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

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0245 • articolo sottoposto a peer review • pubblicato in anteprima il 11 nov. 2025

Pasquale Troncone

Il progetto di un assetto normativo autonomo per la sicurezza dei sistemi informatici e dei dati

La complessità normativa che sta investendo negli ultimi anni la materia penale dell'informatica impone una strategia di razionalità nel sistema delle fonti. Se da un lato la legislazione si muove nella traiettoria di rispondere con norme punitive incriminatrici sempre più rigorose, d'altro lato si registra una disseminazione delle fonti in vari testi legislativi che compromette la configurazione di un assetto sistematico della materia. L'interprete è chiamato a muoversi in un orizzonte normativo sempre più ampio e complesso, caratterizzato anche da nuovi beni giuridici oggetto di tutela che allo stato sembrano tenuti insieme dal nuovo assetto che fa capo alla cybersicurezza. Appare, dunque, necessario ricomporre il quadro normativo progettando un testo legislativo autonomo che riconduca sotto un comune denominatore le numerose fattispecie di reato, conferendo coerenza sistematica alla nuova materia foriera di ulteriori sviluppi.

Cybersicurezza – Reati informatici – Sistemi informatici – Dati digitali – Testo unico

The project for an independent regulatory framework for the security of information systems and data

The regulatory complexity that has affected cybercriminal law in recent years requires a strategy of rationalization in the system of sources. While legislation is moving toward responding with increasingly stringent punitive criminal provisions, there is also a dissemination of sources across various legislative texts, compromising the creation of a systematic framework for the subject. Interpreters are required to navigate an increasingly broad and complex regulatory landscape, also characterized by new legal assets subject to protection that currently appear to be held together by the new framework centered on cybersecurity. It therefore appears necessary to restructure the regulatory framework by designing a separate legislative text that brings together the numerous types of crimes under a common denominator, lending systematic coherence to this new field, which promises further developments.

Cybersecurity – Computer crimes – Information systems – Digital data – Consolidated law

L'Autore è professore associato di Diritto penale presso il Dipartimento di Giurisprudenza 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. Mettere a fuoco le questioni aperte: *quid iuris*?

Questa mattina[1] cominceremo con il fare il punto della situazione su una nuova materia dove il gius-penalista si trova a navigare a vista in un oceano di fonti del diritto di varia natura e collocate su diversi livelli gerarchici. Questo variegato assetto disciplinare impone un intervento di armonizzazione con i principi di governo della materia penale, la cui prospettiva dommatica è chiamata a confrontarsi con strutture normative altamente volatili e con l'intervento regolatore del diritto positivo che si presenta sempre *a-sincrono* rispetto alle vicende tecnologiche che evolvono rapidissimamente e condizionano il bisogno di tutela[2].

L'attenzione del giurista è oggi rivolta a una nuova forma di diritto, un diritto che si forma in divenire, incontrollabile, collocato oltre le fonti della legislazione ordinaria, un diritto spesso autoprodotto come accade per le autonome discipline di regolazione dei comportamenti in Rete adottate dai grandi motori di ricerca. E poi, le scelte selettive dei provider che limitano il diritto degli utenti alla libera navigazione e controllano e selezionano le informazioni da introdurre in Rete sotto le forme di interventi normativi, prescrittivi, vincolanti per gli utenti[3].

I precetti delle norme penali di questo moderno ambito sfidano il limite di legittimità della norma penale in bianco, poiché vi sono molte figure di reato che attendono l'integrazione della descrizione della condotta vietata da altre norme di rango inferiore, entrate nella loro vigenza anche in epoca successiva[4]. Si tratta di una tecnica legislativa certamente opportuna per condotte che ancora non sono prese in considerazione dalla norma penale da integrare, ma che comunque pongono seri problemi per il cittadino circa la piena conoscibilità del precetto vietato e la prevedibilità della

1. Questo testo è la rielaborazione della Relazione tenuta in Pisa alla Scuola Superiore Sant'Anna il 16 giugno 2025 presso il Dipartimento di Giurisprudenza nell'ambito del Convegno: "*Dal Cybecrime alla Cyberwar: presentazione intermedia dei risultati del WP4 del progetto CyberRights-SERICS*".
2. Pica 1999; Parodi–Sellaroli 2020.
3. Zeno-Zencovich 2003; Rodotà 2010, p. 337; Allegri 2016, p. 8.
4. Amato Mangiameli–Saraceni 2019.

responsabilità che ne dovesse derivare per la loro violazione.

Se lo schema originario vedeva la scelta di politica criminale, intesa come uno degli strumenti della politica sociale rivolta al contrasto al crimine, questa volta il paradigma è mutato. Occorre progettare una politica criminale a base tecnologica, una disciplina che integri saperi diversi e che collaborino all'opera di prevenzione e poi di repressione nel contrasto al crimine tecnologico, prendendo atto che gli attori sulla scena non sono più soltanto il criminale, il giudice, la prigione, ma accanto a questi si ritrovano oggi nuovi attori istituzionali e professionalità inedite in campo penale[5].

