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

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0257 • articolo sottoposto a peer review • pubblicato in anteprima il 27 gen. 2026

Teresa Meccariello

Il cyberspazio tra impostazioni tradizionali e consolidamento normativo della "riservatezza"

Il lavoro analizza l'evoluzione dei reati informatici in Italia e il ruolo del dato e della riservatezza come beni giuridici autonomi. La ricerca empirica dell'Unità SERICS di Napoli evidenzia modalità operative ricorrenti e forte concentrazione territoriale dei procedimenti. La riservatezza è proposta come bene unitario di quarta generazione, distinguendo chiaramente tra accesso abusivo (615-*ter* c.p.) e frode informatica (640-*ter* c.p.), con prevalente negazione dell'assorbimento tra le due fattispecie. L'analisi sostiene l'esigenza di una protezione multilivello dell'informazione nella società digitale.

Riservatezza – Sistema informatico – Dato personale – Protezione – Sicurezza digitale

Cyberspace between traditional settings and the regulatory consolidation of privacy

The paper analyzes the evolution of computer crimes in Italy and the role of data and privacy as autonomous legal goods. Empirical research conducted by the SERICS Unit in Naples highlights recurring operational patterns and a strong territorial concentration of cases. Privacy is proposed as a unitary fourth-generation legal interest, clearly distinguishing between unauthorized access (Art. 615-ter c.p.) and computer fraud (Art. 640-ter c.p.), with the prevailing view rejecting the absorption between the two offenses. The analysis supports the need for multi-level protection of information in the digital society.

Privacy – Information system – Personal data – Protection – Digital security

L'Autrice è avvocato e assegnista di ricerca in cyber crime presso il Dipartimento di Scienze Politiche dell'Università degli Studi Federico II di Napoli

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

1. Cenni sulla evoluzione normativa e premessa metodologica

I reati informatici costituiscono una categoria delittuosa complessa, volta alla protezione di beni giuridici fondamentali quali la riservatezza, l'integrità e la disponibilità dei dati, la proprietà intellettuale nonché la sicurezza pubblica. La loro natura mutevole, intrinsecamente tecnica e spesso transnazionale ha reso la risposta normativa, sia a livello nazionale sia sovranazionale, talvolta frammentata e non sempre adeguata.

In Italia, l'evoluzione legislativa[1] è stata significativa: dall'introduzione della Legge n. 547/1993, al recepimento del Codice della Privacy (d.lgs. 196/2003)[2] e, più di recente, alle riforme in materia di cybersicurezza idonee a dare attuazione alle direttive europee NIS1 e NIS2, sino alla modernizzazione con la legge 90/2024 e con la normativa in tema di intelligenza artificiale. Nonostante tali interventi, la disciplina nazionale continua tuttavia a presentare elementi di disomogeneità: le fattispecie penali risultano spesso autonome e scollegate, e la normativa speciale – dalle disposizioni sul diritto d'autore alla disciplina di cui al d.lgs. 231/2000, fino al GDPR – si intreccia con il codice penale in modo non sempre sistematico.

La legge 547/1993 ha introdotto nel codice penale una serie di disposizioni destinate a formare il nucleo originario del diritto penale dell'informatica. Tra le principali, l'art. 615-*ter* c.p. (accesso abusivo a sistema informatico o telematico); l'art. 617-quater c.p. (intercettazione illecita di comunicazioni informatiche o telematiche); l'art. 635-bis e ss. c.p. (danneggiamento di dati e sistemi informatici); l'art. 640-*ter* c.p. (frode informatica). Si tratta di norme pionieristiche, che anticipano molte scelte poi recepite nella Convenzione di Budapest (2001)[3]. Tuttavia, tale intervento si

1. Per una più compiuta analisi delle fonti e dell'evoluzione legislativa in materia di reati informatici v. Flor 2019, p. 97-139.
2. Il Codice della privacy può essere considerato, in un certo qual senso, un duplicato della Carta di Nizza giacché la protezione dei dati personali assume al suo interno un ruolo di diritto con valenza del tutto autonoma. Infatti, con l'art. 1 del Codice è stata attribuita al diritto alla protezione dei dati personali una posizione distinta dal diritto alla riservatezza, venendo rimarcata la sua valenza di diritto fondamentale e la sua dimensione di libertà. Cfr. Costanzo 2008, pp. 49 e 58; Del Ninno 2006, pp. 3-5.
3. Flor 2019, p. 99 s.

concentrava prevalentemente sulla protezione dei sistemi e delle infrastrutture informatiche, lasciando in ombra la dimensione soggettiva dei diritti digitali e, in particolare, il valore del dato quale espressione dell'identità personale.

