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

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0252 • articolo sottoposto a peer review • pubblicato in anteprima il 13 gen. 2026

Sara Lilli

I dati come nuova valuta del cybercrime: mercati criminali, attori e responsabilità penale nell'economia digitale illecita

(Analisi a partire dal report di EUROPOL, IOCTA, 2025)

Il presente contributo si propone di esaminare l'emersione del dato quale risorsa centrale dell'economia criminale digitale, ricostruendo – a partire dal report di Europol IOCTA 2025 (*Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data*) – le dinamiche che ne favoriscono sottrazione, circolazione e sfruttamento sistematico. Lo studio si articola lungo due direttrici:(i) l'analisi della dimensione economico-criminologica del dato, inteso come target, mezzo e merce all'interno dell'*underground data economy*; (ii) la ricostruzione della filiera illecita degli *stolen data* nelle sue fasi di estrazione, distribuzione e riutilizzo, con particolare attenzione alla specializzazione degli attori coinvolti e agli ambienti di scambio. L'analisi consente così di mettere in luce il ruolo autonomo che il dato acquisisce nei processi criminali nel cyberspazio, nonché le conseguenti ricadute sull'impianto e sull'efficacia della tutela penalistica, chiamata a confrontarsi con forme di aggressione ai beni digitali che eccedono gli schemi tradizionali.

Cybercrime – Dati – Mercati illeciti online – Europol – Attori malevoli

Data as the new currency of cybercrime: criminal markets, actors and criminal liability in the illicit digital economy

This contribution examines the emergence of data as a central resource within the digital criminal economy, reconstructing – on the basis of Europol's IOCTA 2025 report (*Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data*) – the dynamics that enable its systematic theft, circulation and exploitation. The study develops along two lines of inquiry: (i) an analysis of the economic and criminological dimension of data, understood as target, tool and commodity within the underground data economy; (ii) the reconstruction of the illicit supply chain of stolen data across its phases of extraction, distribution and reuse, with particular attention to the specialisation of the actors involved and to the environments in which exchanges take place. The analysis highlights the autonomous role that data acquires within criminal processes in cyberspace, as well as the resulting implications for the structure and effectiveness of criminal-law protection, which is increasingly required to address forms of aggression against digital assets that fall outside traditional doctrinal frameworks.

Cybercrime – Data – Illicit online markets – Europol – Malicious actors

L'Autrice è dottoranda del Programma di Interesse Nazionale in Cybersecurity, affiliata presso la Scuola Superiore Sant'Anna di Pisa e la Scuola IMT Alti Studi di Lucca

La ricerca si inserisce nell'ambito del Progetto PNRR "Partenariato Esteso" PE 7 SERICS Security and Rights in the Cyber Space/ Spoke 1: Progetto CybeRights Codice identificativo: M4C2 11.3 - PE0000014 - CUPJ53C22003110001

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

Sommario: 1. Introduzione. – 2. La dimensione economica e criminologica del dato. – 2.1. Il dato come target. – 2.2. Il dato come mezzo. – 2.3. Il dato come merce. – 3. Lungo la filiera criminale degli *stolen data*. – 3.1. Estrazione. – 3.2. Distribuzione. – 3.3. Riutilizzo. – 4. Osservazioni conclusive.

1. Introduzione

Nell'analizzare le dinamiche contemporanee del cybercrime[1], emerge con particolare evidenza il ruolo centrale assunto dai dati personali[2], divenuti – oramai – non soltanto oggetto di tutela[3], ma anche vero e proprio strumento e prodotto dell'economia criminale. L'ultimo rapporto di Europol (*Internet Organised Crime Threat Assessment, 2025*)[4] dedica un'analisi specifica ai crescenti *illicit data markets*[5], mettendo in luce come l'informazione costituisca ormai una risorsa strategica contesa fra attori leciti e illeciti. Il dato viene sottratto, scambiato e utilizzato nuovamente come merce – una *commodity*

1. Sul punto, Wall 2024.
2. Per la definizione di dato personale occorre fare riferimento all'art. 4, n. 1, del Regolamento (UE) 2016/679 (GDPR), che qualifica come tale "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Quanto alla normativa interna, il richiamo è all'art. 4, comma 1, lett. b) del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali o codice privacy), che definisce il dato personale come "Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".
3. La crescente pervasività delle tecnologie digitali e la conseguente espansione della sfera informazionale dell'individuo sono state da tempo identificate in dottrina quali fattori di accresciuta vulnerabilità dell'identità personale nello spazio digitale, in questa prospettiva, si veda, *ex multis*, Gambini 2013, secondo cui "nella società dell'informazione, la grande quantità di dati personali generati dall'odierno mondo elettronico, combinata con le nuove tecnologie a disposizione, che rendono sempre più sofisticati e meno facili da rilevare gli strumenti di raccolta e trattamento delle informazioni personali, aumentano in modo esponenziale i rischi di esposizione delle persone a forme illegittime di intrusione nella propria sfera privata e di spoglio della propria identità".
4. Cfr. Europol 2025.
5. Cfr. Garkava–Moneva–Leukfeldt 2024.

