Cybersecurity e diritto penale. Verso la tutela di un bene giuridico di nuova generazione, tra passato, presente e prospettive future

Roberto Flor*

Ricevuto 6 gennaio 2026 – Accettato 26 gennaio 2026

Sommario

L'Autore svolge, alla luce dell'entrata in vigore su sollecitazione europea di novità legislative in materia di reati informatici, alcune riflessioni relative all'esigenza di tutela penale di beni giuridici di nuova o nuovissima generazione, rispetto a tradizionali e innovative forme di aggressione. Nel considerare questi beni come espressione altresì di inedite forme di manifestazione dei diritti fondamentali, si propone, in particolare, di trovare un fil rouge tra le proteiformi definizioni di "cybersecurity". Di quest'ultima è suggerito un concetto "sostanziale" e "prepositivo" in modo tale che esso possa costituire parametro razionale di orientamento delle scelte anche di politica criminale, ma nella consapevolezza di un necessario e costante dialogo fra discipline. La scienza e il sapere tecnologico dovrebbero influenzare il diritto, in un'ottica di interazione reciproca per la comprensione dei diversi linguaggi.

Parole chiave: cybersecurity, cybercrime, bene giuridico, riservatezza informatica, privacy, CIA Triad

* Università di Verona. roberto.flor@univr.it.

De Iustitia et Iure (ISSNe 3103-2761), 2/2025
DOI: 10.3280/ius2025oa21816

Cybersecurity and criminal law. Towards the protection of a new generation legal assets, between past, present, and future perspectives

Abstract

In light of the entry into force of new European legislation on cybercrime, the Author offers some reflections on the necessity for criminal protection of new and emerging legal assets against traditional and innovative forms of aggression. In considering these assets as expressions of new forms of fundamental rights, he proposes to identify a common denominator among the protean definitions of "cybersecurity". In order to achieve this objective, he proposes the adoption of both a "substantive" and "prepositional" concept of cybersecurity. This approach facilitates its function as a rational parameter for guiding choices, including those pertaining to criminal policy. However, it is imperative to recognize the necessity for constant dialogue between disciplines. It is submitted that science and technological knowledge should have a significant impact on the formulation of legislation, with a view to fostering mutual interaction for the understanding of different languages.

Keywords: cybersecurity, cybercrime, legal asset/interests, IT confidentiality, privacy, CIA triad

1. Introduzione

Il dibattito in Italia sulla nascita di nuovi beni giuridici nel contesto tecnologico si è sviluppato già all'indomani della L 547/1993 – di attuazione della Raccomandazione R (89)-9 del 13 settembre 1989 del Comitato dei Ministri del Consiglio d'Europa sulla criminalità informatica – che ha introdotto nel Codice penale nuove fattispecie incriminatrici. Si tratta del primo intervento sistematico *in subiecta materia*. Il legislatore, infatti, ha inserito le nuove disposizioni incriminatrici ricalcando struttura e contenuto di quelle vigenti, seguendo il parametro guida del bene giuridico protetto[1].

Infatti CP 615-*ter* ("Accesso abusivo a sistemi informatici o telematici") e 615-*quater* ("Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi infor-

[1] Si rinvia a Flor, Marcolini (2022) pp. 147 ss., cui si rinvia per gli ulteriori riferimenti bibliografici.

matici o telematici") sono stati collocati fra i delitti contro l'inviolabilità del domicilio, dopo CP 614; 615 e 615-*bis*. Anche CP 617-*quater* ("Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche"), 617-*quinquies* ("Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche") e 617-*sexies* ("Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche"), che riguardano le comunicazioni «fra sistemi informatici», seguono i precedenti CP 617; 617-*bis* e 617-*ter* i quali, già introdotti nel codice dalla L 98/1974, hanno ad oggetto la tutela della riservatezza e della libertà e segretezza delle comunicazioni «fra persone».

In particolare, dall'entrata in vigore di CP 615-*ter*, si sono susseguite diverse tesi riguardanti il suo oggetto giuridico. È stato sostenuto che la fattispecie tutelasse la "privacy", intesa non più solo nel significato riduttivo di «the right to be let alone»[2], il domicilio informatico, ovvero configurasse un reato plurioffensivo, a tutela anche dell'integrità del sistema, dei programmi, dei dati e delle informazioni[3].

Il nostro legislatore, con la L 48/2008, di ratifica della citata Convenzione Cybercrime, non ha ritenuto necessario modificare la formulazione originaria di CP 615-*ter*, confermando pertanto le scelte di politica criminale degli anni '90.

In questo senso, all'interesse all'esclusività dell'accesso ad uno o più spazi informatici, che costituiscono, nell'odierna società tecnologica e di Internet, un'espansione ideale ed una evoluzione naturale dell'area afferente alla sfera personale dell'individuo, si affianca natu-

[2] Warren, Brandeis (1890) pp. 193 ss.

[3] Cfr. già Mantovani (1994) pp. 17 ss.; Galdieri (1997); Nunziata (1998) pp. 711 ss. Il riferimento al «domicilio informatico» si rinviene ancora nella giurisprudenza di legittimità più recente: Cass. Pen. SS.UU. 7 febbraio 2012, n. 4694, con commento di Flor (2012) pp. 126 ss., cui si consenta di rinviare per gli ulteriori riferimenti bibliografici; cfr. Bartoli (2012) pp. 123 ss.; Cass. Pen. SS.UU. 24 aprile 2015, n. 17325, con commento di Flor (2015) pp. 1296 ss., cui si rinvia per ulteriori riferimenti bibliografici e giurisprudenziali. Vedi anche, in commento a Cass. Pen. SS.UU. 18 maggio 2017, n. 41210, Flor (2018) pp. 506 ss., cui si consenta di rinviare per gli ulteriori riferimenti bibliografici.

ralmente l'interesse all'affidabilità e fiducia della collettività nella sicurezza dello svolgimento dei rapporti giuridici che si instaurano attraverso l'uso di strumenti tecnologici e di spazi informatici.

A prescindere dalle funzioni che si vogliono attribuire alla tutela penale della sicurezza informatica – positiva e negativa[4] – comunque orientate ad assicurare la tutela dell'interesse alla riservatezza informatica ed alla generale correttezza dello svolgimento dei rapporti giuridici, essa deve trovare un bilanciamento con l'esigenza di garantire la libertà di circolazione dei dati e delle informazioni, nonché con la loro libera accessibilità e fruibilità. Tale bilanciamento risulta essere più complesso per la crescente vulnerabilità dei sistemi informatici, dei dati e delle informazioni in essi archiviati, dovuta a forme di aggressione sia "tradizionali" che "tecnologiche" che si evolvono con lo stesso sviluppo tecnologico.

