A Giuseppe

Costanza Bernasconi

Diritto penale e spazio digitale

Contributo allo studio di principi e categorie

Edizioni ETS



www.edizioniets.com

La pubblicazione del presente volume si avvale del «Fondo di Incentivazione alla Ricerca Dipartimentale» (FIRD 2024) per il progetto di ricerca «Homo Sapiens vs Machina Sapiens: dove tracciare la linea delle responsabilità in un mondo ibrido», finanziato dall'Università di Ferrara.

© Copyright 2026
EDIZIONI ETS
Palazzo Roncioni - Lungarno Mediceo, 16, I-56127 Pisa
info@edizioniets.com
www.edizioniets.com

Distribuzione
Messaggerie Libri SPA
Sede legale: via G. Verdi 8 - 20090 Assago (MI)

ISBN cartaceo 978-884677705-8

Il presente PDF con ISBN 978-884677756-0 è in licenza **CC BY-NC**



INDICE

Capitolo primo

Fatto e diritto nel mondo digitale

1. L'impatto delle tecnologie digitali 7
2. Punti di emersione problematici 12
3. In particolare: i comportamenti illeciti 15
4. La criminalità informatica 20
5. Le prime criticità. L'esempio emblematico dell'accesso abusivo a sistema informatico 23
6. Il problematico adattamento delle categorie tradizionali 27
7. Il programma d'indagine 28

Capitolo secondo

Dai reati comuni ai reati digitali

1. Il ricorso a fattispecie a-specifiche 35
2. Interpretazioni estensive e analogiche 37
3. Le nuove fattispecie informatiche 40
4. Dai *computer crimes* ai *cyber crimes* 45
5. Il *file* informatico come "cosa mobile" 49
6. Il *web* come "mezzo di pubblicità" 54
7. *Internet* come "mezzo di stampa" 58
8. Il *web* come "luogo pubblico" o "aperto al pubblico" 64
9. Molestia "col mezzo del telefono" e nuove modalità di intrusione tecnologica non gradita 67
10. Lo sfruttamento sessuale *online* 71

Capitolo terzo

Il fatto digitale nella teoria del reato

1. Il fatto di reato nel contesto digitale 85
2. Il soggetto attivo del reato 86
3. I beni giuridici digitali 87
4. La natura ibrida della condotta 94
5. La smaterializzazione dell'evento e del nesso di causalità 97
6. Il poliedrico volto dell'offesa nel mondo digitale 98
7. La natura permanente dell'offesa 101
8. Complessità della rete e volontà del fatto 105
9. Il caso del *trading* algoritmico 108
10. Ubiquità del fatto e *locus commissi delicti* 113
10.1. L'accesso abusivo ad un sistema informatico 115
10.2. La diffamazione *online* 118

Capitolo quarto

Le piattaforme digitali e i motori di ricerca

1. La responsabilità del *provider* per il reato digitale 123
2. Il problema della posizione di garanzia 128
3. L'analogia *in malam partem* della disciplina in tema di stampa 132
4. La mancata rimozione di contenuti illeciti 137
5. Il *Digital Services Act* 140

Riflessioni conclusive 145

Bibliografia 151

Capitolo primo

FATTO E DIRITTO NEL MONDO DIGITALE

SOMMARIO: 1. L'impatto delle tecnologie digitali. – 2. Punti di emersione problematici. – 3. In particolare: i comportamenti illeciti. – 4. La criminalità informatica. – 5. Le prime criticità. L'esempio emblematico dell'accesso abusivo a sistema informatico. – 6. Il problematico adattamento delle categorie tradizionali. – 7. Il programma d'indagine.

«*La tecnica non si accontenta di essere, e, nel nostro mondo di essere il fattore principale o determinante: essa è divenuta Sistema*»
[J. ELLUL, *Il sistema tecnico. La gabbia delle società contemporanee,* Milano, 2009, 15]

1. *L'impatto delle tecnologie digitali*

Il prepotente e sempre più pervasivo sviluppo delle nuove tecnologie, nonché il loro effetto dirompente sulla vita dell'uomo, hanno, *in primis,* determinato un cambiamento di paradigma di natura sociologica senza precedenti[1]: la fenomenologia della condotta umana e i suoi effetti nel mondo esterno sono stati profondamente alterati nella loro tradizionale fisionomia.

Costituisce, infatti, ormai un dato acquisito che la tecnologia abbia la capacità di modificare il registro delle strutture mentali e sensoriali dell'uomo[2], il modo di sentire il rapporto con sé, con gli altri e con il mondo, di cambiare le regole della convivenza umana, arrivando a influenzare i modelli di controllo sociale[3]. Invero, i mezzi tecnologici non hanno solo la capacità di trasmettere

[1] In tale prospettiva, la rivoluzione digitale è stata definita come un «fatto sociale totale» (così A. GARAPON, J. LASSÈGUE, *La giustizia digitale. Determinismo tecnologico e libertà,* trad. it. a cura di F. MORINI, Bologna, 2021, 80).

[2] *Amplis,* N. CARR, *The shallows. What the Internet is doing to our brains*, trad. it. a cura di S. GARASSINI, *Internet ci rende stupidi? Come la Rete sta cambiano il nostro cervello*, Milano, 2011, *e-Book*, in particolare cap. 7; M. SPITZER, *Digitale demenz. Wie wir uns und unsere Kinder um den Verstand bringen,* trad. it. a cura di A. PETRELLI, *Demenza digitale*, Milano, 2019, *e-Book.*

[3] J. R. AGUSTINA SANLLEHÍ, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?,* in *Estudios penales y criminológicos*, 2021, vol. 41, 713.

messaggi, ma producono l'effetto di modellare la nostra percezione, il nostro pensiero e, conseguentemente, i nostri comportamenti[4].

La c.d. "insurrezione digitale" (o rivoluzione digitale) ha, in altre parole, determinato una vera e propria "mutazione antropologica", che vede «l'emergere di un sistema cervello/mente nuovo: la mente tecno–liquida»[5].

Detta mutazione ha esaltato e plasmato alcune caratteristiche dell'uomo: il narcisismo, l'ambiguità identitaria, la ricerca di emozioni forti, il bisogno di infinite relazioni *light*, il ricorso alla tecno–mediazione nelle relazioni interpersonali[6]. Queste ultime, infatti, sono sempre più virtuali, spesso mediate dai *social network*, con un aumento esponenziale dell'anonimato e una riduzione delle interazioni fisiche[7].

Il fenomeno ha finito per coinvolgere addirittura le interazioni personali più intime, come quelle sessuali[8]. La costante connessione dei nuovi strumenti digitali alla rete ha indotto un numero crescente di soggetti, specie di giovane età, ad esplorare la sessualità secondo nuove modalità, conducendo, da un lato, ad una sorta di progressiva normalizzazione della pornografia, dall'altro lato, alla virtualizzazione della presenza fisica[9].

A questo si aggiunga che le dinamiche digitali permettono a ciascuno di controllare e modificare la propria identità sociale, scegliendo che cosa condividere con gli altri e come farlo, nonché di sperimentare nuovi modi di essere: «il risultato è un'identità fluida, flessibile e precaria, mutevole e incerta»[10].

[4] In argomento, T. PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante* online *nel reato di diffamazione,* in *www.sistemapenale.it,* ottobre 2023, in particolare 7 ss.

[5] T. CANTELMI, *La mente tecno-liquida ai tempi di internet: una nuova sfida per la comprensione umana*, in *www. https://www.psicologiacontemporanea.it/blog/la-mente-tecno-liquida-ai-tempi-di-internet.*

[6] Così e *amplius* T. CANTELMI, *La mente tecno-liquida ai tempi di internet: una nuova sfida per la comprensione umana,* cit.,

[7] E. MAESTRI, *Stupri digitali: una questione di* governance *del cyberspazio,* in *Annali* online *della Didattica e della Formazione Docente,* vol. 16, n. 27/2024, 27. In argomento v., altresì, M. SPITZER, *Connessi e isolati,* trad. di C. TATASCIORE, e-Book, 2018, in particolare cap. V.

[8] *Amplius* G. BEGUINOT, *I reati contro la sfera sessuale della persona al tempo di* internet*, tra criticità tradizionali ed esigenze di prevenzione*, in *Riv. it. dir. proc. pen.*, 2023, 1001 ss.

[9] Sul tema si vedano i diversi contributi contenuti in *La dissoluzione della sessualità umana nell'era digitale,* a cura di C. CIPOLLA, E. CANESTRINI, Milano, 2018, 19 ss.

[10] M. R. ALLEGRI, Ubi social, ibi ius. *Fondamenti costituzionali dei* social network *e profili*

Con un'efficace formula di sintesi, il prof. Floridi ha coniato il neologismo *Onlife* proprio per descrivere l'esperienza che si vive in un mondo iper–connesso dove non esiste più la distinzione tra essere *online* o essere *offline*[11].

Di più: le più recenti e innovative tecnologie cibernetiche stanno mettendo in discussione la distinzione "mezzo–fine" ovvero "agente–strumento" nella definizione dei comportamenti e delle relazioni, al punto che la tecnologia da strumento diviene fine, se non addirittura soggetto[12].

Del resto, già nel celebre dialogo tra Emanuele Severino e Natalino Irti su diritto e tecnica – in cui si cerca di dare risposta al quesito se la tecnica possa essere regolata o si faccia, essa stessa, regola del nostro mondo – si legge: «Nella tecnica totalmente dispiegata, la norma suprema, da cui tutte le altre discendono – la suprema legge "morale" – è agire assumendo come forma dell'agire la volontà di accrescere all'infinito la potenza della tecnica»[13].

Dapprima, infatti, la c.d. rivoluzione informatica ha comportato, sotto diversi profili, la smaterializzazione della realtà[14], introducendo nella vita di ognuno una nuova e parallela dimensione, quella virtuale[15].

In seguito, l'affermarsi di sistemi di intelligenza artificiale ha ulterior-

giuridici della responsabilità dei provider*,* Milano, 2018, 20. In argomento, altresì, S. RODOTÀ, *Persona, libertà, tecnologia. Note per una discussione*, in *Diritto & Questioni pubbliche*, 5/2005, 25 ss.

[11] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, trad. it. a cura di M. DURANTE, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo,* Milano, 2017, 47.

[12] *Amplius* U. GALIMBERTI, *Psiche e techne. L'uomo nell'età della tecnica*, Milano, 1999, in particolare 37 ss.; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto,* n. 1/2019, in particolare 67 ss.

[13] E. SEVERINO, in N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, 2001, 35. Sennonché, prosegue l'Autore, la potenza totalizzante della tecnica è tale per cui il diritto e la politica sono destinate all'estinzione (p. 34). «La morte della verità (e quella di Dio), infatti, significano anche la morte del diritto (p. 23 ss.), cosicché il principio supremo ordinatore sarà la normatività tecnologica che regolerà anche le norme che ancora si illudono di regolare la tecnica» (p. 36 ss.).

[14] Il concetto di "rivoluzione informatica" è apparso per la prima volta nel saggio del 1974 *Information Revolution* dell'economista D. M. Lamberton, che impiegò il termine per evidenziare come la portata innovativa della tecnologia dell'informazione sulla società fosse equiparabile a quella delle rivoluzioni agricola ed industriale.

[15] *Amplius,* D. FONDAROLI, *La tutela penale dei «beni informatici»*, in *Diritto dell'informazione e dell'informatica*, 1996, n. 2, 291 ss.

mente complicato le dinamiche relazionali sotto una molteplicità di aspetti. Infatti, la caratteristica peculiare che qualifica i sistemi di intelligenza artificiale rispetto ad altri sistemi informatici è la crescente autonomia dei primi rispetto ai secondi[16], posto che quest'ultimi, anche se molto sviluppati dal punto di vista tecnologico, si basano pur sempre sull'esecuzione di programmi predefiniti dall'uomo e destinati ad elaborare un insieme predeterminato di dati ed informazioni. Viceversa, i sistemi di IA, come si legge anche nella Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni COM(2018) 237, del 25 aprile 2018, sono sistemi «che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»[17].

Grazie alla capacità di *self-learning*, oggi i dispositivi digitali possono non limitarsi più ad eseguire istruzioni predeterminate, ma sono in grado di adottare soluzioni dinamiche sulla base dell'interazione con il mondo esterno e di sequenze di dati di cui gli uomini non hanno alcuna percezione[18], arrivando financo ad assumere decisioni che possono risultare imprevedibili per gli utilizzatori di tali sistemi, nonché per gli stessi sviluppatori.

In tale prospettiva, solo ora si coglie pienamente la lungimiranza e la potenza della domanda con la quale Alan Turing decise di aprire il noto articolo *Computing Machinery and Intelligence*, pubblicato sulla rivista *Mind* nel 1950: «*I propose to consider the question, "Can machines think?"*».

Sicché, non ci si trova più dinanzi solo a prodotti tecnologici altamente sofisticati, ma ad "entità" che paiono rivaleggiare con l'uomo e trasformarne la stessa identità, replicandone le prerogative e determinando, altresì, da un lato, nuove disuguaglianze, dall'altro, paradossalmente, nuove fragilità[19].

[16] Per tutti, N. Cristianini, Machina sapiens. *L'algoritmo che ci ha rubato il segreto della conoscenza,* Bologna, 2024, 13 ss.

[17] Il documento, dal titolo *L'intelligenza artificiale per l'Europa*, è reperibile al link https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)237&lang=it

[18] Sul tema, di recente e per tutti, E. Maestri, *Contro la riduzione bayesiana dell'intelligenza artificiale,* in https://www.pandorarivista.it /articoli/contro-la-riduzione-bayesiana-dell-intelligenza-artificiale/*,* 18 agosto 2025.

[19] Così G. Razzano, *Il primato dell'essere umano nell'era dell'intelligenza,* in *Bioetica, diritto e intelligenza artificiale,* a cura di A. Patroni Griffi, Milano-Udine, 2023, 105. In argomento, tra gli altri, A. Cappellini, Machina delinquere non potest*? Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia* 2018, 499 ss.; C. Piergallini, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. proc. pen*., 2020, 1745 ss.

Si comprende, dunque, come il cambiamento indotto dall'uso delle tecnologie non sia questione neutra per l'individuo perché crea, a ben vedere, un mondo con caratteristiche inedite; un mondo, questo, che non è possibile evitare e con il quale chiunque deve necessariamente interagire, uno spazio dove le percezioni e le precomprensioni sono diverse da quelle del mondo fisico[20]. «Non siamo infatti esseri immacolati ed estranei, gente che talvolta si serve della tecnica e talvolta ne prescinde. Per il fatto che abitiamo un mondo in ogni sua parte tecnicamente organizzato, la tecnica non è più un oggetto di una nostra scelta, ma è il nostro ambiente, dove fini e mezzi, scopi e ideazioni, condotte, azioni e passioni, persino sogni e desideri sono tecnicamente articolati e hanno bisogno della tecnica per esprimersi»[21].

Ne consegue che le c.d. *ICT* (*Information and Communication Technology*) sono diventate le «più potenti *tecnologie del sé* alle quali siamo mai stati esposti. (…) dovremmo gestirle con attenzione, poiché stanno modificando in maniera significativa i contesti e le pratiche attraverso le quali diamo forma a noi stessi»[22]. Ed è soprattutto il «sé sociale» il principale «canale attraverso cui le *ICT*, e in particolar modo i *social media* interattivi, esercitano il loro profondo impatto sulle nostre identità personali»[23]. Nel mondo digitale «il sé cerca di percepire se stesso come percepito dagli altri, facendo affidamento sulle *ICT* che agevolano fortemente l'esperienza dello sguardo rivolto su di sé. In definitiva, il sé utilizza la rappresentazione digitale di se stesso posta in essere dagli altri per costruire un'identità virtuale tramite la quale aspira ad afferrare la propria identità personale (la domanda "Chi sono per te?" diviene "Chi sono *online*?"), in un meccanismo di *feedback* potenzialmente ricorsivo fatto di aggiustamenti e modificazioni progressive che conducono ad un equilibrio "*onlife*" tra il sé *offline* e quello *online*»[24].

Tanto premesso, il nuovo contesto esistenziale creatosi nel ciberspazio

[20] Nella letteratura straniera, F. MIRÒ, *La victimización por cibercriminalidad social. Un estudio a partirde la teoría de las actividades cotidianas en el ciberespacio,* in *Revista Española de investigatión criminólogica,* n. 11, 2013, 1 ss.

[21] U. GALIMBERTI, *Psiche e techne. L'uomo nell'età della tecnica*, cit., 34. V. anche T. CANTELMI, *La mente tecno-liquida ai tempi di internet: una nuova sfida per la comprensione umana*, cit.

[22] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, cit., 67.

[23] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, cit., 69.

[24] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, cit., 83, 84.

ha offuscato l'intelligenza umana e il modo di percepire la realtà poiché il reale, di fronte all'apparente, viene banalizzato e i livelli di inganno/errore possono proliferare fino a raggiungere livelli preoccupanti[25]. Non di rado, l'utilizzo delle nuove tecnologie favorisce processi che non consentono agli utenti della Rete di afferrare l'idoneità offensiva del proprio *modus exprimendi* o *agendi* e di comprendere come il proprio agire possa avere ricadute negative anche al di fuori del contesto virtuale in cui ci si esprime o si agisce.