– capace di generare valore economico, divenendo così una valuta funzionale al finanziamento e alla perpetuazione, nonché proliferazione, di attività criminali di natura transnazionale. La pervasiva digitalizzazione delle attività quotidiane e la progressiva interoperabilità dei sistemi informativi, tanto pubblici quanto privati, hanno determinato un ampliamento esponenziale della massa di informazioni suscettibili di esposizione a condotte criminose. In tale contesto, i dati personali, finanziari e tecnici – dalle credenziali di autenticazione alle informazioni di pagamento, sino agli elementi funzionali al governo di infrastrutture critiche – sono oggi al centro di un ecosistema illecito complesso, in cui differenti soggetti cooperano secondo logiche di specializzazione e interdipendenza.

Come rileva Europol, la possibilità di aggregare informazioni eterogenee e di sottoporle a processi di rielaborazione tramite sistemi di intelligenza artificiale generativa ha accresciuto in misura esponenziale la capacità trasformativa del dato sottratto, conferendogli una duttilità funzionale che ne moltiplica gli impieghi e ne amplifica la pericolosità. È su questo terreno, mobile e sfuggente, che si misura oggi una delle sfide più delicate per il diritto penale e per l'ordinamento dell'Unione europea: stabilire in che modo un'entità intangibile priva di consistenza fisica, ma dotata di un valore economico e strategico crescente, possa divenire simultaneamente oggetto di appropriazione[6], di circolazione e di condotte penalmente rilevanti.

In tale prospettiva, la riflessione sul dato si pone come passaggio necessario per indagare, nel prosieguo, circa la sua dimensione economica e criminologica, quella cioè che consente di coglierne la traiettoria – dal trattamento lecito allo sfruttamento illecito – all'interno di un sistema di mercato parallelo e che riproduce, *mutatis mutandis*, le logiche del cosiddetto *illicit data ecosystem*[7].

2. La dimensione economica e criminologica del dato

L'analisi di Europol mostra come il processo di sfruttamento del dato – sottratto – confluisca nella più ampia *underground economy*[8], vale a dire quell'area dell'economia digitale connotata da opacità strutturale e assenza di regolazione, nella quale si replicano logiche di mercato proprie dei contesti leciti. I circuiti che la compongono, difatti, si articolano secondo schemi tipici delle economie di piattaforma: divisione del lavoro, strutture reputazionali, meccanismi di *trust–building* e intermediazione tecnica[9]. Tali elementi contribuiscono a consolidare un ecosistema criminale strutturato, dove alcuni soggetti si occupano di ottenere l'accesso ai sistemi informatici compromessi (*initial access brokers*), altri di aggregare e organizzare le informazioni (*data aggregators* o *data brokers*), mentre ulteriori figure si dedicano alla rivendita o al riutilizzo dei dati in attività fraudolente (*end-user criminals*).

Sotto il profilo criminologico, la logica del profitto si innesta su un'infrastruttura tecnologica che consente al dato di assumere una natura riproducibile, potendo essere replicato infinite volte senza perdita di qualità e costi quasi nulli, non rivale, poiché l'uso di un dato da parte di uno non ne impedisce l'utilizzo anche da parte di altri, e cumulativa, in quanto il dato accresce di valore quando lo si

6. Non può essere taciuto, in questa sede, l'approdo cui è pervenuta la giurisprudenza di legittimità, nel ricondurre i dati informatici nell'alveo delle "cose mobili". In una pronuncia divenuta ormai riferimento imprescindibile, la Corte ha affermato che "i dati informatici, contenenti files, [sono] qualificabili 'cose mobili' ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la *sottrazione* da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati e alla restituzione del computer 'formattato'", secondo la ratio per cui "il file, pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano l'esistenza di unità di misurazione della capacità di un file di contenere dati e la differente grandezza dei supporti fisici in cui i files possono essere conservati e elaborati"; v., in dottrina, Costabile 2005.
7. Sul punto, Howell–Fisher–Muniz et al. 2023; cfr. Europol 2025.
8. Cfr. Yip–Shadbolt–Tiropanis–Webber 2012; Greco–Greco 2020, nonché, in chiave ricostruttiva, Tanzi 1983.
9. Sul punto, Howell–Fisher–Muniz et al. 2023, pp. 298-300; Holt 2013.

combina con altri dati (si pensi ai dati anagrafici, i quali diventano più preziosi se associati a dati bancari o medici). L'informazione, privata del suo contesto originario, viene difatti reimpiegata in catene criminali complesse, ove la distinzione tra autore materiale, intermediario e beneficiario tende a sfumare. L'organizzazione delle condotte risponde a logiche imprenditoriali: il furto di dati (fase di *acquisition*) si collega alla rivendita (*distribution*), fino al reimpiego (*exploitation*), contribuendo ad alimentare un modello di *crime-as-a-service*[10] in cui l'informazione costituisce il prodotto principale. Ebbene, nei mercati *darknet* e nei forum specializzati, i dati vengono offerti secondo criteri di qualità, attualità e verificabilità[11], con un valore che varia in base alla tipologia – dati personali, finanziari, tecnici, aziendali – e al potenziale di impiego fraudolento. In tal senso, il dato opera quale vera e propria valuta criminale: è mezzo di pagamento, garanzia di credibilità e strumento di investimento all'interno di un'economia criminale che utilizza la criptovaluta come infrastruttura finanziaria primaria[12].