Il vecchio paradigma, infatti, guardava alla relazione tra persone e poi tra persone e soggetti (anche non fisici – persone giuridiche), oggi occorre guardare a una relazione tra soggetti fondata su un diaframma, un legame intermedio, uno strumentario di natura tecnologica, la cui portata deve essere valutata in termini di relazione complessa, dove non esiste un autore del crimine bensì un apparato tecnico o un'infrastruttura immersi nella immaterialità della condotta; una platea di soggetti offendibili di natura vulnerabile per essere anche sotto-dotati tecnologicamente; una giustizia penale che oltre ai codici è chiamata a utilizzare mezzi altamente sofisticati per accertare i fatti; un processo penale la cui lunghezza può lasciare insoddisfatti i danneggiati se non si dota di un contesto tecnologico oltre che tecnico-giuridico che offra tempestività ed effettività alla decisione[6].

Il tema ha raggiunto una tale dimensione che il penalista tradizionale perde di vista il "fatto reato", la sua articolazione costitutiva, la sua rilevanza sociale, e prende atto che la sua analisi deve affrontare fenomeni di massa, danni a interessi giuridicamente qualificati che riguardano un numero indefinibile di individui – i c.d. reati a soggetto passivo diffuso –; illeciti commessi su un territorio senza confini; identificazione dei responsabili le cui tracce si disperdono in un universo immateriale[7]. L'indagine probatoria per l'accertamento del reato si depotenzia nell'attraversare percorsi che non sono più di semplice constatazione di una circostanza concreta, ma di un apprezzamento che passa per le maglie di discipline tecniche anche diverse da quella giuridica. La prova biologica del DNA divenuta la regina nei reati di sangue viene sostituita nei reati informatici dalla prova tecnologica della produzione e dell'uso del dato digitale.

Anche da un punto di vista didattico occorre aprire gli occhi ai giovani studenti su questo nuovo mondo, destinato a introitare rapidamente il vecchio, insegnando che le regole del vecchio non sono più sufficienti e adeguate a comprendere il nuovo e ricomporre un ordine conferente alle sue caratteristiche.

Anche la categoria della c.d. "quarta rivoluzione industriale" appartiene al lessico di un modello tradizionale, superato, di considerare il rapporto uomo-macchina[8]. Oggi è necessario guardare a un rapporto rovesciato macchina-uomo, non solo perché la macchina si sostituisce all'uomo seguendo la progettazione dell'uomo, ma perché la macchina tende a divenire indipendente dall'uomo e l'uomo è destinato a intervenire solo per correggere o arginare l'azione dei meccanismi tecnologici che compongono una nuova macchina: dal Web 2.0 con interazione tra gli utenti al Web 4.0 con la prevalente operatività dell'Intelligenza Artificiale[9]. La frontiera è la difesa dell'uomo e delle sue libertà rispetto alle iniziative di una "macchina pensante".

Ecco, dunque, che il vasto panorama dei regimi regolativi è talmente ampio e variegato che con la sola esegesi svolta sull'attuale assetto normativo con la disseminazione in vari testi legislativi si rischia di prospettare in maniera caotica e confusa la materia, per cui anche la ricerca di un ordine sistematico dotato di intrinseca razionalità va svolta con rigore ed equilibrio.

5. Picotti–Salvadori–Flor (s.d.), p. 5.
6. Sisto 1985, p. 28.
7. Cadoppi–Canestrari–Manna–Papa 2023.
8. Mantovani 1968; Rodotà 1973.
9. Si tratta della fonte base dettata dal Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024. Il quadro delle fonti del diritto si è completato con la legge n. 132 del 23 settembre 2025 che regola l'uso dell'Intelligenza Artificiale in Italia.

2. Il bisogno crescente di protezione

L'istanza di protezione rivolta al diritto penale deve prendere atto che occorre introdurre un presidio di tutela penale a struttura funzionale composita: da un lato la *Cybersecurity*, vista come difesa del complesso tecnologico, vale a dire dei sistemi e delle strutture informatiche dagli attacchi ostili provenienti dall'esterno; dall'altro la *Sicurezza informatica*, vale a dire la protezione delle informazioni e dei programmi per il loro trattamento[10].

In generale appare più congruente ridefinire la materia come quella della "Sicurezza informatica e dei dati" per compendiare gli entrambi assetti di tutela che meritano una sinergica regolazione giuridica di prevenzione e repressione.

Gli attacchi informatici provenienti dall'esterno – *cyber* attacchi – vengono realizzati con appositi programmi ostili definiti *malware* che analizzano e sfruttano la vulnerabilità dei sistemi informatici e, in questo modo, l'abuso della tecnologia informatica ai fini di profitto illecito può portare alla consumazione di reati che vanno a comporre la classe dei *cybercrimes*.