Inoltre, le "tracce digitali" che il cittadino lascia a disposizione degli algoritmi, sono sempre più numerose e vengono via via arricchite attraverso i gesti della vita quotidiana. Proporzionalmente al numero di richieste di consenso e alla loro reiterazione si riduce la soglia di attenzione, con conseguente debolezza cognitiva e compromissione del processo decisionale. Siamo ormai «assuefatti all'uso dei nostri dati da parte dei *social media* e la sorveglianza digitale è ormai diventata un'esperienza quotidiana per milioni di persone»[26].

2. *Punti di emersione problematici*

Tanto considerato, occorre avere consapevolezza della circostanza che, nel momento in cui ci si accinga a riflettere su quale disciplina applicare ai fatti che hanno luogo nella dimensione digitale, il primo problema che si pone è proprio quello di capire a quale tipo di "fatti" si debba fare riferimento[27].

Ebbene, nel mondo digitale l'utente crede di agire sulla base di una serie di analogie tra le azioni che egli è abituato a porre in essere nel mondo fisico e quelle equivalenti che egli svolge nel *web*. Sennonché, il mondo virtuale rappresenta uno spazio di interazione sociale che prescinde completamente dal contatto personale tra soggetti e nel quale ci si muove tramite interconnessioni con *Internet.* L'identità di ognuno è per lo più rappresentata

[25] J. R. Agustina Sanllehí, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?*, cit., 716, 717.

[26] L. Floridi, *La differenza fondamentale,* eBook, Mondadori, 2025, Parte Prima, par. 1.

[27] O. S. Kerr, *The Problem of Perspective in Internet Law,* in *Georgetown Law Journal,* vol. 91, 2003, 357; A. Morelli, O. Pollicino, *Le metafore della rete. Linguaggio figurato,* judicial frame *e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Rivista AIC*, 2018, n. 1, 19 marzo 2018, 3.

attraverso dati[28] e i comportamenti possono assumere una loro peculiare fisionomia, in realtà neppure immaginabile nel mondo *offline*.

La dimensione creata dalle tecnologie dell'informazione e della comunicazione è, in altre parole, diversa da quella fisica. Sicché, quando le condotte poste in essere nel *cyberspace* integrano o potrebbero integrare ipotesi di reato, occorrerà considerare ed esaminare con grande attenzione il ruolo e la rilevanza che le componenti tecnico–informatiche possono rivestire sulla fisionomia complessiva del fatto.

Detto diversamente: lo spazio digitale si nutre del mondo reale, ma nella nuova dimensione gli individui diventano generatori e consumatori di inedite modalità relazionali, oltre che di informazioni riflesse in dati. Ma tali modalità relazionali e tali dati, segnatamente in alcune situazioni, non sono immediatamente intellegibili con le lenti della realtà *offline*.

Così, per esempio, ci si chiede se il "sesso telematico", in termini di significato giuridico, risulti sovrapponibile al sesso fisico e, conseguentemente, se eventuali abusi coinvolgenti questa sfera siano riconducibili alla disciplina prevista per la realtà *offline*[29].

A sostegno di questa interpretazione si potrebbe addurre proprio il progressivo evaporare, come anticipato, della dicotomia virtuale–reale nelle contemporanee dinamiche sociali basate su un'interazione telematica. Sicché, per esempio, la presenza del reo, davanti al quale la vittima sia costretta a farsi oggetto di un indesiderato appagamento altrui, non dovrebbe considerarsi meno effettiva allorquando sia virtuale, in considerazione del fatto che l'assenza di contiguità spaziale fra reo e persona offesa verrebbe colmata dalla video-conversazione in tempo reale resa possibile dal mezzo telematico[30]. Ma siffatta conclusione – come si vedrà – non è affatto scontata. Non solo: la "virtualizzazione" della presenza può realizzarsi con differenti modalità, oltre che con molteplici strumenti, e le conseguenze, in termini di integrazione del fatto tipico, possono essere sensibilmente diverse negli uni e negli altri casi.

Ma, ancora: occorre chiedersi se sia possibile sussumere nelle fattispecie esistenti, nate per la realtà *offline,* la pubblicazione su *chat* e *social network* di

[28] Secondo L. Floridi (*The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, cit., 109) «la quarta rivoluzione ha portato alla luce la natura intrinsecamente informazionale dell'identità umana».

[29] Sul punto v. *infra* capitolo secondo, paragrafo 10.

[30] G. Beguinot, *I reati contro la sfera sessuale della persona al tempo di internet, tra criticità tradizionali ed esigenze di prevenzione*, in *Riv. it, dir. proc. pen.*, 2023, 1027.

post, fotografie, video diffamatori o espressivi di odio, nonché se sia possibile giungere alla medesima conclusione in relazione alla condotta di chi semplicemente condivide un *post* diffamatorio o odioso altrui o di chi usa la funzione "mi piace" o le *emoticon*[31]. Quali margini di identificazione presentano le modalità comunicative tradizionali con quelle proprie dello spazio digitale?

Non meno delicata è la questione relativa alla possibilità di ricondurre a fattispecie note (*i.e.*: i reati di furto o di appropriazione indebita) la condotta di chi, a seguito di un accesso abusivo, si appropri di informazioni, dotate di valore economico, presenti nel *database* violato.

E infine (ma sempre solo a titolo esemplificativo) occorre chiedersi se lo strumento digitale possa essere equiparato al mezzo del telefono e se lo spazio offerto da un *social network* sia logicamente riconducibile ad un luogo pubblico, per valutare l'eventuale applicazione delle norme che prevedono detti elementi come frammenti della tipicità.

Si tratta, in altre parole, di capire se sia possibile "trasferire" alcuni paradigmi, non solo giuridici, ma prima ancora sociali e culturali, dal campo analogico a quello digitale. E, dunque, in primo luogo, occorre comprendere quale possa essere il margine di adattabilità del testo delle norme esistenti al mutato contesto digitale e alle peculiari caratteristiche dei fatti ivi realizzati[32].

Non basta. Sarà altresì necessario approfondire la tenuta delle categorie concettuali penalistiche e individuare la possibile evoluzione delle chiavi interpretative dei presupposti sostanziali della responsabilità penale.

Per esempio: l'azione, tradizionalmente intesa come movimento del corpo, può essere assimilata all'interazione tra il *click* sulla tastiera di un *computer* e le connessioni automatizzate del *software*?

[31] Sul tema P. CAROLI, *Dei post e delle pene. Considerazioni su eguaglianza,* social network *e giustizia penale*, in *La giustizia penale tra ragione e prevaricazione. Dialogando con Gaetano Insolera*, Roma, 2021, 87; B. FRAGASSO, Like *su* Facebook *ed* hate crimes*: note a margine di una recente sentenza della Cassazione*, in *ww.sistema.penale.it* 2022, n. 5, 63 ss. Nella giurisprudenza, Cass. pen., sez. II, 6 dicembre 2021, n. 4534, in *deJure,* che ha qualificato come propaganda di idee fondate sulla superiorità o sull'odio razziale o etnico il *like* ad un *post* di matrice razzista, poiché renderebbe concreto il pericolo di diffusione dei messaggi tra un numero indeterminato di persone, aumentando la circolazione del *post* medesimo attraverso l'operatività di algoritmi a ciò deputati; Cass. pen., sez. V, 25 settembre 2017, n. 55418, in *deJure,* ad avviso della quale l'inserimento di *like* a video inneggianti al martirio islamico può integrare il reato di apologia del terrorismo ai sensi dell'art. 414, comma 4, c.p.

[32] In termini generali su siffatta problematica, di recente, F. VITARELLI, *Il disvalore penale tra testo e contesto,* Torino, 2025.

L'alternativa dinanzi alla quale si trova l'operatore del diritto è tra una traslazione *sic et simpliciter* degli schemi concettuali tradizionali – dalla natura storicamente umanizzata e antropomorfica – al nuovo contesto tecnologico o, piuttosto, un ripensamento e una rimodulazione (manipolazione?) degli stessi per adeguarli ad uno scenario completamente diverso da quello in cui essi sono stati concepiti[33].

3. *In particolare: i comportamenti illeciti*

Cominciando ad affrontare più da vicino i profili specificamente connessi all'oggetto dell'indagine, è necessario prendere atto di come, di pari passo alla sopra descritta mutazione antropologica indotta dalle nuove tecnologie, siano mutate pure le dinamiche criminose[34], anche e soprattutto in considerazione di talune intrinseche caratteristiche dello spazio digitale[35].

Ci si limita in questa sede, senza nessuna pretesa di completezza, a ricordarne alcune tra quelle che possono esplicare, a vario titolo e con differente intensità, un rilievo sulla genesi e/o sulle modalità di estrinsecazione dei comportamenti illeciti.

Innanzitutto, lo spazio digitale crea una situazione di vulnerabilità particolarmente intensa in capo agli utenti. Vi è, infatti, una maggiore facilità di accesso da parte dell'autore della condotta illecita ai "luoghi" della potenziale vittima e, conseguente, una significativa difficoltà della stessa di escludere da essi il suo eventuale aggressore.

Emblematico sul punto l'orientamento della giurisprudenza di legittimità[36], secondo la quale la natura dematerializzata del ciberspazio consentirebbe di ritenere sussistente l'aggravante della minorata difesa ex art. 61, n. 5, c.p. con riferimento alle circostanze di luogo. Infatti – si osserva – «la

[33] Sul tema, G. MORGANTE, *Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del* law enforcement, in *Riv. it. informatica e diritto,* 2025, 97.

[34] Sul punto, *amplius,* E. U. SAVONA, M. MIGNONE, *The fox and the hunters: how IC Technologies change the crime race,* in *European Journal on Criminal Policy and Research* 10, 2024, 3 ss.

[35] In termini generali, J. R. AGUSTINA SANLLEHÍ, *La arquitectura digital de Internet como factor criminogeno: Estrategias de prevencion frente a la delincuencia virtual,* in *International e-journal of criminal sciences*, 2009, 3, 1 ss.; M. TONELLOTTO, *Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. XVI, 2022, 6 ss.

[36] Cass. pen., sez. VI, 22 marzo 2017, 17937, in *deJure;* Cass. pen., sez. II, 14 gennaio 2021, n. 12427, in *deJure.*

distanza tra il luogo ove si trova la vittima (…) e quello in cui, invece, si trova l'agente, determina una posizione di maggior favore di quest'ultimo, consentendogli di schermare la sua identità e (….) di sottrarsi agevolmente alle conseguenze della propria condotta»[37].

Le vittime *online,* inoltre, spesso non comprendono l'intimità istantanea offerta da *Internet*, facilitando esse stesse la condivisione di preziose informazioni personali con sconosciuti[38]. Sicché, più si rimane connessi, più si rischia di divenire bersaglio di aggressioni di varia natura e portata[39].

In effetti, il ciberspazio è una sfera di comunicazione parallela allo spazio fisico, ma in cui oggetti, beni e azioni devono essere introdotti. La decisione di accedere o entrare nella dimensione digitale non è sempre volontaria, ma spesso, sono proprio le attività quotidiane di ogni utente a determinare ciò che viene in essa convogliato. Ed è innegabile che se i beni di una persona, siano essi legati alla proprietà, alla *privacy*, alla libertà sessuale, ecc., non vengono introdotti in *Internet*, non saranno disponibili e quindi non potranno essere presi di mira da un criminale[40].

Dal punto di vista del potenziale soggetto attivo del reato, nello spazio digitale vi è una minore percezione del rischio e un effetto disinibente (c.d. *online disinhibition effect*[41]) legato all'anonimato o pseudoanonimato di chi opera *online*[42].

[37] Cass. pen., sez. II, 14 gennaio 2021, n. 12427, in *deJure,* punto n. 2 del Considerato in diritto.

[38] In argomento, G. Marotta, *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. VI, 2012, 93 ss., che evoca la c.d. Sindrome di Pollicino, formula con la quale si indica la tendenza di ogni utente del *web* a lasciare piccole tracce, facilmente rintracciabili (ivi, 96).

[39] Sull'argomento, *amplius,* F. Miró Llinares, *La opotunidad criminal en el ciberspacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen,* in *Revista Electrónica de Ciencia Penal y Criminología*, 13.7.2011; J. J. Carrillo Miranda, *Factor humano: la teoría de las Actividades Cotidianas en la Ciberseguridad,* 2020, in *https://www.academia.edu,* novembre 2020.

[40] F. Miró Linares*., La victimización por cibercriminalidad social. Un estudio a partirde la teoría de las actividades cotidianas en el ciberespacio,* cit., 14.

[41] Così, tra gli altri, J. Suler, *The Online Disinhibition Effect*, in *Cyberpsychology & Behavior*, 2004, Vol. VII, n. 3, 321 ss.; N. Lapidot-Lefler, A. Barak, *Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition*, in *Computers in Human Behavior*, 2012, n. 28, 434 ss.

[42] Come è stato osservato, il *web* rappresenta «il più potente veicolo per l'anonimato. Non esiste luogo dove vi siano più *avatar*, *alias*, indirizzi di comodo e false identità che nei *social net-*

Molte persone, pensando di essere schermate da un'identità digitale, non sempre direttamente riconoscibile, dicono e fanno cose che non direbbero o farebbero nella realtà *offline,* guardano alla loro vita come se si trattasse di un gioco con regole e norme che non applicherebbero nella quotidianità[43]. Una volta spento il *computer* e tornati alla routine quotidiana, credono di potersi lasciare alle spalle quel gioco e la propria identità[44]. Senza trascurare che l'uso intensivo della rete e l'elevata permanenza *online* costituiscono «un potentissimo catalizzatore di psicopatologie preesistenti, uno spazio ideale dove esprimere gli aspetti più deteriori e patologici del sé»[45].

I protagonisti di questo "nuovo" mondo si muovono, dunque, in un luogo che, già per sua intrinseca natura, può svolgere un potente ruolo criminogeno. A questo si aggiunga che una recente (e sconvolgente) caratteristica della realtà digitale è rappresentata dalla circostanza che sempre più frequentemente vanno prendendo forma condotte criminali progettate solo per essere documentate con videoriprese, le quali assumono una loro vitalità autonoma nel momento in cui sono condivise e scaricate in rete[46].

In queste strade oscure di *Internet*[47], l'interazione tra criminale e vittima può essere un riflesso molto pallido di quanto avviene nella realtà materiale. Così, per esempio, si è osservato come l'*a–sincronicità* delle relazioni *via–chat*, ossia la possibilità di rispondere a intervalli di tempo più o meno prolungati, vanifichi «l'efficacia inibente di un'interazione immediata e spontanea. In assenza di riscontri immediati, infatti, il flusso dei pensieri dell'internauta rischia di virare verso forme di disinibizione, che altrimenti, nella comunicazione istantanea, sarebbero state immediatamente intercettate»[48].

work. E se nessuno sa chi siamo, possiamo permetterci comportamenti criticabili senza subire conseguenze». Così e *amplius* M. Spitzer *Digitale demenz. Wie wir uns und unsere Kinder um den Verstand bringen,* cit.*,* cap. 5.

[43] J. Suler, *The Online Disinhibition Effect*, cit., 323. In argomento, v. altresì, M. Grandi, *Far Web. Odio, bufale, bullismo. Il lato oscuro dei social*, Milano, 2017, *e-book*;

[44] Ancora J. Suler, *The Online Disinhibition Effect*, cit., 323.

[45] T. Cantelmi, M. Talli*, Psicopatologia del Cyberspazio. Dislocazioni mentali, personalità avatar-mediate, derive autistiche e condotte fuori controllo*, in *Modelli per la mente*, 2008, vol. I, 41.

[46] S. Pierazzi, *I* social*: nuovi modi di comunicare o di esserci? I rischi e le condotte,* in *Nodi virtuali, legami informali:* Internet *alla ricerca di regole,* a cura di P. Passaglia, D. Poletti, Pisa, 2016, 221 ss.

[47] J. R. Agustina Sanllehí, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?,* cit. 717.

[48] T. Pietrella, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive.*

Inoltre, «l'assenza di stimoli facciali e vocali nella comunicazione testuale può causare un'alterazione dei freni inibitori a causa di una possibile *introiezione solipsistica* dell'interlocutore» (….) di un «processo interiore in forza del quale, in una relazione basata sullo scambio di messaggi di testo, la mente umana tende ad attribuire all'interlocutore virtuale (le cui sembianze sono neutre) tratti personali, fisici e vocali, conformi a proprie rappresentazioni interne, influenzate da aspettative, desideri e bisogni. Ciò determina l'introiezione psichica di un personaggio, modellato (inconsciamente) in base alla propria fantasia. Per effetto di questa proiezione psicologica, l'internauta (…) sentirebbe dentro di sé maggior sicurezza nel rapporto (quasi dominasse l'altro, lo conoscesse nell'intimo) e assoluta libertà di dire o agire secondo la propria fantasia»[49].

La comunicazione nel mondo digitale è "disincarnata", poiché la dimensione fisica del corpo e i significati che essa porta con sé non partecipano alle dinamiche relazionali[50]. Tuttavia, in questo modo si può perdere un importante criterio per la comprensione delle emozioni altrui, favorendo lo sviluppo di un "analfabetismo emotivo"[51].

Dal punto di vista criminologico, alcune recenti vicende evidenziano, per esempio, il passaggio da forme tradizionali di molestia individuale a modelli di violenza partecipativa, nei quali il danno viene amplificato dall'interazione di una pluralità di soggetti, spesso gli uni all'insaputa degli altri[52]. La vittima, dunque, non subisce soltanto l'azione del primo autore della diffusione, ma diviene oggetto di una continua esposizione pubblica, difficilmente reversibile a causa della riproducibilità dei contenuti digitali.