Il dato, in questo scenario, si configura simultaneamente come obiettivo, mezzo e merce: obiettivo degli attacchi, strumento per commettere ulteriori reati e merce di scambio in un'economia criminale digitalizzata.

2.1. Il dato come target

Alla luce dell'analisi svolta, il rapporto *IOCTA 2025*, individua proprio nella progressiva *datafication*[13] delle attività economiche e sociali la condizione abilitante che ha reso l'informazione digitale il *bersaglio privilegiato* di gruppi criminali organizzati operanti nello spazio cibernetico, e attivi tanto nei contesti finanziari quanto in quelli geopolitici.

Il dato diviene *target* poiché consente il conseguimento di ulteriori utilità criminali: il suo possesso permette di accedere a identità digitali, reti infrastrutturali, informazioni riservate e risorse economiche. Le intrusioni informatiche odierne non mirano soltanto al danneggiamento dei sistemi, ma alla esfiltrazione selettiva di informazioni suscettibili di sfruttamento o monetizzazione, innestandosi, *ab origine*, in un più ampio processo economico-criminale. Le campagne di *phishing*, i *data breaches* su larga scala, le violazioni di credenziali e i furti di identità costituiscono, ad oggi, le principali modalità di aggressione, spesso accompagnate da sofisticate tecniche di ingegneria sociale volte – anche – a indurre la vittima a fornire volontariamente dati personali. L'interesse criminale verso il dato quale *target* si articola lungo diverse categorie informative, tra loro accomunate dalla suscettibilità a generare valore illecito:

- *dati personali*, ossia informazioni idonee a identificare, anche indirettamente, un individuo (nome, indirizzo, credenziali di accesso, identificativi digitali), la cui appropriazione consente la duplicazione o l'usurpazione dell'identità, facilitando condotte di frode informatica, impersonificazione e abuso di identità;
- *dati finanziari*, quali numeri di carte di pagamento, credenziali bancarie o portafogli digitali, immediatamente monetizzabili nei circuiti dell'economia sommersa;

10. In proposito, il modello del *Cybercrime-as-a-Service* (CaaS) rappresenta una forma evoluta di criminalità informatica, fondata sulla vendita o noleggio di strumenti, competenze e infrastrutture digitali destinati alla realizzazione di reati nel cyberspazio. Il termine as-a-service trae origine da linguaggio informatico – ed economico – del *cloud computing* e si fonda sull'erogazione di risorse e competenze informatiche da parte di fornitori esterni, così permettendo a imprese e utenti di accedere a servizi digitali preconfigurati. Allo stesso modo, in ambito criminale, gli autori di reati possono acquistare o affittare servizi illeciti – come pacchetti di *malware*, accessi a sistemi compromessi o intere campagne di *phishing* – da fornitori specializzati che li mettono a disposizione su piattaforme dedicate. In tal modo, il *CaaS* trasforma l'attacco informatico in un vero e proprio mercato criminale strutturato, basato su logiche economiche di domanda e offerta, in cui la specializzazione dei fornitori e la riduzione delle competenze tecniche necessarie favoriscono la diffusione e la professionalizzazione delle attività illecite. Cfr. Akyazi–Van Eeten–Gañán 2021; Wall 2015; Europol 2023.
11. V. Howell–Fisher–Muniz et al. 2023, p. 302 ss.
12. V. Holt–Smirnova 2014.
13. Sul concetto di "*datafication*" v. Mejias–Couldry 2019.

– *dati tecnici o di sistema*, comprendenti codici di accesso, configurazioni di rete e credenziali amministrative, funzionali a movimenti laterali nei sistemi, escalation di privilegi o all'innesco di attacchi *ransomware*;
– *dati aziendali*, ossia insiemi informativi prodotti o detenuti da un'organizzazione nello svolgimento dell'attività economica, spesso dotati di rilevanza strategica o competitiva[14].

Secondo questa prospettiva, il dato quale *target* si configura come il punto di innesto di una catena criminosa che trascende la singola intrusione: l'informazione acquisita costituisce, simultaneamente, l'epilogo dell'aggressione e il presupposto funzionale di ulteriori fasi dell'iter delittuoso.

2.2. Il dato come mezzo

L'informazione sottratta non è mai statica: una volta fuoriuscita dal contesto originario, essa viene sottoposta a successive operazioni di (ri)utilizzo, arricchimento e rielaborazione, divenendo materia prima per finalità economiche, estorsive o strategiche. Le credenziali di accesso, i dati di pagamento e le informazioni aziendali, ad esempio, fungono da strumenti operativi idonei a condurre attacchi mirati (*targeted attacks*), a veicolare *malware* e a costruire campagne di disinformazione e manipolazione digitale. Il valore economico del dato si manifesta, inoltre, nella funzione abilitante rispetto ad altre forme di criminalità. Secondo Europol, i dati compromessi costituiscono la base operativa per attacchi *ransomware*, frodi finanziarie, attività di spionaggio industriale e sfruttamento sessuale minorile.

