direttore del Servizio centrale anticrimine (Direzione centrale anticrimine della Polizia di Stato); il capo del II Reparto (Comando generale dell'Arma dei Carabinieri).

Allo scopo di contrastare il fenomeno dell'*under-reporting*, è stato attivato un indirizzo di posta elettronica (oscad@dcpc.interno.it) destinato alla ricezione di segnalazioni da parte di istituzioni, associazioni o privati cittadini

(anche in forma anonima) e sono state realizzate una serie di iniziative volte alla diffusione della conoscenza dell'OSCAD, a partire dalla realizzazione di pagine dedicate sui siti internet della Polizia di Stato[32] e dell'Arma dei Carabinieri[33], nonché sul sito del Ministero dell'Interno[34], dove, oltre ad informazioni su organizzazione ed attività dell'OSCAD, sono stati resi disponibili i dati relativi alle segnalazioni gestite dall'Osservatorio, annualmente comunicati all'OSCE (attraverso il link *http://hatecrime.osce.org/italy*), che provvede alla più completa raccolta di dati sugli *hate crimes* a livello internazionale.

Le segnalazioni ricevute, nonché quelle ricavate dall'analisi delle fonti aperte, vengono inoltrate ai competenti uffici della Polizia di Stato o dell'Arma dei Carabinieri, chiedendo ulteriori elementi di informazione in merito e/o interventi mirati; a loro volta, le Forze di polizia inoltrano d'iniziativa all'OSCAD segnalazioni relative ai casi trattati.

Tale flusso informativo alimenta un apposito sistema di monitoraggio gestito dall'Osservatorio che, nel tempo, è divenuto un imprescindibile punto di riferimento – a livello nazionale ed internazionale – in materia di monitoraggio ed analisi dei crimini d'odio. Con riferimento ai crimini d'odio, alle difficoltà legate alla quantificazione dei reati in generale – tra tutte, il fatto che la banca dati interforze non è strutturata per corrispondere a esigenze statistiche, ma per supportare l'operatività delle forze di polizia – si aggiungono ulteriori specifici elementi (*under-reporting* e *under-recording*, nonché la parziale copertura normativa), che rendono particolarmente complessa la raccolta dei dati.

A partire dal 2014 (dati 2013), OSCAD elabora il contributo del Dipartimento della P.S. per la raccolta annuale dei dati sui crimini d'odio effettuata dall'OSCE.

A tal fine, vengono trasmessi i *dati ufficiali SDI* (Sistema d'Indagine) del CED interforze relativi ai reati con finalità discriminatorie che hanno "copertura normativa"[35], ossia quelli di matrice etnico-razziale, nazionale, reli-

---

32) *Https://www.poliziadistato.it/articolo/osservatorio-per-la-sicurezza-contro-gli-atti-discriminatori-oscad.*

33) *Http://www.carabinieri.it/cittadino/servizi/osservatorio-per-la-sicurezza-contro-gli-atti-discriminatori-oscad.*

34) *Https://www.interno.gov.it/it/ministero/osservatori/osservatorio-sicurezza-contro-atti-discriminatori-oscad.*

35) Prevista dalle leggi Reale (L. 654/75) e Mancino (D.l. 122/93, convertito con l. 205/93), come modificate dal d.lgs 21/2018.

giosa e nei confronti di appartenenti a minoranze linguistiche nazionali, nonché quelli commessi nei confronti di persone disabili. Alcuni limiti di tipo normativo e strutturale, rendono attualmente impossibile distinguere le specifiche finalità discriminatorie (ad esempio: quante violazioni riguardino, rispettivamente, "razza", etnia, nazionalità e religione e, in riferimento a tale ultimo contesto, quante siano riferibili ad antisemitismo, islamofobia, odio anticristiano…). Tali dati, vengono integrati con quelli relativi al monitoraggio effettuato dall'OSCAD sulle segnalazioni pervenute in materia di orientamento sessuale ed identità di genere (ambiti privi di specifica copertura normativa).

La formazione delle forze di polizia ha da sempre rivestito una particolare importanza per l'OSCAD, in quanto indispensabile per incrementare la sensibilità e la competenza degli operatori in materia e, conseguentemente, la capacità di risposta operativa al fenomeno, veicolando il messaggio che la cultura del rispetto per i diritti umani e una sempre maggiore efficacia nella prevenzione e nel contrasto dei reati di matrice discriminatoria costituiscono priorità strategiche dell'Amministrazione. Allo scopo di garantire un'offerta didattica aggiornata e multidisciplinare, sono state attivate e sempre più intensificate le relazioni con numerosi *stakeholder* istituzionali e della società civile, con i quali sono state realizzate numerose attività formative congiunte: l'Ufficio Nazionale Antidiscriminazioni Razziali della Presidenza del Consiglio dei Ministri (UNAR, l'*equality body* italiano con il quale OSCAD, nel 2011, ha sottoscritto un apposito protocollo di intesa); il Servizio LGBT del Comune di Torino, capofila della "Rete Ready"[36]; "Amnesty International - Italia"; "Polis Aperta"[37]; "Rete Lenford"[38]; "Cospe"[39]; "Lunaria"[40].

Nell'ambito della pianificazione delle attività relative all'aggiornamento professionale del personale della Polizia di Stato, per il 2012 ed il 2017, le materie di interesse OSCAD – ossia la prevenzione ed il contrasto dei crimini d'odio ed il ruolo dell'Osservatorio – d'intesa con la Direzione centrale per

36) Rete nazionale delle pubbliche amministrazioni anti discriminazioni per orientamento sessuale e identità di genere.
37) Associazione LGBTI di appartenenti a forze di polizia e forze armate.
38) "Avvocatura per i diritti LGBT - Rete Lenford": associazione di avvocati esperti nei diritti LGBTI.
39) "Cooperazione per lo sviluppo dei Paesi emergenti", associazione molto attiva in materia di antirazzismo.
40) Associazione impegnata nella promozione sociale e nell'antirazzismo.

gli istituti di istruzione, sono state inserite tra le cc.dd. "tematiche di interesse generale" destinate a tutto il personale della Polizia di Stato.

Dal 2021, quale evoluzione delle iniziative formative del 2012 e del 2017, è stata prevista una giornata formativa *di interesse generale* denominata "Quando l'odio diventa reato", nel cui ambito sono proposti appositi moduli formativi OSCAD. Numerose sono state le iniziative formative interforze:

– realizzazione, nell'ambito della "Strategia nazionale LGBTI"[41], di un articolato piano pluriennale (2014-2016) di attività formative interforze di livello nazionale o regionale – definite in collaborazione con il Servizio LGBT del Comune di Torino – da erogare al personale delle forze di polizia per un più efficace contrasto all'omotransfobia;

– partecipazione a vari progetti europei per la formazione in presenza del personale di polizia in tema di prevenzione e contrasto degli hate crimes (tra gli altri: *PRISM*, *Experience Crime*, *Come Forward*);

– quanto alle progettualità internazionali, deve essere evidenziata, in modo particolare, la partecipazione, dal 2016 al 2019, al progetto europeo "Facing all the facts"[42] in collaborazione con la Ong "CEJI - Un contributo ebraico per un'Europa inclusiva", partner capofila, in materia di formazione e monitoraggio dei reati di matrice discriminatoria. Nell'ambito dell'iniziativa, è stato realizzato un corso on-line per le forze di polizia composto da tre moduli: "Cos'è un crimine d'odio", "Gli indicatori di pregiudizio (*Bias Indicators*)"[43] e "Le vittime vulnerabili", nonché sei approfondimenti sugli indicatori di pregiudizio in materia di: antisemitismo; islamofobia; omotransfobia; antigipsismo; odio contro i migranti; disabilità. È stata inoltre pubblicata un'approfondita ricerca, effettuata dall'esperta di livello internazionale dott.ssa Joanna PERRY, sui sistemi di raccolta e monitoraggio dei dati, dove, per la prima volta, vengono evidenziati punti di forza e limiti del sistema italiano;

– la collaborazione con l'OSCE è particolarmente intensa anche in ambito formativo. Sono state, infatti, realizzate diverse iniziative nell'ambito della progettualità TAHCLE (*Training Against Hate Crimes for Law Enforcement*) tesa alla formazione di formatori per la prevenzione ed il contrasto

41) Adottata dall'Italia ai fini dell'attuazione della Raccomandazione del Comitato dei Ministri del Consiglio d'Europa CM/REC (2010)5 e coordinata, sul piano nazionale, dall'UNAR.

42) *Https://www.facingfacts.eu/connecting-on-hate-crime; https://www.facingfacts.eu/italy-systems-map-it.*

43) Ossia, elementi e circostanze che possono dimostrare la matrice discriminatoria di un reato.

dei crimini d'odio: a livello nazionale nel 2014 e nel 2018 e a livello regionale, in Lombardia, nel 2017.

3.1.1. La partecipazione a gruppi di lavoro e fori europei ed internazionali

L'attività dell'OSCAD si qualifica anche per la partecipazione a gruppi di lavoro e fori europei ed internazionali concernenti le materie di specifica competenza. Al riguardo, le seguenti attività sono state particolarmente significative:

– partecipazione al "Gruppo di alto livello contro razzismo, xenofobia ed altre forme di intolleranza" della Commissione europea[44], istituito a giugno 2016, nonché ai vari tavoli di lavoro tematici attivati, nell'ambito del Gruppo, su: antisemitismo; odio anti musulmano/islamofobia; raccolta dei dati; *hate speech on-line*; supporto ed l'assistenza alle vittime; formazione;

– partecipazione, nel 2019, ad un meeting di esperti in materia di contrasto all'islamofobia, organizzato dall'OSCE e dalla Ong "Muslim dialogue network", teso alla revisione della bozza di guida pratica OSCE "Comprendere i crimini d'odio di matrice anti musulmana ed affrontare i bisogni in tema di sicurezza delle comunità musulmane", successivamente pubblicata sul sito dell'Organizzazione[45];

– organizzazione in collaborazione con il Consiglio d'Europa, nel 2015, di un meeting internazionale in materia di antidiscriminazione, con uno specifico focus sulle tematiche Rom, Sinti e Caminanti;

– partecipazione al gruppo di lavoro sui crimini d'odio coordinato dalla FRA (*Fundamental Rights Agency*, Agenzia per i diritti fondamentali dell'UE), nel cui ambito l'OSCAD ha avuto la co-leadership del sottogruppo dedicato alla formazione. In questo contesto l'OSCAD è stato inserito, quale buona prassi nazionale, all'interno di un apposito *compendio* riepilogativo delle eccellenze europee per il contrasto ai crimini d'odio (2014-2016)[46].