Il successivo Codice della Privacy (d.lgs. 196/2003), poi riformato alla luce del GDPR, ha segnato un cambio di paradigma: la protezione del dato personale è stata riconosciuta come manifestazione della dignità della persona (art. 2 Cost.) e della libertà personale (art. 13 Cost.). In dottrina questo passaggio è stato definito momento di "costituzionalizzazione del dato", ossia il riconoscimento dell'informazione come nuovo elemento di libertà individuale nella società digitale. Vale a dire "il paradigma tecnologico che si presenta come dominante, come fattore di liberazione della persona e di innovazione irresistibile, dunque, irrinunciabile"[4].

2. La ricerca dell'Unità SERICS Napoli: quadro metodologico e dati territoriali

L'attività di ricerca condotta dall'Unità SERICS di Napoli, nell'ambito dell'assegno finanziato dal progetto SERICS – PNRR MUR M4C2, ha comportato la raccolta e l'esame di un ampio numero di atti giudiziari provenienti dai Tribunali di Benevento, Avellino, Santa Maria Capua Vetere, Torre Annunziata, Napoli e Napoli Nord, con esclusione del solo Tribunale di Nola in ragione dell'insufficienza campionaria. Il lavoro si è concentrato sui reati informatici in senso proprio, vale a dire sulle fattispecie di cui agli artt. 615-*ter* e ss. c.p., analizzate nel periodo 2019-2024.

Sul piano dogmatico, la ricerca ha adottato la distinzione tradizionalmente accolta tra reati in cui il sistema informatico funge da mero strumento di offesa e reati in cui esso costituisce oggetto diretto dell'aggressione. L'indagine ha riguardato esclusivamente questi ultimi, in quanto maggiormente significativi ai fini della ricostruzione dell'evoluzione normativa e concettuale della materia. Tale scelta appare coerente con un processo di trasformazione che, a partire dalla legge 547/1993 sino alle riforme più recenti – tra cui la legge 90/2024 e la normativa sull'intelligenza artificiale – ha condotto a un progressivo ripensamento del bene giuridico sotteso ai delitti informatici e delle modalità di tipizzazione delle condotte[5]. L'evoluzione normativa, infatti, non si è limitata all'introduzione di nuove figure incriminatrici, come l'estorsione informatica, né all'inasprimento del trattamento sanzionatorio, ma ha investito il tema, più profondo, della configurabilità del dato come bene giuridico e della progressiva espansione della riservatezza entro lo spazio delle libertà costituzionalmente protette. In tal senso, si è sostenuto che "le importanti sentenze delle Corti Costituzionali tedesca, rumena e ceca, nonché quella della Corte di Giustizia, sembrano confermare la nascita di nuove forme di manifestazione dei diritti generali della personalità, che possono essere ricondotte al diritto all'autodeterminazione informativa ed al diritto alla riservatezza ed alla sicurezza dei dati e dei sistemi informatici. Il primo conferisce alla persona il potere di determinare, da un lato, il trattamento dei dati e delle informazioni ad essa attinenti, ampliando la tutela del diritto fondamentale alla libertà della vita privata e, dall'altro lato, il 'destino' delle 'aree informatiche' (cyberspace) in cui si manifesta la personalità umana. Il secondo, invece, garantisce l'interesse a non subire indebite interferenze nella sfera di rispetto e disponibilità di 'spazi informatici', indipendentemente dalla qualità (natura) o dalla quantità di dati e informazioni o dalla natura o dimensione dello spazio informatico di pertinenza del o dei soggetti 'titolari', nonché di tutelare l'integrità e la riservatezza dei dati e dei sistemi informatici assicurando così la correttezza e l'affidabilità dei rapporti giuridici che si instaurano nel cyberspace"[6]. Una parte rilevante di questa evoluzione, peraltro, si deve alla normativa speciale: si pensi alla legge sul diritto d'autore, al d.lgs. 231/2000, al Codice della privacy e al GDPR, che hanno anticipato e orientato quella progressiva "giuridicizzazione" del dato informatico oggi al centro del dibattito. In tal senso, si è posto al centro dell'attenzione il bene giuridico nel senso che, nel passaggio dall'on life

4. Caramaschi 2025, p. 40.
5. Sui crimini informatici, prendendo in considerazione la struttura delle fattispecie criminose ed i principali problemi che esse pongono, vedasi Amato Mangiameli–Saraceni 2019.
6. Flor 2010.

all'on line, si è cercato di capire quale fosse il bene giuridico oggetto di tutela nell'ambito del reato informatico[7].