La punta estrema di questo nuovo modo di sviluppare un moderno conflitto è la *cyberwar*, un modo diverso di manifestare ostilità, in cui l'iniziativa offensiva viene sempre portata nell'ombra della difficile identificazione dei responsabili e dove il destinatario ha la necessità di difendersi con gli stessi mezzi e, anzi, mettere in campo sempre nuove e più aggressive armi tecnologiche.

Questa è la ragione per cui, diversamente dal mondo reale, c'è bisogno di forme di tutela differenziata per la difesa dalle ostilità informatiche, una tutela tecnologica e una tutela giuridica che svolgano simultaneamente quella funzione preventiva e punitiva[11].

La realtà insegna che nella finalità degli attacchi è insita la sottrazione o il rendere temporaneamente indisponibili le informazioni di archivio e le operatività delle risorse informatiche in settori nevralgici della società, quali quello commerciale, strategico, militare, sanitario, per ottenere un profitto illecito. Sul piano del danno si stima, infatti, che queste pratiche illegali sempre più diffuse hanno registrato negli ultimi anni un peso economico su scala mondiale di oltre 2000 miliardi di dollari.

Per raggiungere questi obiettivi vengono elaborati sofisticati programmi detti *ransomware*, un tipo di *malware*, applicazione malevole, che viene progettata per infettare il sistema colpito e in questo modo estorcere denaro con il sequestro (blocco dei dati o del sistema) e la criptazione dei file. Si sono registrati nel corso degli ultimi cinque anni attacchi alla Campari (con riscatto richiesto di 15 milioni di dollari nel 2020); Enel (due attacchi nel 2020, nel secondo il ransomware NetWalker ha usato la *tecnica della doppia estorsione*, dopo aver rubato circa 5 tb di dati ha minacciato di renderli pubblici qualora non fosse stato pagato il riscatto di 16 milioni di dollari); Bonfiglioli (2019); Zambon (2020); Geox, Luxottica, Agenzia Territoriale per la Casa di Torino (2021); Comune di Brescia (2021); fino al caso più clamoroso della Regione Lazio, colpita a inizio agosto 2021.

Va subito posto in evidenza che il tema sul piano generale sta acquisendo una configurazione a cerchi concentrici: la gestione politica del settore; la gestione tecnica e la difesa *dei* sistemi informatici; la protezione della persona *dai* sistemi informatici; l'automazione e la responsabilità dei sistemi di Intelligenza Artificiale.

L'idea di tutela dei cerchi concentrici detta le coordinate delle varie competenze sul campo: il primo riguarda le scelte politiche trans-nazionali, come la tutela della libertà e della democrazia; il secondo concerne la complessiva disciplina legislativa nazionale; il terzo tiene conto della disciplina penale come specifico ambito di tutela.

A proposito della tutela penale non si può prescindere dal primo atto sovranazionale che ha coinvolto i singoli stati aderenti, la *Convenzione Cybercrime di Budapest del 2001*, che per la prima volta ha regolato in maniera comune alcune ipotesi

10. Si veda la Comunicazione congiunta al Parlamento europeo e al Consiglio dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, *Resilienza, deterrenza e difesa: verso una cybersicurezza forte per l'Ue*, 13 settembre 2017.
11. A livello di disciplina eurounitaria si veda il Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale e che modifica le Direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), adottato l'11 luglio 2022.

di illecito chiamate ad assumere rilevanza penale in tutti i Paesi sottoscrittori[12].

Questa prima regolazione a livello internazionale ha fatto emergere la necessità di elaborare due distinte categorie normative in campo penale: a) i sistemi informatici quali beni o oggetti di tutela penale; b) i sistemi informatici quali strumenti di commissione dei reati che compaiono come elementi costitutivi della fattispecie incriminatrice[13].

In questo modo assume particolare rilevanza la trasmigrazione della materia informatica dalla categoria dei servizi a quella dei beni, per cui occorre indirizzare la progettualità verso una autonoma e indipendente collocazione sistematica della relativa disciplina penale.

Va sottolineato, peraltro, che in tutti gli interventi legislativi degli ultimi anni, al di là della individuazione di un bene ideale di riferimento, resta al centro dell'interesse del diritto penale e della stesura delle diverse fattispecie incriminatrici uno specifico e ricorrente oggetto materiale del reato. Alla base di tutto il complesso quadro normativo che sta via via delineandosi, infatti, compaiono i sistemi informatici da una parte e i dati digitali o informatici dall'altra, come elementi costitutivi della sicurezza informatica.

3. I valori e i beni giuridici emergenti da tutelare

Nella progettazione normativa degli assetti di tutela non si può non partire dalla persona, identificata da Rodotà in corpo fisico e corpo elettronico, portatrice di interessi specifici: onore, reputazione, riservatezza informatica, sicurezza informatica, proprietà intellettuale, domicilio informatico, genuinità dell'informazione (versus *fake news*).