Inoltre, e sotto diverso profilo, *Internet* è un luogo in cui è possibile pianificare agevolmente un crimine, poiché l'ambiente digitale rappresenta una preziosa fonte di informazioni. L'informazione è l'essenza stessa di *Internet*,

Rilevanza giuridica della comunicazione degradante online *nel reato di diffamazione,* cit., 13.

[49] T. PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante* online *nel reato di diffamazione,* cit. 13, il quale richiama, altresì, J.R. SULER, *The Online Disinhibition Effect,* cit., 322.

[50] M. R. ALLEGRI, Ubi social, ibi ius. *Fondamenti costituzionali dei* social network e profili *giuridici della responsabilità dei* provider*,* cit., 20.

[51] Ancora M. R. ALLEGRI, Ubi social, ibi ius. *Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei* provider*,* cit., 20.

[52] Il riferimento è ai casi noti con il nome delle *chat* ("*Phica*" e "*Mia moglie*") sulle quali erano state condivise immagini intime non consensuali, commenti osceni e volgarità coinvolgenti centinaia di donne.

la quale può essere definita come un enorme *database* che abbraccia quasi tutti i campi del sapere[53]. I contenuti sono, di regola, gratuiti, aggiornati e facilmente reperibili. Sicché, i criminali se ne avvalgono per organizzarsi meglio, per ampliare lo spettro delle loro attività, per aggiornare il loro *modus operandi*, per evitare o ridurre rischi legati alle attività delle forze dell'ordine.

A ciò si aggiunga che le conseguenze di certe forme di criminalità informatica possono essere disastrose: è il caso, ad esempio, degli attacchi contro infrastrutture private e/o pubbliche cruciali, come il controllo del traffico aereo, le telecomunicazioni, le forniture di energia elettrica, i servizi medici e ospedalieri.

Guardando ad un ulteriore aspetto, occorre poi ricordare che l'assenza di confini del *cyberspace* fa sì che sia possibile commettere reati anche a centinaia, se non a migliaia, di chilometri di distanza dal luogo in cui si opera nei confronti di un numero indeterminato, e potenzialmente illimitato, di vittime. Sicché, le condotte nel mondo digitale presentano una intrinseca capacità di amplificare in modo significativo la gravità dell'impatto offensivo sugli interessi tutelati.

Il riferimento va in particolare – come è noto – alle ipotesi di pubblicazione di contenuti pregiudizievoli, i quali, una volta divulgati attraverso i mezzi messi a disposizione dalle nuove tecnologie, divengono fruibili da parte di un pubblico astrattamente confinato, con conseguente incremento esponenziale dell'effetto negativo che da essi deriva. Le tecnologie dell'informazione e della comunicazione agiscono, infatti, "come moltiplicatori di forze", rendendo possibile un impatto su un numero rilevante di vittime con minimo sforzo da parte del soggetto agente[54].

Senza trascurare che i contenuti offensivi possono addirittura sfuggire al controllo dello stesso autore della condotta iniziale. Una sorta di "febbre da condivisione" connota, infatti, l'attuale società, sempre più incentrata su modalità di relazioni impersonali, meccanicamente filtrate da strumenti tecnologici digitali[55], che spesso finiscono per diventare vere e proprie "armi

[53] E. U. Savona, M. Mingone, *The fox and the hunters: how IC Technologies change the crime race,* cit., 8.

[54] E. Maestri, *Stupri digitali: una questione di* governance *del* cyberspazio, cit., 47

[55] U. Galimberti, *Psiche e techne. L'uomo nell'età della tecnica*, cit., in particolare 36.

di distruzione della personalità"[56]. Sicché, nella maggior parte dei casi non è possibile prevedere quanto sarà capillare la diffusione dei contenuti pubblicati, posto che la "viralità" spesso imbocca percorsi casuali e difficilmente pronosticabili[57].

A questi elementi si aggiunge poi la circostanza che risulta tutt'altro che agevole individuare, bloccare ed eventualmente rimuovere detti contenuti[58], i quali, anche se cancellati, potrebbero essere già stati duplicati e ripubblicati da alti utenti in altri luoghi o potrebbero comunque essere rintracciati attraverso le navigazioni a ritroso nel tempo all'interno degli sconfinati archivi *web* oggi esistenti[59]. In breve: *the Internet never forgets.*

4. *La criminalità informatica*

Alla luce di quanto fino ad ora considerato, dovrebbe essere facile intuire come siffatto imponente, e sotto certi aspetti imprevedibile, sviluppo tecnologico non abbia solo rivoluzionato gran parte della nostra quotidianità, ma abbia, altresì, esposto il diritto[60] – e il diritto penale non fa eccezione – a molteplici profonde sollecitazioni, scaturite dalla difficoltà di continuare ad applicare le tradizionali categorie concettuali ad una realtà profondamente trasformata.

L'intento di massima liberalità che – *ab origine* in linea astratta – ha connotato la citata innovazione tecnologica ha, in realtà, lasciato spazio anche ad una sua preoccupante torsione in chiave illecita, alla luce del diffondersi

[56] Così M. Mattia, "Revenge porn" *e suicidio della vittima: il problema della divergenza tra 'voluto' e 'realizzato' rispetto all'imputazione oggettiva degli eventi psichici*, in *www.lalegislazionepenale.eu*, 19 luglio 2019, 4.

[57] G.M. Caletti, *Libertà e riservatezza sessuale all'epoca di* Internet. *L'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale,* in *Riv. it. dir. proc. pen.*, 2019, 2067.

[58] In argomento S. Pietropaoli, *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars interpretandi*, n. 1 del 2017, 70 ss., il quale ricorda come oggi il c. d. diritto all'oblio non sia «più identificabile con il diritto alla cancellazione della memoria e neppure con il diritto alla contestualizzazione, ma è il diritto alla deindicizzazione dai motori di ricerca» (ivi, 73).

[59] R. Brighi, *La vulnerabilità nel cyberspazio,* in *Ars interpretatndi,* n. 1 del 2017, 85, N. Amore, *La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo* cybercrime *disciplinat*o dall'art. 612 *ter* c.p., in *www.lalegislazionepenale.eu*, 20 gennaio 2020, 5, nota n. 16.

[60] *Amplius* e per tutti, G. Pascuzzi, *Il diritto nell'era digitale,* Bologna, 2024.

di molteplici sviluppi patologici nell'uso degli strumenti informatici e tecnologici[61].

Ma, si può davvero sostenere che la criminalità informatica sia una mera questione di mezzo utilizzato[62]?

Invero, come è noto, ormai le problematiche evidenziate non concernono più solo i "reati informatici in senso stretto" (*computer crimes*), vale a dire fattispecie incriminatrici concepibili solo ai danni di un *computer* o di una rete informatica, bensì – in misura ancora più significativa – i c.d. "reati informatici in senso ampio" o cibernetici (*cyber crimes*), ossia quelle fattispecie "comuni" che possono essere realizzate anche nel mondo reale ma che assumono una peculiare fisionomia allorché vengano realizzate nel *cyberspace*[63]. In altre parole, le questioni che verranno analizzate coinvolgono, sia pure talora in maniera differente, tutte le ipotesi nelle quali la *res informatica* è *instrumentum delicti* o *locus commissi delicti.*

In realtà, in una prima fase i *computer crimes* non sono stati percepiti come una originale e specifica categoria di illeciti, ma semplicemente come nuove forme di aggressione a beni giuridici tradizionali, già oggetto di tutela, caratterizzate dal peculiare mezzo impiegato o dall'oggetto materiale della condotta[64]. Tanto che, come meglio si vedrà[65], in occasione del primo significativo intervento volto ad adeguarsi alla nuova realtà[66], il legislatore si è limitato a modificare alcune incriminazioni codicistiche, al fine di ren-

[61] Per tutti, D. S. WALL, *Cybercrime. The Transformation of Crime in the Information Age,* Cambridge, 2024, 1 ss.

[62] *Amplius,* R. POSADA MAYA, *El cibercrimen y sus efectos en la teoria de la tipicidad: de una realidad fisica a una realidad virtual*, *Revista Nuevo Foro Penal*, vol. 13, n. 88, 2017, 72 ss.

[63] Occorre, peraltro, segnalare che siffatta *summa divisio* vale solo in linea di massima, come primissimo criterio orientativo, ma non è in grado di essere rigorosamente applicata a tutte le fattispecie incriminatrici. Vi sono, peraltro, alcuni autori che preferiscono distinguere tra *Crimes against the machine* (o *computer integrity crimes)*, *Crimes that use the machine* (o *computer –enabled or computer related*), *Crimes in the machine* (o *computer content crimes, where the offending focuses upon the content of compiuters*). Così D. S. WALL., *Cybercrime. The Transformation of Crime in the Information Age,* cit., 58 ss.

[64] Sul punto v. espressamente la *Relazione del Disegno di legge n. 2773* ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"), divenuto Legge 23 dicembre 1993, n. 547. In dottrina, F. R. FULVI, *L'unità virtuale del diritto penale dell'informatica,* in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali,* Torino, 2012, 168 ss.

[65] V. *infra* capitolo secondo, paragrafo 3.

[66] Il riferimento è alla l. n. 547 del 1993.

derle idonee a ricomprendere le condotte proprie della (allora) emergente fenomenologia informatica, e ad aggiungere all'interno dei diversi titoli fattispecie incriminatrici di nuovo conio ma per lo più strutturate sul modello di altre già esistenti[67].

In altre parole, l'approccio inizialmente è stato di tipo "analogico", sulla base del presupposto – condivisibile o meno, lo si chiarirà – che la rivoluzione digitale avesse semplicemente comportato una mera riproduzione virtuale della realtà fisica e che dunque fosse, in buona sostanza, sufficiente un adattamento semantico dell'universo giuridico e del lessico già esistente[68].

Si pensi ad un esempio, per tutti, particolarmente emblematico: la necessità di tutelare un sistema informatico ha indotto il legislatore italiano, in prima battuta, a ragionare per analogia con la tutela del domicilio, sul presupposto per cui «i sistemi informatici o telematici (…) costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione»[69]. Da qui è derivata l'introduzione, all'interno del Titolo XII del Codice penale, Capo III, Sezione IV («Dei delitti contro la inviolabilità del domicilio») della fattispecie rubricata "*Accesso abusivo a un sistema informatico o telematico*" (art. 615 *ter*).

Del resto, anche la giurisprudenza, in diverse occasioni, ha riconosciuto che il sistema informatico o telematico, al pari del domicilio, costituisce un «luogo inviolabile delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche»[70].

[67] Sul punto v. *Relazione del Disegno di legge n. 2773* (divenuto Legge 23 dicembre 1993, n. 547), cit.

[68] Sulle insidie insite in siffatto approccio, di recente, G. FIORINELLI, Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche,* in *disCrimen,* 3.1.2023, 1 ss.; G. MORGANTE, *Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del* law enforcement, in *Riv. it. informatica e diritto,* 2025, 95 ss., la quale evoca la "metafora del gemellaggio" o "paradigma del *digital twin",* secondo il quale «la digitalizzazione avrebbe creato "gemelli" di mondi ma soprattutto di diritti a vario titolo speculari rispetto a quelli del mondo analogico» (ivi, 96, 97).

[69] *Relazione del Disegno di legge n. 2773* (divenuto Legge 23 dicembre 1993, n. 547), cit.

[70] Cass. pen., sez. un., 26 marzo 2015, n. 17325, Rv. 263020, punto n. 2.2 del Considerato in diritto.

5. *Le prime criticità. L'esempio emblematico dell'accesso abusivo a sistema informatico*

Nondimeno, sono facilmente riconoscibili le differenze che possono sussistere, in termini di aggressione, tra il domicilio fisico e il sistema informatico. Il che si traduce inevitabilmente in una non trascurabile disomogeneità di problemi che possono riguardare l'applicazione delle relative fattispecie incriminatrici. Tanto che, come è stato osservato, la prassi giurisprudenziale ha «a tal punto avvertito l'esigenza di "forzare" la "gabbia" ermeneutica, derivante dall'immagine prescelta dal legislatore per rappresentare il sistema informatico (*i.e.*: il domicilio), che attualmente la fattispecie di cui all'art. 615 *ter* c.p. finisce per trovare applicazione in casi piuttosto distanti dall'ispirazione originaria della disciplina, perché privi di un disvalore "di intrusione"»[71].

Parrebbe, infatti, che la tipicità del reato in oggetto abbia subito un processo di progressiva ridefinizione in via interpretativa, attraverso la sostituzione della condotta di "accesso abusivo" al sistema con quella di "utilizzo indebito" dello stesso.

Ma per meglio comprendere i termini della questione è utile ricostruire, sia pure in estrema sintesi, l'evoluzione interpretativa che ha interessato la fattispecie in esame.

Secondo un'opzione ermeneutica, che, a seguito di un iniziale disorientamento della prassi[72], pareva aver ricevuto l'avallo delle sezioni unite della Cassazione[73], il giudizio circa l'esistenza del dissenso del *dominus loci* avrebbe dovuto assumere come parametro di valutazione la sussistenza o meno di un'obiettiva violazione, da parte dell'agente, delle prescrizioni im-

[71] Così G. FIORINELLI, Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche,* cit., 13,14.

[72] Sul punto *amplius* C. PECORELLA, *L'attesa pronuncia delle sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo,* in *Cass. pen.,* 2012, 3692 ss.

[73] Cass. pen., sez. un., 27 ottobre 2011, n. 4694, Rv. 251271. Sulla sentenza *de qua* R. BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato,* in *www.penalecontemporaneo.it, Riv. trim.,* n. 1, 2012, 123 ss.; R. FLOR, *Verso una rivalutazione dell'art. 615 ter c.p.,* in *www.penalecontemporaneo.it, Riv. trim.,* n. 2, 2012, 126 ss.; C. PECORELLA, *L'attesa pronuncia delle sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo,* cit., 3692 ss.; I. SALVADORI, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. trim. dir. pen. econ.*, 2012, 369 ss.

partite dal *dominus* stesso circa l'uso del sistema. Detto dissenso non avrebbe, invece, potuto essere formulato unicamente sulla base della direzione finalistica, soggettivamente impressa alla condotta[74]. Sicché, non avrebbero potuto assumere rilievo, per la configurazione del reato, gli scopi e le finalità che avessero motivato l'agente all'ingresso nel sistema[75].

Si era, dunque, in tal modo, esclusa la possibilità di ravvisare il delitto in esame nella condotta del soggetto il quale, avendo titolo per accedere al sistema, se ne fosse avvalso per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente configurabili, ove le suddette finalità fossero state effettivamente realizzate.

In questa prospettiva, dunque, la volontà contraria dell'avente diritto, richiesta dall'art. 615 *ter* c.p., si riteneva integrata esclusivamente allorché il soggetto agente avesse operato illegittimamente, «in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta»[76]. Un eventuale dissenso tacito del *dominus loci non* avrebbe invece potuto essere desunto – come detto – dalla mera finalità perseguita dall'agente[77]. Con la conseguenza che, nei casi in cui il soggetto avesse compiuto sul sistema un'operazione pienamente assentita dall'autorizzazione ricevuta, e avesse agito nei limiti di questa, il reato di cui all'art. 615 *ter* c.p. non avrebbe potuto ritenersi configurabile, a prescindere dallo scopo eventualmente perseguito ed anche se dei dati acquisiti il soggetto si fosse poi servito per finalità illecite[78].

Invero, detta opzione ermeneutica, volta a delimitare l'abusività dell'accesso al solo ingresso in assenza di autorizzazione, parrebbe privilegiare un'interpretazione della fattispecie effettivamente diretta a tutelare il domicilio informatico, inteso come luogo in cui si esplica la personalità del soggetto titolare del domicilio medesimo. In questa prospettiva l'ingresso idoneo ad assumere disvalore sarebbe solo quello privo di legittimazione[79].

[74] Cass. pen., sez. un., 27 ottobre 2011, n. 4694, Rv. 251271, punto n. 4 del Considerato in diritto.

[75] Cass. pen., sez. un., 27 ottobre 2011, n. 4694, Rv. 251271, punto n. 5 del Considerato in diritto.

[76] Cass. pen., sez. un., 27 ottobre 2011, n. 4694, cit., punto n. 4 del Considerato in diritto.

[77] Cass. pen., sez. un., 27 ottobre 2011, n. 4694, cit., punto n. 4 del Considerato in diritto.

[78] Cass. pen., sez. un., 27 ottobre 2011, n. 4694, cit., punto n. 4 del Considerato in diritto.

[79] Così e *amplius,* R. Bartoli, *L'accesso abusivo a un sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato,* cit., 125.

Nondimeno, la giurisprudenza formatasi in epoca successiva alla citata sentenza aveva manifestato l'esigenza di ulteriori precisazioni e specificazioni, in funzione estensiva, della portata del principio di diritto espresso dalle "prime" sezioni unite, segnatamente in merito alla possibilità di ritenere idonea ad integrare la tipicità della fattispecie incriminatrice *de qua* (per lo meno nella forma aggravata contemplata dal secondo comma dell'art. 615 *ter* c.p.) la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che si traducesse in un abuso o sviamento dei poteri conferitigli[80].