C'è stato un iniziale ostracismo a utilizzare le categorie classiche dei diritti; diffidenza che col tempo è stata erosa grazie al lavorio della più autorevole dottrina e giurisprudenza. In tale senso, sono state pioniere le aperture in materia di domicilio informatico, che hanno equiparato lo spazio digitale al domicilio *tout court*. Del pari, pietra miliare è stato altresì il riconoscimento del dato informatico come *res* passibile di apprensione. Proprio la progressiva trasposizione delle libertà fondamentali dal reale al digitale, con progressiva ridefinizione anche di alcune fattispecie tipiche e con la parallela creazione di fattispecie *ad hoc* che, via via, il legislatore italiano ha introdotto nel frastagliato orizzonte della materia, ha consentito di riflettere sulla natura poliedrica e onnicomprensiva della riservatezza.

Il numero complessivo degli atti giudiziari acquisiti nei tribunali del distretto della Corte di Appello di Napoli è pari a circa 7.127, ripartite in percentuali che vedono Benevento detenere lo 0,25%, Santa Maria C.V. lo 0,81%, Avellino lo 0,94 %, Torre Annunziata il 5,61 %, Napoli Nord l'1,04% e Napoli il 91,37 %. Sulla base di tali indici valoriali è stato possibile ricavare una ripartizione percentuale che consente di misurare l'incidenza territoriale dei procedimenti relativi ai reati informatici in senso proprio. L'analisi proporzionale restituisce un quadro territoriale fortemente disomogeneo. Il Tribunale di Napoli, da solo, concentra oltre il 91% dei procedimenti esaminati, rivelando un'incidenza straordinariamente superiore rispetto agli altri territori del distretto. Tale dato, pur potendo riflettere la maggiore popolazione e il ruolo di polo metropolitano del distretto, suggerisce anche una più elevata capacità di emersione, segnalazione e trattazione dei reati informatici, nonché una maggiore densità di attività economiche e finanziarie appetibili per la criminalità digitale. Il valore rilevato per Torre Annunziata (5,61%) costituisce l'unico altro dato statisticamente significativo, confermando la presenza nel territorio vesuviano di un fenomeno criminale informatico strutturato e ricorrente. Gli altri tribunali presentano incidenze molto più basse (tutte inferiori all'1,1%), che possono derivare da diversi fattori: minore popolazione, minor radicamento dei reati informatici, minore capacità investigativa o diverso livello di digitalizzazione dei contesti socio-economici. Va inoltre sottolineato che la proporzione territoriale evidenzia come l'emersione statistica dei reati informatici sia significativamente influenzata sia dalla densità tecnologica sia dalla capacità delle forze dell'ordine e degli uffici giudiziari di intercettare e qualificare adeguatamente tali fenomeni. La fortissima concentrazione presso il Tribunale di Napoli potrebbe, quindi, riflettere non solo una maggiore frequenza dei reati, ma anche una maggiore sensibilità e strutturazione delle attività investigative in materia di cybercrime.

Dal punto di vista territoriale, i dati raccolti mostrano una significativa disomogeneità nell'emersione del fenomeno.