La L 90/2004 ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici") è recentemente intervenuta sul sistema dei reati informatici.

Al di là della rilevanza mediatica di tale intervento, elevato alla stregua di un "giro di vite" contro il cybercrime, seguito poi a stretto giro dalla L 132/2025 ("Disposizioni e deleghe al Governo in materia di Intelligenza artificiale"), il suo impatto, sul piano del diritto penale sostanziale, appare davvero limitato ad un generale inasprimento della risposta sanzionatoria e a taluni "correttivi", fra cui, per citare solo alcuni esempi, l'introduzione di una nuova ipotesi di reato (CP 629, 3), nel tentativo di rispondere alla diffusione (soprattutto) di cyber-attacks "ransomware", di cui si dovranno attendere le prime applicazioni giurisprudenziali per vagliarne effettività ed efficacia, e l'abrogazione, in particolare, di CP 615-*quinquies*, che, in verità, viene collocato fra i reati contro il patrimonio (*ex* CP 635-*quater*.1) con la previsione di due nuove circostanze aggravanti. Oppure si pensi al reato di truffa di cui a CP 640, che viene arricchito da un ulteriore comma (2-*ter*), se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione.

Appare evidente che l'esigenza di assicurare tutela penale della cybersecurity non corrisponde ad una necessità costruita artificialmente,

[4] Cfr. Picotti (2011) pp. 217 ss.

ma esprimerebbe il bisogno «di assicurare una condizione condivisa nella società dell'informazione»[5].

La stessa L 132/2025 in materia di Intelligenza Artificiale evidenzia come, in questo contesto, lo sviluppo di sistemi e di modelli di intelligenza artificiale avvenga su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati. Le disposizioni in essa contenute, inoltre, sono volte a valorizzare l'intelligenza artificiale anche come risorsa per il rafforzamento della cybersicurezza nazionale.

Proprio al fine di garantire il rispetto dei diritti e dei princìpi espressi da tale atto normativo deve essere assicurata, quale precondizione essenziale, la cybersicurezza durante tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale per finalità generali, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza.

Fra il resto la medesima legge ha introdotto alcune aggravanti speciali per «l'aver commesso il fatto mediante l'impiego di sistemi di i.a.» e inserito, nel lungo elenco di circostanze previste al CP 61, 1, l'aggravante comune di cui al n. 11-*decies*, che si applica ai casi in cui il fatto sia stato commesso

«mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato».

[5] Ne è una emblematica dimostrazione l'attacco *hacker* del 12 maggio 2017 denominato "Ransomware/WannaCry" che ha colpito, in più di 150 paesi, enti pubblici e grandi aziende private installandosi all'interno dei sistemi informatici criptando ogni *file* salvato sull'*hard disk* e su eventuali periferiche, chiedendo il pagamento di un riscatto in criptovalute per poter riavere i dati, nonché le piene funzionalità dei sistemi operativi. Vedi Flor (2019) pp. 443 ss.

Con il presente lavoro, anche alla luce dell'entrata in vigore di queste ultime novità legislative, si intendono proporre alcune brevi riflessioni relative all'esigenza di tutela penale di beni giuridici di nuova o nuovissima generazione, rispetto a tradizionali e innovative forme di aggressione. Beni espressione altresì di inedite forme di manifestazione dei diritti fondamentali, tenendo ben presente la necessità di trovare un fil rouge tra le proteiformi definizioni di "cybersecurity".

2. Cybersecurity e tutela penale in Italia

Dopo la L 547/1993 (prima normativa in materia di cybercrime) e la L 48/2008 (di attuazione della Convenzione del Consiglio d'Europa sulla criminalità informatica – Convenzione Cybercrime) non si è assistito ad ulteriori interventi di carattere sistematico, e tanto meno risponde a simile esigenza la recente L 90/2024 che contiene, da un lato misure di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario e, dall'altro lato, interventi nell'ambito dei reati informatici.

Si tratta, quest'ultima, di una legge che, per il vero, si inserisce in un contesto europeo in cui l'Unione europea stessa lavora su vari fronti per promuovere la resilienza informatica, ivi compresa la resilienza operativa digitale per il settore finanziario (si pensi solo, a titolo esemplificativo, al Regolamento UE 2022/2554).

La legislazione penale italiana *in subiecta materia*, infatti, è stata sin dall'origine caratterizzata da un insieme di norme incriminatrici eterogenee, frutto di interventi spesso settoriali o frammentari imposti, da un lato, dalla necessità di colmare alcune lacune emerse nella prassi applicativa, dall'altro lato di dare attuazione alle fonti internazionali ed europee.

Si pensi che per più di 30 anni CP 615-*ter*, fattispecie fulcro nel microsistema dei reati informatici, non ha subito modifiche, tanto che si sono susseguite diverse tesi riguardanti il suo oggetto giuridico. È stato sostenuto, inizialmente, che la fattispecie tutelasse la privacy, intesa non più solo nel significato riduttivo di «the right to be let alone», il domicilio informatico, ovvero configurasse un reato plurioffensivo,

a tutela anche dell'integrità del sistema, dei programmi, dei dati e delle informazioni. Il nostro legislatore poi, nel 2008, non ha ritenuto necessario modificare la formulazione originaria di CP 615-*ter*, confermando pertanto le scelte di politica criminale degli anni '90.

Oggi, anche dopo il limitato intervento del legislatore del 2024 (vedi *infra*), l'individuazione dell'oggetto giuridico tutelato deve avvenire attraverso l'interpretazione sistematica e teleologica di questa fattispecie da porre in relazione ad altri reati, tra cui quelli *ex* CP 615-*quater*; 617-*quater*; 617-*quinquies* e 617-*sexies*.

Nell'era dell'interconnessione, della comunicazione globale e dell'infosfera, nonché dell'accessibilità e della fruibilità delle risorse attraverso la rete e qualsiasi strumento di comunicazione anche mobile, lo "spazio informatico" è rapidamente passato da una dimensione privata o singola ad una "dimensione pubblica". In altri termini all'interesse del singolo si affianca quello super-individuale o di natura collettiva a che l'accesso a tali spazi, ai sistemi e ai dati informatici ed alla stessa rete avvenga per finalità lecite e in modo tale da essere regolare per la sicurezza degli utenti, pur mantenendosi quale «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost.» e strumentale per l'esercizio degli stessi diritti fondamentali dell'individuo.