Ecco perché si impone l'individuazione di un bene giuridico di categoria di nuovo conio, del tutto diverso e onnicomprensivo rispetto alle categorie tradizionali che la dottrina ha utilizzato finora, come ad esempio la riservatezza (*la privacy*) desumendola dalle norme di valore dall'art. 14 Cost. – sulla segretezza della corrispondenza – e dall'art. 15 Cost. – sul domicilio informatico –, e, a livello di regolazione sovranazionale continentale, dal principio di democrazia[14].

Il fulcro dell'assetto di tutela rimane sempre e comunque la persona umana, la sua vita, la sua dignità, seppure con i suoi diritti e la sua operatività rifratta tra realtà concreta e realtà immateriale della Rete, ma da cui non è possibile prescindere in tutti i propositi di protezione di settori e materie che sono semplicemente funzionali al suo sviluppo e alla sua integrità e per nulla assoluti e autonomi[15]. E l'ordinamento giuridico è chiamato a consolidare un sistema di difesa del singolo nell'ambito della collettività in termini di solidarietà umana.

Il passaggio successivo è costituito dalla tutela dei beni funzionali: primo fra tutti il patrimonio, sia in quanto componente informatica sia come finalità di profitto della condotta, oltre a segmenti di mercato, assetti tecnologici, infrastrutture tecniche ed altro[16].

La lesione di questi beni determina, non solo un danno al titolare dell'interesse, ma un rilevante danno reputazionale per le aziende che in questo modo si presentano vulnerabili sul mercato. Senza tenere conto dei sensibili rischi e nocumento per la propria clientela, come accaduto recentemente nel caso di Intesa San Paolo a Bari con accesso abusivo e sottrazioni massive di informazioni sensibili della clientela.

Esaminando il caso dalla prospettiva teleologica in materia penale si tratta di interessi di una categoria composita, dove a emergere non è un singolo bene bensì un "luogo di tutela", in perfetta analogia con il concetto di pubblica economia, anch'esso ampio campo di tutela con interessi differenziati che lo compongono.

12. La cui attuazione nel nostro ordinamento è avvenuta con la legge n. 48 del 18 marzo 2008.
13. Si veda a tale proposito il Disegno di legge 2773 Ministro di Grazia e Giustizia, XI legislatura Camera dei Deputati, secondo il quale le nuove fattispecie criminose rappresentano semplicemente "… nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, ecc.), già oggetto di tutela nelle diverse parti del corpo del codice".
14. Rossato 2014, p. 21.
15. Picotti 2013.
16. Pecorella 2006.

In realtà, in termini di assetto di tutela si prende atto della necessità di apprestare protezione alla sicurezza del settore informatico cogliendo gli stessi profili teorici della tutela dei beni comuni, come avviene per l'acqua, le matrici ambientali. La gestione svolta in maniera non egoistica di un macro-bene, bensì in forma collettiva, dove appunto quella gestione collettiva va a coincidere con la forma di protezione.

Si assiste in questo modo a una prima svolta importante. L'utente non è più tale, ma diventa consumatore, acquisendo i profili identificativi e qualificativi della vittima: si pensi alla profilazione anagrafica, la profilazione professionale, la profilazione sanitaria, ecc.

Da qui la considerazione della posizione di vulnerabilità implicita del soggetto, il quale si trova in quella posizione, per il solo fatto di navigare in Rete, di chi agisce sulla base di un suo consenso presunto, di un consenso non espresso esplicitamente e formalmente, ma indirettamente per il fatto di trovarsi in Rete e sulla base di questa qualificazione viene riconosciuto dagli altri utenti e profilato in modo da essere identificato, seppure non abbia ceduto espressamente il proprio profilo identificativo con il suo consenso.

4. Per una decisa svolta dommatica

Per la sicurezza del settore informatico la dommatica tradizionale deve essere necessariamente rivisitata in ragione delle peculiarità del nuovo ambito normativo. A partire dal concetto di *Cyberspazio* che non ha un territorio di riferimento dove si consumano reati e, dunque, non radica una competenza processuale sempre agevolmente definibile, perché diventa difficile stabilire le coordinate di consumazione del fatto reato a seconda dell'evento o della condotta [17]. Il concetto di libertà di agire che è alla base della fisiologia dell'ecosistema della Rete vede come suo corrispettivo l'autodeterminazione ad agire in ambiti territoriali sempre diversi.

Le note questioni di un controllo preventivo o successive da parte dei provider nel caso *Vividown c. Google* hanno segnato un momento importante per individuare le posizioni di controllo e garanzia in capo alle società che forniscono servizi in Rete e per essi alle persone fisiche le rappresentano[18].