---

44) *Https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51025*.

45) *Understanding Anti-Muslim Hate Crimes - Addressing the Security Needs of Muslim Communities: A Practical Guide*, su *https://www.osce.org/odihr/muslim-security-guide.*

46) *Http://fra.europa.eu/en/theme/hate-crime/compendium-practices?countries_eu=All&&&page=1*; *http://fra.europa.eu/en/promising-practices/observatory-security-against-acts-discrimination-OSCAD*.

3.1.2. L'attività di sensibilizzazione e divulgazione

Il 21 gennaio 2020, è stato organizzato, presso la Sala polifunzionale della Presidenza del Consiglio dei Ministri, in Roma – alla presenza, tra gli altri, del Ministro dell'interno, del Ministro per le pari opportunità e del Capo della Polizia - Direttore Generale della Pubblica Sicurezza – il convegno dal titolo "Le vittime dell'odio", che ha costituito un momento di riflessione al fine di promuovere la cultura dell'inclusione e contrastare ogni forma di razzismo. Il convegno è stato strutturato in diversi *panel*, ciascuno dei quali dedicato ad una particolare tipologia di discriminazione: razza-etnia, credo religioso, orientamento sessuale, disabilità. In ogni sessione si sono alternati momenti di riflessione proposti da esperti, anche di livello internazionale, stralci di video e testimonianze di vittime.

È stato realizzato l'inserto "Quando l'odio diventa reato - Caratteristiche e normativa di contrasto degli *hate crimes*", pubblicato all'interno del mensile ufficiale della Polizia di Stato "Polizia Moderna" del mese di gennaio 2020 e presentato nell'ambito del citato evento "Le vittime dell'odio". L'inserto costituisce uno strumento informativo, di facile lettura, per meglio comprendere crimini e discorsi d'odio, le loro caratteristiche e specificità, gli indicatori di pregiudizio, le vittime vulnerabili e la normativa di riferimento, sia a livello nazionale che internazionale.

L'elaborato è stato pubblicato – in italiano ed in inglese – sui siti istituzionali del Ministero dell'interno[47], della Polizia di Stato[48] e dell'Arma dei Carabinieri[49], ne è stata data ampia diffusione tra le forze di polizia ed è stato inoltrato, nella versione in inglese, a tutti gli *stakeholder* europei ed internazionali.

Il 7 dicembre 2018, è stata presentata alla stampa la "Breve guida dell'ebraismo per gli operatori di polizia", elaborata d'intesa con l'UCEI (Unione delle Comunità Ebraiche Italiane), con l'obiettivo di aiutare gli operatori di polizia ad espletare al meglio i propri compiti, offrendo loro uno strumento di conoscenza rispetto ad alcune fondamentali specificità dell'ebraismo italiano, informazioni indispensabili per interfacciarsi nel modo più corretto ed effi-

47) *Https://www.interno.gov.it/sites/default/files/allegati/inserto_reati_odio_-_oscad.pdf.*
48) *Https://www.poliziadistato.it/statics/26/quando-odio-diventa-reato.pdf.*
49) *Https://www.carabinieri.it/docs/default-source/default-document-library/quando-l-odio-diventa-reato*.

ciente con le persone di fede ebraica. La guida pubblicata sul sito internet del Ministero dell'Interno[50], è stata ampiamente diffusa tra le Forze di polizia e tra le comunità ebraiche attraverso l'UCEI, nonché presentata in vari tavoli di lavoro internazionali, dove ha riscosso notevole apprezzamento.

3.2. Gruppo tecnico di lavoro per la ricognizione sulla definizione di antisemitismo approvata dall'IHRA

L'antisemitismo rientra nel più ampio *genus* delle discriminazioni religiose, al pari dell'islamofobia, dell'anticristianesimo e di ogni altra manifestazione di intolleranza e discriminazione verso chi professa un credo religioso.

Si tratta di una manifestazione molto ricorrente nella storia che viene fatta risalire ad una pluralità di cause, non solo la paura del diverso, ma anche e soprattutto, nelle religioni monoteiste, la tutela dell'ortodossia a difesa della casta sacerdotale.

Un significativo passo in avanti nella difesa della libertà religiosa e della cultura della tolleranza e del rispetto si è avuto il 17 gennaio del 2020 con l'approvazione in Italia della definizione di antisemitismo dell'IHRA:

"*L'antisemitismo è una certa percezione degli ebrei che può essere espressa come odio per gli ebrei. Manifestazioni di antisemitismo verbali e fisiche sono dirette verso gli ebrei o i non ebrei e/o alle loro proprietà, verso istituzioni comunitarie ebraiche ed edifici utilizzati per il culto*".

Ad accompagnare la definizione ci sono undici esempi illustrativi, di cui sette si riferiscono a Israele, in una controversa equiparazione di antisemitismo e antisionismo.

L'*International Holocaust Remembrance Alliance* (IHRA) è un'organizzazione intergovernativa fondata nel 1998 dal Primo Ministro svedese Goran Persson per promuovere e divulgare l'educazione sull'Olocausto ed il sostegno agli impegni della Dichiarazione del Forum internazionale di Stoccolma. L'IHRA conta oggi 34 Paesi membri, un Paese di collegamento e sette Paesi osservatori.

La definizione di antisemitismo è stata redatta dall'IHRA e pubblicata il 28 gennaio 2005 sul sito web dell'agenzia dell'Unione europea, l'Osservatorio europeo dei fenomeni di razzismo e xenofobia (EUMC). Si trattava di una bozza di lavoro che di fatto l'EUMC non ha mai adottato, tant'è che nel

50) *Https://www.interno.gov.it/it/stampa-e-comunicazione/pubblicazioni/guida-allebraismo-operatori-polizia*.

2013 la FRA (L'Agenzia per i diritti fondamentali), che è formalmente subentrata all'EUMC, la ha anche rimossa dal sito.

Il 26 maggio 2016, IHRA ha adottato una definizione operativa non legalmente vincolante di antisemitismo che è stata adottata in occasione della riunione plenaria di Bucarest dell'IHRA il 30 maggio 2016.

Si tratta di fatto della stessa definizione del 2005 pubblicata sul sito dell'EUMC corredata peraltro dagli stessi undici esempi.

La definizione operativa, come tutte le decisioni dell'IHRA, non è legalmente vincolante, ma di fatto costituisce un punto di partenza per trovare in una definizione comune, un'identica norma di linguaggio e un identico approccio culturale e di metodo.

È assolutamente necessario riportare di seguito anche gli undici esempi illustrativi perché danno senso compiuto alla dichiarazione stessa. Va, inoltre, precisato che le manifestazioni possono avere come obiettivo lo Stato di Israele perché concepito come una collettività ebraica. Tuttavia, le critiche *tout court* verso Israele simili a quelle rivolte a qualsiasi altro Paese, non possono essere considerate antisemite.

«*Esempi contemporanei di antisemitismo nella vita pubblica, nei mezzi di comunicazione, nelle scuole, al posto di lavoro e nella sfera religiosa includono (ma non si limitano a):*

– incitare, sostenere o giustificare l'uccisione di ebrei o danni contro gli ebrei in nome di un'ideologia radicale o di una visione religiosa estremista;

– fare insinuazioni mendaci, disumanizzanti, demonizzanti o stereotipate degli ebrei come individui o del loro potere come collettività: per esempio, specialmente ma non esclusivamente, il mito del complotto ebraico mondiale o degli ebrei che controllano i mezzi di comunicazione, l'economia, il Governo o altre istituzioni all'interno di una società;

– accusare gli ebrei come popolo responsabile di reali o immaginari crimini commessi da un singolo ebreo o un gruppo di ebrei, o persino da azioni compiute da non ebrei;

– negare il fatto, la portata, i meccanismi (per esempio le camere a gas) o l'intenzione del genocidio del popolo ebraico per mano della Germania Nazionalsocialista e dei suoi seguaci e complici durante la Seconda Guerra Mondiale (l'Olocausto);

– accusare gli ebrei come popolo o Israele come Stato di essersi inventati l'Olocausto o di esagerarne i contenuti;

– accusare i cittadini ebrei di essere più fedeli a Israele o a presunte priorità degli ebrei nel mondo che agli interessi della loro nazione.

– negare agli ebrei il diritto dell'autodeterminazione, per esempio sostenendo che l'esistenza dello Stato di Israele è una espressione di razzismo.

– applicare due pesi e due misure nei confronti di Israele richiedendo un comportamento non atteso da o non richiesto a nessun altro stato democratico;

– usare simboli e immagini associati all'antisemitismo classico (per esempio l'accusa del deicidio o della calunnia del sangue) per caratterizzare Israele o gli israeliani.

– fare paragoni tra la politica israeliana contemporanea e quella dei Nazisti.

– considerare gli ebrei collettivamente responsabili per le azioni dello Stato di Israele.

Gli atti di antisemitismo sono considerati crimini quando vengono definiti tali dalla legge del Paese (per esempio, negazione dell'Olocausto o la distribuzione di materiali antisemiti in alcuni Paesi).

Gli atti criminali sono considerati antisemiti quando l'obiettivo degli attacchi, sia che siano persone o proprietà – edifici, scuole, luoghi di culto o cimiteri – sono scelti perché sono, o sono percepiti, ebrei, ebraici o legati agli ebrei».

A seguito dell'adozione da parte dell'IHRA, la definizione operativa è stata adottata per uso interno da una serie di istituzioni governative e politiche. Ad oggi tale definizione è stata adottata o riconosciuta da 25 Paesi che sono tenuti anche a nominare un coordinatore nazionale per la lotta all'antisemitismo.