"Personal data is particularly valuable to the perpetrators […] as preparatory means of achieving their criminal goals"[15]: i dati personali costituiscono dunque mezzi preparatori, idonei a facilitare – e spesso a rendere possibile – la realizzazione dell'offesa principale. Si pensi alle frodi online, ad esempio, informazioni quali età, interessi, localizzazione, indirizzi e-mail, numeri di telefono, date di nascita o dati di pagamento consentono ai criminali di costruire profili accurati delle vittime, aumentando la verosimiglianza delle narrative fraudolente e facilitando l'accesso non autorizzato ai conti o alle risorse finanziarie dei soggetti colpiti; allo stesso modo, ovvero in ambito di *child sexual exploitation*, la disponibilità di informazioni personali consente l'individuazione, l'adescamento o la manipolazione di soggetti vulnerabili, accrescendo la portata offensiva dell'azione criminosa. Questa funzione *strumentale* permette ai dati di divenire mezzi di intermediazione tra più fasi del crimine: dalla compromissione iniziale dei sistemi, alla diffusione delle informazioni, fino al loro impiego per la realizzazione di ulteriori attività fraudolente o estorsive, nonché criminose.

2.3. Il dato come merce

Nella prospettiva delineata dal report *IOCTA 2025*, il dato sottratto non si esaurisce nella dimensione funzionale all'esecuzione dell'attacco, ma subisce un processo di conversione economica che lo trasforma in una vera e propria *merce* criminale. Europol osserva che l'informazione viene "stolen and converted into a commodity to be further exploited by other criminal actors in their operations", successivamente immessa in circuiti commerciali illeciti – *marketplaces* specializzati, forum sotterranei e canali cifrati *end-to-end* – ove assume una collocazione merceologica differenziata in ragione della tipologia, del grado di sensibilità e dell'utilità operativa per l'acquirente. Tale fenomeno, lungi dal rappresentare un mero riflesso accessorio dell'attacco informatico, si configura come elemento strutturale dell'economia criminale che opera nello spazio cibernetico. Gli ambienti digitali deputati allo scambio di informazioni illecitamente acquisite tendono, in maniera sempre più evidente, a organizzarsi secondo architetture che ricalcano, quasi specularmente, quei siti – legittimi – di *e-commerce* (si pensi, per esempio, ad Amazon), pur operando entro un perimetro contraddistinto da strutturale opacità e anonimato. L'esame dei principali forum internazionali evidenzia, in particolare, come la quota preponderante delle inserzioni – superiore, in taluni contesti, all'ottanta per cento del totale[16] – riguardi i dati necessari alla clonazione di carte di pagamento, le

14. Cfr. Lucas 2010; Eick–Fyock 1996.
15. Cfr. Europol 2025.
16. Giova rammentare un'analisi condotta nel 2014 sui principali forum criminali, dalla quale è emerso che l'84,3% dei beni offerti consisteva in dati sottratti – per lo più informazioni di pagamento e credenziali di accesso ad

credenziali di autenticazione, gli insiemi completi di dati identificativi e finanziari relativi agli utenti, nonché gli accessi a servizi bancari e commerciali. Tali beni vengono scambiati attraverso transazioni che si articolano secondo meccanismi consolidati di formazione del prezzo, sistemi reputazionali, procedure di verifica della qualità e una ripartizione funzionale dei ruoli tra gli attori coinvolti, delineando così un ambiente che presenta tratti di sorprendente stabilità interna nonostante la sua natura clandestina.

3. Lungo la filiera criminale degli *stolen data*

La ricostruzione empirica fornita dall'indagine di Europol consente di delineare la struttura operativa dell'economia criminale dei dati, organizzata secondo una sequenza funzionale di attività – estrazione, distribuzione e (ri)utilizzo (Fig. 1) – che ne delinea l'intera catena di trattamento illecito. Ciascuna fase è presidiata da attori specifici e si realizza attraverso mercati digitali interconnessi, nei quali il dato viene progressivamente trasformato da informazione a merce.

3.1. Estrazione

La fase di estrazione segna il momento genetico dell'intero ciclo criminale del dato, poiché in essa si realizza la prima (e più rilevante) violazione del potere di fatto e di diritto che il titolare esercita sull'informazione. È il frangente in cui l'illecito si manifesta nella sua dimensione sorgiva: l'acquisizione del dato – mediante intrusioni informatiche, tecniche di *exfiltration* o condotte di ingegneria sociale – segna il punto di rottura dell'originaria relazione tra il soggetto e la propria sfera informativa, traducendosi in una forma di spossessamento digitale. Gli attori che, ordinariamente, presidiano questa fase – noti come *initial access brokers* (*IABs*) – rappresentano il primo anello della catena criminale e operano con un grado di specializzazione tale da costituire un vero e proprio mercato primario dell'accesso illecito. Entro questo medesimo contesto operativo si collocano, *Advanced Persistent Threats* (*APT*) e gli *hybrid threat actors*, attori dotati di un livello di sofisticazione tecnica e di una capacità operativa tali da trascendere le finalità meramente lucrative proprie della criminalità informatica comune. Gli APT – spesso finanziati, sostenuti o direttamente organizzati da apparati statuali – perseguono obiettivi di lungo periodo, quali l'acquisizione indebita di informazioni di valore governativo, industriale o infrastrutturale, nonché attività di spionaggio digitale e compromissione sistemica di reti critiche. Gli *hybrid threat actors*[17], a loro volta, possono essere entità statuali o non statuali che impiegano una pluralità di strumenti – informatici e informativi – al fine di destabilizzare istituzioni, apparati pubblici o imprese strategiche, sfruttando l'ecosistema illecito del dato come moltiplicatore di capacità offensiva. I pacchetti di accesso[18], calibrati per livello di privilegio e tipologia di bersaglio, vengono poi venduti nei mercati digitali dedicati – forum specializzati, *darknet marketplaces*, canali cifrati – che ne consentono la circolazione secondo logiche di anonimato e di tracciabilità inversa.