Per cui, da un lato, è innegabile che una componente di tale "area riservata" riguardi la facoltà, il potere, il diritto del titolare di gestire in modo autonomo le utilità e le risorse del sistema informatico, nonché i contenuti delle comunicazioni informatiche (o telematiche), indipendentemente dalla loro natura; dall'altro lato, appare indispensabile un bilanciamento con le esigenze connesse alla "sicurezza informatica". Sia quest'ultima che la "riservatezza informatica", dunque, contribuiscono a delineare un livello anticipato e preventivo di protezione rispetto al momento dell'effettiva lesione dell'integrità delle informazioni, dei programmi o dei sistemi informatici, nonché alla presa di cognizione dei contenuti dei dati ivi archiviati o trattati, anche di natura riservata o segreta. Simile prospettiva di tutela, che valorizza i profili funzionali della sicurezza informatica, è direttamente rafforzata da dati normativi, espliciti ed autonomi. *In primis*, CP 615-*ter* offre protezione penale solo ai sistemi protetti da "misure di sicurezza". Le

diverse tesi interpretative sul "ruolo" di tale elemento costitutivo convergono su almeno una argomentazione comune e insuperabile: la legge penale non definisce la natura delle misure protettive e non richiede che esse siano efficaci e idonee. A tali misure, dunque, il legislatore sembra aver ragionevolmente affidato il compito di manifestare lo *ius excludendi alios* del titolare dello spazio informatico. In secondo luogo, CP 615-*ter*, 2, n. 3, prevede un aumento della pena e la procedibilità d'ufficio se dal fatto derivi la «distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti». La L 90/2024 ha apportato un sensibile inasprimento sanzionatorio per le ipotesi aggravate di cui al comma 2, prevedendo la pena della reclusione da 2 a 10 anni inserendo, proprio nell'ipotesi di cui al n. 3, dopo le parole: «ovvero la distruzione o il danneggiamento» le seguenti: «ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare».

Questa locuzione, da un lato e sul piano sistematico, pare voler rafforzare la già stretta connessione fra riservatezza, integrità e sicurezza informatiche, offese o messe in pericolo dalle condotte previste da CP 615-*ter*. Dall'altro lato, il legislatore è caduto nel medesimo errore del legislatore del 2013 quando, questo ultimo, con la L 119/2013 (di conversione con modificazioni del DL 93/2013) ha introdotto in CP 640-*ter* un nuovo comma, che sanziona ancora oggi la frode informatica commessa mediante sostituzione (furto o indebito utilizzo) dell'identità digitale in danno di uno o più soggetti. L'espressione "furto" di identità digitale sembra richiamare (impropriamente) le condotte di sottrazione e impossessamento previste da CP 624, che sono tecnicamente riferite ad un oggetto fisico-materiale, espresso dal termine "cosa".

Riproporre a più di dieci anni di distanza l'espressione "sottrazione" riferita ai dati sembra confermare un difetto di comprensione della "regola tecnologica", essendo i dati, per loro stessa natura, insuscettibili di sottrazione ed impossessamento.

La rapidità dell'evoluzione tecnologica ha sempre rappresentato

una sfida per il diritto e, in particolare, per la legislazione e la giurisprudenza penale. Proprio la comprensione della regola tecnologica costituisce e probabilmente costituirà un fattore determinante, in quanto deve entrare nelle scelte di politica criminale, come la tecnologia entra e entrerà sempre più frequentemente fra gli strumenti investigativi e decisori, gli elementi costitutivi della fattispecie incriminatrice, le note modali di realizzazione della condotta, nonché quale oggetto di tutela se non di espressione essenziale dell'oggettività giuridica, anche quale spazio immateriale e a-territoriale attraverso cui persone, enti ed istituzioni prestano le loro attività ed i loro servizi e garantiscono la regolarità dei rapporti giuridici. La comprensione della regola tecnologica dovrebbe guidare altresì l'interpretazione della fattispecie legale, nel limite dei possibili significati penalmente rilevanti del testo, per evitare "acrobazie" ermeneutiche espressione di approcci decisamente "vintage", nascosti in argomentazioni solo apparentemente di stampo evolutivo ma, di fatto, risultato persino di applicazioni analogiche *in malam partem* dettate da una serie di fattori contingenti, fra cui la preoccupazione di lasciare vuoti di tutela penale. Il rischio da evitare è quello "scollamento" fra il contesto tecnologico-sociale, le scelte del legislatore e l'interpretazione delle singole disposizioni.

Deve aggiungersi che, per quanto attiene ai "fatti" tipizzati dai delitti di danneggiamento informatico, anche dopo l'intervento del legislatore del 2024, la dimensione del bene giuridico tutelato non sembra potersi ridurre al patrimonio del titolare dei sistemi o dei dati, che rimane sullo sfondo. Essa è invece estesa all'integrità e alla disponibilità dei dati e dei sistemi informatici e telematici se non persino, per quanto riguarda le incriminazioni di cui a CP 635-*ter* e 635-*quinquies* – strutturati come delitti di attentato – l'ordine pubblico. L'elemento comune e l'area di intersezione fra dimensione individuale e dimensione collettiva del bene tutelato, è costituita dall'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 di uno o più soggetti "titolari", ovvero dal potere di determinare, in sé, il "destino" di tali aree informatiche in cui si manifesta

la personalità umana. Il rafforzamento della tutela penale della riservatezza e sicurezza informatiche era comunque già assicurata sia dalla fattispecie ostacolo di cui a CP 615-*quater* – che sanziona condotte prodromiche all'accesso abusivo ad un sistema informatico o telematico tramite una decisa anticipazione della punibilità – sia dalla norma di cui a CP 615-*quinquies* (ora confluita sostanzialmente nel nuovo CP 635-*quater*.1) sia, infine, dalle citate disposizioni di cui a CP 617-*quater*; 617-*quinquies* e 617-*sexies*. Con riferimento a queste ultime è facile notare come la stessa innovazione tecnologica abbia contribuito ad ampliare il raggio di tutela della segretezza della comunicazione, costituzionalmente garantito da Cost. 15, andando oltre la segretezza del contenuto della comunicazione e attraendo nella sua orbita i dati esterni alle comunicazioni.