Il Regno Unito è stato il primo Paese ad aver adottato la definizione (12 dicembre 2016), seguito da Israele (22 gennaio 2017), mentre l'Italia, come si è detto, ha approvato la definizione il 17 gennaio del 2020, senza però includere gli esempi che, come si è visto, sono parte integrante della dichiarazione stessa. La Professoressa Milena Santerini è stata nominata coordinatrice nazionale contro l'antisemitismo.

Il 1º giugno 2017, il Parlamento europeo ha approvato una risoluzione che invita gli Stati membri dell'Unione europea e le loro istituzioni ad adottare e applicare la definizione operativa di antisemitismo proposta dall'IHRA. Appare al riguardo doveroso citare anche la dichiarazione del Consiglio UE del 2 Dicembre 2020, secondo la quale *il ricorso coerente alla definizione operativa legalmente non vincolante di antisemitismo dell'IHRA serve ad identificare gli indicatori di pregiudizio e può aiutare le agenzie governative e le organizzazioni non governative a rispondere in modo più efficace ai crescenti fenomeni di antisemitismo.*

Infine è stato pubblicato il "Manuale per l'utilizzo pratico della definizione di antisemitismo elaborata dall'IHRA" commissionato dalla Commissione europea e pubblicato congiuntamente con l'IHRA con il supporto della presidenza tedesca del Consiglio dell'Unione europea.

Il manuale, elaborato dall'"Associazione federale dei Dipartimenti per la ricerca e l'informazione sull'antisemitismo" (Bundesverband RIAS), fornisce una visione di insieme delle buone pratiche in materia di prevenzione e contrasto dell'antisemitismo, poste in essere da parte delle organizzazioni internazionali, dalla società civile e dalle comunità ebraiche in tutta Europa.

Ripercorso l'*excursus* storico che ha portato all'adozione anche in Italia della definizione dell'IHRA occorre fare alcune considerazioni sul merito. Intanto appare doveroso precisare che, se da un lato è vero che per combattere un nemico comune bisogna avere una definizione comune della minaccia, dall'altro è anche vero che non ci troviamo di fronte ad una norma vincolante. Si tratta certamente di un punto di partenza per orientare le decisioni e le politiche dei Governi, rendendo centrale il tema dell'antisemitismo come utile guida nell'educazione e nella formazione. Ma la circostanza stessa che in Italia l'adozione sia stata parziale dimostra come il tema sia ancora molto controverso, soprattutto nella duplice valenza ermeneutica di antisemitismo e antisionismo.

Come più volte sottolineato ci troviamo di fronte ad uno strumento di "soft law", non una norma immediatamente vincolante, ma piuttosto una dichiarazione di principio, come quelle adottate nell'ambito delle maggiori organizzazioni internazionali ed in particolare quelle dell'Assemblea generale delle Nazioni Unite o la stessa Carta dei diritti fondamentali dell'Unione europea che è stata anch'essa qualificata come *soft law*.

3.2.1. Intervista a Noemi Di Segni, Presidente dell'UCEI (Unione delle Comunità Ebraiche Italiane)

Con riferimento all'adesione dell'Italia alla definizione di antisemitismo dell'IHRA e nell'ambito del lavoro di ricerca svolto per la redazione della presente trattazione, il 19 aprile scorso ho realizzato un'intervista, che si riporta di seguito per estratti, alla dott.ssa Noemi Di Segni, Presidente dell'Unione delle Comunità Ebraiche Italiane:

1) Presidente come nasce la definizione di antisemitismo dell'IHRA?

La definizione di antisemitismo dell'IHRA rappresenta un risultato politicamente molto importante e denota attenzione verso l'antisemitismo. Per le Comunità ebraiche questa definizione rappresenta soltanto uno punto di

partenza, l'inizio di un percorso dove l'approvazione della definizione di antisemitismo costituisce un momento strategico perché contiene anche il tema di Israele, che è un tema delicato in cui si manifesta l'odio della delegittimazione e della demonizzazione. A tale definizione possiamo riconoscere una valenza politica importante, ma anche una valenza operativa perché è un punto di partenza che aiuta a comprendere e capire le situazioni e a saperle classificare, indica a chi rivolgersi per programmare azioni ed interventi e con chi fare un lavoro di formazione. Sicuramente tale definizione è difficile da trasportare in un'aula giudiziaria, la questione della rilevanza penale necessita ancora di approfondimento e di interventi legislativi ad hoc.

2) La definizione di antisemitismo è accompagnata da 11 esempi. Che valore hanno questi esempi e quanto sono importanti nella lotta all'antisemitismo?

Gli esempi sono importanti perché bisogna seguirli pezzo per pezzo e segmento per segmento per comprendere cosa fare. Alcuni riguardano il tema di Israele e toccano temi strategici. Tra i fenomeni più preoccupanti per Israele c'è sicuramente il boicottaggio realizzato dal BDS Italia - movimento per il boicottaggio, il disinvestimento e le sanzioni contro Israele; la radicalizzazione islamica, ma anche l'odio on-line, rivolto al singolo o alla comunità: un odio subdolo, perché non è un odio di violenza ma un odio che genera ostilità, diffidenza e si alimenta grazie alla disinformazione e all'azione di quei gruppi di estrema destra che professano e propagandano l'odio razziale.

3) Che significato ha per le comunità ebraiche italiane l'approvazione della definizione di antisemitismo dell'IHRA da parte del nostro Paese?

L'approvazione della definizione è fondamentale, ma è altrettanto importante recepire la definizione. Recepire vuol dire varare delle politiche che combattano l'antisemitismo, significa contrastare il fenomeno ed affrontarlo con specifiche politiche rispetto ad ogni singola categoria: l'odio per Israele, il negazionismo, le derive di odio razziale di alcuni movimenti di estrema destra, il boicottaggio.

4) Alla luce della sua esperienza quali potrebbero essere i prossimi passi nella lotta all'antisemitismo?

Sicuramente il primo passo è riconoscere il problema: e questo è stato fatto attraverso l'approvazione della definizione di antisemitismo adottata dall'IHRA. Un altro passo importante è varare un piano di lotta all'antisemitismo, intervenendo con politiche e programmi di inclusione. È di fondamentale importanza procedere segmento per segmento rispetto ad ogni interlocutore della società civile per la costruzione e per la formazione di coscienza e conoscenza. Dal punto di vista legislativo c'è spazio per un miglioramento

della legislazione che richiede però grande cura ed attenzione perché la libertà di espressione va garantita e tutelata ma in nome di essa non si può diffondere l'odio. Quindi un percorso pedagogico, di formazione, legislativo e anche rivolto al mondo dei media.

5) A suo parere che impatto ha avuto la pandemia globale nel diffondersi della sfiducia e dell'odio nella nostra società e quali potrebbero essere gli strumenti di contrasto nel campo dell'antisemitismo.

Il diffondersi del Covid ha generato paura ed incertezza, lo sfruttamento della paura del virus è stato lo strumento per inculcare l'odio, il complottismo, la sfiducia nella scienza, nel pericoloso tentativo di mettere in discussione qualsiasi cosa. La definizione, come ho già detto, rappresenta un punto di partenza, aiuta a capire le situazioni e a classificarle per orientare le azioni, per comprendere in quale ambiente lavorare, con chi fare un percorso educativo, di formazione, di condivisione di valori. Aiuta a programmare azioni ed iniziative che devono potersi sviluppare nel tempo, con un programma governativo di interventi in contesti e settori diversi. La definizione dell'IHRA è fondamentale, ma è una working definition*, è un punto di partenza che aiuta a definire tutte le singole problematiche che debbono essere affrontate e sulle quali bisogna lavorare.*

3.3. L'Italia e l'antisemitismo

Come analizzato nei capitoli precedenti il tema dell'odio in Italia viene ricondotto nel *genus* dell'antidiscriminazione nella sua accezione normativamente prevista e punita di discriminazione etnica, razziale, nazionale e religiosa.

Senza ripercorrere l'esegesi normativa[51] appare però opportuno sottolineare come, sia pur nella limitata gamma di manifestazioni di odio e di discri-

51) Gli strumenti giuridici volti a contrastare la discriminazione antisemita che risiede in un linguaggio violento sono costituti in primo luogo dalla legge Scelba (*Norme di attuazione della XII disposizione transitoria e finale (comma primo) della Costituzione*) del 1952, volta alla repressione penale della riorganizzazione del disciolto partito fascista, dell'apologia del fascismo e delle manifestazioni fasciste. Successivamente la legge Mancino (*Misure urgenti in materia di discriminazione razziale, etnica e religiosa*), entrata in vigore nel 1993, ha previsto la reclusione di chi diffonde in qualsiasi modo idee fondate sulla superiorità o sull'odio razziale o etnico, o di chi incita alla discriminazione o all'odio o commette violenza o atti di provocazione alla violenza, per motivi razziali, etnici, nazionali o religiosi e il divieto di ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione, all'odio o alla violenza per

minazioni previste nel nostro ordinamento, trovi cittadinanza il tema della discriminazione religiosa.

Quindi l'antisemitismo, che rappresenta una delle condotte di discriminazione religiosa, ha copertura normativa sia pur entro il perimetro ben definito delle fattispecie previste dagli artt. 384-*bis* e 384-*ter*.

Quel *quid pluris* che porta a dare un significato particolare all'antisemitismo rispetto alle altre discriminazioni religiose si coglie peraltro nel dettato normativo ed in particolare nell'ultimo comma dell'art. 604-*bis* dove si introduce un esplicito riferimento alle teorie negazioniste:

"*Si applica la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale*".

Come si può notare dal dettato normativo il legislatore separa concettualmente due categorie che devono considerarsi due concetti ontologicamente autonomi e non certo un endiade, *sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio.*

La Shoah è senz'altro un genocidio ma assume valenza ontologicamente autonoma in ordine alla manifestazione più estrema dell'antisemitismo.