3.2. Distribuzione

Una volta perfezionato l'accesso illecito e acquisita la disponibilità effettiva delle informazioni esfiltrate, il baricentro dell'azione criminosa si sposta fisiologicamente verso la fase della distribuzione. L'informazione viene immessa in circolazione all'interno di mercati digitali che riproducono, con fedeltà strutturale, le dinamiche e le architetture dei *marketplaces* legittimi. È in questa dimensione intermedia che il dato viene sottoposto a operazioni di selezione, aggregazione e correlazione, perdendo progressivamente ogni riferimento al suo contesto originario e assumendo una forma autonoma, standardizzata, commerciabile. Nei principali *darknet markets*, i *data brokers* operano

account digitali – commercializzati, poi, secondo schemi di determinazione del prezzo sensibili alle dinamiche concorrenziali interne alle piattaforme, Holt–Smirnova 2014.

17. Si veda, in merito, Maigre 2022.

18. In particolare, rientrano tra le offerte tipicamente commercializzate dagli *initial access brokers* le credenziali di accesso a servizi RDP, le credenziali VPN, gli accessi a firewall e dispositivi di rete, le credenziali per ambienti cloud, nonché backdoor già installate in sistemi aziendali e *footholds* persistenti, idonei a garantire una presenza continuativa dell'attaccante all'interno dell'infrastruttura compromessa, si veda Europol 2025.

come fornitori professionali di dataset, pubblicando annunci corredati da descrizioni tecniche, campioni di prova e sistemi reputazionali idonei a certificare l'affidabilità del venditore e la qualità del prodotto. Gli *administrators* e i *moderators*[19], dal canto loro, esercitano funzioni di gestione e controllo: amministrano le piattaforme, risolvono controversie, vigilano sul rispetto delle regole interne e garantiscono la correttezza delle transazioni, mediante l'impiego di sistemi *escrow*, fondati su criptovalute. Oltre ai tradizionali *marketplaces* del *dark web*, il panorama degli spazi di scambio conosce oggi l'emersione di canali paralleli, ospitati su piattaforme di messaggistica cifrata, come *Telegram* (in gruppi privati)[20], nonché altre piattaforme basate su crittografie *end-to-end* – che consentono transazioni rapide, decentralizzate e caratterizzate da un più elevato livello di anonimato, riducendo la vulnerabilità dei circuiti di scambio rispetto agli interventi di *take-down* delle autorità di *law enforcement*[21].

3.3. Riutilizzo

L'ultima fase della filiera è rappresentata dal riutilizzo – o *exploitation* – momento nel quale il dato illecitamente acquisito e successivamente distribuito viene reimpiegato quale *input* operativo per una pluralità di condotte ulteriori: campagne di *phishing* mirato, attacchi ransomware, frodi finanziarie multilivello, attività di spionaggio industriale, nonché forme di sfruttamento sessuale minorile. Gli attori che operano in questa fase sono gli *end-user criminals*, spesso inseriti in strutture transnazionali flessibili o in alleanze operative, la cui funzione primaria è la monetizzazione del dato e, più in particolare dataset, attraverso meccanismi estorsivi, appropriazioni fraudolente o successive rivendite a catena. È in tale segmento che il dato manifesta la sua massima forza criminogena: l'informazione sottratta genera nuova informazione utile al compimento di ulteriori reati, alimentando un ciclo potenzialmente infinito. Talvolta, il riutilizzo, per ciò stesso, non costituisce la mera conclusione del processo economico-criminale, ma il suo punto di rigenerazione: l'informazione reimpiegata produce infatti esiti ulteriori – nuove credenziali, nuovi accessi, nuovi elementi identificativi – i quali vengono, *ex novo*, immessi nella fase di distribuzione, secondo un modello che può qualificarsi, secondo le dovute cautele concettuali, come un'*economia circolare del dato illecito*. In questo senso, la fungibilità, la replicabilità e la non rivalità dell'informazione, come detto, costituiscono presupposti strutturali che ne consentono l'utilizzo reiterato e cumulativo.

4. Osservazioni conclusive

Senza concentrarsi sulle singole fattispecie penali che vengono in rilievo all'interno dell'ecosistema criminale del dato, come sopra descritto, il presente contributo ha inteso osservare l'approccio dell'ordinamento italiano a tale materia, evidenziandone gli elementi di continuità e, soprattutto, le criticità strutturali che emergono nell'attuale scenario tecnologico.