Ma non basta. Occorre ripensare a tutta la dommatica, ai principi di orientamento della materia penale, per adattare ad essa la nuova classe di reati, ripensando all'introduzione di "buone pratiche" legislative per metterla in sincronia con quelle vigenti e allestire nuove ipotesi di reato, puntuali, precise, definite, effettive, pronte ad essere utilizzate dal giudice[19]. Un novero di reati che si caratterizza per le particolari modalità di realizzazione della condotta e per lo strumentario tecnologico in uso nel mondo dematerializzato della Rete che si risolve nella precisione della norma penale come verifica in sede processuale.

Sul piano della struttura del fatto-reato la prima considerazione investe la natura della condotta. Si tratterà di descrivere solo reati di azione, sembrerebbe, confinando il caso dell'omissione colpevole alla regola degli obblighi giuridici dell'art. 40 cpv c.p.

Come valutare e individuare, poi, la causa determinante o la contemporanea esistenza di altre cause che hanno dato vita all'evento facendo ricorso a una disciplina datata al 1930 che già con il banco di prova del disastro innominato non ha fornito adeguate risposte. E in questo caso come può giocare l'incidenza della causa individualizzante sul piano statistico di probabilità e possibilità nell'ottica fornita dalla sentenza Franzese? In questo ambito la relazione causa/effetto come va intesa, dal momento che se nella realtà concreta si può raggiungere un ragionevole grado di certezza,

17. PERUSIA 2001, p. 1835. Più recentemente la Suprema Corte su rinvio pregiudiziale del Tribunale di Perugia ha dettato un importante principio di diritto sulla questione, in Cass. pen., Sez. III, Sent. n. 38511 del 18 settembre 2024, "L'unico parametro di riferimento applicabile è perciò quello di cui al comma 3 dell'art. 9 cod. proc. pen., a tenore del quale la competenza per territorio 'appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto all'art. 335'".
18. Ci sia consentito rinviare a TRONCONE 2014, p. 2060.
19. Secondo le coordinate tradizionali della materia penale, in FIANDACA–MUSCO 2019, p. 43: "…in altri termini assurge a bene giuridico soltanto quell'interesse, o quell'accorpamento di interessi, idonei a realizzare un determinato scopo utile per il sistema sociale o per una sua parte". Sull'assetto delle figure di reato di parte speciale in ordine alla tutela di funzioni, si rinvia a MOCCIA 1995, p. 344.

nel caso della Rete diventa difficile sceverare tra le tante cause che intervengono e si affiancano a quella iniziale e forse perdono vigore per effetto di quelle sopravvenute, queste ultime saranno da reputare sempre eccezionali? Né va escluso il tema del concorso di persone che non si pone soltanto nella prospettiva della individuazione dell'azione oggettivamente svolta, ma soprattutto per la necessità che le indagini giudiziarie abbiano come obbiettivo l'accertamento probatorio di tutti i contributi alla consumazione del reato.

L'evento. In senso naturalistico o sarà da intendere in senso giuridico come sembra suggerire il contesto dematerializzato in cui prende ragione? Tra le pieghe della valutazione del fatto non può mancare il riferimento all'elemento soggettivo e da qui il dilemma se, ai fini risarcitori, va considerato il rischio sociale della navigazione in Rete che qualunque utente dovrà considerare nel momento in cui ne fa accesso, e la rilevanza della colpevolezza a chiudere il cerchio dell'accertamento della responsabilità penale.

Sul piano della risposta punitiva occorre tenere nella debita considerazione anche la responsabilità amministrativa degli enti del d.lgs. n. 231/2001[20]. Soprattutto armonizzando le cause estintive del reato di natura premiale o deflattiva con la legislazione di settore, valorizzando la riabilitazione dell'ente alla luce degli interventi correttivi conformi alle leggi, di *compliance*.

Il vero problema però resta quello di valorizzare gli scudi protettivi per le vittime come ci indirizzano le fonti europee, bersagli di danni che non sempre è possibile qualificare con parametri econometrici.

Esiste inoltre lo scottante problema della permanenza degli eventi dannosi in Rete e, per questo, ipotizzare reati a consumazione prolungata o si tratta soltanto di effetti persistenti di un reato a consumazione istantanea?[21] Come nella corruzione?[22]

Possono permanere in Rete senza soluzione di continuità i patrimoni informativi di persone decedute, i cui eredi non sempre hanno competenza e capacità tecnologiche per gestire la correttezza di quelle informazioni[23]. È possibile ipotizzare l'istituzione di un'Autorità in Rete chiamata a gestire i patrimoni informativi dispersi che potrebbero offendere la memoria dei trapassati?

Le perplessità sono tante, come si vede, e non aiutano gli esempi che quotidianamente registriamo nei vari tribunali territoriali, come quello della richiesta di archiviazione avanzata dalla Procura di Torino di qualche mese fa in ordine a un caso di diffamazione in Rete, sventata dall'intervento correttivo del GIP[24]. Chissà perché, secondo il PM delle indagini, la dematerializzazione dovrebbe depotenziare il contenuto offensivo di espressioni che ledono la reputazione di una persona, e non ritenere che l'effetto moltiplicatore del rimbalzo le rende ancora più cariche di lesività! E cosa penseranno i figli e gli eredi quando leggeranno in Rete frasi e contenuti non rettificati, non è quello un danno che prende vita dal riflesso indiretto dell'originario primo danno?