Sotto il profilo qualitativo emerge una notevole uniformità nelle condotte e nei modelli operativi. In tutti i tribunali esaminati i capi di imputazione risultano prevalentemente costruiti come concorso tra accesso abusivo e frode informatica, in perfetta coerenza con l'impostazione dogmatica che distingue la tutela del domicilio informatico dall'offesa al patrimonio conseguente all'alterazione o manipolazione dei dati. Nei tribunali maggiori si riscontrano, inoltre, anche contestazioni relative agli artt. 616, 617-*quater* e 617-*sexies* c.p., a dimostrazione di una gamma più ampia di condotte perseguite e di una maggiore sofisticazione dei casi esaminati. La figura dell'autore risulta generalmente riconducibile a un singolo individuo operante in concorso con soggetti in larga parte non identificati; nei casi in cui tali soggetti vengono individuati, essi risultano quasi sempre legati da rapporti familiari o fiduciari. Le dinamiche delle condotte, però, permettono di pensare a una criminalità informatica organizzata e strutturata sebbene non in maniera associativa. Le vittime, perlopiù inconsapevoli, comprendono privati cittadini, istituti bancari, società e Poste Italiane. Significativa è la quasi totale assenza delle pubbliche amministrazioni tra i soggetti passivi ovvero le persone offese, circostanza che indica una selezione delle vittime basata sulla vulnerabilità tecnica e sull'immediata disponibilità economica.

7. Picotti 2004, pp. 21-94.

La metodologia di esecuzione del reato è pressoché identica nei vari territori: essa si apre con un contatto fraudolento tramite posta elettronica o SMS (phishing), prosegue con l'induzione della vittima a comunicare dati sensibili o codici di accesso e culmina nell'intrusione nel sistema informatico e nella realizzazione dell'operazione fraudolenta. La costanza della tecnica, congiunta all'impossibilità di rilevare livelli elevati di competenza informatica negli autori, suggerisce l'utilizzo di strumenti fraudolenti facilmente reperibili e utilizzabili anche da soggetti privi di specifiche capacità tecnologiche.

Quanto alla qualificazione giuridica delle condotte, si rileva un quadro sostanzialmente coerente con gli orientamenti giurisprudenziali consolidati. Numerose decisioni, in particolare nell'area napoletana, qualificano l'accesso abusivo come antecedente non punibile quando esso costituisce mera condotta strumentale e priva di autonoma offensività rispetto alla frode informatica. Ciò si inserisce in un solco interpretativo secondo cui l'art. 615-*ter* tutela il domicilio informatico, mentre l'art. 640-ter si concentra sull'alterazione fraudolenta dei dati. Coerentemente, in alcuni casi il reato di frode informatica è stato ritenuto assorbente rispetto all'indebita utilizzazione dei codici di accesso prevista dall'art. 55, comma 9, d.lgs. 231/2007, quando tale condotta costituisce parte integrante del percorso criminogeno. Non mancano, tuttavia, pronunce che individuano forme di responsabilità concorrente anche in capo al titolare dell'account o dello strumento informatico sul quale confluiscono i fondi illeciti, come segnalato da una decisione del Tribunale di Benevento del 2022, ove è stata esclusa l'automatica irrilevanza della sua condotta rispetto alla frode.

3. La riservatezza come bene giuridico unico di quarta generazione

Proseguendo nell'analisi e alla luce dei risultati emersi dalla ricerca empirica condotta dall'Unità SERICS di Napoli, il tema della riservatezza come bene giuridico unitario di quarta generazione appare particolarmente fecondo e funzionale a ricomporre in un quadro sistematico coerente la frammentarietà normativa che caratterizza le fattispecie incriminatrici in materia di criminalità informatica. La progressiva emersione di comportamenti illeciti aventi ad oggetto dati, sistemi e processi informativi, nonché la sostanziale omogeneità rilevata nelle modalità operative delle condotte esaminate nel territorio distrettuale, confermano che l'oggetto della lesione penale non è più riconducibile alle categorie classiche del patrimonio o della libertà individuale, ma si concentra piuttosto sull'informazione come entità giuridica autonoma e come fulcro della dimensione digitale contemporanea. In questo senso, la nozione di riservatezza si presta a fungere da principio unificante[8], in grado di ricomprendere e sintetizzare la pluralità di interessi protetti dalle norme vigenti. Il bene giuridico della riservatezza assume così una configurazione estesa, che ricomprende non solo la protezione dei dati personali – intesa quale autodeterminazione informativa, coerente con il paradigma introdotto dal GDPR – ma anche la tutela dell'integrità, della disponibilità e della confidenzialità delle informazioni, indipendentemente dalla loro natura personale o meno. Tale ampliamento si giustifica alla luce della trasformazione digitale e dell'interconnessione permanente tra soggetti, sistemi e reti, nel quale la vulnerabilità informativa diviene direttamente incidente sulla sfera individuale e sulla dimensione collettiva. La tutela penale, pertanto, non può limitarsi a proteggere il singolo dato, ma deve necessariamente estendersi al contesto sistemico che ne consente la gestione, la conservazione e l'elaborazione, divenuto esso stesso oggetto di condotte criminose quali l'accesso abusivo, la manipolazione fraudolenta o l'illecita appropriazione.