La legislazione penale italiana in materia di criminalità cibernetica si presenta, *ab origine*, come un insieme di norme incriminatrici eterogenee, frutto di interventi settoriali e frammentari (da ultimo con la legge 90 del 2024[22]), adottati non

19. Per una trattazione puntuale sulla struttura dei ruoli all'interno dei *darknet markets* si veda, *ex multis*, Peersman–Pencheva–Rashid 2021; White–Kakkar–Chou 2019.

20. Cfr. Garkava–Moneva–Leukfeldt 2024.

21. Un esempio significativo della capacità di coordinamento sovranazionale nel contrasto agli ecosistemi criminali digitali è costituito dall'operazione *Cookie Monster*. L'azione congiunta eseguita nell'aprile 2023 da FBI, Europol ed Eurojust, con il concorso di numerose autorità di *law enforcement* europee ed extra-UE, ha condotto allo smantellamento di *Genesis Market*, marketplace illecito di primaria rilevanza, specializzato nella commercializzazione di credenziali di accesso, cookie di sessione e *digital fingerprints* riconducibili a sistemi compromessi. L'operazione ha determinato il sequestro dell'intera infrastruttura telematica, nonché l'esecuzione di perquisizioni e arresti coordinati in oltre tredici Paesi, incidendo in modo decisivo su una piattaforma che metteva a disposizione milioni di identità digitali destinate a essere impiegate in attività fraudolente ed estorsive; v., nel sito di Europol, *Takedown of notorious hacker marketplace selling your identity to criminals.*

22. Circa le *disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*.

Fase	Attori principali	Mercati/ambienti di scambio
1. Estrazione	– Initial Access Brokers (IABs) – Hacker individuali o gruppi APT Insider Threats	– Forum specializzati deepweb e darkweb – Canali E2EE (Telegram, Discord) – Marketplace di accessi ("Access-as-a-Service")
2. Distribuzione	– Marketplace operators – Moderatori e venditori su dark web – Reti affiliate di broker	– Dark web markets (es. BreachForums, Hydra, RAMP) – Canali Telegram privati – Circuiti "trusted" peer–to–peer
3. Riutilizzo	– End-users criminali (frodi, ransomware, CSE) – Money mule networks – Gruppi di riciclaggio o disinformazione	– Piattaforme di pagamento illecite – Circuiti crypto off–chain – Network di frode integrata (ad es. BEC, phishing-as-a-service)

Tab. 1 — *Fasi, attori e mercati della filiera criminale del dato (tabella elaborata dall'Autrice sull'analisi condotta da Europol nel report IOCTA 2025)*

soltanto per colmare le lacune emerse nella prassi applicativa, ma anche per dare attuazione alle prescrizioni sovranazionali – in particolare agli stringenti obblighi di incriminazione derivanti dalla normativa europea e dagli atti del Consiglio d'Europa. Il primo atto organico fu la legge 23 dicembre 1993, n. 547, che introdusse nel Codice penale il primo nucleo sistematico di reati informatici, recependo (benché con ritardo rispetto ad ordinamenti tecnologicamente più avanzati) la lista minima e buona parte della lista facoltativa previste dalla Raccomandazione R(89)9 del Consiglio d'Europa. Con tale intervento, il legislatore si confrontò per la prima volta con condotte offensive aventi ad oggetto i nuovi "beni" dell'ecosistema digitale – dati, programmi e sistemi informatici – riconoscendo la necessità di una tutela penalistica differenziata. Tuttavia, l'ampiezza e la rapidità evolutiva dei fenomeni criminali che si sono progressivamente manifestati nel cyberspazio[23] hanno reso evidente l'impossibilità di racchiudere i crimini informatici entro un modello unitario e hanno orientato le scelte legislative verso una tecnica di *accostamento sistematico*. In assenza di un nuovo titolo dedicato esclusivamente ai "fatti di abuso della tecnologia informatica"[24] – soluzione espressamente scartata dal legislatore, che ritenne la peculiarità tecnologica insufficiente a giustificare una sezione autonoma del libro II[25] – le nuove incriminazioni sono state distribuite all'interno delle sezioni codicistiche esistenti "che ad essi, pur nella loro autonomia, sono apparse più vicine", prendendo atto che le diverse manifestazioni del fenomeno della criminalità informativa costituiscono "nuove forme di aggressione caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici […] già oggetto di tutela nelle diverse parti del corpo del codice penale"[26]. La ricostruzione svolta consente di cogliere come l'evoluzione tecnologica – e, in particolare, la progressiva affermazione della dimensione cibernetica – abbia inciso in modo strutturale sul sistema penale, tanto sul versante delle categorie dogmatiche quanto su quello delle tecniche di tutela. L'odierno cyberspace, caratterizzato da automazione diffusa, iperconnettività globale e continua produzione di dati, non rappresenta più un mero contesto

23. Per un approfondimento, Picarella 2025.
24. Cfr. Pecorella 2000.
25. Nello specifico, si fa riferimento alla discussione in Parlamento di una proposta di legge in tema di criminalità informatica, d'iniziativa dei deputati Cicciomessere ed altri (Camera dei deputati, XI legislatura, n. 1174) che prevedeva, invece, l'introduzione di una nuova sezione nel Capo III del titolo XII del Codice penale, così nominata "Sezione IV - *Dei delitti in materia informatica e telematica*", v. sul punto Pecorella 2000.
26. Cfr. Camera dei deputati, XI legislatura, disegno di legge n. 2773. Presentazione del Ministro di Grazie e Giustizia (G. Conso), p. 3.