---

gli stessi motivi sopra evidenziati. Con la l. n. 115 del 2016 è stata attribuita rilevanza penale alle affermazioni negazioniste della Shoah; è sempre dello stesso anno l'istituzione della Commissione "Jo-Cox" sull'intolleranza, la xenofobia, il razzismo e i fenomeni d'odio. Ancora, in occasione dell'entrata in vigore della legge n. 167 del 2016, "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea*", è stato modificato l'aggravante di negazionismo all'art. 3-*bis* dell'art. 3 l. 654/1975. Quanto alle novità, il 6 aprile 2018 è entrato in vigore il decreto legislativo n. 21 del 2018, il quale, tra le altre modifiche al codice penale, ha trasferito all'art. 604-*bis*, ora rubricato *Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa*, la fattispecie criminosa originariamente prevista dall'articolo 3 della legge n. 654/1975 (di ratifica ed esecuzione della Convenzione contro il razzismo adottata dalle Nazioni Unite a New York nel 1966): l'articolo in questione punisce chiunque propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Èdi fondamentale rilevanza sottolineare come nella disposizione in questione, inoltre, al comma terzo, è prevista l'applicazione della pena alla reclusione in caso di negazione, minimizzazione in modo grave o apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale.

L'adozione della definizione dell'IHRA costituisce un ulteriore passo in avanti in questo percorso di democrazia e tolleranza, di rispetto e crescita culturale.

L'OSCAD, inoltre, ha partecipato ai lavori del "Gruppo tecnico di lavoro per la ricognizione sulla definizione di antisemitismo approvata dall'IHRA" coordinato dalla professoressa Milena Santerini, Coordinatrice nazionale per la lotta all'antisemitismo. La relazione finale del Gruppo costituisce una vera e propria strategia nazionale di lotta all'antisemitismo. In questo documento, per quanto attiene al Ministero dell'Interno, oltre all'intensificazione delle attività di formazione/sensibilizzazione delle forze di polizia, è stata auspicata l'attivazione di "*un unico punto di raccolta dati sugli atti di antisemitismo, sia per quanto riguarda i crimini d'odio sia per quanto riguarda gli incidenti di tipo antisemita* (i cosiddetti *hate incidents*, ovvero quegli atti che pur non oltrepassando la soglia della punibilità penale destano comunque preoccupazione nelle comunità e che per le forze di polizia rappresentano dei campanelli di allarme in quanto potenziali precursori di crimini veri e propri) *al fine di acquisire una visione più completa del fenomeno in Italia e realizzare un'azione di monitoraggio coordinata tra gli organismi che attualmente svolgono questo compito*".

L'OSCAD, inoltre, nell'assumere una sempre maggiore centralità nella lotta contro l'antisemitismo, nel 2020 ha provveduto all'elaborazione di un report per la FRA (Agenzia per i diritti fondamentali dell'UE) sui crimini d'odio antisemiti, opportunamente disaggregati secondo le categorie criminologiche dell'OSCE.

3.4. Antisemitismo e iniziative di prevenzione

Se reprimere l'odio antisemita è l'inevitabile conseguenza di condotte antigiuridiche, prevenire l'odio vuol dire educare al rispetto, alla tolleranza, al pluralismo. Prevenire in questo caso vuol dire conoscenza, formazione e crescita culturale. Per questo l'OSCAD ha intensificato la collaborazione con l'UCEI (l'Unione delle Comunità Ebraiche Italiane) e con il CDEC (Centro di Documentazione Ebraica Contemporanea). Questa collaborazione si è tradotta nella realizzazione di una Guida all'Ebraismo, periodicamente aggiornata, distribuita al personale delle forze di polizia ed utilizzata in numerose iniziative formative. È stato, altresì, predisposto un canale di comunicazione diretto al fine di monitorare e condividere tutti gli episodi di antisemitismo, anche quelli ben al di sotto delle rilevanza penale, per poter intervenire tempestivamente su qualsivoglia indicatore di pregiudizio. Tale monitoraggio dei cosiddetti *hate incidents* va ben oltre le funzioni di polizia intese *strictu sensu*,

laddove la linea di demarcazione che legittima l'intervento delle forze di polizia è data dalla rilevanza penale della condotta posta in essere. Nel caso di specie il monitoraggio degli *hate incidents* trova la sua ragione d'essere nella volontà di innalzare la soglia dell'attenzione, nella piena consapevolezza che cogliere tempestivamente indicatori di pregiudizio significa arginare l'odio ed evitare che tracimi in condotte antigiuridiche. Non si chiede all'operatore un giudizio di valore, che certamente non gli deve appartenere, ma solo di mantenere alta l'attenzione per evitare che si crei un humus favorevole a manifestazioni di odio.

Infine, in ambito europeo e in particolare in ambito Europol, la Germania ha assunto la guida di un gruppo di lavoro proprio in tema di antisemitismo. Immediata è stata l'adesione dell'Italia a tale iniziativa a cui ha peraltro fatto seguito anche un contatto con Felix Klein, Commissario del Governo federale tedesco per la vita ebraica in Germania e per la lotta all'antisemitismo. Un impegno, dunque, anche in ambito multilatelare attraverso Europol e bilatelare con la Germania che ha lanciato l'iniziativa durante il suo semestre di Presidenza e con tutti quei Paesi che manifestano uguale sensibilità sul tema.

4. Odio e suprematismo: le nuove minacce

4.1. USA: la minaccia dei suprematisti bianchi

I *Suprematisti bianchi* sono gruppi – nati e cresciuti in rete, diffusi in Europa e negli Stati Uniti, ben radicati sul territorio – che si rifanno all'ideologia "ariana", veicolando idee e programmi islamofobi e, in molti casi, antisemiti.

Le loro idee vengono veicolate tramite internet attraverso migliaia di siti, che indottrinano e addestrano sul web gli affiliati e chiunque voglia farsi giustizia da sé; con un programma che professa non solo una "caccia all'islamico", ma anche una guerra contro chi è a favore dell'aborto o di politiche sociali di aiuto a profughi e immigrati.

Questi gruppi che hanno come centro gli Stati Uniti, si sono diffusi rapidamente a macchia d'olio dalla Gran Bretagna alla Francia fino all'Italia. Attualmente negli Usa si contano oltre 1120 gruppi razzisti sostenitori di idee come la supremazia bianca basata sulla teorica superiorità di questa razza su afroamericani, ispanici, arabi o ebrei.

La situazione politica e sociale degli Stati Uniti ha visto, negli ultimi

tempi, una polarizzazione sempre più forte della popolazione, sia per la campagna elettorale per le elezioni Presidenziali, sia per la diffusione della pandemia da Covid 19, sia per l'esplosione delle proteste per il Black Lives Matter ed infine per l'assalto a Capitol Hill.

L'accesissimo confronto elettorale e le restrizioni imposte per limitare la diffusione del virus, con conseguente crisi economica ed enorme aumento della disoccupazione, hanno portato in superficie una serie di movimenti che fanno riferimento sia ai temi dell'estrema destra che a quelli dell'estrema sinistra.

Tali movimenti erano ovviamente già presenti nella società americana, ma la peculiarità del momento storico ha costituito l'humus perfetto affinché potessero riversarsi nelle manifestazioni di piazza che nell'anno in corso hanno letteralmente flagellato il Paese. In tal senso negli Stati Uniti si sono riaccese le battaglie per i diritti civili delle minoranze, con particolare riguardo a quella di origine afroamericana, a seguito dell'uccisione durante un controllo di polizia di George Floyd a Minneapolis (Minnesota) il 25 maggio 2020.

In tale contesto sociale esplosivo sia i movimenti di estrema sinistra che quelli di estrema destra sono scesi nelle piazze, sfruttando manifestazioni spontanee di cittadini, o inserendosi in quelle organizzate dal Black Lives Matter cercando di ottenere l'attenzione dei media e fare proseliti per la loro propaganda politica.

Da tali eventi e spinte sociali sono emersi una serie di gruppi saliti agli onori delle cronache per le loro partecipazioni alle manifestazioni di piazza e per la costante azione di propaganda, portata avanti avvalendosi della capacità di amplificazione della rete e della garanzia di anonimato che essa può garantire.

Tra essi quelli che hanno registrato maggiore seguito sono: Proud Boys, Boogaloo, Three Percenters, QAnon, AtomWaffe Division e The Base.

Pur con alcune differenze riguardo alle modalità di azione, alla tipologia di propaganda effettuata ed alla selezione degli appartenenti, Proud Boys, Boogaloo e Three Percenters pongono alla base della loro ideologia la necessità del cittadino americano di ribellarsi ad una forma di Governo che usurpa i diritti dei cittadini andando oltre i poteri concessigli dalle leggi fondamentali degli Stati Uniti e cioè: la Dichiarazione d'Indipendenza, La Costituzione e la Carta dei diritti (Bill of rights), che contiene i primi dieci Emendamenti alla Costituzione stessa. Proprio tale autoreferenzialità dei predetti gruppi statunitensi ed il fortissimo richiamo alle norme ed alle vicende storiche e costituzionali del Paese rende i movimenti in argomento i meno interessati alla proiezione internazionale ed intercontinentale della loro ideologia e delle loro azioni. Il diritto di portare armi, garantito ai cittadini americani dal II Emen-

damento alla Costituzione, viene visto proprio come un baluardo di democrazia popolare contro gli eccessi di potere dei Governi, che possono essere "legittimamente" contrastati da milizie di cittadini armati.

Alla luce di ciò va letto lo schieramento di appartenenti a tali movimenti, armati con fucili d'assalto e armi da guerra palesemente esibite, durante le manifestazioni spontaneamente sviluppatesi nei due mesi del lockdown per protestare contro i decreti dei Governatori degli Stati che imponevano lo 'Stay at home' e la chiusura delle attività imprenditoriali ed industriali. La più eclatante di queste proteste ha visto alcune centinaia di manifestanti armati marciare verso il Campidoglio dello Stato del Michigan, dove hanno tentato di invadere l'aula dell'Assemblea legislativa statale per cercare di spingere il Governatore (Partito democratico) Gretchen Whitmer a ritirare i decreti emessi per contrastare la diffusione della pandemia.