Le esigenze di tutela penale devono trovare un bilanciamento con la necessità di garantire la libertà di circolazione dei dati e delle informazioni, nonché con la loro libera accessibilità e fruibilità. Tale bilanciamento risulta essere più complesso per la crescente vulnerabilità dei sistemi informatici, dei dati e delle informazioni in essi archiviati, dovuta a forme di aggressione sia "tradizionali" che "tecnologiche" che si evolvono con lo stesso sviluppo tecnologico[6].

3. Le componenti strutturali della definizione di cybersecurity nel prisma delle fonti internazionali, europee ed interne

La c.d. cybersecurity non può rappresentare solo una questione, o peggio un ostacolo, di ordine tecnico. Al contrario, la sua rilevanza nella costellazione sempre più variegata dell'ecosistema digitale la eleva ad una innovativa espressione dei diritti fondamentali e se non ad un diritto fondamentale. Questo approccio è confermato anche nella letteratura straniera, che sempre più spesso fa riferimento a «Human-Centric Approach to Cybersecurity»[7], oppure a «Cybersecurity as a

[6] Vedi Flor (2019) pp. 443 ss.
[7] Deibert (2018).

human rights»[8] o, ancora, ponendosi la seguente questione, almeno nel panorama europeo: «New right to cybersecurity?»[9].

In effetti, mentre si assiste ad una generale condivisione sull'importanza della cybersecurity, non vi è consenso unanime relativamente all'approccio "metodologico", "contenutistico" e "definitorio" a tale concetto, almeno sul piano del diritto penale sostanziale.

Non è raro imbattersi, in letteratura, in argomentazioni che sovrappongono piani diversi, confondendo la cybersecurity nel contesto della sicurezza nazionale (se non internazionale) – ossia del perimetro di sicurezza cibernetica nazionale al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale – la cybersecurity nel contesto pubblico e la cybersecurity nel settore privato, ovvero cybersecurity intesa quale risultato di un processo organizzativo rispetto alle componenti strutturali del concetto stesso di cybersecurity.

Appare ora necessaria una ulteriore precisazione, di carattere non solo terminologico. A fenomeni "in costante movimento", come quelli riconducibili al settore della cyber-criminality, dovrebbero corrispondere, da un lato, settori dell'ordinamento ad elevato coefficiente di adattamento e, dall'altro lato, un diritto giudiziale flessibile. In campi nuovi o "sperimentali" queste caratterizzazioni del sistema giuridico potrebbero, al contempo, trasmettere un senso di instabilità e di irritazione. Ma proprio la specificità di tali campi o settori necessita del ricorso ad una semantica tecnica che possa riempire termini "tradizionali", comprensibili al giurista ed all'opinione pubblica, con contenuti

[8] Shackelford (2019).

[9] Chiara (2024), in cui l'Autore concentra l'analisi su «three legal challenges brought about by a theoretical framework for development of a new right to cybersecurity. They regard: i) the need for a new right to cybersecurity against the background of the existing fundamental right to security (Art. 6 EU Charter of Fundamental Rights, CFR); ii) the actual content of this new right; and, iii) how such a new right could be implemented».

adattabili al nuovo contesto tecnologico, attenendosi quanto più fedelmente possibile sia al testo redatto dal legislatore, sia ai significati correnti di un termine attribuiti dalla realtà o, meglio, dalla regola tecnologica. Nell'ambito delle ICTs la concezione dello "spazio", inteso quale "area" fruibile dall'utente per il trattamento di dati e informazioni, si basa sull'immaterialità dell'ambiente, che non sempre può essere delimitato entro confini fisici (server, singolo sistema o device, smartphone ecc.) o territoriali. Esso può assumere una duplice dimensione. La prima può essere definita "globale" o "pubblica" e viene tendenzialmente utilizzata per descrivere Internet o, meglio, il World Wide Web, ossia ambiti "aperti" a tutti gli utenti. La seconda, invece, è di carattere "individuale" o "privato" e identifica un'area riservata ad uno o più soggetti legittimati ad accedervi attraverso diverse modalità di autenticazione.

Il concetto di cybersecurity (inteso sia riferito alla sicurezza nazionale – nell'ambito della quale si assiste ad una estensione ad un ampio numero di "operatori" di un complesso insieme di obblighi, con penetranti poteri preventivi, prescrittivi e sanzionatori delle Autorità governative e indipendenti – sia in quello relativo al settore pubblico o privato) non può che essere concepito come un comprehensive concept e, in linea con questo approccio "integrato", che comprende l'information security, dunque, esso esprime anche – e forse in modo preminente – l'interesse alla protezione contro le minacce alla riservatezza, all'integrità, alla disponibilità ed all'affidabilità di dati e informazioni, nonché dei computers, di ogni device o di ogni rete o sistema attraverso cui tali dati e tali informazioni vengono trattati[10].

Cybersecurity che, in tal senso, da un lato si distingue dalla nozione di cybersafety, la quale sembra includere i rischi connessi agli informational contents dei dati e delle informazioni trattati nel cyberspace, con ripercussioni dirette e indirette sull'uomo; dall'altro lato, può essere intesa quale processo proattivo e reattivo volto proprio alla protezione ideale dell'interesse degli uomini e delle organizzazioni ad essere liberi da minacce, in specie da quelle alla CIA-Triad – la triade Confidentiality, Integrity e Availability – che costituisce, al tempo stesso, il fulcro, la core area della information security o cybersecurity

[10] *Ibidem.*

e il modello guida della sua governance, a cui può collegarsi l'esigenza di protezione dell'affidabilità di sistemi informatici, reti, dati e informazioni ivi contenuti o tramite di essi trattati.

In estrema sintesi, la nozione di cybersecurity potrebbe essere edificata su almeno tre livelli, tutti meritevoli di protezione, pur tenendo presente le esigenze afferenti alla "sicurezza nazionale": 1. infrastrutturale (devices, hardware, software e reti); 2. informazionale (ossia riguardante il patrimonio informativo della persona o dell'ente, non necessariamente di carattere personale); 3. personale "in senso stretto" (che riguarda la data protection, ossia la tutela dei dati personali). Questa possibile costruzione di un modello concettuale di cybersecurity coinvolge altresì non solo le mere attività di gestione e prevenzione dei rischi interni al cyberspazio, ma sembra includere indistintamente la dimensione virtuale così come quella reale, per cui risulta necessario ridefinire il ruolo dello Stato e delle istituzioni pubbliche, sia a livello nazionale che sovranazionale, in relazione alla tutela della cybersicurezza[11].