operativo delle condotte, ma un ambiente normativo e relazionale autonomo, nel quale si generano, circolano e si consumano nuove condotte penalmente rilevanti. In tale prospettiva, il diritto penale non può limitarsi a recepire passivamente nuove figure di reato, ma deve ripensare la propria funzione regolatoria alla luce delle trasformazioni che investono i concetti tradizionali di azione, evento, nesso causale e colpevolezza. Le condotte cibernetiche presentano, difatti, modalità esecutive non più interamente riconducibili alla diretta volontà dell'agente, non solo per effetto dell'automazione o dell'impiego di algoritmi adattivi, ma – nel caso specifico del mercato illecito dei dati – soprattutto per la spontanea dinamica di replicazione, diffusione e riutilizzo del dato sottratto, che tende a emanciparsi dal controllo dell'autore iniziale. Una volta immesso nel circuito criminale, il dato diviene oggetto di successive acquisizioni, manipolazioni e monetizzazioni ad opera di una pluralità indeterminata di soggetti, protraendo e ampliando l'offesa ben oltre il momento dell'intervento umano che ne ha provocato la prima compromissione. Ne emerge una frattura rispetto allo schema classico di imputazione penale, fondato su una relazione lineare tra agire, causalità ed evento, e ciò impone al penalista un profondo aggiornamento delle categorie concettuali e metodologiche tradizionali[27]. A ciò si aggiunge che molte condotte consumate nel cyberspace presentano caratteristiche ibride: esse si svolgono entro una dimensione materiale-immateriale nella quale l'offesa ai beni giuridici può manifestarsi in forme nuove – talvolta puramente funzionali o tecnologiche – ma non per questo meno gravi o meno meritevoli di tutela. La lesione della riservatezza informatica, la compromissione dell'integrità dei sistemi o la diffusione incontrollata di contenuti lesivi sono fenomeni che possono produrre effetti equivalenti, sul piano del danno, a quelli delle corrispondenti offese "tradizionali", quando non addirittura più penetranti e persistenti. Ne deriva la necessità di una lettura sistematica del concetto di bene giuridico protetto, all'interno della quale assumono un rilievo centrale beni nuovi o riqualificati, come la sicurezza delle reti, la riservatezza informatica e l'integrità del patrimonio digitale personale e collettivo. La loro tutela non è più esclusivamente rimessa all'autonomia del singolo, poiché la struttura stessa delle reti e l'interdipendenza globale dei servizi impongono l'introduzione di doveri di protezione, talvolta di natura pubblicistica, il cui inadempimento può integrare responsabilità penalmente rilevanti. Sul piano più strettamente sistematico, appare indispensabile delineare criteri di imputazione adeguati alla specificità dei fenomeni digitali. In particolare, assume rilievo la distinzione tra il momento di perfezione formale e quello di esaurimento sostanziale del reato, utile per comprendere le modalità di protrazione dell'offesa nel tempo digitale, nonché per definire la partecipazione di ulteriori soggetti – attivi od omissivi – che contribuiscono alla diffusione del fatto lesivo in rete. Tale distinzione risulta cruciale soprattutto nelle fattispecie commesse tramite sistemi automatizzati o tramite la circolazione virale dei contenuti on line. La stessa nozione di colpevolezza richiede un ripensamento critico: l'elemento psicologico deve essere valutato in relazione alla prevedibilità degli effetti tecnologici, alla scelta consapevole di impiegare sistemi autonomi, alla tolleranza del rischio inerente alla diffusione dei contenuti nel cyberspazio. Non si tratta di superare le garanzie del diritto penale liberale, ma di adattarne i criteri a condotte la cui effettiva portata lesiva si manifesta in un ambiente nel quale il controllo umano è solo parziale e spesso mediato da strumenti algoritmici. Affinché il diritto penale dell'informatica non si riduca a un un impianto ricostruttivo che opera per proiezioni, e non per realtà, è necessario ricordare che metafore e analogie possono svolgere un ruolo utile *soltanto ex post*, come strumenti descrittivi semplificatori, ma non possono – né devono – assolvere una funzione epistemica *ex ante*. È dunque imprescindibile che legislatore e interprete si confrontino direttamente con la struttura effettiva dei fenomeni digitali, evitando di lasciare che rappresentazioni metaforiche o semantiche – per quanto seduttive – orientino impropriamente la costruzione dogmatica. Solo emancipandosi da tali suggestioni sarà possibile restituire al concetto di "crimine informatico" una significatività sistematica, capace di ricomprendere anche le nuove forme di aggressione ai beni digitali, in particolare quelle che caratterizzano il

27. In questo senso, Picarella 2025.

mercato illecito dei dati e la loro circolazione criminale[28]. Ciò implica la necessità di un costante dialogo tra giuristi e tecnologi, affinché il diritto possa continuare a svolgere la sua funzione di garanzia, senza arretrare di fronte alle trasformazioni epocali della rivoluzione cibernetica, ma anzi governandole attraverso un apparato concettuale rinnovato e strumenti operativi adeguati alla complessità del mondo digitale.