Proud Boys - Movimento fondato nel 2016 definito come un gruppo di estrema destra, con ideologia islamofobica, misogina, sciovinista e, benchè formalmente rifiutata, suprematista bianca. Il leader Enrique Tarrio, cittadino americano di origine afro-cubana utilizza spesso la propria origine etnica per dimostrare l'infondatezza di tale accusa. Nonostante cio, le azioni condotte nel corso delle manifestazioni pubbliche e la presenza tra le loro fila di soggetti provenienti da posizioni razziste e delusi del Ku Klux Klan, oltre che di elementi appartenenti a frange neo-naziste, lascia chiaramente intendere l'effettiva tendenza suprematista dei suoi appartenenti. Appartenenti armati con fucili d'assalto e armi da guerra hanno preso parte sia alle manifestazioni per protestare contro l'adozione delle restrizioni della libertà di movimento e d'impresa per contrastare la diffusione del Covid 19 sia a quelle del Black Lives Matter. I Proud Boys sono stati banditi da tutti i principali social media, come Facebook, Instagram, Twitter e Youtube per i messaggi d'odio che postavano.

Boogaloo - Movimento di estrema destra i cui membri si ritengono parte di una milizia civica che sta preparando la Seconda guerra civile americana, chiamata nel loro gergo appunto Boogaloo. Per quanto i primi richiami al Boogaloo siano cominciati ad apparire in rete, più precisamente sulla piattaforma 4Channel, sin dal 2012, è dal 2019 che tale movimento sembra aver preso una vera e propria consistenza. Si tratta di un movimento antigovernativo che professa l'odio verso le forze di polizia, considerate il braccio armato utilizzato dai Governi per limitare la libertà dei cittadini. I suoi membri prendono spesso parte alle manifestazioni di piazza, tra cui quelle del Black Lives Matter ed anti-lockdown, imbracciando armi da guerra e rendendosi riconoscibili per il particolare abbigliamento utilizzato, composto fondamentalmente da pantaloni tattici/mimetici e da colorate camicie hawaiane. La riaffermazione del diritto

di portare armi da parte dei cittadini, tutelato dal II Emendamento alla Costituzione, ed il contrasto di tutti i tentativi dei vari Stati di limitare tale diritto rimangono i punti fermi della loro lotta politica. Al riguardo l'FBI ed il DHS hanno diramato al mondo del Law Enforcement americano un alert sulla possibilità che i movimenti di destra, tra cui il Boogaloo, potessero sfruttare le manifestazioni di piazza che imperversavano nel Paese, per indirizzarle verso il compimento di danneggiamenti ed atti di violenza strumentali alla loro strategie politiche.

Three Percenters (o 3 Percenters) - Movimento di estrema destra che viene spesso indicato come una vera e propria milizia, attivo tra gli Stati Uniti ed il Canada, prende il suo nome dalla contrastata idea che solo il 3 per cento dei coloni americani imbracciò le armi per ribellarsi alla monarchia inglese ma riuscì a sconfiggere uno degli eserciti più forti del mondo. Anche in questo caso la difesa del II Emendamento della Costituzione e del conseguente diritto di possedere e portare armi, costituiscono la parte principale della propaganda del gruppo e la base delle loro azioni dimostrative, insieme al diritto di resistere alla tendenza dei Governi centrali ad intromettersi negli affari locali. Per tale motivo gli appartenenti al movimento ritengono che la massima autorità "legale" del Paese siano gli Sceriffi delle Contee, eletti dai loro concittadini e deputati alla tutela del bene comune e delle libertà dei loro elettori.

Atomwaffen Division (AWD) - Conosciuto anche come National Socialist Order, è un gruppo di estrema destra con chiara connotazione terroristica fondato nel 2015 da Brandon Russell negli Stati Uniti meridionali, i cui componenti in rete si sono definiti "molto fanatici, una banda ideologizzata di camerati che fa sia attivismo sia addestramento dei militanti". Di forte richiamo neo-nazista, ritenuta troppo estrema anche da molti dei predetti gruppi di destra, considera nemici sia le minoranze, i gay e gli ebrei, che il Governo federale degli Stati Uniti, di cui in alcuni video di propaganda hanno bruciato la bandiera e la Costituzione. Ha accolto tra le sue fila numerosi elementi reclutati nei campus universitari ed altri provenienti dall'esercito e dal Law Enforcement, che si ritiene vengano utilizzati per addestrare gli altri affiliati all'uso delle armi e per insegnargli le tecniche di guerriglia. I suoi membri sono stati spesso coinvolti in aggressioni ed azioni criminali. È un gruppo noto per cercare contatti internazionali con altri soggetti di estrema destra, specialmente in Europa ed in Russia.

The Base - Gruppo di estrema destra attivo dall'estate del 2018, fondato da Rinaldo Nazzaro (cittadino americano), che richiama espressamente l'ideologia nazista ed invoca uno Stato etnico bianco, la cui fondazione può avvenire attraverso un processo terroristico di sovvertimento violento dei governi esi-

stenti. La strategia adottata è in questo caso quella di radicalizzare cellule indipendenti e lupi solitari che possano portare avanti autonomamente i loro attacchi, finalizzati alla creazione di uno Stato indipendente, eliminando le minoranze, in particolare quelle afro-americane ed ebree.

QAnon - Primo dei movimenti che non cercano una legittimazione costituzionale del loro operato, QAnon è una teoria cospirativa di estrema destra che parte dall'assunto che il mondo è governato da un Deep State (gruppo di gestione del potere di secondo livello che utilizzerebbe l'affiliazione di rappresentanti delle amministrazioni pubbliche per indirizzarne la politica ufficiale), collegato a sua volta ad un circolo internazionale di pedofili e ad una rete finanziaria in mano ai Sionisti. Tale Deep State si sarebbe opposto all'azione dell'Amministrazione Trump che sarebbe salita al potere per scardinare questo sistema. La resa dei conti avverrà in un giorno del giudizio, definito The Storm (la Tempesta) o The Great Awakening (il Grande Risveglio), in cui il Presidente in carica metterà fine allo status quo. I primi richiami a tale teoria sono cominciati ad apparire sulla piattaforma 4Chan nell'autunno del 2017 ad opera di tale Q che, allo stato attuale, potrebbe nascondere dietro tale pseudonimo un gruppo di attivisti.

4.2. QAnon dagli USA in Europa

Per quanto le teorie propugnate possano sembrare irreali e deliranti, compresa quella che identifica in Hillary Clinton uno dei massimi rappresentanti del Deep State e che, dopo la sconfitta elettorale, sarebbe stata segretamente incarcerata e sostituita da un sosia, QAnon riesce ad avere un grande seguito in rete[52]. I soggetti che fanno richiamo a tali teorie cospirazioniste sono apparsi in molte delle manifestazioni che hanno incendiato le piazze degli Stati Uniti, ma anche in quelle europee sotto la spinta della pandemia.

L'ormai noto simbolo Q ha fatto la sua prima grande entrata europea alle manifestazioni anti-Covid a Berlino, Londra e Parigi.

A Berlino estremisti di destra hanno ostentato i simboli di QAnon assieme alle bandiere del Reich durante un tentato assalto al palazzo del Parlamento. Nel corso della seconda grande manifestazione organizzata in Germania contro le misure anti-Covid a Costanza, si sono dati appuntamento gruppi

52) Nel dicembre 2020, Twitter ha chiuso circa 70.000 account legati alla teoria cospirazionista, con casi di numerosi account gestiti da un solo individuo.

di ogni colore politico e nonostante il divieto di ostentare simboli di estremismi sia stato osservato, le teorie e i principi di QAnon sono stati presenti e diffusi tra i manifestanti.

Gli esperti delle teorie complottiste sono convinti che la pandemia abbia agito come benzina sul fuoco nella diffusione di Qanon in Europa, complice l'incertezza portata dal COVID, la crisi economica e la struttura tentacolare del movimento.

Nel 2020, infatti, abbiamo tutti a nostre spese compreso come la pandemia rappresenti un biotipo perfetto per le narrazioni di cospirazione, una minaccia globale e potenzialmente fatale, con un'origine poco chiara e senza mezzi comprovati per combatterla e superarla.

Inoltre le misure di blocco e stagnazione sociale, la minaccia all'esistenza professionale e privata di molte persone, associata alla possibilità di avere molto tempo libero con poche distrazioni hanno determinato una situazione di forte instabilità anche psicologica nella società, che spesso ha trovato una via d'uscita su Internet, ove è estremamente semplice imbattersi nelle cd. ideologie del complotto.

Tali ideologie hanno il vantaggio di semplificare l'inspiegabile perché offrono facili spiegazioni. In un mondo di cospirazione, nulla accade più per caso, a tutto viene attribuita una ragione. Ci sono nozioni chiaramente definite di bene e male, e ogni individuo che ci crede può scegliere e combattere per ciò che considera buono e coraggioso. Inoltre, queste narrazioni consentono all'individuo di vedere se stesso come persona in possesso della "verità", con una missione ben precisa: quella di diffondere la narrazione "risvegliando" gli altri concittadini.

É insita in ciò la pericolosità di tale movimento: la capacità ovvero di richiamare sostenitori con ideologie differenti, senza che sia necessaria l'adesione totale ad un programma ben definito. Chi si allinea lo fa scegliendo la narrativa che più preferisce. Ci sono gli anti-sistema e gli anti-vaccino, dove le motivazioni alla base delle proteste e quelle alla base di Qanon si sovrappongono.

Ad un'analisi più approfondita è possibile riscontrare delle analogie con il mondo delle sette: nelle strategie di reclutamento anche on-line volte a far leva sulla fragilità delle persone, l' utilizzo di messaggi semplici e chiari in grado di fornire tutte le risposte, l'idea di far parte di un disegno più grande nel quale coloro che hanno risentito delle disastrose conseguenze della pandemia in termini lavorativi, psicologici e sociali riscoprono di avere un ruolo ben preciso ed un obiettivo ben definito.