La dimensione europea della cybersicurezza ha acquisito sempre maggiore rilevanza, con l'Unione Europea che ha adottato un ruolo di primo piano nella definizione di politiche e regolamentazioni comuni. Con l'adozione del pacchetto legislativo in materia, e con particolare riferimento alla Direttiva UE 2022/2555 (direttiva NIS2) l'Unione ha delineato un quadro giuridico che mira a innalzare notevolmente il livello minimo di sicurezza delle reti e delle informazioni in tutto il territorio europeo. La sfida non è più quella di una mera armonizzazione tra le differenti legislazioni nazionali, ma quella di ottenere dei benefici comuni attraverso l'istituzione di infrastrutture comuni e di forme di cooperazioni tra Stati membri[12].

Venendo alla protezione penale della CIA-Triad, essa è affidata, in particolare, ad un nucleo essenziale di fattispecie incriminatrici previste dalla Direttiva UE 2013/40 e volte a sanzionare l'accesso illecito a sistemi di informazione (art. 3), l'interferenza illecita relativamente ai sistemi (art. 4), l'interferenza illecita relativamente ai dati (art. 5) e l'intercettazione illecita (art. 6). In particolare, le incriminazioni di cui

[11] Si veda Ursi (2023).
[12] *Ibidem*.

agli artt. 3 e 6 sono dirette alla protezione della confidenzialità di dati e sistemi, mentre quelle di cui agli artt. 4 e 5 tutelano l'integrità e la disponibilità di dati e sistemi.

L'atto europeo si inserisce armonicamente in un quadro di contrasto alla cyber-criminalità delineato a livello internazionale dalla Convenzione Cybercrime del Consiglio d'Europa del 2001. La CIA-Triad trova protezione, infatti, nel titolo I del Trattato ("Offese contro la confidenzialità, l'integrità e la disponibilità di dati e sistemi informatici"), in cui si impone agli Stati di prevedere come reati l'accesso illegale (art. 2), l'intercettazione illegale (art. 3), l'interferenza [illecita] relativa ai dati (art. 4) e l'interferenza [illecita] relativa ai sistemi (art. 5)[13].

Da ultimo, ma non certo per importanza, per quanto attiene più specificatamente alla data protection, l'attuale riferimento normativo è il DLGS 101/2018 contenente le disposizioni per l'adeguamento della normativa nazionale ai principi del GDPR.

Com'è noto, a distanza di molti anni dall'introduzione del reato di trattamento illecito di dati personali (DLGS 196/2003, 167) ed a seguito delle nuove sollecitazioni provenienti dal diritto europeo, il legislatore italiano è nuovamente intervenuto in materia di *privacy* arricchendo il quadro delle scelte sanzionatorie di natura penale, proponendo una trilogia punitiva in materia di trattamento illecito di dati (gli artt. 167 "Trattamento illecito di dati", 167-*bis* "Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala" e 167-*ter* "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala"), pur optando per non riproporre la fattispecie di omessa adozione di misure minime di sicurezza (*ex* DLGS 196/2003, 169).

Per quanto riguarda il settore del trattamento dei dati nell'ambito delle indagini penali, il DLGS 51/2018 (di attuazione della Direttiva UE 2016/680), all'art. 43 prevede il reato di trattamento illecito di dati[14] per violazione del principio di liceità del trattamento, ovvero

[13] La stessa Convenzione delle Nazioni Unite contro il cybercrime, adottata dall'Assemblea Generale dell'ONU il 24 dicembre 2024, riprende quel nucleo essenziale di fatti meritevoli di criminalizzazione riconducibili alle esigenze di tutela delle componenti strutturali della cybersecurity. Cfr. Dimetto (2025) pp. 108 ss.

[14] La fattispecie di reato prevede: «1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dall'articolo

delle disposizioni sul trattamento di categorie particolari di dati personali o sul divieto di profilazione finalizzata alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali.

A questa fattispecie si aggiungano quelle previste dagli artt. 44 e 45 (rispettivamente "Falsità in atti e dichiarazioni al Garante" e "Inosservanza dei provvedimenti del Garante").

Il comune denominatore della nuova disciplina ruota intorno alla clausola di sussidiarietà, che rende i fatti suscettibili di applicazione succedanea rispetto a disposizioni incriminatrici più significative e contrassegnate da un carico sanzionatorio superiore.

Le disposizioni penalistiche contenute nella disciplina a tutela dei dati personali, in particolare, costituiscono fattispecie meramente sanzionatorie di precetti extrapenali e, nel complesso, sono dirette a regolare e a proteggere le diverse procedure di trattamento dei dati funzionali alla tutela della vita personale e privata di un individuo e, per quanto riguarda il DLGS 51/2018, anche alla garanzia del buon ed affidabile andamento delle indagini penali per fini giustizia. Per cui l'apparato normativo a tutela dei dati personali si pone in rapporto di *species* a *genus* rispetto alla riservatezza personale, la quale ultima, nelle sue ulteriori componenti, non solo è tutelata da altre ipotesi di reato[15], ma può trovare protezione penale anticipata in quanto potenzialmente ricompresa in un'area molto più ampia di espansione della personalità stessa dell'individuo, ossia la riservatezza informatica (la cui offesa non presuppone necessariamente la "violazione" dei dati personali)[16].

5, comma 1, è punito, se dal fatto deriva nocumento, con la reclusione da sei mesi a un anno e sei mesi o, se la condotta comporta comunicazione o diffusione dei dati, con la reclusione da sei mesi a due anni. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dall'articolo 7 o dall'articolo 8, comma 4, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni».

[15] Si pensi solo, ad esempio, a CP 615-*bis* "Interferenze illecite nella vita privata".

[16] Area più ampia di espansione della personalità dell'individuo che assume rilevanza costituzionale. Già in passato si è riconosciuto al diritto alla riservatezza rilievo costituzionale, facendo leva sui principi della Carta (Cost. 2; 13; 14; 15; 27; 29) o su previsioni del diritto sovranazionale (CEDU 8 e Dichiarazione Universale dei diritti dell'uomo 12). Dal concetto di "vita privata" si è poi distinta la riservatezza in senso stretto sino a ritenere che la vita privata, da una parte, e la riservatezza,

Il moderno concetto di privacy, dunque, esprime non solo lo *ius excludendi alios* dalla conoscenza di informazioni private, ma anche il diritto (positivo) al controllo dei propri dati e delle proprie informazioni personali[17], che assume peculiare rilievo nell'attuale società tecnologica, in cui si assiste normalmente a trattamenti automatizzati su larga scala.