Si era, infatti, osservato che «sarebbe un errore di non poco conto considerare la realtà "criminologica" del delitto di accesso abusivo a un sistema informatico o telematico come caratterizzata prevalentemente – sul piano quantitativo come qualitativo – da accessi "esterni" ai sistemi. (….) La realtà giudiziaria, al contrario, dimostra come sempre più frequenti, subdoli e difficili da fronteggiare siano gli accessi "interni", o meglio i trattenimenti indebiti nei sistemi, posti in essere da soggetti che del sistema hanno le "chiavi di accesso" ma che tale chiave possono lecitamente utilizzare solo per specifici e limitati fini»[81].

Ebbene, pochi anni più tardi, quello che era sembrato un approdo interpretativo della nuova fattispecie è stato rimesso in discussione da un nuovo pronunciamento delle medesime sezioni unite, ad avviso delle quali integra il delitto previsto dall'art. 615 *ter* (anche) «la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso (nella specie, Registro delle notizie di reato: Re. Ge.), acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita»[82].

Infatti, alla stregua di siffatta rilettura della fattispecie, non dovrebbe considerarsi estranea alla sfera di applicazione della stessa la situazione nel-

[80] Così, Cass. pen., sez. un. 18 maggio 2017, n. 41210, Rv. 271061, punto n. 4 del Considerato in diritto.

[81] C. Parodi, *Accesso abusivo a sistema informatico: può essere sufficiente lo "sviamento di potere"?*, in *www.ilpenalista.it,* 18 settembre 2017.

[82] Cass. pen., sez. un., 18 maggio 2017, n. 41210, in *C.e.d.* 271061, punto n. 13 del Considerato in diritto. Sulla pronuncia *de qua* R. Flor, *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere",* in *Dir. pen. proc.,* 2018, 506 ss.

la quale l'accesso o il mantenimento nel sistema informatico dell'ufficio a cui è addetto il pubblico ufficiale o l'incaricato di pubblico servizio, seppur avvenuto a seguito di utilizzo di credenziali proprie dell'agente, si connoti, tuttavia, per l'abuso delle funzioni, integrando, cioè, «uno sviamento di potere, un uso del potere in violazione dei doveri di fedeltà che ne devono indirizzare l'azione nell'assolvimento degli specifici compiti di natura pubblicistica a lui demandati»[83].

Sennonché, in tal modo il parametro di riferimento per valutare l'abusività dell'accesso parrebbe coincidere non tanto con l'insieme delle disposizioni impartite dal *dominus loci*, bensì con il complesso delle previsioni che regolano e indirizzano l'attività amministrativa verso i fini determinati dalla legge: ne consegue che detta "abusività" verrebbe ravvisata nella violazione della regola di imparzialità e trasparenza che regge l'azione amministrativa, frustrando però in tal modo la *ratio* dell'orientamento che verosimilmente – *ab origine* – voleva evitare una dilatazione del concetto di "accesso abusivo" oltre i limiti imposti dalla necessità di tutelare i diritti del proprietario del "sistema"[84].

Tanto premesso, e come già rilevato da parte della dottrina, «la volontà (se non la necessità) degli interpreti di sottrarsi ai vincoli ermeneutici derivanti dalla (talora controproducente) metafora del domicilio ha allora reso l'art. 615 *ter* c.p. una fattispecie dai confini piuttosto indefiniti, interpretata dalla giurisprudenza secondo cadenze che ormai prescindono dal testo normativo e che perciò possono dar vita a risvolti incompatibili con il principio di legalità penale»[85].

Basti pensare che in tempi recenti è stata ritenuta integrata la fattispecie in oggetto anche in un caso di trasmissione di dati, destinati a rimanere riservati, concernenti la clientela di una banca, da un soggetto abilitato ad accedervi a un soggetto non autorizzato a prenderne cognizione, posto che – si legge nella pronuncia – «i principi espressi per il pubblico funzionario possono essere trasfusi anche al settore privato, nella parte in cui vengono in rilievo i doveri di fedeltà e lealtà del dipendente che connotano indubbiamente anche il rapporto di lavoro privatistico». Sicché, dovrebbe consi-

[83] Ancora Cass. pen., sez. un., 18 maggio 2017, n. 41210, cit., punto n. 7 del Considerato in diritto.

[84] In questo senso, prima dell'intervento della seconda citata pronuncia delle sezioni unite, Cass. pen., V, 20 giugno 2014, n. 44390, Rv. 260763, punto n. 5 del Considerato in diritto.

[85] G. Fiorinelli, Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche,* cit., 14.

derarsi abusivo qualunque comportamento del dipendente che si ponga in contrasto con i suddetti doveri, posto che, in tal modo, si manifesterebbe «la "ontologica incompatibilità" dell'accesso al sistema informatico, connaturata ad un utilizzo dello stesso estraneo alla *ratio* del conferimento del relativo potere»[86].

6. *Il problematico adattamento delle categorie tradizionali*

L'esemplificazione dalla quale ha preso le mosse questa riflessione dimostra come il *modus operandi* seguito *ab origine* dal nostro legislatore si sia caratterizzato per una «geometrica rigidità sia sul piano della selezione dei beni giuridici, sia su quello propriamente lessicale»[87].

Nondimeno, siffatta impostazione ha costituito un limite alla completa comprensione dei tratti originali delle nuove fenomenologie. Infatti, da un lato, sul piano lessicale, l'attaccamento rituale alle formule tradizionali talora non ha consentito la corretta messa a fuoco delle questioni emergenti; dall'altro lato, la scelta di preservare la coerenza sistematica del codice si è tradotta nell'eccessiva artificiosità di alcuni segmenti della disciplina[88].

Basti pensare, per rimanere ancorati alla fattispecie sulla quale si sta discorrendo, all'affermazione della giurisprudenza in forza della quale il luogo di consumazione del delitto di cui all'art. 615 *ter* c.p. è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente[89], identificando nell'atto fisico della "digitazione", l'unica condotta umana di natura materiale. Da qui deriva la conseguenza, paradossale sul piano logico, che la violazione del domicilio informatico (della persona offesa) si deve ritenere integrata presso il domicilio dell'autore del fatto[90].

Solo nel corso del tempo, ci si è resi conto di come il reato nella dimensione digitale possa, invero, presentare rilevanti fronti di criticità rispetto ai

[86] Cass. pen., sez. V, 29 novembre 2018, n. 565, Rv. 274392, punto n. 3.1.2 del Considerato in diritto, là dove si richiama Cass. pen., sez. un., 18 maggio 2017, n. 41210, cit.

[87] F. Berghella, R. Blaiotta, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, 2330.

[88] F. Berghella, R. Blaiotta, *Diritto penale dell'informatica e beni giuridici*, cit., 2330.

[89] Cass. pen., sez. un., 24 aprile 2015, n. 17325, Rv. 263020.

[90] G. Fiorinelli, Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche,* cit., 24.

paradigmi di incriminazione propri della realtà analogica e alle tradizionali categorie del diritto penale.

Quandanche, infatti, ci si trovi effettivamente dinanzi a forme di aggressione nei confronti di beni già tutelati, le fenomenologie criminose risultano caratterizzate da tratti fisionomici del tutto peculiari[91], primi tra i molti la totale o parziale smaterializzazione della condotta, una rapidissima velocità di esecuzione della stessa, il potenziale anonimato dell'autore, nonché la portata globale del fatto, non più connotato da precisi vincoli di natura territoriale[92].

Da tale premessa, è facile intuire il disorientamento del giurista in merito alla persistente adeguatezza, o meno, del tradizionale approccio nella configurazione e interpretazione del reato cibernetico.

L'idea che la realtà virtuale non fosse pienamente sovrapponibile a quella *offline* è, tuttavia, emersa solo poco a poco. La tentazione (ma al contempo la difficoltà) di ricondurre il nuovo fenomeno all'interno delle coordinate giuridiche esistenti è ben rappresentata, come anticipato, anche dal frequente utilizzo di un linguaggio metaforico[93].

Nondimeno, questo approccio, di per sé, non deve stupire se è vero che, come osservato, «non si può immaginare l'inconoscibile se non movendo dalla conoscenza, ossia per metafore della realtà»[94].

7. *Il programma d'indagine*

Il punto di partenza da cui muovere per una corretta comprensione delle questioni sollevate dalla rivoluzione digitale è, dunque, rappresentato dall'esigenza di una attenta lettura della nuova realtà, sia sotto il profilo fenomenologico, sia sotto il profilo giuridico. La rivoluzione indotta dalle nuove tecnologie è stata, infatti, correttamente definita come «un vero e proprio "vaso di Pandora" di reati e sfide»[95].

[91] Sul punto v. *infra* capitolo terzo.

[92] Su questi e altri profili v. *infra* capitolo terzo.

[93] In questo senso e *amplius* G. FIORINELLI, Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche,* cit., 6 ss., alla quale si rinvia per un'ampia esemplificazione.

[94] F. GALGANO, *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto*, Bologna, 2010, 14.

[95] E. U. SAVONA, M. MINGONE, *The fox and the hunters: how IC Technologies change the crime race,* cit., 7.

A fronte di questo nuovo scenario, l'operatore del diritto spesso si trova, però, in difficoltà nel gestire inedite forme di aggressione nei confronti di beni giuridici tradizionali e addirittura nel mettere a fuoco nuovi interessi emergenti, neppure immaginabili prima dell'avvento delle nuove tecnologie.

Così, da un lato, il legislatore non di rado fatica ad abbracciare, con la creazione di nuove fattispecie incriminatrici, le fenomenologie criminose legate alla dimensione digitale, le quali si evolvono con una rapidità che può essere superiore alla capacità della norma di "fotografarle". Sicché, accade non di rado che anche ipotesi di reato di recente conio, volte a soddisfare emergenti esigenze di tutela, risultino già "vecchie" nel momento stesso in cui vedono la luce.

Dall'altro lato, anche la prassi applicativa non sempre riesce o può, stante il prezioso argine del principio di stretta legalità, reagire dinanzi a comportamenti offensivi vieppiù insidiosi, sofisticati e mutevoli nelle loro forme di estrinsecazione.

Questa trasformazione solleva, infatti, non pochi problemi, sia concettuali sia latamente culturali, e l'impostazione giuridica tradizionale fatica a tenere il passo con l'evoluzione della dimensione tecnologica[96].

Del resto, come già osservato, le ricerche hanno fino ad oggi fornito una moltitudine di tassonomie del reato digitale nel tentativo di meglio evidenziarne le caratteristiche; tuttavia, la maggior parte di esse non sembra sufficiente a comprenderne appieno tutte le peculiarità. Nondimeno, siffatta inadeguatezza non deriverebbe da errori degli autori, bensì dalla continua evoluzione del mondo della sicurezza informatica e del crimine informatico[97].

Infine, non si può prescindere dalle peculiari caratteristiche dei vari tipi di strumenti informatici in continua evoluzione , ognuno dei quali si contraddistingue per funzioni e impostazioni proprie. Un sito *web*, un *blog* o un *social network* possono presentare profili specifici, gli uni rispetto agli altri,

[96] *Amplius,* U. Pagallo, *Profili tecnico-informatici e filosofici,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 17. Per un'analisi interdisciplinare sul punto, altresì*,* T. C. King, N. Aggarwal, M. Taddeo, L. Floridi, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions,* in *Science and Engineering Ethics*, 2020, vol. 26, 89 ss.

[97] Z. R. A. Mooney, X. Zhang, J. D. Crabtree, *Understanding cybercrime: A three-generation approach,* in *Issues in Information Systems*, 2022, vol. 23, n. 3, 27.

e il diritto penale non può ignorarli, facendo di tutta l'erba un fascio, nel tentativo di risolvere le diverse problematiche e pervenire ad un'allocazione tecnicamente corretta delle conseguenze giuridiche[98]. Infatti, le considerazioni giuridiche che si possono di volta in volta svolgere, in relazione ai differenti profili teorici e applicativi, non sono indistintamente valide per tutti i *format* offerti dalla rete.

Si pensi, ancora una volta a titolo esemplificativo, all'invio di una *e–mail* offensiva dell'onore e/o della reputazione altrui all'interessato e a più destinatari in copia o di analogo messaggio all'interno di una *chat* condivisa da più utenti[99]. Ebbene, in siffatta ipotesi, ci si pone il problema di comprendere se si possa ritenere integrato il reato di diffamazione o, piuttosto, un fatto di ingiuria, posto che l'offeso teoricamente ha la possibilità di rispondere istantaneamente alla *e–mail* o al messaggio denigratorio, coinvolgendo tutti destinatari. Sennonché, a ben vedere, la risposta a questo interrogativo dipende, innanzitutto, da una più attenta considerazione dei meccanismi di funzionamento e delle caratteristiche proprie di ciascun mezzo tecnologico utilizzato[100].

I molteplici profili di complessità che caratterizzano le dinamiche criminose nel mondo digitale impongono, dunque, una rinnovata riflessione che abbia lo scopo di rendere compatibili le istanze di tutela, così come emergono nella loro nuova configurazione, con i principi fondamentali e le garanzie del diritto penale. Occorre allora verificare con equilibrio la tenuta dei classici meccanismi ascrittivi della responsabilità, senza farsi trascinare

[98] F. P. Lasalvia, *La diffamazione via web nell'epoca dei social network,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 351.

[99] Su siffatta casistica, tra le altre, Cass. pen., sez. I, 21 novembre 2023, n. 409, in *deJure,* ad avviso della quale «integra il delitto di diffamazione, e non la fattispecie depenalizzata di ingiuria aggravata dalla presenza di più persone, l'invio di messaggi contenenti espressioni offensive nei confronti della persona offesa su una *chat* condivisa anche da altri soggetti, nel caso in cui la prima non li abbia percepiti nell'immediatezza, in quanto non collegata al momento del loro recapito»; Cass. pen., sez. V, 5 giugno 2025, n. 29458, Rv. 288503, secondo la quale «la pubblicazione di un video offensivo sui *social network* configura sempre il reato di diffamazione aggravata e non quello meno grave di ingiuria, ormai depenalizzato, anche se la persona a cui è indirizzato l'insulto è "virtualmente presente". La semplice possibilità per la persona offesa di seguire la diretta e inserire commenti non è sufficiente a creare un contraddittorio immediato o un rapporto diretto con chi offende, né assicura una reale parità tra le parti».

[100] In argomento, *amplius,* L. Scopinaro, *Internet e delitti contro l'onore*, in *Riv. it. dir. proc. pen.*, 2000, in particolare 619 ss.; T. Pietrella, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante online nel reato di diffamazione,* cit., 28.

dalla aprioristica suggestione di ritenere superati le categorie e i principi del diritto penale classico.

In relazione a questa originale realtà l'operatore del diritto deve, infatti, innanzitutto comprendere a quale *stress* sia sottoposta l'architettura giuridica del diritto per verificare, poi, se i suoi tradizionali strumenti di lavoro possano, in realtà, funzionare ancora o se, piuttosto, debbano essere adattati o – addirittura – abbandonati.

Ci si limita ad anticipare alcuni aspetti che si andranno a toccare, senza, tuttavia, alcuna pretesa di esaurire, con le poche pagine di questo lavoro, questioni che richiederanno ulteriori e più approfondite riflessioni.

Innanzitutto, occorrerà verificare la tenuta di alcuni principi fondamentali di garanzia dinanzi alla tentazione di estendere, se non addirittura deformare, fattispecie incriminatrici originariamente nate per far fronte a fenomenologie criminose destinate ad esaurirsi nella realtà *offline*[101]. Il riferimento è, come facile intuire, innanzitutto al principio di legalità nella sua più peculiare declinazione della tassatività e del correlato divieto di analogia.

Inossidabile suona ancora il monito rivolto al giurista di "smascherare" ogni tentativo di applicazione analogica del diritto penale, non di rado camuffata sotto le spoglie di un'interpretazione estensiva[102]. L'applicazione analogica, infatti, espone il cittadino a «un'azione repressiva eccedente rispetto a quella espressamente autorizzata dal divieto»[103]. Tanto che vi è chi auspica, nella prospettiva di protezione dell'individuo, un superamento della "tradizionale declinazione lessicale" del divieto di analogia, per riconoscere, apertamente, cittadinanza costituzionale, come ulteriore pilastro dello Stato di diritto, al "diritto fondamentale" a non vedersi applicare la legge penale per analogia[104].

In secondo luogo, si tenterà di comprendere quali ricadute possano avere, per esempio, la dematerializzazione (almeno parziale) della condotta, la possibile automazione della stessa, l'interazione con sistemi di intelligenza

[101] V. *infra* capitolo secondo.

[102] Sull'importante funzione del divieto di analogia nel preservare gli irrinunciabili spazi di libertà dal diritto penale, G. MARINUCCI, *L'analogia e la "punibilità svincolata dalla conformità alla fattispecie penale"*, in *Riv. it. dir. proc. pen.*, 2007, 1254 ss. Analogamente, T. VORMBAUM, *Il diritto penale frammentario nella storia e nella dogmatica*, trad. it. di M. DONINI, in *www.penalecontemporaneo.it, Riv. trim.*, n. 1, 2015, 51 ss.

[103] F. GIUNTA, *Diritto penale. Un'introduzione*, Pisa, 2024, 25.

[104] Così V. MANES, *Introduzione ai principi costituzionali in materia penale,* Torino, 2024, 92.

artificiale, nonché la natura ubiqua del fatto di reato, sulle regole d'imputazione oggettiva e soggettiva, sulla determinazione del momento e del luogo di consumazione, sull'eventuale rilevanza penale di comportamenti anche successivi alla formale perfezione della fattispecie[105].