Non importa aderire a tutta l'ideologia basta anche una sola idea in co-

mune per generare l'odio come l'erronea convinzione che l'assenza di occupazione sia dovuta alla presenza di stranieri sul territorio o ancora che in un prossimo futuro si assisterà ad un'inversione del tasso di natalità in cui persone di altre razze ed etnie prenderanno il sopravvento sugli altri. Tutto ciò, associato ad una disinformazione pilotata per generare divisione, isolamento e avversione nella gente, è in grado di generare confusione, paura e adesione ai movimenti più estremi che utilizzano i problemi derivanti dalla pandemia come opportunità per allargare le maglie del loro consenso sociale.

Nella pandemia stiamo assistendo anche ad una nuova ondata di diffusione di massa di narrazioni antisemite. Infatti le narrazioni di cospirazione del 2020 hanno rivolto sempre più la loro attenzione ai governi, alla scienza e ai media, cui viene attribuita una "ebraicità" aperta o nascosta, intesa anche come l'incarnazione della modernità, libertà, uguaglianza, liberalità, razionalità.

Nel 2020, le narrazioni di cospirazione sulla pandemia COVID-19 sono iniziate con il razzismo contro le persone percepite come asiatiche (poiché il virus ha avuto origine in Cina, e lo stesso ex presidente degli Stati Uniti Donald Trump ha ripetutamente parlato di "virus cinese"), la negazione dell'esistenza del virus o false storie su presunte cure. I gruppi antidemocratici hanno riconosciuto, inoltre, l'opportunità di utilizzare le narrazioni della cospirazione non solo per diffondere l'incertezza all'interno delle loro società ("Il Governo vuole davvero il meglio per noi o siamo solo soggetti di prova?"), ma anche per diffondere l'antisemitismo ("Chi c'è dietro il 5G e le campagne di vaccinazione globale e quale nuovo ordine mondiale verrà introdotto lungo il percorso?").

Questi gruppi hanno anche cercato di spingere le persone ad agire, legittimandone la violenza ("Nessuno sta facendo nulla, dobbiamo agire ora prima che sia troppo tardi per i nostri figli, se necessario armati di pistole"), per fomentare il nazionalismo ("I nostri valori e le tradizioni vengono distrutte quando tutti sono resi uguali") e diffondere instabilità mettendo in discussione la credibilità della scienza, della medicina e della stampa ("Chi li paga? Quali piani stanno portando avanti?"). Per stimolare questo stato d'animo, sono state create numerose piattaforme di "media alternativi". Anche i canali YouTube e Telegram dedicati ai temi della cospirazione COVID-19 hanno registrato una rapida crescita sia del numero che della copertura. Ad esempio, canali di estrema destra, ma anche sostenitori della medicina alternativa ed esoteristi. Il denominatore comune di tutti questi diversi gruppi è l'antisemitismo e la lotta alla democrazia parlamentare.

Il fatto che i social network siano il motore principale di questi dibattiti

non solo ha portato a una rapida radicalizzazione di tali discorsi e dei loro sostenitori, ma anche a una internazionalizzazione degli stessi, laddove il palcoscenico di queste teorie si è fatto sempre più quello internazionale. In questo scenario si collocano le continue esortazioni del Q rivolte ai seguaci a svegliarsi, pensare da soli e partecipare. Questa tecnica ha portato i sostenitori ad auspicare per la società intera un'esegesi comune, un'interpretazione collettiva, la necessità di essere uniti per formare una comunità, il che si riflette anche nel noto slogan "WWG1WGA" ("Dove andiamo uno, andiamo tutti").

In questo modo, QAnon si è sviluppato come una sorta di super cospirazione che facilmente è stata in grado di assorbire le narrazioni di cospirazione già esistenti e integrare condizioni e situazioni locali.

"Trust the Plan" è un motto chiave di QAnon: ciò che non capisci ora, è ancora corretto perché c'è un piano. Alla luce di esso anche mesi dopo le elezioni, i fan di Trump che credono in QAnon pensano che la vittoria di Joe Biden o non sia reale o faccia parte del "piano". Queste sono caratteristiche distintamente simili a quelle di una setta e dimostrano che i fan di QAnon hanno consapevolmente evitato la realtà per vivere in un mondo delirante estremamente pericoloso che negli Stati Uniti, non di rado, ha portato alla commissione di reati ed al perpetrarsi di episodi di violenza.

4.3. L'odio ai tempi del Covid: una panoramica europea

Il senso di comunità, il carattere partecipativo e l'integrazione delle narrazioni cospirative già esistenti a livello locale hanno reso QAnon attraente per tutti i movimenti antidemocratici ed estremisti anche nel vecchio Continente.

La diffusione delle narrazioni di QAnon è iniziata, infatti, in gruppi anti-UE, islamofobi, e di estrema destra in Europa, ma come sottolineato non sono mancate le narrazioni antisemite e anti-establishment, anti-governative e anti-lockdown. Inizialmente, QAnon si è diffuso in altri Paesi di lingua inglese come Regno Unito, Canada e Australia.

Nel Regno Unito, sono stati soprattutto i fan della Brexit ad aver adottato il racconto della cospirazione. Molti gruppi usano elementi di QAnon, come le storie delle élite globali o dei gruppi di pedofili, per screditare il Governo e per criticare le sue misure anti pandemia.

Subito dopo, però, le cd. "Q-Drops" sono state tradotte in varie lingue europee. La più grande comunità QAnon tra i Paesi non anglofoni esiste attualmente in Germania, che grazie anche all'utilizzo di canali Telegram, conta almeno 150.000 followers. La maggior parte dei sostenitori del movimento di

estrema destra e cospirazionista Reichsbürger ha posto le proprie storie di cospirazione sotto lo stendardo Q, arrivando ad affermare che la Repubblica federale di Germania è uno stato illegale e non sovrano, che non ha mai firmato un trattato di pace dopo la seconda guerra mondiale e non si è mai data una costituzione, motivo per cui il "Reich tedesco" dai tempi pre nazisti sarebbe ancora esistente.

La presunta protezione dell'infanzia di Q ("Save the children") ha avuto una forte risonanza anche nel mondo della cospirazione tedesca[53]. In quel Paese molti sostenitori di "Q" si definiscono "genitori preoccupati". Per decenni, il presunto impegno a proteggere i bambini dalla pedofilia è stato un problema con il quale la scena di estrema destra tedesca ha cercato, non senza successo, di colpire la società nel suo insieme, al fine di diffondere il razzismo (perché sostengono, di fronte a schiaccianti prove empiriche del contrario, che gli autori sono sempre migranti). Anche le celebrità hanno fatto la loro parte: il noto cantante pop Xavier Naidoo ha pianto in un video di YouTube nel maggio 2020 per i bambini che sarebbero stati tenuti prigionieri dalle *élite* per la produzione di sangue, rendendo così QAnon noto al pubblico mainstream più ampio possibile in Germania.

In Francia, è il movimento populista dei Gilet Gialli, critico nei confronti del Governo, ad essere interessato alla retorica e alle narrazioni di QAnon, in particolare alle narrazioni cospirative del "Deep State", che detiene le vere redini del potere politico.

Sono stati fondati gruppi "Gilet gialli contro la pedocriminalità", così come gruppi che vogliono combattere il "Nuovo ordine mondiale", un argomento antisemita che ruota attorno a piani segreti per un dominio del mondo (spesso ebraico). Anche membri della scena anti-vaccinazione francese sono presenti all'interno del movimento. I gruppi di Telegram hanno raggiunto 20.000 fan, e negli stessi il medico Didier Raoult, che raccomanda l'idrossiclorochina come farmaco COVID-19, viene celebrato come un combattente contro il presidente Emmanuel Macron. Anche la Chiesa francese è sospettata di essere "malvagia". I gruppi Q francesi si descrivono come "un gruppo di patrioti francesi, anti-globalizzazione, che fanno campagna per il risveglio del-

53) La popolarità di QAnon in Germania è cominciata intorno alla fine di febbraio 2020, quando nel Paese cominciò l'operazione Defender Europe 20, una enorme esercitazione militare che vide coinvolte migliaia di soldati americani nell'ambito della NATO. Sui social tedeschi, qualcuno iniziò a sostenere che l'operazione fosse in realtà un tentativo di Trump di "liberare" la Germania dalla cancelliera Angela Merkel.

le nazioni". Il loro obiettivo dichiarato è "informare i francesi, e più in generale, tutti i francofoni che sono manipolati dai media tradizionali, sugli interessi mondiali di oggi".

In Italia sono soprattutto i no-vax che utilizzano le teorie di Q per ribellarsi ai piani del Governo. Anche qui, i gruppi di Telegram contano fino a 20.000 membri. I fan di Q hanno attaccato l'ex Presidente del Consiglio italiano Giuseppe Conte, che, a detta loro, avrebbe voluto instaurare una dittatura, mentre lodano le politiche di estrema destra. Molto spesso tra di essi il nazionalismo viene utilizzato come pretesto per liberare l'Italia dall'UE. Anche nella manifestazione di piazza avvenuta a Roma il 6 aprile 2021, alle categorie di lavoratori scesi in piazza per manifestare civilmente contro le restrizioni dovute alla pandemia, si sono aggiunti alcune frange estremiste che cavalcano le proteste per farle degenerare in guerriglia urbana. I segnali che arrivano dalle piazze sono monitorati anche dall'intelligence. Sicuramente le frange estremiste che vanno dalla destra radicale, a realtà legate al mondo antagonista, alla galassia anarchica sino alla criminalità comune, usano la crisi sanitaria per rilanciare proteste anti sistema e fomentare disordini di piazza. In questo contesto anche se non sono comparse bandiere e simboli espliciti di Qanon, paradigmaticamente era presente un manifestante modenese, che ha evocato l'assalto a Capitol Hill, vestendo i panni dello sciamano Jake Angeli, noto per l'irruzione al Congresso Usa.

Nei Paesi Bassi, i movimenti di destra islamofobi che simpatizzano con Geert Wilders usano elementi della narrativa di QAnon e spingono i loro seguaci ad agire, con il motto: "Non fare nulla non è più un'opzione". Inoltre, una delle più importanti influencer europee di QAnon, Janet Ossebaard, originaria dei Paesi Bassi, nel suo film "Fall of the Cabal", diventato virale nel marzo 2020, ha per la prima volta collegato i motivi di QAnon e le storie di cospirazione europee.