E poi come è possibile trattare la punibilità di una fonte infettiva, di un *malware* che si propaga in un *device* e si diffonde in Rete? In questo caso occorrono gli ingegneri ad accompagnare il legislatore e prevedere in maniera inequivocabile l'appropriata terminologia da utilizzare, forse con una tabella integrativa della legge come è avvenuto con il d.p.r. n. 309/90 in materia di stupefacenti.

Il punto più oscuro resta però quello della effettività della pena, quale può essere la risposta punitiva in termini di rieducazione aderente a quel tipo, alla natura di quel reato? Forse le c.d. pene tecnologiche e quali?

E le misure cautelari reali come vanno congegnate? E le pene o le misure tecnologiche inabilitative, come spesso si è sentito del c.d. "ergastolo

20. Fondaroli 2019; Monti 2022.

21. Si ricorda che la giurisprudenza è ferma, alla luce della norma vigente, a ritenere la diffamazione con il mezzo del Web un reato di natura istantanea che non diviene permanente per gli effetti persistenti dell'offesa in Rete, come stabilisce Cass. pen., Sez. V, Sentenza n. 32533 dell'11 luglio 2025.

22. Aimi 2020.

23. Marseglia 2025.

24. Tribunale di Torino, Ufficio del GIP, ordinanza del 14 gennaio 2025, in "Giurisprudenza penale" (online), 20 gennaio 2025.

informatico", come vanno irrogate e controllate? L'esperienza del braccialetto elettronico per le misure alternative ci fornisce spunti di esperienza importanti per comprendere la fallibilità di un sistema tecnologico che non si mostra ancora all'altezza delle sfide da affrontare.

Infine, quale risposta indennitaria per la vittima in permanente minorata difesa tecnologica?

Va ricordato a tale proposito che la nuova legge sull'Intelligenza Artificiale n. 132 del 2025, però esclusivamente per le ipotesi di reato in essa contenute, ha introdotto una nuova specifica aggravante con il n. 11-*decies* all'art. 61 c.p. sulla minorata difesa della vittima.

5. Da dove cominciare? La necessità di un Codice autonomo

Riteniamo sia giunto il momento di dare vita a un'esperienza legislativa destinata a sciogliere tutti i nodi sistematici di questa complessa materia che acquista progressivamente una sempre maggiore ampiezza mettendo in campo un corpo normativo unico che potrebbe assumere la denominazione di "Codice per la sicurezza informatica e dei dati".

In questo modo si darebbe valore a una nuova area di tutela penale racchiusa nella denominazione cybersicurezza, dove il comune denominatore è costituito dai mezzi informatici e i dati digitali che le danno vita.

La prassi applicativa degli ultimi anni registra preoccupanti crepe interpretative dovute alle asincroniche simmetrie tra tecnologia in evoluzione e disciplina giuridica in costante ritardo che spinge l'opera dei giudici verso una giurisprudenza creativa oltre il rigido testo normativo. In questo modo si evidenziano i limiti di una legislazione improvvisata e sprovvista dal suo nascere di un criterio organizzativo sistematico che fornirebbe la chiave di lettura a soluzioni coerenti[25]. L'opera legislativa, purtroppo, si attesta sull'esigenza di dettare norme secondo la necessità contingente priva di una strategia di lunga durata, inserendo nuove figure di reato o innumerevoli aggravanti in norme penali già esistenti sotto i più diversi interessi giuridici di categoria che frammentano sempre di più il contesto della materia.

Occorrerebbe invece richiamare l'impegno deontologico del legislatore nella cura della legge, verso una formulazione anche lessicale che non debba lasciare margini al dubbio nei destinatari in termini convenzionali di prevedibilità della condanna, e nel giudice chiamato ad applicarla con sufficiente precisione[26].

Va ricordato che diversamente dal passato è stato dettato un vincolo normativo al legislatore con l'art. 3-*bis* c.p., "Principio della riserva di codice", vale a dire l'obbligo di disciplinare in modo organico fattispecie incriminatrici appartenenti a una stessa materia[27]. Una materia che va individuata sulla base del comune denominatore intorno al quale strutturare il precetto e che trova il suo punto di qualificazione giuridica, il suo comune denominatore di principio, appunto, nella "Sicurezza informatica e dei dati".

Da un punto di vista della tecnica normativa occorre fare leva sull'art. 15 del codice penale, "Materia regolata da più leggi penali o da più disposizioni della medesima legge penale", e mettere in campo figure di reato, seppure nel *genus* già esistenti nella legislazione, nella *species* distinte per elementi specializzanti, come si è proceduto – forse in maniera sovrabbondante – con il delitto di danneggiamento dell'art. 635-*bis* c.p. e non come avvenuto con l'introduzione del terzo comma dell'art. 629 c.p. che punisce l'estorsione informatica non come una semplice circostanza ma come una autonoma ipotesi di reato.

