RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0148 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Gaetana Morgante

L'estensione dello statuto penale della criminalità organizzata di stampo mafioso alla cybercriminalità diretta contro sistemi informatici e telematici "pubblici"

L'Autrice è professoressa ordinaria di Diritto penale alla Scuola Superiore Sant'Anna di Pisa

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

---

1. Il Disegno di legge AC 1717 *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* prevede un ricorso molto significativo allo strumento penalistico, da intendersi, ai fini che qui interessano, come comprensivo di tutte le componenti della complessa filiera che va dalle attività di intelligence *praeter notitiam criminis* all'esecuzione della pena comminata con condanna definitiva. Rinviando ai contributi che precedono per l'esame delle ragioni di fondo e dei contenuti sostanziali di questa scelta di politica criminale nella prospettiva multilivello degli obblighi derivanti, tra gli altri, dal recepimento della c.d. NIS 2 e dalla proposta novella del sistema penale domestico, le riforme riguardanti le più gravi ipotesi di cybercriminalità si pongono in linea di continuità con la tendenza, ormai pluriennale, del legislatore ad estendere l'ambito di applicazione delle disposizioni sostanziali e processuali previste dall'ordinamento per la prevenzione della ed il contrasto alla criminalità organizzata di tipo mafioso ad altre ipotesi di reato parimenti idonee a destare un particolare allarme sociale (si pensi, per limitarsi agli esempi più rilevanti, alla criminalità corruttiva e a quella con finalità di terrorismo). Per meglio comprendere i termini della questione e declinare in maniera conforme al principio generale di tassatività e determinatezza il significato penalistico del predetto riferimento alla *gravità* e all'*idoneità* a destare particolare allarme sociale delle più severe forme di cybercriminalità, giova ricordare come il report *Internet Organised Crime Threat Assessment* (IOCTA) curato dall'*European Cybercrime Centre* (EC3) costituito presso Europol, restituisca, sulla scorta di una complessa elaborazione di informazioni *evidence-based*, la misura e la crescente diffusività di attività criminali che, per complessità, estensione territoriale e potenzialità offensiva nei confronti di vittime individuali, collettive ed istituzionali sono ben lontane dal poter essere commesse da un singolo autore individuale su modello *lonely wolf* essendo, al contrario, riferibili ad una cybercriminalità organizzata sempre più caratterizzata dalla costituzione

e dallo sviluppo di un vero e proprio ecosistema criminale radicato e multiforme. L'ampia casistica esaminata anche grazie all'intensa cooperazione internazionale tra le agenzie di *law enforcement* consente di dar conto della frequente organizzazione di strutture che riflettono il modello della holding operante a livello globale e dedita a varie forme di attività criminali transnazionali grazie ad una struttura ideata, sviluppata e finanziata con un approccio *competence-based* assolutamente inedito ai tradizionali studi ed alle consolidate analisi – anche empiriche - sulla criminalità organizzata di tipo mafioso. L'elevato livello di competenze tecniche richieste per porre in essere le tre principali forme di cybercriminalità organizzata menzionate da Europol, vale a dire i *cyberattacks*, l'*on line fraud* e la *child sexual exploitation*, rende necessario che il *business plan* del gruppo criminale si sviluppi, innanzi tutto, attraverso un vero proprio servizio HR di cui fanno parte i reclutatori di coloro che sviluppano, forniscono e sono in grado di utilizzare tecnologie funzionali alla commissione dei reati. Sono, poi, sviluppate attività, per così dire para-finanziarie che vanno dal *fund raising* all'analisi economica di costi e capacità di produzione di *economic gain* dei reati pianificati. Non mancano, inoltre, competenze più strettamente *legal* volte, anche grazie alla complicità di professionisti in situazioni talvolta limitrofe a quelle del c.d. *grey market* in ragione della possibilità del coinvolgimento di soggetti operanti, anche, in contesti leciti, a fornire ai gruppi criminali consulenze utili ad eludere le indagini delle Autorità competenti e rimodulare con estrema rapidità, ove necessario, i *pattern* di realizzazione dei reati per evitarne l'emersione. Si tratta, come rilevato, di uno schema strutturale in gran parte inedito in quanto caratterizzato, ad un tempo, dalla suddivisione in ruoli tipica dell'associazionismo criminale di tipo mafioso ma anche dalla struttura pulviscolare caratteristica della criminalità organizzata terroristica con una graduazione dell'elemento dell'*intuitus personae*, pure tipico dei gruppi *mafia-type*, a seconda delle esigenze del piano criminale dall'estensione massima che riguarda il consulente che fornisce la tecnologia da utilizzare per la realizzazione dei reati al rilievo minimo dell'hacker che presti in forma anonima i suoi servizi limitando, spesso, il suo coinvolgimento ad un solo segmento dell'*iter criminis*. L'identificazione degli elementi di gravità, per così dire, criminologica di queste forme di cyberorganizzazione illecita si affianca, nel Disegno di legge AC 1717, a presupposti maggiormente riferiti alle vittime come risulta dall'analisi integrata delle disposizioni del disegno e delle leggi complementari variamente richiamate.