Proprio l'evoluzione tecnologica ha determinato la rilevanza pubblicistica delle disposizioni relative alla tutela dei dati personali, che emerge inequivocabilmente dall'inderogabilità delle disposizioni sul trattamento dei dati (comprese quelle relative alla sicurezza ed alla riservatezza dei dati e dei sistemi) e dalla disciplina delle funzioni dell'Autorità Garante, che sembrano esse stesse evidenziare la volontà di assicurare tutela anticipata della riservatezza personale[18].

Senza addentrarsi in modo maggiormente dettagliato nelle aree di criticità che caratterizzano la loro applicazione, ciò che rileva è che le componenti della cybersecurity assumono autonoma tutela penale, anche nell'ambito delle attività di indagine per l'accertamento dei reati, in un sistema che ha dovuto confrontarsi con multiformi "riposiziona-

dall'altra, costituiscano un'endiadi, due momenti dell'unitario nucleo di tutela che connota il diritto alla privacy (Patrono (1986) p. 574, che riconosceva piena cittadinanza all'interno della Costituzione al diritto alla riservatezza, ritenendo la tesi di Bricola – fondata sulla distinzione sopra citata – eccessivamente formalistica). Parlava già di varietà semantica del tema che finisce per contaminarne la natura giuridica Giacobbe (1974) p. 694, secondo cui «L'enunciazione delle diversità terminologiche adottate dalla dottrina per classificare il fenomeno studiato, evidenzia l'incertezza che ha caratterizzato la ricerca dei contenuti della situazione giuridica che si è inteso definire». Cfr. Loiodice e Santaniello (2000); nonché Troncone (2011) pp. 177 ss. Si veda già Franceschelli (1960); Morsillo (1966); Bricola (1967) pp. 1079 ss.; Mantovani (1968) pp. 61 ss.; Palazzo (1975) pp. 126 ss.; Frosini (1981) pp. 5 ss.; Giannantonio, Losano e Zeno-Zencovich (1999); Manna (2003) pp. 727 ss.; Manna (2005) pp. 195 ss.; Fioriglio (2008); da ultimo cfr. D'agostino (2019) pp. 1 ss.

[17] Si riprende, in tal senso, l'impostazione teorica di Baldassarre (1997) pp. 45 ss.

[18] Cfr. Lamanuzzi (2017) pp. 221 ss. Potrebbe risultare opinabile, però, l'affermazione (ripresa da Torre (2004) pp. 239 ss.) secondo cui la «*privacy*, comunemente intesa nell'accezione minimale di *right to be let alone*, deve – come si è detto – «mutare il suo contenuto da diritto alla riservatezza a diritto all'autodeterminazione informativa». Tale ultimo concetto assume, infatti, contorni per il vero diversi, non semplicisticamente riducibili o riferibili, nel loro contenuto, alla "*privacy*".

menti tecnologici" che hanno segnato un reale mutamento di paradigma.

4. Conclusioni

La complessità ed il costante mutamento proteiforme della società tecnologica determina inevitabilmente la nascita di nuovi interessi meritevoli di tutela anche penale, che possono risultare espressione di nuove manifestazioni di "tradizionali" diritti fondamentali.

Sotto questo ultimo aspetto dovrebbe tornare maggiormente al centro della discussione nei rapporti fra diritto penale e tecnologia l'oggettività giuridica, quale irrinunciabile presidio liberale.

Con la consapevolezza che il bene giuridico «è categoria descrittiva, classificatoria ed ermeneutica, della dogmatica classica, da Birnbaum a Binding e Liszt, e da Arturo Rocco a Grispigni in poi. Che poi esso abbia conosciuto stagioni liberali, critiche, ma anche metodologiche, funzionali e altresì costituzionali, è altra questione». Che in una sua accezione liberale e non metodologica esso serva comunque «a delimitare alcune classi di condotte, è altrettanto vero, però le prestazioni di queste potenzialità selettive sono ancora modeste. Il bene giuridico da solo non basta ed è sbagliato chiedergli troppo»[19].

Evitando di elevare il bene giuridico a «paradigma supremo ed esclusivo di conoscenza del reato»[20], e guardando invece alle esigenze di razionalità punitiva, non è altrettanto possibile disconoscerne l'imprescindibilità epistemologica, quale «tratto unificante degli altri requisiti della struttura del reato» nel prisma dei principi liberali e garantisti[21].

[19] Donini (2013) pp. 5 ss.

[20] L'espressione trae spunto da Contieri (2019) pp. 8 ss., che rinvia alle opere di Sina (1962) pp. 24 ss.; Jäger (1957) pp. 6 ss. La medesima espressione è ripresa da Rippa (2021) pp. 1 ss.

[21] Fra la ormai sterminata letteratura penalistica si veda, senza alcuna pretesa di esaustività, a partire da Rocco (1913); Pisapia (1948); Pagliaro (1965); Stella (1973) pp. 1 ss.; Bettiol (1959) pp. 705 ss.; Neppi Modona (1965); Bricola (1973) pp. 14 ss.; Mantovani (1977) pp. 445 ss.; Pulitanò (1981) pp. 111 ss.; Vassalli (1982) pp. 629 ss.; Fiandaca (1982) pp. 42 ss.; Angioni (1983); Stile, a cura di (1985); Donini

«Chi oggi attacca o sminuisce il bene giuridico, si pone per ciò stesso in collisione con la base fondativa del principio di offensività»[22].

Lo stesso adeguamento, nella prospettiva di una interpretazione evolutiva degli elementi strutturali della fattispecie incriminatrice, a nuove manifestazioni fenomeniche del contesto tecnologico è soluzione percorribile e maggiormente efficace, in molti casi, rispetto ad un approccio interventistico del legislatore penale che potrebbe scontare evidenti criticità di fronte alla rapidità del progresso tecnico. Ma ciò può valere solo in presenza di fattispecie già in astratto suscettibili di plurime chiavi di lettura sotto il profilo dell'oggettività giuridica/offensività[23].

Anche se il compito di definire il tipo criminoso, dunque, «come sintesi descrittiva di un contenuto omogeneo di disvalore» è affidata al legislatore, il giudice si può muovere con una certa libertà nella «concretizzazione del tipo», dovendo però sempre riferirsi alla descrizione legislativa[24].