Un Testo Unico coordinato sotto la denominazione di un nuovo catalogo di reati eviterebbe i continui rinvii sistematici che gli attuali testi contengono, sottraendo omogeneità e coerenza alla normativa di settore.

Peraltro, seguendo l'esempio delle direttive dell'Unione europea, sarebbe addirittura

25. Posizione più volte ribadita, tra gli altri, da Fumo 2013, p. 775: "Forse anche per questo – muovendosi in un'ottica di stampo contenutistico – il legislatore ha ritenuto di non varare un corpus unitario di (nuove) norme repressive, ma ha scelto di prevedere le 'nuove condotte criminali' (se non tutte, almeno le più rilevanti), collocandole 'topograficamente' negli habitat normativi che sembravano – di volta in volta – più opportuni. Non sempre si è trattato però di scelte felici"; Picotti 2020, p. 709.
26. Viganò 2025.
27. Donini 2018.

auspicabile una sinossi normativa in apertura del provvedimento, contenente la esatta definizione dei vari requisiti e dei concetti come elementi di tipicità contenuti nelle diverse figure di reato.

Ad esempio, non è sempre chiaro in quale modo il legislatore declini il concetto di vantaggio, cosa diversa dal profitto, eppure utilizzato indifferentemente, come nel caso della finalità ulteriore a quella esclusivamente economica nel furto[28].

Con questo indirizzo non vi sarebbe stato alcun problema nel ritenere infondata la qualificazione normativa di una semplice SIM in quella di apparato telefonico, nessuna assimilazione per analogia sarebbe stata mai ipotizzata a partire dal terreno tecnologico oltre che giuridico, nodo sciolto invece nel 2024 con una pronuncia della Suprema Corte di Cassazione[29].

Attualmente, invece, assistiamo a degli innesti normativi di nuove fattispecie nelle classi di reato tradizionali e di parti di norme nei precetti preesistenti che non sempre mostrano una decisiva coerenza: delitti contro la libertà morale, contro l'inviolabilità del domicilio, contro l'inviolabilità dei segreti, contro il patrimonio.

Ad esempio, il c.d. *revenge porn* o meglio la "Diffusione illecita di immagini o video sessualmente espliciti" dell'art. 612-*ter* c.p. è una forma di trattamento illecito di dati personali, è violazione della riservatezza, e tuttavia non si trova nel Codice del trattamento dei dati personali perché in apertura dell'art. 167 CdP vi è una clausola di sussidiarietà espressa che lo esclude[30]. Su questa scia si pone la nuova figura di delitto di "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale" introdotta con l'art. 612-*quater* c.p. dalla legge n. 132 del 2025 consistente nella manipolazione di dati nota come *deepfake*.

A ben vedere, si tratta del medesimo fatto, con le medesime modalità di realizzazione, sebbene con un diverso disvalore il che implica che il disvalore autonomo dell'art. 167 CdP ha ceduto il passo e viene dequalificato solo per ragioni di misura della pena.

A titolo di pura esemplificazione va segnalata la profonda interrelazione tra i delitti degli artt. 615-*ter* "Accesso abusivo ad un sistema informatico" e 615-*quater* "Detenzione, diffusione e installazione abusiva di apparecchiature, codici e latri mezzi atti all'accesso a sistemi informatici o telematici" del codice penale e quello previsto nel Codice del trattamento dei dati all'art. 167-*bis* "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala" che sembra replicarne i caratteri seppure armonizzati con una clausola di sussidiarietà espressa.

Ad esempio, il campo patrimoniale delle criptovalute vede nei loro meccanismi di funzionalità un trattamento di dati non personali, contenuti nelle due chiavi informatiche che ne regolano la titolarità. Non c'è uno scambio di valuta bensì uno scambio di dati che coincide con uno scambio di valori economici. Andrebbe, dunque, ipotizzata una disciplina specifica nel campo informatico, per assicurare la stessa tutela che il codice penale riserva alla moneta ufficiale in corso, prima la lira oggi l'euro.

Su questo tema si agita senza sicuri approdi la giurisprudenza degli ultimi anni, non avendo il legislatore regolato al pari delle monete virtuali il regime giuridico della circolazione delle criptovalute e il criterio di valorizzazione attribuito dal mercato, marcandola soltanto a fini fiscali quale forma di accumulazione della ricchezza e rendendo in questo modo anche ardua l'applicazione di tutte le ipotesi di sequestro penale degli artt. 240 e ss. c.p. finalizzati alla confisca[31].