Riferimenti bibliografici

S. Ahmed, M. Gentili, D. Sierra-Sosa, A.S. Elmaghraby (2022), *Multi-layer data integration technique for combining heterogeneous crime data*, in "Information Processing & Management", vol. 59, 2022, n. 3

A. Aktoudianakis (2020), *Fostering Europe's Strategic Autonomy – Digital sovereignty for growth, rules and cooperation*, in "European Policy Centre", 2020

U. Akyazi, M. van Eeten, C.H. Gañán (2021), *Measuring Cybercrime–as–a–Service (CaaS) Offerings in a Cybercrime Forum*, in "Proceedings of the Workshop on the Economics of Information Security (WEIS)" (Delft, 2021), Delft University of Technology, 2021

G. Costabile (2005), *Scena criminis, documento informatico e formazione della prova penale*, in "Diritto dell'informazione e dell'informatica", 2005, n. 3

S.G. Eick, D.E. Fyock (1996), *Visualizing Corporate Data*, in "AT&T Technical Journal", vol. 75, 1996, n. 1

Europol (2025), *Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data*, Internet Organised Crime Threat Assessment (IOCTA), Publications Office of the European Union, 2025

Europol (2023), *Cyber–attacks: The Apex of Crime-as-a-Service*, Europol Spotlight Report, Publications Office of the European Union, 2023

G. Fiorinelli (2023), *Nomina nuda tenemus? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche*, in "Discrimen.it", 2023

M. Gambini (2013), *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in "Espaço Jurídico: Journal of Law", vol. 14, 2013, n. 1

T. Garkava, A. Moneva, E.R. Leukfeldt (2024), *Stolen Data Markets on Telegram: A Crime Script Analysis and Situational Crime Prevention Measures*, in "Trends in Organized Crime", 2024

F. Greco, G. Greco (2020), *Organised crime: underground economy and regulations to combat cybercrime*, in "European Journal of Political Science Studies", vol. 4, 2020, n. 1

T.J. Holt (2013), *Exploring the social organisation and structure of stolen data markets*, in "Global Crime", vol. 14, 2013, n. 2-3

T.J. Holt, O. Smirovna (2014), *Examining the structure, organization, and processes of the international market for stolen data*, in "Global Crime", 2014

C.J. Howell, T. Fisher, C.N. Muniz et al. (2023), *A Depiction and Classification of the Stolen Data Market Ecosystem and Comprising Darknet Markets: A Multidisciplinary Approach*, in "Journal of Contemporary Criminal Justice", vol. 39, 2023, n. 2

28. "D'altronde, l'esigenza di pervenire a una sistematizzazione del tema, in una prospettiva sostanziale, deriva non tanto da una astratta necessità di concepire il 'diritto penale del cybercrime' quale autonoma partizione sistematica, ma piuttosto dall'urgenza di far sì, ad esempio, che a tale fenomeno corrisponda un trattamento giuridico adeguato e omogeneo, e non, invece, come ora accade, conseguenze sanzionatorie del tutto disarticolate", così Fiorinelli 2023.

A. Lucas (2010), *Corporate Data Quality Management: From Theory to Practice*, in "Proceedings of the 5th Iberian Conference on Information Systems and Technologies" (Santiago de Compostela, 2010), 2010

M. Maigre (2022), *Cyber threat actors: how to build resilience to counter them*, in "Hybrid CoE Papers", 2022, n. 11

U.A. Mejias, N. Couldry (2019), *Datafication*, in "Internet Policy Review", vol. 8, 2019, n. 4

M. Pecorella (2006), *Diritto penale dell'informatica* (ristampa con aggiornamento), Cedam, 2006

L. Peersman, D. Pencheva, A. Rashid (2021), *Tokyo, Denver, Helsinki, Lisbon or the Professor? A Framework for Understanding Cybercriminal Roles in Darknet Markets*, in "Proceedings of the 2021 APWG Symposium on Electronic Crime Research (eCrime)", IEEE, 2021

L. Picarella (2025), *Criminalità in rete: dalle piattaforme illegali alle cybermafie*, Donzelli Editore, 2025

S. Tanzi (1983), *The underground economy. Causes and consequences of this worldwide phenomenon,* in "Finance and Development", vol. 20, 1983, n. 4

D.S. Wall (2024), *Cybercrime: The transformation of crime in the information age*, John Wiley & Sons, 2024

D.S. Wall (2021), *Cybercrime as a transnational organized criminal activity*, in F. Allum, S. Gilmour (eds.), "Routledge Handbook of Transnational Organized Crime", Routledge, 2021

D.S. Wall (2015), *Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, in "The European Review of Organised Crime", vol. 2, 2015, n. 2

R. White, P.V. Kakkar, V. Chou (2019), *Prosecuting darknet marketplaces: challenges and approaches*, in "Department of Justice Journal of Federal Law & Practice", vol. 67, 2019

M. Yip, N. Shadbolt, T. Tiropanis, C. Webber (2012), *The digital underground economy: A social network approach to understanding cybercrime*, in "Digital Futures 2012: The Third Annual Digital Economy All Hands Conference", 2012