2. Traendo le mosse dall'art. 18 del DDL, modificativo dell'art. 13 del d.l. 13 maggio 1991, n. 152 (convertito in legge 12 luglio 1991, n. 203 e recante, per l'appunto, provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa) laddove inserisce il nuovo comma 3-*bis*, emerge la previsione dell'estensione delle disposizioni di cui ai commi 1, 2 e 3 del decreto medesimo relative alla *disciplina delle intercettazioni di conversazioni e comunicazioni* anche quando si procede con riferimento ai delitti, consumati o tentati, previsti dall'art. 371-*bis*, co. 4-*bis* c.p.p. (a sua volta introdotto dall'art. 2-*bis* co. 3, lett. b) del d.l. 10 agosto 2023, n. 105, convertito in l. 9 ottobre 2023, n. 137) per i quali il procuratore nazionale antimafia e antiterrorismo esercita le funzioni di impulso e coordinamento dell'attività nei confronti dei procuratori distrettuali. Si tratta, in particolare, dei procedimenti per i delitti di cui agli artt. 615-*ter*, terzo comma, 635-*ter* e 635-*quinquies* c.p. nonché, «quando i fatti sono commessi in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità», in relazione ai procedimenti per i delitti di cui agli artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p. Analoga estensione dello statuto sostanziale e processuale dei delitti in materia di criminalità organizzata si prevede in almeno altri due ambiti paradigmatici della normativa in materia. Il primo è costituito dalla protezione dei collaboratori di giustizia laddove con l'articolo 17 si introducono modifiche al d.l. 15 gennaio 1991, n. 8 prevedendo che le disposizioni aventi ad oggetto il procedimento di assegnazione delle speciali misure di protezione e i benefici penitenziari previsti per i collaboratori ed i testimoni di giustizia di cui al comma 1 (lettere a, b e c) siano estese anche agli autori dei reati informatici modificati o introdotti con il DDL, i quali collaborando con l'autorità giudiziaria si trovino in grave pericolo per le forme di cooperazione attivate o le dichiarazioni rilasciate. A tal ultimo proposito, con l'articolo 20 del Disegno di legge si apportano modifiche alla l.

11 gennaio 2018, n. 6 ed in particolare al comma 2 dell'articolo 11, relativo al procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, al fine di prevedere che la Commissione centrale richieda il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, non solo per le fattispecie delittuose di cui all'art. 51, commi 3-*bis*, 3-*ter* e 3-*quater* c.p.p., ma anche nel caso di cybercrimes di cui all'art. 371-*bis*, comma 4-*bis* c.p.p. Si prevede, altresì, un allungamento a due anni dei termini di durata massima delle indagini preliminari, oltre che per i delitti di criminalità organizzata, anche per i delitti previsti dagli artt. 615-*ter*, 615-*quater*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quater*.1 e 635-*quinquies* c.p., «quando il fatto è commesso in danno di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico». Giova, altresì, menzionare l'estensione ai cybercrimes di cui all'art. 371-*bis*, co. 4-*bis* dei benefici penitenziari di cui all'art. 16-*novies* l. 15 marzo 1991, n. 82 (art. 17, co. 1, lett. c) del DDL). In particolare, si prevede che nei confronti delle persone condannate per uno dei gravi delitti informatici or ora menzionati, analogamente a quanto disposto per i delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale o per uno dei delitti di cui all'art. 51, co. 3-*bis* c.p.p., possano essere disposte la concessione delle circostanze attenuanti previste dal codice penale o da disposizioni speciali, la liberazione condizionale, la concessione dei permessi premio e l'ammissione alla misura della detenzione domiciliare qualora abbiano prestato, anche dopo la condanna, taluna delle condotte di collaborazione di cui all'art. 47-*ter* del regolamento penitenziario.