Interessante anche l'accoglienza Q nei Paesi dell'ex Repubblica di Jugoslavia, Slovenia, Croazia, Bosnia-Erzegovina e Serbia. Qui ci sono gruppi Q nazionalisti, ma il più grande si chiama "QAnon Balkan" e vuole utilizzare QAnon per unire le persone nella regione. Il loro motto è: "Non dividiamo persone per religione e nazione, perché siamo tutti ostaggi di una manciata di globalisti, psicopatici pericolosi, che hanno messo i loro burattini a capo dei nostri Stati e istituzioni".

In Grecia, dove non ci sono molti follower attivi di QAnon, i post che utilizzano gli hashtag pertinenti mescolano narrazioni Q con pregiudizi antirom e razzismo contro i migranti neri.

In Ungheria, invece, c'è un forte legame con l'antisemitismo: Q interessa

i seguaci di cospirazioni che ruotano attorno ad adrenochrome, gli illuminati, il satanismo, lo "Stato profondo" e l'odio verso George Soros.

In Lituania, un Paese con appena 2,7 milioni di abitanti, esiste un gruppo Facebook QAnon con 7.300 membri. Nell'agosto 2020, il ricercatore canadese Marc-André Argentino ha studiato i Q-group europei nei social network, evidenziando come non ve ne sia traccia solo in Estonia, Montenegro e Albania.

Il pericolo di QAnon e altri mondi della cospirazione risiede nella costante radicalizzazione e nella costrizione o urgenza ad agire, che può sfociare in una disponibilità a usare la violenza. Quindi, "Fidati del piano" diventa improvvisamente "Sii il piano".

Anche se ciò non accade, tuttavia, resta un altro pericolo: una volta che le persone si sono abituate ai meccanismi antirazionali e antidemocratici delle ideologie del complotto, ci sono buone probabilità che le conservino, anche se abbandonano QAnon.

Conclusioni

"*Abbiamo visto una forza che avrebbe scosso il nostro Paese, anziché tenerlo insieme. Lo avrebbe distrutto, se avesse significato rinviare la democrazia. Questo sforzo è quasi riuscito. Ma se può essere periodicamente rinviata, la democrazia non può mai essere permanentemente distrutta*" (Amanda Gorman).

L'odio può distruggere ogni cosa e persino la democrazia americana che, con le sue estreme contraddizioni in termini di libertà, ricchezza, povertà e straordinarie opportunità, può essere messa in pericolo da sentimenti di disprezzo, di superiorità e di avversione. Recentemente il Presidente Biden ha scritto "Il razzismo, la xenofobia e altre forme di intolleranza non sono problemi esclusivi degli Stati Uniti. Sono problemi globali. Sotto la mia amministrazione gli Stati Uniti guideranno la discussione su queste difficili questioni in Patria, nelle istituzioni internazionali e in tutto il mondo. L'odio non può avere un porto sicuro in America. Non dovrebbe avere un porto sicuro in nessuna parte del mondo, dobbiamo unirci per fermarlo".

La storia ci ha insegnato che a volte è l'odio stesso, il male profondo che avvelena le coscienze, a svolgere suo malgrado un'azione salvifica, scatenando una rivolta morale in grado di risvegliare le potenzialità del bene. È quello che sta accadendo negli Stati Uniti di fronte al fenomeno del suprematismo che, come abbiamo analizzato, sta tentando di minare alla radice la coscienza democratica, tollerante ed inclusiva di un popolo. Questo è accaduto

infinite volte nella storia dell'umanità: dopo olocausti, guerre ed attentati l'uomo ha sempre reagito riscattandosi dal buio delle coscienze e della ragione.

Nel presente lavoro ho analizzato il fenomeno degli *hate crimes*, nella loro dimensione internazionale ed unionale, le caratteristiche criminologiche e come l'ordinamento italiano si appresta a contrastarli, recependo convenzioni e direttive internazionali.

Ho, altresì, inteso ripercorrere l'esperienza di un organismo, l'OSCAD, l'Osservatorio per la sicurezza contro gli atti discriminatori del Ministero dell'interno, unicum nel panorama europeo ed internazionale, ma soprattutto l'impegno del sistema di *law enforcement* italiano per poter sviluppare una cultura del rispetto e della non discriminazione. Nella consapevolezza che l'unico potere reale di cui dispone una democrazia non è nell'esercizio della forza da parte dello Stato ma della reputazione di cui godono le forze dell'ordine nel momento in cui sono chiamate ad esercitare quel potere.

Da funzionario di polizia ho tratteggiato i contorni tecnico giuridici dell'odio, inteso come discriminazione razziale, nazionale, etnica e religiosa, consapevole che la sensibilità del legislatore è strettamente legata alla maturità e alla sensibilità che una comunità sviluppa in un determinato momento storico. Le forme di odio non sono certamente riconducibili a solo quattro categorie, sono ovviamente molte di più e solo la maturazione della coscienza collettiva potrà portare verso un ordinamento più compiuto, in grado di includere un ben più ampio ventaglio di manifestazioni di odio. Un esempio per tutti la misoginia, l'odio verso le donne. Il femminicidio, come nel 1990 ha scritto Diana Russel nel libro realizzato insieme a Jill Radford "The politics of woman killing" è una precisa categoria criminologica: una violenza estrema dell'uomo contro la donna in quanto "donna". Ebbene a questa categoria criminologica di odio non corrisponde uno specifico *ius puniendi*, così come non esiste per l'omofobia o per la disabilità.

Noi forze di polizie, insieme con tutti gli altri attori sociali interessati, dobbiamo lavorare affinché la coscienza collettiva maturi una maggiore sensibilità ed il legislatore possa farsene interprete. Nel 1996 lo stupro di una donna era un reato contro la morale e non contro la persona ed il codice civile del 1942 all'art. 144 definiva i limiti della potestà maritale sulla moglie. Tanto è stato fatto negli anni contro questa forma di odio, e tanto ancora possiamo fare in quanto il percorso verso un diritto naturale che affranchi l'uomo e la donna dall'odio è una strada ancora molto lunga da percorrere, ma dobbiamo sempre voltarci indietro e vedere da dove siamo partiti.

E così per altre forme di odio lo stesso Aristotele, uno dei padri del giusnaturalismo, nel distinguere tra ciò che è giusto per natura da ciò che è giusto

per legge, riteneva che l'uomo nasce libero o schiavo e questo risponde ad un principio secondo natura! Nel 1960 Ruby Bridges fu la prima afroamericana a fare ingresso sotto scorta in una scuola di bianchi a New Orleans. E se pensiamo che l'Italia sia immune da queste ombre nella storia forse vale la pena citare ancora una volta il codice civile del 1942 che all'art. 91 introduceva pesantemente nel nostro ordinamento la questione razziale limitando fortemente i matrimoni misti.

Da ultimo il tema della dimensione ontologica dell'odio. L'odio è istinto e quindi risponde a leggi naturali mentre il bene è figlio della ragione e quindi della capacità di mediare e limitare i conflitti e ricercare le vie della socializzazione? Se così fosse dovremmo arrivare alla conclusione che l'odio e con esso l'aggressività e la violenza, sono espressione della natura umana e quindi un'entità costitutiva ed essenziale, mentre il bene, e con esso la mediazione e la socializzazione, sono cultura e come tale un'entità posteriore ed accessoria.

In realtà questo tema è stato ampiamente dibattuto sia in filosofia che in letteratura, potremmo quasi parlare di una dimensione filosofica dell'odio! Nella storia del pensiero filosofico prevale una visione profondamente pessimistica di ciò, che trova nel XVII secolo una delle sue massime espressioni con Thomas Hobbes il quale ritiene che l'uomo sia naturalmente feroce contro i propri simili. Nel suo *Homo homini lupus* l'unico rimedio è l'affermazione di un potere statale assoluto in grado di imporre il rispetto della reciproca convivenza contro un eterno *bellum omnia contra omnes*. Ma questo pessimismo raggiunge abissi anche più profondi nel pensiero di Nietzsche e in Schopenhauer che individua l'essenza del mondo come "volontà di vivere" e vede in essa la radice di tutti i mali. Qualcosa di simile la ritroviamo persino nel pensiero cristiano dove il peccato originale è la causa del male nell'essere umano, il libero arbitrio che allontana dal disegno divino per sua natura, armonioso e misericordioso. Ma nel Cristianesimo l'uomo è riscattato dal mistero della Grazia e dell'Incarnazione, quale momento salvifico e di redenzione.

A scrivere finalmente una parola di speranza ci pensano due etologi, Konrad Lorenz nel suo libro "Il cosiddetto male" dove parla dell'istinto all'aggressività e alla violenza come qualcosa che non può essere considerato negativamente in quanto risponde a regole di sopravvivenza, al ciclo naturale della catena alimentare. Cosa diversa è quando questo istinto diventa patologico ed insensato, e purtroppo solo l'uomo e non l'animale conosce gli abissi della violenza aberrante e fine a se stessa. A trovare un punto di equilibrio è un altro etologo, Irenaus Eibl-Eibensfeldt che, nel suo libro "Amore e Odio",

individua nell'essere umano, come egualmente presenti, tanto le potenzialità del bene che quelle del male.

Dopo questo rapido ed assolutamente non esaustivo excursus nell'odio nella sua dimensione filosofica ed ontologica occorre ritornare alla dimensione criminologica più attinente alle finalità e agli obiettivi di questo lavoro. Ma forse era necessario acquisire la consapevolezza che esiste la possibilità di una visione, ancorchè materialista ed evoluzionista, che le potenzialità del bene siano biologicamente presenti nell'essere umano altrimenti il lavoro stesso delle forze di polizia sarebbe inevitabilmente espressione di quell'autoritarismo di uno Stato di concezione hobbesiana per rendere possibile la civile convivenza. D'altra parte come sostiene Steven Pinker, docente di neuroscienze nel suo libro "Il declino della violenza", i migliori angeli della nostra coscienza, rappresentati dall'empatia, la capacità di mediazione e dalla cultura, stanno inevitabilmente prevalendo sui nostri peggiori demoni rappresentati dalla predazione, la violenza, le ideologie estreme. E questo perché le società occidentali hanno affermato principi quali l'uso statale della forza, il libero commercio e perché no, la stessa femminilizzazione della società.