La convergenza funzionale delle fattispecie previste dagli artt. 615-*ter* e ss. c.p. mostra chiaramente come il legislatore abbia tentato di costruire un sistema di protezione articolato ma tendenzialmente ispirato a un medesimo nucleo assiologico: la tutela dell'informazione in quanto tale[9]. Le sovrapposizioni rilevate nella prassi applicativa, e confermate dall'analisi delle sentenze del distretto di Corte di Appello di Napoli esaminate nel periodo 2019-2024, evidenziano come le violazioni dell'integrità o della disponibilità dei dati rappresentino spesso l'antecedente logico necessario per la successiva aggressione al patrimonio mediante

8. Troncone 2020.
9. Sul punto, per una più compiuta analisi, vedasi Galiano–Leogrande–Massari–Massaro 2020.

frode informatica, sicché i due piani risultano inevitabilmente intrecciati. L'idea di un bene giuridico unitario, lungi dall'essere una costruzione meramente teorica, trova dunque riscontro concreto nel fatto storico, nella ripetizione delle modalità esecutive e nella costante contiguità tra condotte che, pur astrattamente distinte, si realizzano nella medesima dimensione informativa.

Dottrina autorevole[10] ha da tempo posto in evidenza la natura poliedrica della riservatezza, intesa come bene giuridico complesso e capace di abbracciare interessi individuali, collettivi e, in alcune ipotesi, persino sovraindividuali. Le elaborazioni recenti hanno ulteriormente precisato tale prospettiva, sottolineando come la riservatezza si configuri non solo quale diritto alla protezione dei dati, ma anche quale garanzia dell'identità digitale e presupposto strutturale della fiducia nei sistemi informativi. In questa direzione, la riservatezza assume una natura sistemica, idonea a sostenere l'intero impianto sociale ed economico fondato sull'elaborazione digitale, e ciò spiega perché la sua lesione, anche quando apparentemente minima, possa generare effetti espansivi potenzialmente dirompenti.

Una simile prospettiva consente di superare la tradizionale frammentazione normativa e interpretativa, orientando l'intervento punitivo verso la protezione dell'informazione come elemento essenziale della persona e della collettività. Ciò offre una chiave di lettura coerente non solo dei reati informatici attualmente codificati, ma anche delle nuove sfide poste dall'evoluzione tecnologica[11]: dall'intelligenza artificiale all'Internet delle cose, dalla blockchain ai sistemi predittivi basati su grandi basi di dati. In tali contesti, l'informazione non è più un mero supporto, bensì la struttura stessa che sostiene l'interazione tra individui, enti e infrastrutture, divenendo così un bene giuridico di primaria rilevanza. L'adozione della riservatezza come bene giuridico unitario permette, quindi, di fornire una risposta penalistica più razionale, proporzionata e orientata alla sostanza del fatto lesivo, costituendo al contempo un criterio guida per il necessario aggiornamento della disciplina in un ecosistema tecnologico in rapida e continua evoluzione[12].

4. Riflessioni conclusive

Nel quadro interpretativo ricostruito alla luce della riservatezza come bene giuridico unitario, la questione dell'assorbimento tra il delitto di accesso abusivo a sistema informatico (art. 615-*ter* c.p.) e quello di frode informatica (art. 640-*ter* c.p.) pone un problema sistematico di particolare rilevanza, poiché consente di misurare la tenuta dell'assetto attuale della parte speciale rispetto all'evoluzione tecnologica. Benché nella pratica applicativa le due condotte si manifestino spesso in un *continuum* fattuale – come confermato dai dati raccolti nella ricerca SERICS, in cui l'accesso abusivo rappresenta frequentemente la fase prodromica della frode informatica – l'orientamento prevalente di dottrina e giurisprudenza nega, allo stato, la possibilità di un assorbimento sistematico. Ciò in quanto i due reati tutelano beni giuridici ontologicamente distinti: l'art. 615-*ter* c.p. protegge l'integrità, la riservatezza e la disponibilità del sistema informatico quale "domicilio digitale", mentre l'art. 640-*ter* c.p. ha per oggetto la tutela del patrimonio contro condotte fraudolente realizzate mediante manipolazione o inganno informatico.