3. L'enfasi posta nel Disegno di legge sulla combinazione tra il sensibile innalzamento delle pene edittali e l'estensione dell'applicazione delle disposizioni in materia di indagini preliminari, mezzi di ricerca della prova, processo e misure premiali ai collaboratori di giustizia consente di recuperare, pur se non espressamente emergente dalla formulazione letterale delle disposizioni che lo compongono, il rilievo del carattere "organizzato" degli autori del reato nella selezione, conforme ai principi di tassatività e determinatezza, delle più gravi ipotesi di cybercrimes. Il carattere spiccatamente multiforme e la rapidità ad adattarsi alle necessità poste dall'attuazione del loro piano criminale e delle sempre mutevoli forme di elusione dei controlli operati da parte delle Autorità preposte a livello nazionale e globale rende la segretezza e la complessità dei cybergruppi criminali una sorta di condizione di esistenza e sopravvivenza. Non è infrequente che gruppi criminali diversi collaborino per la realizzazione di alcune attività sfruttando la loro localizzazione geografica e massimizzando la capacità di eludere le investigazioni. Da questo angolo visuale la cybercriminalità organizzata può giovarsi di alcuni *booster* di segretezza che preservano la cifra oscura che affligge questa materia ed ha motivato il rilievo, posto dal DDL, sugli obblighi di segnalazione e denuncia degli attacchi. Si tratta, innanzi tutto, per limitarsi ad uno degli aspetti più significativi, del *dark web* che risulta singolarmente funzionale a supportare l'intero *iter criminis* dalla fase genetica del reclutamento e della ricerca delle tecnologie utili alla commissione dei reati, alla fase in itinere dell'individuazione e del raggiungimento dei target più numerosi di vittime ai, non infrequenti, casi di erogazione di servizi di *continous monitoring* delle attività poste in essere (cross border e non) all'occultamento dei proventi del reato e dei rispettivi responsabili. Emerge, dunque, la necessità di un intervento sinergico e multistakeholder che faccia leva, ad un tempo, sull'emersione degli attacchi, sullo sfruttamento di tutti gli strumenti sostanziali e processuali messi a disposizione dalla legislazione in materia di contrasto alla criminalità organizzata, alla predisposizione di incentivi fino alla concessione di misure di protezione per i casi di dissociazione e alla collaborazione di coloro che, essendo intranei all'organizzazione criminale, possono fornire alle Autorità procedenti informazioni altrimenti difficili da reperire. La predetta scelta di politica criminale si inscrive nel *carrot and stick approach* che, a livello domestico così come europeo ed internazionale, esprime una delle cifre più caratteristiche dell'intervento penale in materia di criminalità organizzata. Non mancano, invero, come anche nella tormentata storia dell'introduzione e delle numerose riforme intervenute nel sistema di contrasto della criminalità organizzata di tipo mafioso, rilievi di ordine generale in merito all'accettabilità, si consenta, etica prim'ancora che giuridica di