Non si può, infine, trascurare il ruolo degli *Internet service providers*, enormemente mutato nel corso del tempo e non più riconducibile a quello originario di mero convitato di pietra. Si tratterà dunque di verificare se ci siano gli estremi per un loro coinvolgimento nel processo di ascrizione di una responsabilità penale per gli illeciti destinati a consumarsi sugli spazi digitali da loro gestiti[106].

La tecnologia e il diritto penale sono quindi, inderogabilmente, chiamati a instaurare nuove forme di dialogo per meglio affrontare le ricadute indotte dallo spostamento di buona parte dei reati nel nuovo spazio *sui generis*[107]. Diversamente, la complessità concettuale e linguistica della nuova dimensione digitale rischia di porre il legislatore e il giudice in una condizione di inferiorità cognitiva. Occorre, in altre parole, guardarsi «dal duplice pericolo che la scienza espropri il diritto, e che il diritto ignori o rinneghi la scienza»[108].

Tanto premesso, appare chiaro come la rapidità dell'evoluzione tecnologica rappresenti un'enorme sfida per il diritto penale, destinata a non esaurirsi nel momento presente. La comprensione del bagaglio concettuale e del lessico tecnologico costituisce, e costituirà vieppiù, un fattore determinante, che non potrà essere pretermesso né in sede applicativa, né – tanto meno – nelle future scelte di politica criminale, in quanto condizionante in maniera significativa l'individuazione e la corretta giustapposizione degli elementi costitutivi delle fattispecie incriminatrici, nonché la stessa individuazione degli oggetti di tutela.

In diverse occasioni anche la prassi ha espressamente riconosciuto la necessità di dover considerare in modo nuovo quelle «categorie giuridiche

[105] V. *infra* capitolo terzo.

[106] Sul punto *infra* capitolo quarto.

[107] Così e *amplius,* J. R. AGUSTINA SANLLEHÍ, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?,* cit., 710.

[108] Così, e *amplius,* G. FIANDACA, *Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale,* in *Diritto & questioni pubbliche,* 2005, n. 5, 23. Su siffatto profilo problematico, altresì, G. FORTI, *L'immane concretezza. Metamorfosi del crimine e controllo penale,* Milano, 2000, in particolare 159 ss.

(…) coniate in epoche in cui erano del tutto sconosciute le attuali tecnologie informatiche»[109].

Nondimeno, non si può escludere che là dove il forzoso ricorso alla tutela penale comporti uno snaturamento di dette categorie, quale limite invalicabile dell'intervento punitivo, risulti preferibile invocare tecniche alternative di tutela, di natura civile od amministrativa. Infatti, cercare di ricondurre i nuovi paradigmi aperti dal *medium* digitale entro i confini dei concetti e dell'elaborazioni da tempo utilizzati per governare quanto accade nella realtà analogica non è sempre un'operazione possibile o esente da forzature.

Appare, infatti, sempre più fondato il dubbio che «il *Nomos* penalistico possa imbrigliare con successo la forza travolgente della Téchne»[110].

[109] Cass. pen., sez. II, 7 novembre 2019, n. 11959, in *deJure,* punto n. 1.4 del Considerato in diritto.

[110] F. Giunta, *Il valore della dignità*, in *Sussidiario di diritto penale. Parte speciale*, a cura di F. Giunta, 2023, cap. XIV, § 9 (consultabile su *disCrimen*).

Capitolo secondo

DAI REATI COMUNI AI REATI DIGITALI

SOMMARIO: 1. Il ricorso a fattispecie a-specifiche. – 2. Interpretazioni estensive e analogiche. – 3. Le nuove fattispecie informatiche. – 4. Dai *computer crimes* ai *cyber crimes*. – 5. Il *file* informatico come "cosa mobile". – 6. Il *web* come "mezzo di pubblicità". – 7. *Internet* come "mezzo di stampa". – 8. Il *web* come "luogo pubblico" o "aperto al pubblico" – 9. Molestia "col mezzo del telefono" e nuove modalità di intrusione tecnologica non gradita. – 10. Lo sfruttamento sessuale *online*.

«*Le forme della normatività tradizionali, forti o deboli che siano,*
saranno sempre più costrette, per sopravvivere e impedire di essere
annientate dalle forme antagoniste, a non intralciare
il funzionamento ottimale della tecnica di cui esse si servono
come mezzo per prevalere: e la loro struttura normativa
sarà sempre più costretta a conformarsi a questa "esigenza"».
(E. Severino, in N. Irti, E. Severino, *Dialogo su diritto*
e tecnica, Roma–Bari, 2001, 37)

1. Il ricorso a fattispecie a-specifiche

Come anticipato e meglio si vedrà[1], i reati realizzati nello spazio digitale sono caratterizzati da peculiari caratteristiche che li differenziano rispetto ai reati, per così dire, *offline*.

Lo sviluppo rapido delle nuove tecnologie ha agito, da un lato, modificando i tratti fisionomici di archetipi delinquenziali classici, già radicati nel tessuto sociale, dall'altro, favorendo l'emersione di forme criminali inedite, in grado di compiersi e di articolarsi solamente per mezzo e all'interno dei nuovi sistemi di comunicazione digitale.

Sennonché, prima che il legislatore intervenisse nel tentativo di inquadrare giuridicamente le nuove fenomenologie criminose legate alla rivoluzione tecnologica, la tutela penale affidata alle fattispecie già esistenti si muoveva

[1] V. *infra* capitolo terzo.

pericolosamente tra interpretazioni estensive e analogie *in malam partem* di concetti e categorie che non sempre avrebbero, invece, potuto adattarsi alla nuova realtà[2].

Antecedentemente al complesso di riforme che ha portato alla progressiva introduzione dei *computer crimes,* prima, e dei *cyber crimes,* poi, o all'espressa estensione di fattispecie esistenti alle dinamiche digitali, i tentativi di applicazione dell'impianto normativo esistente in relazione a condotte realizzate nei confronti di strutture tecnologiche o nello spazio digitale si sono rivelati non di rado deludenti e potenzialmente lesivi del principio di stretta legalità[3].

L'acquisita consapevolezza dell'inadeguatezza degli strumenti normativi a disposizione dell'operatore del diritto integrò il primo motore propulsivo verso la progressiva adozione di una nuova disciplina che potesse colmare siffatta lacuna.

Ma, per comprendere meglio i termini della questione, appare opportuno procedere con ordine, muovendo proprio da un accenno alle difficoltà che hanno caratterizzato la "prima fase" di emersione di condotte riconducibili – per le loro proprie modalità di estrinsecazione o per l'oggetto materiale delle stesse – alla nuova realtà virtuale.

Invero, i primi studiosi, soprattutto statunitensi, che, verso la fine degli anni '70, si occuparono dei nascenti fenomeni di criminalità informatica definirono gli stessi come *old wine in new bottles*[4]. La resistenza a cambiamenti strutturali nel sistema penale, in altre parole, si è basata, per un certo periodo di tempo, sull'illusione che ci si trovasse dinanzi a "vino vecchio collocato in otri nuovi"[5].

In siffatta prospettiva, dunque, non vi sarebbe stata la necessità di costruire norme incriminatrici *ad hoc*, dal momento che i comportamenti crimi-

[2] Riflette sulla questione evidenziata, in un momento anteriore all'introduzione dei *computer crimes,* A. Alessandri, *Criminalità informatica,* in *Riv. trim. dir. pen. econ.*, 1990, 652 ss.

[3] N. Bussolati, *L'associazione per delinquere "informatica",* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 250.

[4] Così, I. Salvadori, *Dal* cybercrime all'artificial intelligence crime. *Brevi cenni sui profili penali*, in *Criminalità informatica e intelligenza artificiale. Quaderno della Rivista trimestrale della Scuola di perfezionamento per le Forze di Polizia,* Roma, 2022, 57. Nella letteratura straniera, per tutti, P. N. Grabosky, *Virtual Criminality: Old Wine in New Bottles?,* in *Social & Legal Studies* 2001,10, 243 ss.

[5] J. R. Agustina Sanllehí, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?,* in *Estudios penales y criminológicos*, 2021, vol. 41, 714.

nosi resi possibili o facilitati dall'utilizzo illecito degli strumenti informatici avrebbero potuto essere ricondotti nello spettro applicativo dei reati già contemplati dai legislatori nazionali.

Nondimeno, divenne presto chiaro come la criminalità informatica non si caratterizzasse unicamente per il mezzo impiegato, bensì anche in virtù di connotazioni destinate a coinvolgere pressoché tutti gli elementi del reato, nonché per l'emergere di nuovi interessi meritevoli di protezione, nei confronti dei quali si sarebbero rivelate inadeguate le ipotesi di reato esistenti[6].

Sicché, come metaforicamente ricordato, sarebbe stato meglio riconoscere che il crimine informatico è lo stesso vino, ma in bottiglie diverse, non solo nuove, ma diverse, in cui probabilmente il modo tradizionale di bere non era più valido[7].

2. *Interpretazione estensive e analogiche*

Invero, già prima dell'entrata in vigore della l. n. 547 del 1993[8], la normativa contenuta nel Codice Rocco non presentava particolari problemi di applicabilità, allorché la condotta criminosa avesse avuto ad oggetto lo strumento tecnologico nella sua materialità[9].

In tale prospettiva, per esempio, non ha sollevato particolari criticità l'inquadramento del danneggiamento o del furto di un *computer* nelle fattispecie esistenti, né di analoghi comportamenti che avessero avuto ad

[6] Anche la letteratura straniera si è posta il problema di capire se i "tipi" penali vigenti nei diversi ordinamenti giuridici potessero essere interpretati in forma estensiva o se, al contrario, tale operazione potesse integrare un'analogia *in malam partem.* Sul punto, nell'ordinamento spagnolo, C.M. ROMEO CASABONA, *De los delitos informáticos al cibercrimen. Una aproximación conceptuale y político-criminal,* in *El cibercrimen: nuoevos retos jurídico-penales, nuevas respuestas político-criminales,* a cura di C. M. ROMEO CASABONA, Granada, 2006, 14 ss.

[7] F. MIRÓ LLINARES, *La opotunidad criminal en el ciberspacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen,* in *Revista Electrónica de Ciencia Penal y Criminología*, 13.7.2011, 43.

[8] L. 23 dicembre 1993, n. 547 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica").

[9] Così anche la *Relazione del Disegno di legge n. 2773* ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"), divenuto Legge 23 dicembre 1993, n. 547, consultabile al link *https://www.penale.it/legislaz/rel_ddl_2773_XI_leg.htm*.

oggetto supporti materiali (si pensi ai *floppy disk*) sui quali fossero stati memorizzati dati.

Diverso è, invece, presto apparso il discorso in relazione a condotte criminose poste in essere nei confronti di beni immateriali, quali i *software* o i dati informatici non memorizzati su supporti materiali[10]. Un'applicazione della normativa (allora) vigente in siffatte ipotesi avrebbe, infatti, comportato un'estensione analogica *in malam partem* della stessa.

Per quanto l'orientamento prevalente, anche giurisprudenziale, si fosse espresso in questi termini, non sono tuttavia mancate prese di posizione volte a ritenere applicabili anche in detti casi le fattispecie esistenti, in virtù di un'asserita (mera) interpretazione estensiva delle medesime.

Si pensi, solo a titolo esemplificativo, all'orientamento concernente due nozioni che, non a caso, saranno oggetto di modifica (e aggiornamento "telematico") proprio in forza della l. n. 547 del 1993. Il riferimento va al concetto di "documento" e a quello di "cosa".

Quanto al primo, occorre ricordare l'indirizzo secondo il quale l'archivio informatico di una P.A. avrebbe potuto essere considerato – già prima dell'introduzione dell'art. 491 *bis* c.p. – alla stregua di un registro tenuto da un soggetto pubblico, con la conseguenza che la condotta del pubblico ufficiale che, nell'esercizio delle sue funzioni e facendo uso dei supporti tecnici di pertinenza della P.A., avesse confezionato un falso atto informatico destinato a rimanere nella memoria dell'elaboratore, avrebbe potuto integrare una falsità in atto pubblico, a seconda dei casi, materiale o ideologica, punibile rispettivamente ai sensi degli artt. 476 e 479 c.p. Invero – si legge – «l'art. 491 *bis* c.p. non avrebbe svolto una funzione innovativa, rendendo punibile un fatto che era in precedenza lecito, dal momento che l'art. 476 c.p. era applicabile ai documenti informatici anche prima che ciò fosse stabilito dall'art. 491 *bis* c.p.». In tale prospettiva, in altre parole, non vi sarebbero stati argomenti letterali, logici o sistematici tali da impedire la riconducibilità nella previsione dell'art. 476 c.p. o in quella dell'art. 479 c.p. della

[10] Sul punto v. anche la *Relazione del Disegno di legge n. 2773*, divenuto Legge 23 dicembre 1993, n. 547, cit., ad avviso della quale le condotte di sottrazione di dati, programmi e informazioni apparivano di dubbia riconducibilità all'art. 624 c.p., «pur nell'ampio concetto di "cosa mobile" da esso previsto: stando alla definizione contenuta nel secondo comma di tale disposizione, l'estensione del concetto non va oltre le "energie" (tra cui quella elettrica) aventi valore economico, tra le quali i dati o le informazioni non sono sussumibili». Analogo ragionamento viene svolto in relazione alle fattispecie di danneggiamento.

condotta del pubblico ufficiale che, nell'esercizio delle sue funzioni, avesse formato un atto informatico sostanzialmente o formalmente falso[11].

Quanto, invece, al concetto di "cosa", appare altresì utile ricordare l'orientamento che aveva ritenuto possibile interpretare detto termine, sì da includervi anche i programmi installati in dispositivi informatici. Così, per esempio, ben prima che l'art. 392 fosse modificato in senso tecnologico, la giurisprudenza di merito aveva ritenuto integrato il delitto di *Esercizio arbitrario delle proprie ragioni mediante violenza sulle cose* in capo a colui il quale, in qualità di dipendente di una società elaboratrice di programmi elettronici, ritenendo di esercitare un proprio diritto, avesse sottratto dall'elaboratore di un'azienda parte di uno di tali programmi, precedentemente concesso in uso alla medesima, sempre che l'attività dell'agente avesse determinato una modificazione tale del programma stesso, da renderlo inutilizzabile secondo la sua normale destinazione[12].

Ma analoghi problemi di adattamento alle nuove forme di manifestazione digitale delle condotte avevano coinvolto anche altre ipotesi di reato. Si pensi, solo a titolo esemplificativo, alla fattispecie di danneggiamento, nella misura in cui sono state ricondotte alla stessa le ipotesi di cancellazione o alterazione del *sofware*[13], e alla fattispecie di truffa, nei casi in cui la condotta artificiosa veniva rivolta nei confronti di un *computer*[14].

Le complessità del quadro interpretativo, già evidenti in relazione a casi relativamente semplici quali quelli esemplificati, si sono progressivamente moltiplicate a fronte di nuove dinamiche criminose idonee a realizzare per via telematica inedite forme di aggressione nei confronti di beni giuridici tradizionali o di nuovi interessi emergenti, in un contesto di progressiva disintegrazione dei confini tra reale e virtuale.

Da siffatta presa d'atto sono dunque scaturite le prime iniziative normative specificamente volte ad attribuire rilievo alla dimensione digitale del reato[15].

[11] Così, Cass. pen., sez. V, 27 gennaio 2005, n. 11930, Rv. 231706; nello stesso senso, Cass. pen., sez. V, 24 novembre 2003, n. 11915, Rv. 228741.

[12] Così, Tribunale di Torino, 12 dicembre 1983, in *Giur. mer.*, 1984, 1173 ss.

[13] Su siffatta casistica Tribunale di Torino 23 ottobre 1989, in *deJure.*

[14] Tra le altre, Tribunale di Roma, 14 dicembre 1985, in *deJure.*

[15] *Amplius* e per tutti, C. PECORELLA, *Reati informatici,* in *Enc. Dir., Annali,* X, Milano, 2017, 707 ss.

3. *Le nuove fattispecie informatiche*

L'attuale quadro normativo in materia di criminalità informatica è il frutto di molteplici interventi legislativi, peraltro fortemente condizionati da indicazioni di fonti internazionali e sovranazionali[16], che risulterebbe impossibile esaminare in modo esaustivo in questa sede.

Ci si limita a ricordare come, sulla spinta della Raccomandazioni del Consiglio d'Europa del 9 settembre 1989, n. R (89)–9[17], il legislatore italiano, abbia approvato – come primo intervento organico – la già citata legge 23 dicembre 1993, n. 547 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica")[18].

La Raccomandazione intendeva, in particolare, promuovere una strategia condivisa contro le nuove fenomenologie criminose, suggerendo agli Stati membri criteri comuni secondo cui orientare le scelte di tutela penale in materia ed offrendo un'elencazione delle condotte rilevanti per l'integrazione dei reati informatici.

In tale prospettiva, con la l. n. 547 del 1993 sono state, da un lato, introdotte all'interno del codice nuove fattispecie delittuose (gli artt. 615 *ter*, 615 *quater,* 615 *quinquies*, 617 *quater*, 617 *quinquies* e 617 *sexies*, 635 *bis*, 640 *ter*, 623 *ter*) e, dall'altro lato, modificate previsioni esistenti con esplicito riguardo ai beni informatici. Il riferimento è agli artt. 392, 420, 491 bis, 616, 621.