La differenza strutturale tra i beni giuridici coinvolti è stata ribadita da un'ampia parte della dottrina e dalla giurisprudenza. Pur potendo le condotte concatenarsi nel fatto storico, l'accesso abusivo rappresenta una lesione autonoma e antecedente di un bene diverso da quello patrimoniale, sicché non può essere attratto nel paradigma del delitto complesso[13]. Ciò nella misura in cui ai fini dell'assorbimento, non basta la mera strumentalità dell'accesso alla frode; ciò che rileva è la coincidenza o meno dei beni giuridici protetti, essendo l'istituto del concorso apparente fondato su un criterio di specialità e non di mera consequenzialità

10. Troncone 2020.

11. Parodi–Sellaroli 2020, pp. 681-682.

12. Frosini 1981, p. 196. Per l'Autore L'ingresso nella società digitale ha dato vita ad un processo di astrazione dell'uomo dalla natura verso un mondo virtuale con la conseguenza che i problemi non possono essere ricondotti alle categorie tradizionali, ma occorre, invece, riconsiderare i valori e le forme di tutela.

13. Fiandaca–Musco 2021, pp. 431-434.

cronologica[14]. In questa prospettiva l'accesso abusivo determina una compromissione dell'integrità del sistema informativo che non può considerarsi assorbita da una successiva lesione patrimoniale, poiché si realizza su un piano logico e offensivo distinto, avente una sua piena rilevanza lesiva.

La giurisprudenza più recente si colloca sul medesimo solco interpretativo. La Corte di Cassazione ha infatti affermato che la condotta di accesso abusivo non può ritenersi assorbita nel delitto di frode informatica, trattandosi di fattispecie che "preservano beni giuridici non sovrapponibili: il domicilio informatico e il patrimonio" (Cass., sez. V, 27 giugno 2021, n. 28418). La Suprema Corte ha ulteriormente precisato che, anche quando l'accesso costituisce la condizione necessaria per la successiva frode, esso non si riduce a un mero momento preparatorio, ma conserva un'autonoma valenza offensiva, in quanto incide sulla sfera di riservatezza del titolare del sistema (Cass., sez. II, 9 marzo 2021, n. 9874). Tale orientamento risulta coerente con la ricostruzione dottrinale della riservatezza come bene giuridico autonomo e multidimensionale: la violazione dell'integrità del sistema non si esaurisce nella lesione patrimoniale, ma costituisce già di per sé un'aggressione alla "identità informatica" del soggetto, elemento essenziale della sua sfera personale nella società digitale.

Ne deriva che il concorso materiale tra art. 615-ter e 640-*ter* c.p. è, allo stato, la soluzione ordinaria, poiché l'azione lesiva si dispiega su piani distinti che il legislatore ha voluto presidiare autonomamente. La possibilità di assorbimento, evocata in talune pronunce isolate come ipotesi eccezionale, non trova fondamento nel principio di specialità né appare compatibile con il disegno complessivo di tutela delineato dalla parte speciale. L'accesso abusivo, infatti, non è una condotta meramente ancillare, ma un'aggressione diretta all'integrità del sistema informativo, che richiede una reazione penale distinta anche quando costituisce la premessa della frode.

L'impianto normativo vigente rivela così la volontà del legislatore di garantire una protezione multilivello dell'informazione: prima come forma di riservatezza, poi come risorsa economicamente rilevante. Pertanto, la separazione tra le due fattispecie – e la conseguente esclusione di un assorbimento sistematico – risulta pienamente coerente con la ricostruzione della riservatezza quale bene giuridico autonomo e centrale nel diritto penale informatico. Solo riconoscendo la duplice dimensione dell'offesa (al sistema e al patrimonio) il diritto penale può garantire una tutela adeguata alla complessità delle condotte criminose digitali, evitando soluzioni riduttive che finirebbero per impoverire la protezione dell'informazione quale infrastruttura essenziale della società contemporanea.