Queste riflessioni, però, non possono che partire dalla obiettiva rilevanza di un approccio proattivo e reattivo nella tutela penale della CIA-Triad, in uno scenario evanescente ed estremamente mutevole in

(2003); Donini (1999) pp. 267 ss.; Fiandaca (2014); Manes (2005). Vedi anche Caterini (2004); Romano (2011) pp. 33 ss.

[22] Donini (2013) p. 6.

[23] Un auspicato ingresso del sapere tecnico scientifico (dell'informatica e dell'ingegneria informatica) in una attenta riflessione in merito a scelte di politica criminale, nonché del linguaggio proprio di quelle scienze fra gli elementi strutturali della fattispecie legale gioverebbe all'ermeneutica, perché le scienze giuridiche, «che hanno a che fare addirittura con il dover essere, e non con l'essere, non riguardano il solo linguaggio o gli enunciati legislativi (le disposizioni), ma il risultato delle interpretazioni di esse (le norme) (…) contengono progetti di modifica delle diverse realtà e in questi progetti sono contenuti saperi empirici che condizionano la legittimità e il contenuto delle leggi stesse». Questi saperi sono decisivi per la stessa interpretazione delle leggi «come progetti di intervento sulla realtà» (vedi Donini (2015) pp. 95 ss.). Se intervenire, quando intervenire e in che modo intervenire sono le domande che dovrebbe porsi il legislatore di fronte all'innovazione tecnologica, tenendo presente, sul piano metodologico, che come sostenuto da Calo (Calo (2025)), «Technology has no fixed meaning but varies by observer and by context, and changes over time».

[24] Si veda Palazzo (1992) pp. 453 ss.

cui è forse davvero giunto il momento, riprendendo le parole di Rodotà, «di pensare ad un sistema di diritti per il più grande pubblico che l'umanità abbia mai conosciuto»[25].

Il tentativo di ricostruzione dogmatica delle componenti strutturale della cybersecurity, che giunge all'indomani della L 90/2024, tramite la quale il legislatore penale sarebbe potuto intervenire in modo sistematico sul sistema dei reati informatici, pur valorizzando la tutela di beni collettivi, lungi dal voler limitarsi a contribuire a delimitare la "tipicità" delle fattispecie incriminatrici, vuole offrire un contributo alla elaborazione di un concetto "sostanziale" e "prepositivo" di cybersecurity, capace di assurgere, nella prospettiva di riforma o di adeguamento del sistema penale sostanziale e processuale, a parametro razionale di orientamento delle scelte anche di politica criminale, nella consapevolezza di un necessario e costante dialogo fra discipline, in quanto la scienza penale, in generale, «è fatta da diversi attori che usano oggi molti linguaggi, tra i quali ci sono anche la dogmatica classica e quella moderna, ma sempre più forti sono gli apporti della comparazione e di saperi extragiuridici»[26]. La scienza e il sapere tecnologico dovrebbero influenzare il diritto, in un'ottica di interazione reciproca per la comprensione dei diversi linguaggi. Oggi è proprio la complessità dei linguaggi tecnico-scientifici a mettere il legislatore ed il giudice in una condizione di inferiorità cognitiva, che nel peggiore dei casi si traduce in un approccio casistico culturalmente arretrato rispetto al livello di progresso tecnologico raggiunto. È condivisibile la conclusione a cui giunge una parte della dottrina nell'affrontare, più in generale, il problema dei rapporti tra scienza e diritto e delle controversie tecnico-scientifiche nel diritto e nel processo penale, ossia che si tratti di un «paradosso al quale oggi non ci si può sottrarre». Si tratta di «saperlo gestire, guardandosi dal duplice pericolo che la scienza espropri il diritto, e che il diritto ignori o rinneghi la scienza. Impresa realizzabile in linea di astratto principio, ma difficile nei fatti»[27].

Lo stesso adeguamento, nella prospettiva di una interpretazione evolutiva degli elementi strutturali della fattispecie incriminatrice, a nuove

[25] Si veda Rodotà (2014).
[26] Si veda Donini (2010) pp. 127 ss., in specie p. 178.
[27] Vedi Fiandaca (2005) pp. 22-23.

manifestazioni fenomeniche del contesto tecnologico è soluzione percorribile e maggiormente efficace, in molti casi, rispetto ad un approccio interventistico del legislatore penale che potrebbe scontare evidenti criticità di fronte alla rapidità del progresso tecnico. Ma ciò può valere solo in presenza di fattispecie già in astratto suscettibili di plurime chiavi di lettura sotto il profilo dell'oggettività giuridica/offensività[28].

Riferimenti bibliografici

Angioni V. (1983). *Contenuto e funzioni del concetto di bene giuridico*. Milano.

Bartoli R. (2012). *L'accesso abusivo a un sistema informatico (art. 615*-ter *c.p.) a un bivio ermeneutico teleologicamente orientato*. In: *Dir. pen. contemp.*, 1.

Baldassarre A. (1997). *Diritti della persona e valori costituzionali*. Torino.

Bettiol G. (1959). *L'odierno problema del bene giuridico*. In: *Riv. it. dir. pen*.

Bricola F. (1967). *Prospettive e limiti della tutela penale della riservatezza*. In: *Riv. it. dir. proc. pen*.

Bricola F. (1973). *Teoria generale del reato*. In: *NNDI*, 14.

Calo R. (2025). *Law and Technology: A Methodical Approach.* Oxford. DOI: 10.1093/9780197526170.001.0001.

Caterini M. (2004). *Reato impossibile e offensività. Un'indagine critica*. Napoli.

Chiara P.G. (2024). *Towards a right to cybersecurity in EU law? The challenges ahead*. In: *Computer Law & Security Review*, 53. DOI: 10.1016/j.clsr.2024. 105961.

Contieri E. (2019). *Dialettica del bene giuridico. Per il recupero di una prospettiva costituzionalmente orientata*. Napoli.

D'Agostino L. (2019). *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101*. In: *Arch. pen*., 1.

Deibert R.J. (2018). *Toward a Human-Centric Approach to Cybersecurity*. Cambridge. DOI: 10.1017/S0892679418000618.

Dimetto M. (2025). *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*. In: *Freedom, Security and Justice.*

Donini M. (1999). *Teoria del reato*. In: *Dig. disc. pen*., 14.