Innanzitutto, dunque, con il citato primo intervento organico il legisla-

[16] Per una più specifica ricostruzione degli interventi normativi, nonché della loro matrice a livello internazionale e sovranazionale, si rinvia a R. FLOR, Cyber-criminality*: le fonti internazionali ed europee*, in *Trattati giuridici.* Cybercrime*,* diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, Milano, 2019, 97 ss.

[17] In argomento, G. TADDEI ELMI, R. ORTU, P. CIFALDI, *La Raccomandazione del Consiglio d'Europa del 9 settembre 1989 n. R (89)-9 e la Legge 23 dicembre 1993 n. 547 in materia di* computer crimes*: una analisi comparativa,* in *Informatica e diritto,* 1996, n. 1, in particolare 121 ss. Per un esame critico dei contenuti della Raccomandazione, C. LARINNI, *Garantismo europeista: un ossimoro? A proposito dell'accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)*, in *Criminalia* 2019*,* 301 ss.

[18] In argomento, per tutti, L. PICOTTI, *Reati informatici*, in *Enc. giur. Treccani*, XXIX, Roma, 1993, 1 ss.; F. MUCCIARELLI, *Commento alla legge 23 dicembre 1993, n. 547. Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica,* in *Leg. pen.,* 1996, 57 ss.

tore italiano ha attribuito rilievo ad un certo numero di condotte idonee ad integrare i c.d. reati informatici in senso stretto, vale a dire quelli non concepibili a prescindere dall'esistenza di un sistema digitale.

Si tratta di illeciti all'interno della cui descrizione è sempre presente almeno un elemento che richiama espressamente le tecnologie informatiche: si pensi, a titolo esemplificativo, alla condotta dell'introdursi o mantenersi in un sistema informatico o telematico o a quella della contraffazione, alterazione o soppressione di un documento informatico.

Nondimeno, la scelta normativa non è stata nel senso di creare una sezione a parte dedicata ai nuovi *computer crimes*, probabilmente anche in considerazione della circostanza che i delitti in questione tendono a ledere beni giuridici di diversa natura. Le neonate incriminazioni sono state, dunque, topograficamente collocate all'interno di diversi titoli del Libro secondo del Codice penale, sulla base della "somiglianza" dell'interesse di volta in volta protetto rispetto a quelli già oggetto di considerazione.

Sicché, il legislatore si è sostanzialmente limitato a ridefinire e/o aggiungere elementi rispetto a quelli tipizzati da fattispecie già esistenti, secondo un criterio di analogia, intendendo l'ambiente informatico come la mera riproduzione smaterializzata della vita reale.

Così facendo, tuttavia, almeno per un certo periodo di tempo, si è perpetuata l'idea che, in fondo, l'esigenza di tutela che si andava affermando potesse essere soddisfatta per il tramite di semplici meccanismi di estensione della disciplina vigente, giacché «le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice»[19].

La tecnica di costruzione dei nuovi illeciti presentò, dunque, come comu-

[19] Così la *Relazione del Disegno di legge n. 2773*, divenuto Legge 23 dicembre 1993, n. 547, cit., la quale, più nei dettagli precisa che la soluzione adottata è parsa preferibile «nella convinzione che la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo; d'altra parte, il criterio seguito dal legislatore del 1930 nel prevedere i vari raggruppamenti di reati è ispirato all'unità dell'oggetto giuridico, inteso quanto meno come unico interesse di categoria, mentre le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice». La Relazione è disponibile al link: http://legislature.camera.it/_dati/leg11/lavori/stampati/pdf/50216.pdf.

ne denominatore l'idea che fosse possibile non discostarsi eccessivamente dal paradigma di reati esistenti considerati "vicini" alle nuove fenomenologie criminose.

In diversi casi, peraltro, il rapporto di simmetria non coinvolge esclusivamente il bene giuridico protetto, ma altresì la struttura della fattispecie. Il riferimento è, per esempio, alla tutela del domicilio informatico. Infatti, non solo i sistemi informatici o telematici sono stati considerati come «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14 della Costituzione»[20], ma anche la struttura della relativa fattispecie è stata delineata sulla falsariga di quella già prevista dall'art. 614 c.p.

La l. n. 547 del 1993, come già anticipato, oltre ad avere introdotto ipotesi di reato fino a quel momento inedite, è altresì intervenuta su alcune nozioni allo scopo di rivederle ed aggiornarle in chiave digitale.

Nell'ambito di siffatta seconda tipologia di intervento, è stato aggiunto all'art. 392 c.p. un nuovo (ultimo) comma ai sensi del quale, agli effetti della legge penale, «si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico».

In tal modo, si è, dunque, effettuata l'espressa (necessaria) equiparazione – ai fini indicati – tra le "cose", da un lato, ed entità (i programmi informatici), prive, invero, di una materialità riconducibile ai canoni tradizionali, dall'altro lato.

Come chiaramente precisato nella citata *Relazione al disegno di legge n. 2773*, la *ratio* di una siffatta integrazione, che incide sulla fattispecie di esercizio arbitrario delle proprie ragioni commesso mediante violenza sulle cose, risiede «nella necessità di non lasciare privi di sanzione comportamenti di sicuro rilievo delittuoso e che appaiono assimilabili alle ipotesi di danneggiamento o di mutamento di destinazione. Si tratta, ad esempio, della "mutilazione" o del rendere, anche parzialmente, inservibili programmi informatici in ordine ai quali l'agente vanti pretesi diritti, ancorché si trovino nella disponibilità altrui, ovvero dell'impedire o dell'alterare il funzionamento di sistemi informatici o telematici, azioni realizzate con l'intento di esercitare diritti che potrebbero essere fatti valere innanzi al giudice, e per i quali si ricorra, invece, ad una sorta di autotutela, e cioè a quel "farsi ragione da

[20] *Relazione del Disegno di legge n. 2773*, cit., p. 9.

sé medesimo" che la norma contenuta nell'art. 392 c.p. mira appunto a reprimere. L'inserimento della disposizione che si propone *appare connesso alla già sottolineata difficoltà dell'assimilazione dei programmi informatici alle "cose mobili"*, ond'è che, nonostante qualche tentativo avutosi al riguardo in giurisprudenza, certamente resta assai problematico il sussumere le manifestazioni del particolare fenomeno cui si e fatto cenno nella previsione di reato contenuta nell'art. 392 c.p.»[21].

L'art. 491 *bis* c.p., intitolato "Documenti informatici", è stato invece introdotto dalla l. n. 547 del 1993 (e successivamente modificato dalla l. n. 48 del 2008 e dal d.lgs. n. 7 del 2016) allo scopo di colmare un possibile vuoto di tutela rispetto alle ipotesi di falsificazioni documentali realizzate, appunto, su documenti informatici.

In tale prospettiva, il legislatore ha ritenuto di poter (dover) estendere a questi ultimi le disposizioni dettate per le falsità in atti, giudicando possibile la loro equiparazione ai documenti tradizionali, così come del resto esplicitamente stabilito dalla disposizione di cui all'art. 621, comma 2, c.p.[22].

Nondimeno, la giurisprudenza si è da subito orientata – come già anticipato – nel senso di ritenere che l'art. 491 *bis* c.p. non avesse, in realtà, fatto altro che confermare un'interpretazione già desumibile dalle disposizioni codicistiche in tema di falso documentale[23]. Non si sarebbe trattato, dunque, di norma innovativa, bensì solo interpretativa, volta a chiarire, «peraltro *ad abundantiam*, che le fattispecie di falso (in atti pubblici o in scritture private) sono ravvisabili anche quando la falsificazione sia avvenuta tramite (o sia stata consumata su) supporto informatico»[24]. Sicché, la sua funzione non sarebbe quella di autonoma nuova incriminazione, bensì solo quella di legittimare un'interpretazione estensiva, che sarebbe già stata resa possibile dagli artt. 476 e 479 c.p. Ne sarebbe, dunque, derivata la punibilità dei fatti di falso informatico anche se commessi prima dell'introduzione dell'art. 491 *bis* c.p.

Sennonché, come osservato da attenta dottrina, siffatta lettura deve essere

[21] *Relazione del Disegno di legge n. 2773*, cit., p. 8 (corsivo aggiunto).

[22] In argomento *amplius,* I. SCORDAMAGLIA, *La falsità in documento informatico,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. PARODI, V. SELLAROLI, Milano, 2020, 323 ss.

[23] Così Cass. pen., sez. V, 27 gennaio 2005, n. 11930, Rv. 231706; nello stesso senso, Cass. pen., sez. V, 24 novembre 2003, n. 11915, Rv. 228741. Cass. pen., sez. V, 18 giugno 2001, n. 32812, Rv. 219945.

[24] Cass. pen., sez. V, 18 giugno 2001, n. 32812, Rv. 219945.

sottoposta ad accurato vaglio critico poiché, se fosse vero che l'art. 491 *bis* c.p. si è limitato ad esplicitare quanto in precedenza già scritto nel codice, si verrebbe a negare la ragion d'essere dell'intervento legislativo[25]. Senza dimenticare che lo stesso legislatore aveva affermato che la l. n. 547 del 1993 doveva avere la funzione di estendere la tutela ordinamentale contro le falsificazioni dei "documenti informatici", a conferma che prima della novella le aggressioni di tal fatta dovevano ritenersi prive di tutela penale.

A questo si aggiunga che la nozione di documento informatico non è completamente sovrapponibile a quella tradizionale di documento, presentando rispetto a questa diversi elementi di novità[26]. Con la conseguenza che l'art. 491 *bis* parrebbe svolgere un'autentica funzione di nuova incriminazione, volta ad attribuire carattere di illiceità a fatti che, prima della sua introduzione, ne erano privi.

Anche la modifica dell'art. 420 c.p., concretizzatasi nella previsione di due nuovi commi, si era resa necessaria al fine di estendere la tutela penale apprestata dalla fattispecie di *Attentato a impianti di pubblica utilità* anche ai sistemi informatici o telematici, nonché ai dati, alle informazioni o ai programmi in essi contenuti (così espressamente la *Relazione del Disegno di legge n. 2773*, cit.). Siffatta previsione è stata poi successivamente abrogata dalla l. n. 48 del 2008, con la quale è stata data attuazione alla Convenzione di Budapest.

Ulteriori interventi di aggiornamento tecnologico posti in essere dalla l. n. 547 del 1993 hanno, inoltre, coinvolto rispettivamente l'art. 616, comma 4, c.p., con l'estensione della nozione di corrispondenza anche alle comunicazioni informatiche o telematiche, ovvero effettuate con ogni altra forma di trasmissione a distanza, nonché l'art. 621 c.p., al quale è stato aggiunto un comma (il secondo) volto ad estendere la tutela in tema di segreti, precisando che «agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi».

[25] Così M. GROTTO, *Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell'art. 491 bis c.p.,* in *Diritto dell'informazione e dell'informatica,* 2006, 592.

[26] Ancora, per articolate considerazioni sul punto, M. GROTTO, *Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell'art. 491 bis c.p.,* cit., 592 ss.

4. *Dai* computer crimes *ai* cyber crimes

Nel momento in cui il legislatore adottò la sopra citata l. n. 547 del 1993 *Internet* ancora non esisteva, ma avrebbe fatto ingresso di lì a poco, evidenziando presto una sopravvenuta inadeguatezza delle neonate previsioni penalistiche.

Del pari, e per converso, l'evoluzione dello spazio cibernetico e la conseguente possibilità di accedervi con estrema facilità da parte di chiunque hanno funto da straordinario volano rispetto alla emersione di nuove fenomenologie criminose, connotate da una maggiore pervasività e, quindi, da un aumentato disvalore penale rispetto ai cosiddetti reati informatici o *computer crimes* in senso stretto[27].

Ben presto, dunque, divenne chiaro che non si trattava più di fronteggiare solo le condotte illecite che avessero coinvolto il singolo dispositivo o il singolo supporto, ma aggressioni di ben più ampia portata, nei confronti dei più disparati interessi tutelati, all'interno della rete globale.

Come già anticipato[28], il reato informatico (in senso stretto) o *computer crime* si identifica con fattispecie costruite, sul piano della formulazione, con elementi di tipizzazione connessi a procedimenti di automatizzazione di dati o informazioni, ovvero legati a modalità, oggetti o attività di carattere tecnologico, senza i quali non sarebbero neppure concepibili.

Con l'avvento di *Internet* emerge, invece, un nuovo tipo di legame tra informatica e criminalità, nel senso che diviene chiaro come nel *cyberspace* anche fattispecie incriminatrici che non presentano espressamente elementi tipici di carattere informatico possono però assumere tratti fisionomici peculiari allorché commesse tramite la tecnologia o la rete[29].

In siffatta diversa prospettiva, dunque, la categoria è "aperta" e ha assunto un'importanza ed un'estensione via via crescenti, di pari passo con l'evolversi e l'espandersi del *cyberspace* e delle sue potenzialità[30].

[27] Sul processo di evoluzione dei reati connessi all'utilizzo delle nuove tecnologie, nella letteratura straniera: C.M. ROMEO CASABONA, *De los delitos informáticos al cibercrimen. Una aproximación conceptuale y político-criminal,* in *El cibercrimen: nuoevos retos jurídico-penales, nuevas respuestas político-criminales,* a cura di C. M. ROMEO CASABONA, Granada, 2006, 1 ss.

[28] V. *supra* capitolo primo.

[29] *Amplius* e per tutti, S. SEMINARA, *Internet (diritto penale)*, in *Enciclopedia del Diritto, Annali*, VII, Milano, 2014, 567 ss.

[30] L. PICOTTI, Cybercrime *e diritto penale,* in *Diritto penale dell'informatica. Reati della*

Come è facile intuire, infatti, può trattarsi di comportamenti che offendono i più diversi beni giuridici (anche già in precedenza tutelati ma) che divengono, di regola, particolarmente temibili se commessi nella dimensione digitale. Senza trascurare che in non pochi casi proprio la peculiare invasività delle modalità tecnologiche può evidenziare la necessità di tutelare nuovi interessi, frutto, appunto, essi stessi dello sviluppo informatico.

Dunque, all'interno della categoria dei *computer crimes* in senso ampio (o *cyber crimes*) si possono ora ricomprendere sia reati "necessariamente informatici" sia illeciti solo "eventualmente informatici", rispetto ai quali l'utilizzazione delle summenzionate tecnologie informatiche ha solo ampliato l'ambito delle possibili forme di realizzazione[31].

Peraltro, la caratteristica di "non luogo" dello spazio digitale[32], unitamente alla sterminata capacità diffusiva delle nuove tecnologie hanno evidenziato vieppiù la tendenziale natura transnazionale degli illeciti cibernetici. Siffatta consapevolezza ha, dunque, indotto il Consiglio d'Europa a predisporre una Convenzione sul *Cybercrime* (la c.d. Convenzione di Budapest del 23 novembre 2001)[33].

Si tratta del primo accordo internazionale riguardante i reati commessi tramite *Internet* o altre reti informatiche. La *ratio* che animò il legislatore della Convenzione fu da ravvisare nell'esigenza di promuovere l'adozione, da parte

rete e sulla rete, a cura di C. Parodi, V. Sellaroli, Milano, 2020, 714.

[31] Per un esame degli elementi che, sotto il profilo oggettivo e soggettivo, connotano i *cybercrimes,* cfr. P. M. Sabella, *Il fenomeno dei cybercrimes nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali,* in *Informatica e diritto,* 2017, 148, ad avviso del quale: «Il *cybercrime* può essere definito come un comportamento delittuoso posto in essere mediante l'uso distorto o abusivo dei sistemi *hardware* e *software*, comprendenti genericamente l'accesso illegale, la manipolazione e l'intercettazione di dati, l'interferenza con il corretto funzionamento di strumenti informatici e l'uso improprio di dispositivi, contraddistinto tendenzialmente dalla coesistenza di alcuni elementi quali: a) l'anonimato del soggetto attivo o la sua difficoltosa reperibilità; b) l'automatizzazione parziale o totale della condotta; c) la significativa intensità del momento volitivo del dolo; d) l'indebolimento delle coordinate spazio-temporali per una corretta identificazione del *tempus* e del *locus commissi delicti*».

[32] Su cui v. *infra* capitolo terzo, paragrafo 10.

[33] Sul tema *amplius,* L. Picotti*, La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale, in Dir. pen. proc.,* 2008, 700 ss.; C. Sarzana di Sant'Ippolito, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa, in Dir. pen. proc.,* 2008, 1562 ss.*;* R. Flor, Cyber-criminality*: le fonti internazionali ed europee,* in *Trattati giuridici.* Cybercrime*,* cit., 97 ss.

degli Stati membri, di sistemi di tutela appositamente dedicati ai nuovi reati del *cyberspace* che assicurassero una disciplina tendenzialmente uniforme all'interno degli ordinamenti nazionali aderenti[34]. Tale obiettivo apparve di fondamentale importanza anche per assicurare il requisito della doppia incriminazione, presupposto di molte forme di cooperazione internazionale, più che mai necessarie in relazione a forme di estrinsecazione del reato di regola destinate a non essere relegate all'interno dei confini nazionali.

La citata Convenzione è stata ratificata dall'Italia con la legge 18 marzo 2008, n. 48[35], con la quale, tra le altre cose e per quanto qui più direttamente interessa, sono stati inseriti nel codice penale gli artt. 495 *bis*, 635 *ter*, *quater* e *quinquies*, 640 *quinquies* ed è stata, altresì, prevista la responsabilità degli enti per un'ampia serie di reati informatici[36].