In definitiva, le condotte di sopraffazione della criminalità in questo settore sono particolarmente pervasive e insidiose, peraltro attivate in uno spazio indistinto che si scontra con i nostri strumenti di tutela tradizionali che alla base registrano spazi

28. Cass. SS.UU. pen., Sent. n. 41570 del 25 maggio 2023.
29. Cass. pen. Sez. VI, Sent. n. 42941 dell'11 settembre 2024, che ha dichiarato illegittimo estendere la norma dell'art. 391-*ter* c.p., che vieta l'introduzione di apparecchi telefonici cellulari in carcere, anche alla scheda SIM, negandone la natura di "dispositivo mobile".
30. Correra–Martucci 1986.
31. Corasaniti 2012, p. 819. Così come anche previsto all'art. 30 – *Abusivismo – della Legge sui mercati delle cripto-attività*, d.lgs. n. 129 del 5 settembre 2024.

finiti, confini certi, elementi identificativi concreti e incontrovertibili[32].

Occorre, dunque, ricalibrare in termini moderni il catalogo "dei delitti e delle pene" di questa materia, destinato a confrontarsi con una nuova e diversa realtà, quella immateriale, e che, nostro malgrado, invoca nuove mappe e coordinate di navigazione per la salvaguardia delle nostre libertà.

Riferimenti bibliografici

A. Aimi (2020), *Le fattispecie di durata. Contributo alla teoria dell'unità o pluralità di reato*, Giappichelli, 2020

A. Alessandri (1990), *Criminalità informatica*, in "Rivista trimestrale di diritto penale dell'economia", 1990

M.R. Allegri (2016), Riflessioni e ipotesi di costituzionalizzazione del diritto di accesso a Internet, in "Rivista AIC", 2016, n. 1

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

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

G. Corasaniti (2012), *Brevi note in tema di confisca obbligatoria di beni e strumenti di commissione dei reati informatici alla luce della legge 15 febbraio 2002 n. 12*, in "Diritto dell'informazione e dell'informatica", 2012

M. Correra, P. Martucci (1986), *I reati commessi con l'uso del computer. Banche dati e tutela della persona*, Cedam, 1986

M. Donini (2018), *La riserva di codice (art. 3-bis cp) tra democrazia normante e principi costituzionali. Apertura di un dibattito*, in "La legislazione penale", 20 novembre 2018

G. Fiandaca, E. Musco (2019), *Diritto penale. Parte generale*, Zanichelli, 2019

D. Fondaroli (2019), *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.Lgs. n. 231/2001*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime – omnia – Trattati giuridici", Utet, 2019

M. Fumo (2013), *La condotta nei reati informatici*, in "Archivio penale", 2013

F. Mantovani (1968), *Mezzi di diffusione e tutela dei diritti umani*, in "Archivio giuridico", 1968

R. Marseglia (2025), Privacy *e tutela dei dati personali* post mortem, Esi, 2025

S. Moccia (1995), *Dalla tutela di beni alla tutela di funzioni: tra illusioni e riflussi illiberali*, in "Rivista italiana di diritto e procedura penale", 1995

A. Monti (a cura di) (2022), *Cybercrime e responsabilità da reato degli enti. Prevenzione e modello organizzativo e indagini preliminari*, Giuffrè, 2022

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

C. Pecorella (2006), *Diritto penale dell'informatica*, Cedam, 2006

E. Perusia (2001), *Giurisdizione italiana anche per le offese on line su un sito straniero*, in "Cassazione penale", 2001

32. Alessandri 1990.

G. Pica (1999), *Diritto penale delle tecnologie informatiche*, Utet, 1999

L. Picotti (2020), *Cybercrime e diritto penale*, in C. Parodi, V. Sellaroli (a cura di), "Diritto penale dell'informatica. Reati della rete e sulla rete", Giuffrè, 2020

L. Picotti (2013), *Tutela penale della persona e nuove tecnologie*, Cedam, 2013

L. Picotti, I. Salvadori, R. Flor (s.d.), *Reati informatici, riservatezza, identità digitale*, in "www.aipdp.it", s.d.

S. Rodotà (2010), *Una costituzione per Internet?*, in "Politica del diritto", 2010

S. Rodotà (1973), *Elaboratori elettronici e controllo sociale*, il Mulino, 1973

A. Rossato (2014), *Sulla natura dei beni comuni digitali*, in A. Pardi, A. Rossato (a cura di), "I beni comuni digitali. Valorizzazione delle informazioni pubbliche in Trentino", Quaderni della Facoltà di Giurisprudenza, Trento, 2014

F.P. Sisto (1985), *Diritto penale dell'informatica e recupero dei modelli tradizionali*, in "Critica penale", 1985

P. Troncone (2014), Il caso *Google* (e non solo). Il trattamento dei dati personali e i controversi requisiti di rilevanza penale del fatto, in "Cassazione penale", 2014

F. Viganò (2025), *Chiarezza della legge e principi costituzionali*, in "Sistemapenale.it", 30 settembre 2025

V. Zeno-Zencovich (2003), *Informatica ed evoluzione del diritto*, in "Il diritto dell'informazione e dell'informatica", 2003