Pur nel quadro ricostruttivo che attribuisce ai reati informatici una tutela multilivello dell'informazione, non manca una parte minoritaria della dottrina che, muovendo da un approccio maggiormente pragmatico, ha ipotizzato la possibilità di configurare un rapporto di assorbimento tra il delitto di accesso abusivo (art. 615-*ter* c.p.) e il delitto di frode informatica (art. 640-*ter* c.p.) quando la condotta di intrusione nel sistema costituisca un mero segmento esecutivo della fraudolenta manipolazione informatica. Secondo questa lettura, l'accesso illecitamente realizzato sarebbe del tutto "assorbito" nella successiva alterazione del sistema quando non esprime un autonomo disvalore offensivo, ma rappresenta soltanto la fase strumentale necessaria alla lesione patrimoniale. Nelle ipotesi di fraudolenta sottrazione di credenziali bancarie tramite intrusioni minime, è stato affermato, per esempio, che può astrattamente delinearsi un rapporto di progressione criminosa tale da consentire un concorso apparente di norme, poiché "la condotta di penetrazione nel sistema si esaurisce nella realizzazione dell'inganno informatico"[15]. In termini simili, è stato osservato che qualora l'accesso abusivo abbia un livello di offensività "praticamente neutro", l'intera sequenza possa essere sussunta nella fattispecie di frode informatica, configurandosi una sorta di specialità funzionale "in senso inverso"[16]. Tale impostazione, tuttavia, rimane allo stato del tutto minoritaria e non recepita dalla giurisprudenza, la quale continua a ritenere che l'accesso abusivo leda autonomamente la sfera di riservatezza informatica, mentre la frode informatica aggredisce il

14. Mantovani 2021, pp. 406-409.

15. Palazzo 2018, pp. 512-514.

16. Picotti 2019, pp. 243-245.

patrimonio, impedendo ogni configurazione di assorbimento strutturale. La ricostruzione tradizionale – oggi dominante – valorizza la pluralità dei beni giuridici coinvolti[17] e la necessità di mantenere distinti i due titoli di reato, anche quando l'intrusione costituisce il presupposto logico della manipolazione fraudolenta. Tuttavia, la stessa esistenza di una dottrina che paventa l'assorbimento dimostra come il tema resti aperto e come la crescente unitarietà del bene della riservatezza, inteso in senso esteso, continui a stimolare una riflessione sistematica sulla possibilità di riordinare le fattispecie informatiche alla luce di una maggiore coerenza offensiva.

Riferimenti bibliografici

A.C. Amato Mangiameli, G. Saraceni (2019), *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli (II ed.), 2019

O. Caramaschi (2025), *Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni?*, in "Rivista italiana di informatica e diritto", 2025, n. 1

P. Costanzo (2008), *La dimensione costituzionale della privacy,* in G.F. Ferrari (a cura di) "La legge sulla privacy dieci anni dopo", EGEA, 2008

A. Del Ninno (2006), *La tutela dei dati personali. Guida pratica al Codice della privacy (d.lgs. 30.6.2003, n. 196)*, Cedam, 2006

G. Fiandaca, E. Musco (2021), *Diritto penale. Parte speciale*, vol. II, Zanichelli, 2021

R. Flor (2019), *Cyber-criminality: le fonti internazionali ed europee*, in "Cybercrime – Diritto e procedura penale dell'informatica", Utet, 2019

R. Flor (2010), *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in "Diritto Penale Contemporaneo", 2010

V. Frosini (1981), *Il diritto nella società tecnologica*, Giuffrè, 1981

A. Galiano, A. Leogrande, S.F. Massari, A. Massaro (2020), *I dati non personali: la natura e il valore*, in "Rivista italiana di informatica e diritto", 2020, n. 1

F. Mantovani (2021), *Diritto penale. Parte speciale*, Cedam, 2021

F. Palazzo (2018), *Corso di diritto penale. Parte speciale*, Giappichelli, 2018

C. Parodi, V. Sellaroli (2020), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020

L. Picotti (2019), *Diritto penale e tecnologie informatiche: una visione d'insieme*, in "Cybercrime", Utet, 2019

L. Picotti (2004), *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in "Il diritto penale dell'informatica nell'epoca di Internet", Cedam, 2004

P. Troncone (2020), *La tutela penale della riservatezza e dei dati personali: profili dommatici e nuovi approdi normativi*, Edizioni Scientifiche Italiane, 2020

17. Parodi–Sellaroli 2020, pp. 712-723.