Donini M. (2003). *Alla ricerca di un disegno. Scritti sulle riforme penali in Italia*, Padova.

Donini M. (2010). *Tecnicismo giuridico e scienza penale cent'anni dopo. La prolusione di Arturo Rocco (1910) nell'età dell'europeismo giudiziario*. In: *Criminalia*.

Donini M. (2013). *Il principio di offensività. Dalla penalistica italiana ai programmi europei*. In: *Dir. pen. cont. trim*., 4.

[28] Per ogni ulteriore approfondimento si consenta di rinviare Flor e Marcolini (2022).

Donini M. (2015). *Scienza penale e potere politico*. In: *Riv. it. dir. proc. pen*.
Fiandaca G. (2005). *Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale*. In: *D.&Q. pubb.*
Fiandaca G. (1982). *Il bene giuridico come problema teorico e come criterio di politica criminale*. In: *Riv. it. dir. e proc. pen*.
Fiandaca G. (2014). *Sul bene giuridico. Un consuntivo critico*. Torino.
Fioriglio G. (2008). *Il diritto alla privacy. Nuove frontiere nell'era di internet*, Bologna.
Flor R. (2012). *Verso una rivalutazione dell'art. 615*-ter *c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet*. In: *Dir. pen. contemp.*, 2.
Flor R. (2015). *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*. In: *Dir. pen. proc.*
Flor R. (2018). *La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere"*. In: *Dir. pen. proc*., 4.
Flor R. (2019). *Cybersecurity ed il contrasto ai* cyber-attacks *a livello europeo: dalla* CIA-Triad Protection *ai più recenti sviluppi*. In: *Diritto di Internet*, 3.
Flor R., Marcolini S. (2022). *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*. Torino.
Franceschelli B. (1960). *Il diritto alla riservatezza*. Napoli.
Frosini V. (1981). *La protezione della riservatezza nella società informatica*. In: *Inform. dir.*
Galdieri P. (1997). *Teoria e pratica nell'interpretazione del reato informatico*. Milano.
Giacobbe G. (1974). *Il diritto alla riservatezza in Italia*. In: *Dir. e soc.*
Giannantonio E., Losano M.G. e Zeno-Zencovich V. (1999). *La tutela dei dati personali. Commento alla l. 675/96*. Padova.
Jäger H. (1957). *Strafgesetzgebung und Rechtsgüterschutz bei Sittlichkeitsdelikten. Eine kriminalsoziologische Untersuchung*. Stuttgart.
Lamanuzzi M. (2017). *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*. In: *JusOnline*, 1.
Loiodice A., Santaniello G. (2000). *La tutela della riservatezza*. In: *Trattato di diritto amministrativo diretto da Giuseppe Santaniello*. Vol. 26. Padova.
Manes V. (2005). *Il principio di offensività nel diritto penale. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza*. Torino.
Manna A. (2003). *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali*. In: *Dir. inf.*
Manna A. (2005). *Privacy on line: quali spazi per la tutela penale?*. In: *Dir. Internet*.
Mantovani F. (1968). *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*. In: *Arch. giur*.
Mantovani F. (1977). *Il principio di offensività del reato nella Costituzione*. In:

Aspetti e tendenze del diritto costituzionale. Scritti in onore di Costantino Mortati. Milano.
Mantovani M. (1994). *Brevi note a proposito della nuova legge sulla criminalità informatica*. In: *Crit. dir*.
Morsillo G. (1966). *La tutela penale del diritto alla riservatezza*. Milano.
Nunziata M. (1998). *La prima applicazione giurisprudenziale del delitto di «accesso abusivo ad un sistema informatico»* ex *articolo 615*-ter *c.p.* In: *Giur. mer*.
Neppi Modona G. (1965). *Il reato impossibile*. Milano.
Pagliaro A. (1965). *Bene giuridico e interpretazione della legge penale*. In: *Studi in onore di Francesco Antolisei*. II. Milano.
Palazzo F. (1975). *Considerazioni in tema di tutela della riservatezza*. In: *Riv. it. dir. proc. pen.*
Palazzo F. (1992). *I confini della tutela penale: selezione dei beni e criteri di criminalizzazione*. In: *Riv. it. dir. proc. pen*.
Patrono P. (1986). *Privacy e vita privata (dir. pen.)*. In: *ED*, 35.
Picotti L. (2011). *Sicurezza informatica e diritto penale*. In: Donini M., a cura di, *Sicurezza e diritto penale*. Bologna.
Pisapia G. (1948). *Introduzione alla parte speciale del diritto penale*. Milano.
Pulitanò D. (1981). *La teoria del bene giuridico fra codice e Costituzione*. In: *Quest. Crim*.
Rippa F. (2021). *La pubblica amministrazione come oggetto di tutela penale: tra nuove derive eticizzanti e necessità di recupero del suo significato oggettivo-funzionale*. In: *De Iustitia*.
Rocco A. (1913). *L'oggetto del reato e della tutela giuridica penale*. Torino.
Rodotà S. (2014). *Il mondo della rete. Quali i diritti, quali i vincoli.* Roma-Bari.
Romano M. (2011). *La legittimazione delle norme penali: ancora su limiti e validità della teoria del bene giuridico*. In: *Criminalia*.
Sina P. (1962). *Die Dogmengeschichte des strafrechtlichen Begriffs "Rechtsgut"*. Basel.
Shackelford S. (2019). *Should Cybersecurity Be a Human Right? Exploring the 'Shared Responsibility' of Cyber Peace*. In: *Stanford Journal of International.* DOI: 10.2139/ssrn.3005062.
Stella F. (1973). *La teoria del bene giuridico e i c.d. fatti inoffensivi conformi al tipo*. In: *Riv. it. dir. proc. pen*.
Stile A.M., a cura di (1985). *Bene giuridico e riforma della parte speciale*. Napoli.
Torre V. (2004). *La gestione del rischio nella disciplina del trattamento dei dati personali*. In: L. Picotti, a cura di, *Il diritto penale dell'informatica nell'epoca di internet*. Padova.
Troncone P. (2011). *Il delitto di trattamento illecito di dati personali*. Torino.
Ursi R., a cura di (2023). *La sicurezza nel cyberspazio.* Milano.
Vassalli G. (1982). *Considerazioni sul principio di offensività*. In: *Studi Pioletti*. Milano.
Warren S.D., Brandeis L.D. (1890). *The Right to Privacy*. In: *Harvard L. Rev*., 4-5.