RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0244 • articolo non sottoposto a peer review • pubblicato in anteprima il 27 gen. 2026

Gaetana Morgante – Gaia Fiorinelli

Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e *law enforcement*

Introduzione

G. Morgante è professoressa ordinaria in Diritto penale alla Scuola Superiore Sant'Anna di Pisa
G. Fiorinelli è ricercatrice t.d. in Diritto penale alla Scuola Superiore Sant'Anna di Pisa

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

La sezione monografica "Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement" raccoglie i contributi di diversi *team* di ricerca coinvolti nel Progetto PNRR "Partenariato Esteso" PE7 *SERICS – SEcurity and RIghts in the CyberSpace*, finanziato dall'Unione europea – Next Generation EU – Spoke 1 – *CybeRights* – WP4 (*Cybercrime e Cyberdiplomacy*).

In particolare, il gruppo di ricerca multidisciplinare afferente al WP4 – che riunisce la Scuola Superiore Sant'Anna di Pisa, l'Università di Trento, l'Università degli Studi di Napoli Federico II, l'Università degli Studi di Verona e l'Università degli Studi di Milano – contribuisce allo sviluppo di un concetto integrato e olistico di cybersicurezza, quale obiettivo generale del progetto *CybeRights*, mediante le competenze e gli strumenti concettuali del diritto penale sostanziale e processuale, della criminologia, del diritto internazionale e delle scienze politiche e strategiche.

La transizione digitale che connota in modo pervasivo l'epoca attuale esercita, infatti, un profondo impatto sul fenomeno criminale, generando nuove vulnerabilità, nuove opportunità delittuose e dinamiche inedite di vittimizzazione, che si manifestano in uno spazio strutturalmente svincolato dai confini geografici e giurisdizionali. In questa prospettiva, i modelli penalistici di prevenzione e contrasto dei reati informatici, ai danni di individui, imprese, amministrazioni pubbliche e infrastrutture critiche, richiedono un ripensamento sostanziale, in dialogo costante con la ricerca criminologica, al fine di elaborare strumenti di tutela più efficaci e concettualmente solidi. Parallelamente, il panorama delle fonti sollecita un rinnovato sforzo di sistemazione teorica, sviluppandosi entro strutture multilivello sempre più articolate, che sovrappongono cooperazione internazionale, armonizzazione europea e interventi nazionali, ai quali si affiancano forme di regolazione privatistica o tecnologica, in un quadro di co-regolazione pubblico-privata. A fronte di un "arsenale" penalistico così articolato, l'analisi dei dati giudiziari restituisce, per converso, con particolare efficacia le difficoltà di *enforcement* del diritto penale nel cyberspazio, a partire dalle criticità nell'identificazione degli autori dei reati, nell'attribuzione degli attacchi e, in definitiva, nell'emersione di un fenomeno criminale che rimane caratterizzato da una consistente cifra oscura.

Del resto, la transizione digitale produce altresì un significativo impatto sui profili procedurali e sui poteri e mezzi d'indagine, aprendo a nuove modalità d'investigazione sui reati informatici (e non): accanto a un'inedita esigenza di standardizzazione delle tecniche di raccolta, conservazione e utilizzazione delle prove digitali, ciò pone l'urgente necessità di un bilanciamento di tali pratiche con la salvaguardia dei diritti fondamentali. Invero, la digitalizzazione dei poteri investigativi contribuisce indubbiamente al (necessario) incremento della loro efficienza ed efficacia, ma impone di mitigarne la strutturale intrusività, nel complesso scenario della cooperazione internazionale, europea e pubblico-privata.

Proprio con riferimento a quest'ultimo profilo, non può trascurarsi come la criminalità digitale assuma progressivamente un rilievo sempre maggiore al livello delle relazioni internazionali e delle dinamiche geopolitiche, collocandosi in un'area di confine in cui sfumano le distinzioni tra atti criminali e atti di natura bellica, mentre anche la morfologia delle sanzioni si trasforma (si pensi, ad esempio, al c.d. *EU Cyber Diplomacy Toolbox*, che ha istituito forme di risposta sul piano *diplomatico* rispetto alle attività informatiche dolose). Il diritto internazionale si intreccia così stabilmente con il diritto penale sostanziale e processuale, quale piano della cooperazione ma anche quale autonoma fonte di disciplina delle condotte nel cyberspazio, richiedendo lo sviluppo di strumenti analitici per interpretare le tendenze emergenti e i futuri scenari di applicazione delle tecnologie informatiche alla sicurezza e alla difesa internazionale.

Nelle prospettive indicate, lo stesso concetto di cybersicurezza si scompone in un prisma di significati: (nuovo) bene giuridico da tutelare, condizione per la protezione dei diritti individuali e collettivi nel cyberspazio, fondamento e limite delle indagini digitali, nonché dimensione strategica per il diritto e le relazioni internazionali.

I contributi raccolti in questa Sezione monografica si inseriscono in questo quadro, con l'obiettivo di offrire una prospettiva critica sulle trasformazioni del fenomeno criminale nello spazio digitale, sulla necessità di un assestamento concettuale e assiologico nel diritto penale, sulle nuove dimensioni della cooperazione e sull'applicazione del diritto internazionale, nonché sul ruolo delle piattaforme digitali e sul coordinamento dei poteri investigativi nel rispetto delle garanzie costituzionali dell'ordinamento multilivello.