Interventi legislativi successivi hanno poi, a più riprese e a macchia di leopardo, introdotto altre modifiche al codice penale, prevedendo, ad esempio, nuove e inedite forme di violazione della riservatezza sessuale compiute attraverso lo strumento informatico (si pensi alla fattispecie di *Diffusione illecita di immagini o video sessualmente espliciti,* di cui all'art. 612 *ter*[37]) o semplici circostanze aggravanti in relazione fenomeni criminosi già noti e tipizzati (il riferimento è, per esempio, all'aggravante per i delitti di atti persecutori e di addestramento ad attività con finalità di terrorismo anche internazionale, di istigazione a delinquere, quando i fatti siano commessi attraverso strumenti informatici o telematici[38]).

Venendo a tempi più recenti, l'innestarsi, nella realizzazione dei com-

[34] In argomento, E. ALBAMONTE, *Il reato informatico nella prassi giudiziaria: le linee giuda internazionali per il contrasto ai nuovi fenomeni criminali*, in *Rivista Elettronica di Diritto, Economia, Management*, 2013, n. 3, 146 ss., il quale, tra l'altro, analizza in modo dettagliato le prassi criminose di maggior rilievo in tema di reati informatici.

[35] L. 18 marzo 2008, n. 48 ("Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno").

[36] In argomento G. MINICUCCI, *Reati informatici e responsabilità degli enti: vecchi e nuovi scenari,* in *disCrimen,* 24.9.2022.

[37] *Amplius* e per tutti, N. AMORE, *La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p.*, in *www.lalegislazionepenale.eu*, 20.1.2020; C. PAONESSA, *Ai confini del c.d.* Revenge porn. *Tessere di un mosaico normativo*, in *Criminalia* 2021, 283 ss.; D. MICHELETTI, *L'*interversio pubblicationis *quale elemento costitutivo della fattispecie di* revenge porn, in *disCrimen,* 7.1.2022, 1 ss.

[38] Novità, queste, introdotte, rispettivamente, dal d. l. n. 93 del 2013 e dal d. l. n. 5 del 2017.

portamenti nello spazio digitale, di componenti espressione della c.d. intelligenza artificiale ha di nuovo acceso i riflettori sull'esigenza di adeguare l'assetto normativo anche a siffatto emergente fenomeno. Sicché, ad oggi, l'ultima tappa di questo complesso iter evolutivo è stata rappresentata dalla legge 23 settembre 2025, n. 132, che ha introdotto previsioni volte appunto ad attribuire rilievo all'utilizzo dell'intelligenza artificiale nella realizzazione di comportamenti illeciti[39].

In tale prospettiva si segnala, in particolare, la nuova fattispecie di cui all'art. 612 *quater* (*Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*)[40], oltre che diverse circostanze aggravanti idonee a ricollegare incrementi sanzionatori all'utilizzo dell'IA.

Si pensi, per rimanere alla disciplina codicistica, all'art. 61, n. 11 *undecies,* e all'art. 294, comma 2, c.p.

Il primo ha introdotto nella parte generale del codice penale una circostanza aggravante comune che ricollega l'incremento sanzionatorio al fatto di avere commesso il reato «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».

Il secondo ha, invece, previsto per la fattispecie di *Attentati contro i diritti politici dei cittadini,* un inasprimento di pena allorché la condotta di inganno, contemplata nel primo comma tra le possibili forme di realizzazione del reato, sia posta in essere mediante l'impiego di strumenti di intelligenza artificiale.

La sintetica e rapsodica rassegna di alcuni degli ultimi interventi normativi consente di ricavare un importante dato metodologico, rappresentato dalla condivisibile progressiva transizione verso un modello "autonomista" del reato cibernetico, non più appiattito sul "gemello analogico" ma costru-

[39] In argomento L. SCOLLO, *L'intelligenza artificiale entra nel Codice penale*, in *Dir. pen. e proc.*, 2025, 693 ss.

[40] Sul fenomeno, prima dell'introduzione della fattispecie incriminatrice, C. PAONESSA, *La diffusione di contenuti illeciti* online. *Obblighi di incriminazione e contrasto del "*deepfake" *nella direttiva (UE) 2024/1385,* in *Criminalia* 2024, 229 ss. Sulla nuova fattispecie, B. FRAGASSO, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura*, in *www.sistemapenale.it,* n. 10, 2025, in particolare 162 ss.; L. SCOTTI, *Deepfake sessuale e legalità penale: il costo costituzionale della tipizzazione dell'offesa artificiale*, in *Questione Giustizia*, 16 giugno 2026.

ito sul peculiare modo di essere della criminalità *online*[41]. In altre parole, si coglie lo sforzo da parte del legislatore di costruire tipologie di offesa non derivate da quelle omologhe delle realtà analogica.

Nondimeno, per quanto i citati interventi normativi abbiano integrato importanti tasselli nell'opera di adeguamento del sistema penale alle sfide poste dal progresso tecnologico e dall'avvento dei sistemi di intelligenza artificiale, in realtà le questioni interpretative che a tutt'oggi solleva la disciplina vigente nell'attribuire rilievo a comportamenti che possono coinvolgere lo spazio digitale sono molteplici, come ben dimostra anche la prassi applicativa.

Infatti, nonostante lo sforzo posto in essere dal legislatore nel tentativo di fotografare normativamente la nuova realtà, indirizzi "estensivi" sono stati adottati anche di recente, a fronte di risultati applicativi giudicati inappaganti – se non addirittura contrari al più comune senso di giustizia – dinanzi alla complessità e al continuo evolversi della vita reale[42].

Ci si limiterà in questa sede a riportare alcune esemplificazioni che rappresentano, però, emblematicamente quanto possano essere differenti gli esiti interpretativi a seconda che si faccia prevalere un approccio attento più alle esigenze di tutela che ai principi e, al contempo, quanto possa essere labile il confine tra asserite interpretazioni estensive delle norme e veri e propri casi di analogia *in malam partem*[43].

5. *Il* file *informatico come "cosa mobile"*

Una questione tutt'oggi controversa attiene, per esempio, alla possibilità di qualificare i dati informatici come cose mobili ai sensi delle disposizioni

[41] In questo senso G. MORGANTE, *Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del* law enforcement, in *Riv. it. informatica e diritto,* 2025, 103 ss.

[42] Su siffatta problematica, in termini generali, G. MARTIELLO, «*Vincolo testuale» ed interpretazione nel diritto penale: la necessità di una riconciliazione,* in *Criminalia* 2022, 417 ss.

[43] In argomento, in termini generale, F. GIUNTA, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla giurisprudenza,* in *Criminalia* 2010, 347 ss.; M. DONINI, *Il diritto giurisprudenziale penale. Collisioni vere e apparenti con la legalità e sanzioni dell'illecito interpretativo,* in *www.penalecontemporaneo.it,* n. 3, 2016, 13 ss.; D. MICHELETTI, Jus contra lex. *Un campionario dell'incontenibile avversione del giudice penale per la legalità,* in *Criminalia* 2016, 161 ss.

della legge penale e, in particolare, di poterli valutare quali oggetto materiale dei reati contro il patrimonio[44].

La giurisprudenza più risalente, infatti, sembrava concorde nell'escludere che i *files* potessero formare oggetto del reato di cui all'art. 624 c. p., osservando che la semplice copiatura non autorizzata di dati contenuti in un supporto informatico altrui non comporta la perdita del possesso della *res* da parte del legittimo detentore. Una tale interpretazione avrebbe trovato conferma – si legge e vale la pena ricordarlo – «nella esplicita volontà del Legislatore che nella Relazione al disegno di legge n. 2733 (con il quale si è introdotta nel codice penale una disciplina di contrasto della criminalità informatica) ha espressamente precisato che la condotta di sottrazione di dati, programmi, informazioni di tal genere non è riconducibile alla norma incriminatrice sul furto, in quanto i dati e le informazioni non sono comprese nel concetto, pur ampio, di "cosa mobile" in essa previsto; ed ha ritenuto altresì "non necessaria la creazione di una nuova ipotesi di reato osservando che la sottrazione di dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto), altro non è che una "presa di conoscenza" di notizie, ossia un fatto intellettivo rientrante, se del caso, nelle previsioni concernenti la violazione dei segreti. Ciò, ovviamente, a parte la punibilità ad altro titolo delle condotte strumentali, quali ad esempio, quelle di violazione di domicilio (art. 614 c.p.)»[45].

Nondimeno, la prassi applicativa più recente ha cercato, invece, di "aggiornare" al progressivo sviluppo tecnologico la nozione di cosa mobile. Sicché, in diverse occasioni la giurisprudenza ha ritenuto che il dato informatico possa, invero, essere oggetto di delitti contro il patrimonio, considerandolo cosa in senso fisico.

Dapprima, le sezioni unite della Cassazione hanno riconosciuto, in ter-

[44] In argomento, *amplius,* L. SCOPINARO, Internet *e reati contro il patrimonio,* Torino, 2007, in particolare 103 ss.

[45] Cass. pen., sez. IV, 26 ottobre 2010. n. 44840, Rv. 249067. Precedentemente, nello stesso senso, Cass. pen., sez. IV, 13 novembre 2003, n. 3449, Rv. 229785. Per un'applicazione della fattispecie di accesso abusivo a sistema informatico nell'ipotesi di duplicazione delle procedure informatiche facenti parte del patrimonio aziendale, da parte del programmatore di una società di elaborazione dati, in concorso con uno dei soci originari, che aveva deciso di intraprendere un'analoga attività per conto proprio, Cass. pen., sez. V, 7 novembre 2000, n. 12732, Rv. 21774, con nota di L. CUOMO, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico,* in *Cass. pen.,* 2002, 1018 ss.

mini generali, che i dati informatici possano essere passibili di sequestro preventivo, equiparandoli alle cose, pur riconoscendo in essi entità non suscettibili «di apprensione, possesso e custodia (*id quod tangi potest*), trattandosi di un prodotto del pensiero umano che circola liberamente nella rete telematica in forma dematerializzata»[46].

Successivamente, si è registrata una ancora più netta presa di posizione della giurisprudenza di legittimità[47]. La vicenda dalla quale aveva preso origine il processo, che ha poi condotto alla pronuncia della Cassazione, riguardava le condotte poste in essere da un soggetto, già dipendente di una società, il quale, dopo essersi dimesso, veniva assunto da una nuova compagine societaria, di recente costituzione, operante nello stesso settore. Sennonché, prima di presentare le dimissioni, il dipendente aveva restituito il *notebook* aziendale, a lui affidato nel corso del rapporto di lavoro, con l'*hard dis*k formattato, senza traccia dei dati informatici originariamente presenti, che in parte venivano ritrovati nella disponibilità dell'imputato su altri *computer* da lui utilizzati. Per siffatta condotta l'ex dipendente veniva ritenuto responsabili per il reato di appropriazione indebita di cui all'art. 646 c.p.

Tanto premesso, la questione che la Corte si è trovata ad affrontare concerneva appunto la possibilità di qualificare i dati informatici, in particolare singoli *file*, come cose mobili, ai sensi delle disposizioni della legge penale e, specificamente, in relazione alla possibilità di costituire oggetto di condotte di appropriazione indebita. «La Corte non ignora – si legge nella pronuncia – l'esistenza di ragioni di ordine testuale, sistematico e di rispetto dei principi fondamentali di stretta legalità e tassatività delle norme incriminatrici, che potrebbero contrastare la possibilità di qualificare i *files* come beni suscettibili di rappresentare l'oggetto materiale dei reati contro il patrimonio. Occorre, però, approfondire la valutazione considerando la struttura del *file*, inteso quale insieme di dati numerici tra loro collegati che non solo nella rappresentazione (grafica, visiva, sonora) assumono carattere, evidentemente, materiale; va, altresì, presa in esame la trasferibilità dei *files* tra dispositivi che li contengono, oltre che nell'ambiente informatico

[46] Cass. pen., sez. un., 20 gennaio 2015, n. 31022, Rv. 264089, punto n. 4 del Considerato in diritto. Sulla pronuncia *de qua* L. PAOLONI, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa:* ubi commoda, ibi et incommoda*?,* in *Cass. pen.,* 2015, 3437 ss.

[47] Cass. pen., sez. II, 7 novembre 2019, n. 11959, Rv. 278571.

rappresentato dalla rete *Internet*; allo stesso tempo, occorre interpretare talune categorie giuridiche che, coniate in epoche in cui erano del tutto sconosciute le attuali tecnologie informatiche, devono necessariamente esser nuovamente considerate, al fine di render effettiva la tutela cui mirano le disposizioni incriminatrici dei delitti contro il patrimonio»[48].

Sicché – si prosegue – l'assunto da cui muove l'orientamento maggioritario, giurisprudenziale e della dottrina, nel ritenere che il dato informatico non possieda i caratteri della fisicità, propri della "cosa mobile" (nella nozione penalistica di quel termine) non sarebbe condivisibile[49]. Piuttosto, assumerebbe rilievo decisivo «la capacità del *file* di essere trasferito da un supporto informatico ad un altro, mantenendo le proprie caratteristiche strutturali, così come la possibilità che lo stesso dato viaggi attraverso la rete *Internet* per essere inviato da un sistema o dispositivo ad un altro sistema, a distanze rilevanti, oppure per essere "custodito" in ambienti "virtuali" (corrispondenti a luoghi fisici in cui gli elaboratori conservano e trattano i dati informatici); caratteristiche che confermano il presupposto logico della possibilità del dato informatico di formare oggetto di condotte di sottrazione e appropriazione»[50]. Conclusivamente, «indiscusso il valore patrimoniale che il dato informatico possiede, in ragione delle facoltà di utilizzazione e del contenuto specifico del singolo dato, la limitazione che deriverebbe dal difetto del requisito della "fisicità" della detenzione non costituisce elemento in grado di ostacolare la riconducibilità del dato informatico alla categoria della cosa mobile[51]».

Sennonché, le argomentazioni attraverso le quali si perviene a siffatta con-

[48] Cass. pen., sez. II, 7 novembre 2019, n. 11959, Rv. 278571, punto n. 1.4 del Considerato in diritto. Sulla pronuncia *de qua,* N. PISANI, *La nozione di "cosa mobile" agli effetti penali e i* files *informatici: il significato letterale come argine all'applicazione analogica,* in *Dir. pen. proc.,* 2020, 651 ss.; A. SCARCELLA, *Dato informatico, nozione penale di cosa mobile ed appropriazione indebita,* in *Cass. pen.,* 2021, 556 ss.; C. PAGELLA, *La Cassazione sulla riconducibilità dei file al concetto di "cosa mobile" oggetto di appropriazione indebita: un caso di analogia* in malam partem*?,* in *www.sistemapenale.it,* 4 marzo 2021; M. CARANI, *L'appropriazione indebita dei dati informatici: perché i* files *si possono considerare cose mobili,* in *Cass. pen*., 2020, 4159 ss.; L. BARILE, *Appropriazione indebita di* file *informatici: tra interpretazione estensiva e divieto di analogia, Il diritto penale è 'cosa mobile'*, in *www.sistemapenale.it*, n. 3 del 19 marzo 2021. Sulla questione in oggetto (e su altre analoghe ipotesi di analogia), in termini generali, G. MARINUCCI, E. DOLCINI, G. L. GATTA, *Manuale di diritto penale, Parte generale*, Milano, 2024, 92, 93.

[49] Cass. pen., sez. II, 7 novembre 2019, n. 11959, Rv. 278571, punto n. 1.5.3.

[50] Cass. pen., sez. II, 7 novembre 2019, n. 11959, Rv. 278571, punto n. 1.7.

[51] Cass. pen., sez. II, 7 novembre 2019, n. 11959, Rv. 278571, punto n. 1.8.3.

clusione non appaiono esenti da profili problematici e tutt'altro che fondato appare il dubbio che la giurisprudenza abbia forzato la nozione penalistica di cosa e violato gli stretti limiti della legalità penale.

La sentenza in commento, ad avviso di parte della dottrina, avrebbe realizzato una vera e propri «creazione giurisprudenziale di una inedita nozione di "cosa mobile"»[52]. Ma il senso linguistico dell'espressione sembra, invece, opporre una resistenza insuperabile alla riconducibilità del *file* informatico alla relativa nozione[53].

Certo, non si può disconoscere che le condotte di aggressione unilaterale al bene *file* informatico, al pari di quelle che colpiscono qualsiasi altra "cosa mobile" in senso stretto, potrebbero essere portatrici di un disvalore, sostanzialmente equivalente[54]. Nondimeno, dette condotte presentano una dubbia riconducibilità allo schema dei delitti di furto e appropriazione indebita. Sicché, appare evidentissimo lo scivolamento nel procedimento analogico[55], il quale, se assecondato, potrebbe condurre agli esiti più disparati, difficilmente prevedibili dal destinatario delle norme.

Peraltro, proprio la circostanza che il legislatore abbia limitato l'estensione del concetto di cosa ai dati informatici solo in relazione a determinate fattispecie ed istituti dimostrerebbe l'impossibilità di pervenire ad un'equiparazione generalizzata[56]. Circostanza, questa, idonea a rafforzare la convinzione che il problema della tutela dei beni informatici non possa «essere risolto attraverso disinvolte operazioni interpretative, tese a forzare i limiti delle tradizionali fattispecie dei reati contro il patrimonio»[57].