un patto volto a favorire la *criminal disclosure* da parte degli autori di gravi reati. Pur non essendo questa la sede per approfondire un tema di tale complessità, l'impianto generale del DDL risulta condivisibile nella ricerca di un sostenibile equilibrio tra la prevenzione delle più gravi forme di cybercriminalità organizzata anche attraverso azioni di capacity building volte ad aumentare la resilienza di tutti i soggetti potenzialmente coinvolti nelle diverse vesti di componenti di agenzie di law enforcement o di potenziali vittime a vari livelli di cybervulnerabilità, l'innalzamento della risposta sanzionatoria sulla scorta della funzione di prevenzione generale negativa della pena e, *last but not least,* l'incentivo a chi sia stato coinvolto nelle più gravi forme di *organized cybercrimes* a dissociarsi e collaborare con l'Autorità procedente. L'approccio multistakeholder risulta, infine, cruciale nel colmare il gap che spesso drammaticamente caratterizza la capacità e la tempestività di *detection* e *reaction* del sistema e l'attitudine dei gruppi criminali a rispondere *real time* agli ostacoli all'attuazione del rispettivo piano criminale. A tale scopo la circolarità del flusso informativo suggerito dall'art. 21 del Disegno di legge appare particolarmente efficace laddove, per un verso, prevede la riforma del comma 4 dell'art. 17 della l. 4 agosto 2021, n. 109 stabilendo che il personale dell'ACN addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, rivesta la qualifica di pubblico ufficiale con la conseguenza che la trasmissione immediata delle notifiche di incidente ricevute all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione costituisce adempimento dell'obbligo di cui all'art. 331 c.p.p. e, per altro verso, che quando acquisisce la notizia dei delitti di cui all'art. 371-*bis*, co. 4-*bis* c.p.p., il pubblico ministero ne dia tempestiva informazione all'Agenzia sempre assicurando il raccordo informativo con l'appena ricordato organo del Ministero dell'interno. L'ambizione risulta, dunque, per quanto specificamente attiene alla prevenzione e al contrasto della cybercriminalità organizzata, quella di un processo di *law enforcement by design* ove, facendo ricorso alle *best practice* del sistema italiano di prevenzione e contrasto della mafia e sfruttando l'innovazione tecnologica sostenuta anche dall'Agenzia per la Cybersicurezza Nazionale, le attività maggiormente a rischio poste in essere dai soggetti potenzialmente più vulnerabili siano *ab origine* svolte, *rectius* disegnate, in modo da essere quanto più resistenti e resilienti ed opporre all'organizzazione criminale un'altrettanta efficace organizzazione della risposta (anche penale) del sistema.

Riferimenti bibliografici

G. Amarelli (2018), *Contiguità mafiosa e controllo penale: dall'euforia giurisprudenziale al ritorno alla legalità*, in G. Acocella (a cura di), "Materiali per una cultura della legalità", Giappichelli, 2018

A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di) (2023), *Cybercrime*, Utet, 2023

A. Di Nicola (2022), *Towards digital organized crime and digital sociology of organized crime*, in "Trends in Organized Crime", May 2022

C. Fijnaut (2008), *Controlling Organized Crime and Terrorism in the European Union*, in M.C. Bassiouni, V. Militello, H. Sarzger (eds.), "European cooperation in penal matters: issues and perspectives", Cedam, 2008

F. Hagan (2006), *"Organized crime" and "organized crime": Indeterminate problems of definition*, in "Trends in Organized Crime", vol. 9, 2006, pp. 127-137

J.B. Jacobs (2020), *The Rise and Fall of Organized Crime in the United States*, in "Crime and Justice", vol. 9, 2020, pp. 17-67

M. Joutsen (2006), *The European Union and Cooperation in Criminal Matters: the Search for Balance*, HEUNI Paper 25, 2006

A. Lavorgna (2020), *Organized crime and cybercrime, in The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan, 2020

S. Lupo (1996), *Mafia*, in "Enciclopedia delle Scienze Sociali", Treccani, 1996

V. Militello, B. Huber (2001), *Towards a European Criminal Law Against Organised Crime. Proposals and Summaries of the Joint European Project to Counter Organised Crime,* Iuscrim, 2001

V. Mitsilegas (2001), *Defining Organised Crime in the EU: the Limits of European Criminal Law in the Area of "Freedom, Security and Justice*, in "European Law Review", vol. 26, 2001

M. Romanelli (2019), *Criminalità organizzata e terrorismo: la circolazione dei modelli criminali e degli strumenti di contrasto*, in "Sistema penale", 20 dicembre 2019

F. Spiezia (2020), *Attacco all'Europa. Un atlante del crimine per comprendere le minacce, le risposte, le prospettive*, Piemme, 2020

E. Viano (a cura di) (2016), *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, Springer, 2016

C. Whelan, D. Bright, J. Martin (2024), *Reconceptualising organised (cyber)crime: The case of ransomware*, in "Journal of Criminology", vol. 57, 2024, n. 1