Nell'avviarmi alle conclusioni e nel ripercorrere il lavoro dell'OSCAD appare evidente come la consapevolezza maturata dalle forze di polizia di dover sviluppare una cultura del rispetto e della non discriminazione, costituiscano le fondamenta di una democrazia matura. Quella italiana è un'esperienza che non ha termini di confronto in altri Paesi dove, benché le forze di polizia lavorino ispirate a solidi principi democratici, non è stata specificamente maturata un'analoga esperienza sul tema dell'odio e della non discriminazione. L'Italia ha intrapreso questa strada dieci anni fa e nel 2020, un anno terribile per la pandemia che ha scosso l'umanità intera, l'Osservatorio per la sicurezza contro gli atti discriminatori si è visto riconoscere il premio CIDU per i diritti umani per il lavoro svolto nel promuovere la cultura del rispetto, della tolleranza e della non discriminazione. Un lavoro che non è solo analisi del fenomeno, formazione, emersione del sommerso. È decisamente molto altro e molto di più, è la dimostrazione tangibile di un sistema di forze di polizia che ha maturato una coscienza democratica a volte persino superiore rispetto al sentire collettivo al punto da concorrere alla stessa crescita verso una più ampia, completa e diffusa tutela delle vittime più vulnerabili. L'odio genera mostri e provoca il silenzio delle coscienze, un sistema di forze di polizia che abbia dentro di sè gli anticorpi del rispetto e della tolleranza consente di fermare quei mostri e di ridare voce alle coscienze stesse.

Bibliografia

Akdeniz Y., *Racism on the Internet*, Council of Europe publications, 2010

Balkin J.M., *Old School/New School Speech Regulation*, 2014

Benkler Y., *La ricchezza della rete*, Milano, 2007

Bianchi C., *Hate speech. Il lato oscuro del linguaggio*, Laterza, 2021

Caruso C., *La libertà di espressione in azione. Contributo a una teoria costituzionale del discorso pubblico*, Bononia University Press, Bologna, 2014

Couldry N., *Media, Society, World: Social Theory and Digital Media Practice*, Polity Press, Bristol, 2012

De Lorenzo G., *Vittima e carnefice*, PS editore, 2020

European Union Agency For Fundamental Rights (FRA), *Esperienze e percezioni di antisemitismo. Seconda indagine sulla discriminazione e i reati generati dall'odio subiti dagli ebrei nella UE*, 2018

European Union Agency For Fundamental Rights (FRA), *Essere di colore nell'UE*, 2018

European Union Agency For Fundamental Rights (FRA), *Evitare la profilazione illecita oggi e in futuro: una guida*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2019

Ferrini C. - Paris O., *I discorsi dell'odio. Razzismo e retoriche xenofobe sui social network*, Carocci, 2019

Fronza E., *Il negazionismo come reato*, Milano, 2012

Gardini G., *Le regole dell'informazione. Principi giuridici, strumenti, casi*, Torino, 2009

Gasparini I., *L'odio ai tempi della rete: le politiche europee di contrasto all'on-line hate speech*, Jus, 2017

Goisis L., *Crimini d'odio. Discriminazioni e giustizia penale*, Napoli, 2019

Harris D.J., *Cases and Materials on International Law*, Sweet & Maxwell, Londra, 2004

Jori M., *Diritto, nuove tecnologie e comunicazione digitale*, Giuffrè, Milano, 2013

Manetti M., *L'incitamento all'odio razziale tra realizzazione dell'eguaglianza e difesa dello Stato,* in Aa.Vv., *Studi in onore di Gianni Ferrara*, Torino, 2005

Mensi M. - Falletta P., *Il diritto del web. Casi e materiali*, Padova, 2015

Monteleone R., *Le radici dell'odio: Nord e Sud a un bivio della storia*, Dedalo edizioni, 2002

Morozov E., *The Net Delusion. The dark side of internet freedom*, Public Affairs, New York, 2012

Nunziato D., *Virtual freedom*, Stanford Law Books, Stanford, California, 2009

Orofino M., *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Giappichelli, Torino, 2014
Osce, *Hate Crime Laws. A Practical Guide*, Odihr, Varsavia, 2009
Pace A., *Problematica delle libertà costituzionali*, Padova, Cedam, 2003
Pesce F., *Omofobia e diritto penale: al confine tra libertà di espressione e tutela dei soggetti vulnerabili*, in *Dir. pen. cont*., 2015
Puglisi G., *La parola acuminata. Contributo allo studio dei delitti contro l'eguaglianza, tra aporie strutturali ed alternative alla pena detentiva*, in RIDPP, 2018
Pulitano Scaffardi L., *Oltre i confini della libertà di espressione e l'istigazione all'odio razziale*, Cedam, Padova, 2009
Sunstein C., *Republic.com. Cittadini informati o consumatori di informazioni?*, Il Mulino, Bologna, 2003
Tega D., *Le discriminazioni razziali ed etniche. Profili giuridici di tutela*, Armando editore, Roma, 2011
Tesauro A., *La propaganda razzista tra tutela della dignità umana e danno ad altri*, in RIDPP, 2016
Venturoli M., *La vittima nel sistema penale. Dall'oblio al protagonismo?*, Napoli, 2015
Vigevani G.E. - Viviani Schlein M.P., *Percorsi di diritto dell'informazione*, Giappichelli, Torino, 2006
Weber A., *Manual on hate speech*, Council of Europe, 2009
Wyatt C., *Ban Racists from social media, antisemitism repost says*, BBC news, 9 febbraio 2015.
Ziccardi G., *L'odio on-line. Violenza verbale e ossessione in rete*, Milano, 2016

Webgrafia

Carta di Roma: *http://cartadiroma.org*
Coalizione Italiana: *http://cilditalia.org*
Consiglio d'Europa: *https://coe.int*
COSPE onlus: *http://cospe.org*
EUR lex: *http://eur-lex.europa.eu*
Facebook: *https://facebook.com*
Federacion sos racism: *http://sosracismo.eu*
http://adl.org/assets/pdf/combating-hate/ADL-Responding-to-Extremist-Speech-Online

http://carabinieri.it/cittadino/servizi/osservatorio-per-la-sicurezza-contro-gli-atti-discriminatori-oscad
http://coe.int/t/dghl/monitoring/ecri/Country-by-country/Italy/ITA/CbC-IV-201-002-ITA
http://conventions.coe.int/Treaty/EN/Treaties/Html
http://documenti.camera.it/leg17/dossier/Testi
http://echr.coe.int/Documents/FS_Hate_speech_ENG
http://eeas.europa.eu./delegations/council_europe/documents
http://eff.org/it/issues/cda
*http://europa.eu.int/comm/employment_social/news/2002/feb/proposal_jai_*
*http://europarl.europa.eu/meetdocs/2004_*
http://fra.europa.eu/en/promising-practices/observatory-security-against-acts-discrimination-OSCAD
http://fra.europa.eu/en/theme/hate-crime/compendium
http://fra.europa.eu/sites/default/files/fra_working_party_on_hate_crime_-meeting_report.pdf
http://hatecrime.osce.org/italy
http://humanrights.gov.au-our-work/projects-cyber-racism
http://newsone.com/979755/hate-speech-and-the-internet-a-vehicle-for-violence
https://adl.org/sites/default/files/documents/pyramid-of-hate
https://ec.europa.eu/newsroom/just/item
https://facingfacts.eu/connecting-on-hate-crime
https://facingfacts.eu/italy-systems-map-it
https://interno.gov.it/it/ministero/osservatori/osservatorio-sicurezza-contro-atti-discriminatori-oscad
https://interno.gov.it/it/stampa-e-comunicazione/pubblicazioni/guida-alle braismo-operatori-polizia
https://interno.gov.it/sites/default/files/allegati/inserto_reati_odio_-_oscad
https://osce.org/odihr/muslim-security-guide
https://poliziadistato.it/articolo/osservatorio-per-la-sicurezza-contro-gli-atti-discriminatori-oscad
https://poliziadistato.it/statics/26/quando-odio-diventa-reato
Parliamentary Assembly: *http://assembly.coe.int*
UNESCO: *http://unesdoc.unesco.org*
WebNews: *http://webnews.it*

Giurisprudenza

Cass. Pen., sez. I, sent. n. 724 del 21 gennaio 1998
Cass. Pen., sez. I, sent. n. 7812 del 16 giugno 1999
Cass. Pen., sez. III, sent. n. 7421 del 26 febbraio 2002
Cass. Pen., sez. V, sent. n. 37609 dell'11 luglio 2006
Cass. Pen., sez. III, sent. n. 37390 dell'11 ottobre 2007
Cass. Pen., sez. III, sent. n. 37581 del 7 maggio 2008
Cass. Pen., sez. II, sent. n. 16328 del 3 maggio 2012
Cass. Pen., sez. III, sent. n. 36906 del 14 settembre 2015

AVVERTENZE

La rivista è inviata gratuitamente alle Amministrazioni, Comandi e Uffici delle Forze di polizia e a tutti gli enti interessati all'attività delle Forze di polizia, con riferimento particolare ai temi del coordinamento «interforze» e della cooperazione internazionale di polizia.

I manoscritti e le pubblicazioni da recensire devono essere inviati alla Segreteria di redazione, possibilmente in duplice copia, e senza obbligo di restituzione.

È facoltà della Direzione pubblicare i manoscritti e recensire le pubblicazioni.

Direzione, Redazione e Segreteria: Piazza di Priscilla, 6
00199 Roma - Tel. 06/46524260 - 06/46524034

Registrazione presso il Tribunale di Roma n. 33 del 22 febbraio 2018
(gia registrato al n. 282 del 5 maggio 1992 e al n. 274 dell'8 maggio 1987)

Iscrizione al Registro degli Operatori di Comunicazione
n. 31195 del 19 marzo 2018

Finito di stampare nel mese di gennaio 2022
Tip. DP Printing S.r.l.
Monterotondo (Roma) - www.dpprinting.it

ISSN 2283-3048