[52] N. Pisani, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali,* cit., 652.

[53] G. Fiandaca, E. Musco., *Diritto penale. Parte speciale. I delitti contro il patrimonio*, vol. II, tomo secondo, Torino, 2023, 29. Analogamente, F. Mantovani, G. Flora, *Diritto penale. Parte speciale, II, Delitti contro il patrimonio,* Milano, 2024, 25.

[54] Così anche N. Pisani, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali,* cit., 653.

[55] N. Pisani, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, cit., 654. Nello stesso senso, L. Barile, *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia, Il diritto penale è 'cosa mobile'*, cit., 149.

[56] Il riferimento è all'art. 254 *bis* c.p.p., introdotto dalla l. n. 48 del 2008, il quale prevede la possibilità di sequestro probatorio dei dati informatici.

[57] G. Fiandaca, E. Musco, *Diritto penale. Parte speciale. I delitti contro il patrimonio*, cit., 29.

L'unica strada percorribile sembra, piuttosto, quella che affida al legislatore il compito di modificare il quadro normativo esistente, analogamente a quanto, peraltro, già accaduto in relazione ad altri profili di disciplina strettamente connessi alla dimensione digitale[58], nonché – in un passato più remoto – all'esigenza di chiarire e/o "aggiornare" concetti presenti nel materiale linguistico con il quale sono costruite le norme. Si pensi, in quest'ultima prospettiva, all'introduzione, ad opera della l. n. 205 del 1999, del secondo comma dell'art. 624 c.p., con il quale è stato normativamente precisato che «agli effetti della legge penale, si considera cosa mobile anche l'energia elettrica e ogni altra energia che abbia un valore economico».

6. *Il* web *come "mezzo di pubblicità"*

Come è noto, le condotte di diffamazione sono state vieppiù facilitate dalla possibilità di un numero esponenziale di utenti della rete di esprimere giudizi su tutti gli argomenti trattati, «per cui alla schiera di "opinionisti *social*" spesso si associano i cosiddetti "odiatori sul *web*", che non esitano – dietro l'anonimato – ad esprimere giudizi con eloquio volgare ed offensivo»[59].

Sicché, un altro tema rilevante attiene alla possibilità di considerare il *web* come "mezzo di pubblicità" ai fini dell'applicazione dell'aggravante prevista per la diffamazione dall'art. 595, comma 3, c.p.[60].

Ebbene, dottrina e giurisprudenza non hanno mai dubitato che, in termini generali, il riferimento a "qualsiasi altro mezzo di pubblicità" potesse essere letto nel senso di includervi astrattamente anche gli strumenti telematici, se pur non esplicitamente indicati dalla *littera legis*.

[58] Sul punto v. *supra* paragrafo 3.

[59] Così Cass. pen., sez. V, 8 novembre 2018, n. 12546, punto n. 2.1. del Considerato in diritto. In argomento, per tutti, A. Spena, *La parola(-)odio. Sovraesposizione, criminalizzazione e interpretazione dello* hate speech*,* in *Criminalia* 2016, 577 ss.

[60] *Amplius* E. Mazzanti, *Il delitto di diffamazione al tempo dei* social network*: punti fermi e spunti problematici*, in *Nodi virtuali, legami informali:* Internet *alla ricerca di regole,* a cura di P. Passaglia, D. Poletti, Pisa, 2016, 207 ss.; F. P. Lasalvia, *La diffamazione via* web *nell'epoca dei* social network*,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, in particolare 341 ss.; A. Gullo, *Delitti contro l'onore,* in *Trattato teorico pratico di diritto penale,* diretto da F. C. Palazzo, C. E. Paliero, M. Pelissero, *Reati contro la persona,* a cura di F. Viganò, Torino, 2022, 232 ss.

In tale prospettiva si ricorda una delle prime pronunce della giurisprudenza di legittimità che si è trovata a decidere una questione – così si legge – «che presenta, senza dubbio, alcuni caratteri di novità», richiedendo di «verificare come si caratterizzi il delitto di diffamazione consumato con quel nuovo mezzo di trasmissione-comunicazione che prende il nome di *internet*». Infatti, «il legislatore, pur mostrando di aver preso in considerazione la esistenza di nuovi strumenti di comunicazione, telematici ed informatici (si veda, ad esempio, l'art. 623 *bis* c.p. in tema di reati contro la inviolabilità dei segreti), non ha ritenuto di dover mutare o integrare la lettera della legge con riferimento a reati (e, tra questi, certamente quelli contro l'onore), la cui condotta consiste nella (o presuppone la) comunicazione dell'agente con terze persone. E, tuttavia, che i reati previsti dagli artt. 594 e 595 c.p. possano essere commessi anche per via telematica o informatica, è addirittura intuitivo»[61].

Sennonché, prosegue la Corte, «partendo da tale – ovvia – premessa, si giunge agevolmente alla conclusione che l'utilizzo di *internet* integra una delle ipotesi aggravate di cui dell'art. 595 c.p. (comma terzo: "offesa recata... con qualsiasi altro mezzo di pubblicità"). Anche in questo caso, infatti, con tutta evidenza, la particolare diffusività del mezzo usato per propagare il messaggio denigratorio rende l'agente meritevole di un più severo trattamento penale»[62].

Invero, se la prima parte del ragionamento della Corte appare senza dubbio condivisibile, la conclusione tratta merita, invece, di essere approfondita. Una corretta impostazione e soluzione della specifica questione attinente alla possibile applicazione dell'aggravante di cui al terzo comma dell'art. 595 c.p. impone, infatti, di evitare visioni semplicistiche dello spazio digitale, che portino a ritenere sempre e automaticamente integrata la circostanza *de qua* per il semplice fatto che vengano utilizzati mezzi messi a disposizione dalle nuove tecnologie.

Non si può trascurare la circostanza che il *cyberspace* si parcellizza in realtà in numerosi e peculiari *format*, diversi tra loro per caratteristiche di funzionamento e capacità di diffusione dei contenuti. Come è stato di recente precisato anche dalla stessa giurisprudenza, gli strumenti di comunicazione

[61] Cass. pen., sez. V, 17 novembre 2000, n. 4741, Rv. 217745. Successivamente, nello stesso senso, tra le altre, Cass. pen., sez. V, 16 ottobre 2012, n. 40980, Rv. 25044.

[62] Cass. pen., sez. V, 17 novembre 2000, n. 4741, Rv. 217745.

digitale non sono tutti uguali e non funzionano tutti nel medesimo modo[63]. Si pensi, ad esempio, alla pubblicazione di un *post* diffamatorio su una pagina pubblica *Facebook* con profilo aperto, da un lato, e all'invio del medesimo messaggio offensivo mediante *e–mail* a pochi diversi destinatari precisamente individuati, dall'altro lato. Nel primo caso il contenuto diffamatorio raggiungerebbe un numero elevatissimo ed indefinito di persone, nel secondo, invece, solamente poche e determinate persone. O si pensi, ancora, alle molteplici possibilità di utilizzo, da parte del singolo utente, dell'applicativo *Whatsapp*.

Tanto premesso, occorre verificare di volta in volta e con attenzione quale mezzo di comunicazione sia stato utilizzato, e con quali modalità, per comprendere se debba o meno ritenersi sussistente l'aggravante in oggetto, posto che "mezzi di pubblicità" sono esclusivamente quelli che consentono effettivamente un'estesa comunicazione *in incertam personam*, cioè alla massa indeterminata del pubblico[64].

Paradigmatiche, al riguardo, sarebbero effettivamente le ipotesi di pubblicazione sui siti *web* o sui *social network*, ma solo a condizione che gli stessi siano accessibili a tutti, senza filtri all'ingresso[65]. Sicché, per esempio, è stata ritenuta configurata la diffamazione aggravata ai sensi dell'art. 595, comma 3, c.p. nella pubblicazione su un *blog*, ad opera del gestore dello stesso (c.d. *blogger*), di una lettera aperta a contenuto diffamatorio[66].

Viceversa, non dovrebbero considerarsi mezzi di diffusione al pubblico le comunicazioni *ad certas personas,* quindi neppure la diffusione di contenuti offensivi in spazi riservati, non liberamente accessibili da chiunque[67]. In questi casi, infatti, verrebbe meno la possibilità di ricondurre la comunica-

[63] Cass. pen., sez. I, 11 settembre 2024, n. 42783, in *deJure*, punto n. 2 del Considerato in diritto.

[64] Tribunale di Milano, 11 febbraio 2016, n. 1624, in *www.penalecontemporaneo.it,* 1.3.2016. In dottrina, in questo senso, L. Bisori, *I delitti contro l'onore,* in *Trattato di diritto penale. Parte speciale,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, vol. VIII*, I delitti contro l'onore e la libertà individuale*, Milano, 2010, 85 ss.

[65] F. P. Lasalvia, *La diffamazione via* web *nell'epoca dei* social network*,* cit., 345.

[66] Cass. pen., sez. V, 8 novembre 2018, n. 12546. Sulla pronuncia *de qua* v. C. Pagella, *La Cassazione sulla responsabilità del* blogger *per contenuti diffamatori (commenti) pubblicati da terzi,* in *www.penalecontemporaneo.it,* 17 maggio 2019.

[67] Sul tema, G. Corrias Lucente, *La diffamazione a mezzo* Facebook, in *MediaLaws,* 25.2.2013, par. 2.

zione ad un "mezzo di pubblicità" e, conseguentemente, la *ratio* che giustificherebbe l'applicazione dell'aggravante prevista dall'art. 595, comma 3, c.p.

Parte della giurisprudenza, tuttavia, spesso assume apoditticamente la natura di mezzo di pubblicità del *web*, che viene solitamente qualificato in termini presuntivi come strumento potenzialmente capace di raggiungere un numero indeterminato di persone[68].

Invero, siffatte affermazioni non parrebbero tenere in debita considerazione talune caratteristiche di funzionamento degli strumenti digitali e dei *social network* in particolare. Se è vero, infatti, che gli utenti possono scegliere se rendere il proprio profilo, e tutte le informazioni ivi immesse, accessibile da chiunque, è ben possibile (e per nulla infrequente) che viceversa vengano privilegiate impostazioni volte delimitare e restringere l'effettiva conoscenza di dette informazioni. Sicché, ove le stesse risultino visibili esclusivamente da una cerchia di destinatari determinata o determinabile, lo strumento di comunicazione utilizzato non può certo ritenersi equiparabile ad un mezzo di diffusione al pubblico[69].

Ne consegue che la diffamazione commessa tramite *social network* potrebbe, ma non deve necessariamente, qualificarsi come aggravata dall'uso del mezzo di pubblicità. Spetterà, infatti al giudice verificare in concreto se il fatto sia avvenuto "pubblicamente" o "privatamente"[70].

Date queste premesse, in modo assolutamente condivisibile, di recente la Corte di Cassazione ha escluso la sussistenza della circostanza aggravante di cui all'art. 227, comma 2, c.p.m.p. (pressoché identica, nella sua formulazione, al comma 3 dell'art. 595 c.p.) in un'ipotesi in cui l'offesa all'onore e alla reputazione di un soggetto era stata realizzata all'interno di una chat di *Whatsapp,* il cui gruppo era costituito da 156 utenti. Si è, infatti, riconosciuto che l'evoluzione tecnologica ha consentito di ampliare le forme di comunicazione tramite la rete *internet*, da ritenersi tendenzialmente uno strumento che rientra nella previsione di legge ove si evocano altri mezzi di pubblicità. Siffatta situazione, tuttavia, si verificherebbe quando un contenuto lesivo viene reso *"pubblico"* su un qualsiasi sito *internet* ad

[68] Così, per esempio, Cass. pen., sez. I, 28 aprile 2015, n. 24431, Rv. 264007. Nella giurisprudenza di merito, tra le altre, Tribunale di Livorno, Ufficio indagini preliminari, 2 ottobre 2012, n. 38912, in *deJure.*

[69] Così F. P. LASALVIA, *La diffamazione via* web *nell'epoca dei* social network*,* cit., 348.

[70] F. P. LASALVIA, *La diffamazione via* web *nell'epoca dei* social network*,* cit., 348. Nello stesso senso G. CORRIAS LUCENTE, *La diffamazione a mezzo* Facebook, cit.

accesso libero. Nessuna questione, in questo caso, potrebbe porsi in relazione al necessario rispetto del principio di tassatività. Nondimeno, si sottolinea altresì come gli strumenti di comunicazione digitale non siano tutti uguali e non funzionino tutti nel medesimo modo. In particolare – si osserva - «una *chat* dell'applicativo *Whatsapp* è, per le sue caratteristiche ontologiche, uno strumento di comunicazione di certo *"agevolante"* ma al contempo *"ristretto"*, nel senso che il messaggio (di testo o immagine che sia) raggiunge esclusivamente i soggetti iscritti (e reciprocamente accettatisi) alla medesima *chat*»[71].

Tanto considerato, un passaggio della pronuncia in particolare merita di essere evidenziato, nella parte in cui si ricorda che ad essere rilevante, invero, non è il numero di iscritti alla *chat* bensì la *"conformazione tecnica"* del mezzo, tesa a realizzare uno scambio di comunicazioni destinate a rimanere riservate all'interno di un numero circoscritto di destinatari. In altre parole, la diffusione del messaggio a più soggetti – gli iscritti alla *chat* – avviene in un contesto informatico che se, da un lato, consente la rapida divulgazione dei contenuti, dall'altro lato, non comporta la perdita di una essenziale connotazione di riservatezza della comunicazione, destinata ad un numero identificato e previamente accettato di persone. Sicché, si renderebbe evidente la tensione con il principio di tassatività in ambito penale, ove si volesse realizzare una equiparazione tra i diversi strumenti comunicativi, in rapporto ad una previsione di legge ove si evoca espressamente un *"mezzo di pubblicità"*[72].

7. Internet *come "mezzo di stampa"*

Un'ulteriore questione rilevante e tuttora non pacifica attiene alla possibilità di assimilare le comunicazioni via *Internet* alla stampa, con la conseguente applicabilità della relativa disciplina. Il riferimento è, in particolare,

[71] Cass. pen., sez. I, 11 settembre 2024, n. 42783, in *deJure,* punto n. 2 del Considerato in diritto. Nello stesso senso Cass. pen., sez.. I, 19 maggio 2023, n. 37618, Rv. 285248, punto n. 4.2 del Considerato in diritto. Sulla pronuncia *de qua* C. Rossi, *Non ricorre l'aggravante dell'uso di un mezzo di pubblicità nel caso di diffusione di un messaggio offensivo in una "*chat*" attraverso "*WhatsApp*"*, in *Cass. pen.,* 2024, 1006 ss.

[72] Cass. pen., sez. I, 11 settembre 2024, n. 42783, cit., punto n. 2 del Considerato in diritto.

all'art. 57 c.p.[73], che punisce il direttore responsabile a titolo di colpa per le ipotesi di omesso controllo[74].

Ebbene, secondo la dottrina e la giurisprudenza maggioritarie, in termini generali *Internet* non sarebbe equiparabile alla stampa, sicché un'estensione della relativa disciplina, e in particolare del predetto schema di imputazione, costituirebbe un'evidente violazione del divieto di analogia in *malam partem*[75].

Il problema diviene però più complesso in relazione alle vere e proprie testate giornalistiche *online*.

Per meglio comprendere i termini della questione occorre ricostruire alcuni passaggi, muovendo da un'importante pronuncia delle Sezioni Unite della Cassazione che, nel 2015[76], al fine di estendere talune garanzie, ha mo-

[73] Invero, prima delle recente dichiarazione di illegittimità costituzionale ad opera di Corte cost. n. 150 del 2021 la questione coinvolgeva anche la possibilità di applicare o meno la circostanza aggravante contemplata dall'art. 13 l. n. 47 del 1948.

[74] In argomento, M. MIGLIO, *La responsabilità dell'amministratore di un gruppo* Facebook *per i commenti offensivi pubblicati da altri utenti: un travagliato percorso giurisprudenziale,* in *www.giurisprudenzapenale.com,* 9 settembre 2016; E. BIRRITTERI, *Diffamazione e* Facebook*: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica* in malam partem *delle norme sulla stampa*, in *www.penalecontemporaneo.it, Riv. trim.,* n. 4 del 2017, 286 ss.

[75] Nella giurisprudenza, per tutte, Cass. pen., sez. V, 15 maggio 2008, n. 24018, in *deJure,* che evoca il «tentativo infecondo di estendere, in ambito penale, alle comunicazioni telematiche la normativa sulla stampa». Nella giurisprudenza di merito, Tribunale di Oristano, 25 maggio 2000 (in *Riv. it. dir. proc. pen.,* 2001, 1405 ss.), ad avviso del quale «alla diffamazione realizzata mediante divulgazione di frasi offensive tramite un sito *web* non sono applicabili le disposizioni speciali previste per la diffamazione commessa con l'uso del mezzo della stampa o con l'uso del mezzo della radio televisione stante il divieto di analogia in materia penale». Sulla pronuncia, L. SCOPINARO, *Diffamazione via* Internet*: applicabilità della circostanza aggravante relativa all'uso del mezzo di pubblicità,* in *Riv. it. dir. proc. pen.,* 2001, 1410 ss. In dottrina, per tutti, V. ZENO ZENCOVICH, *La pretesa estensione alla telematica del regime della stampa. Note critiche,* in *Diritto dell'informazione e dell'informatica,* 1998, 15 ss.; C. MELZI D'ERIL, G. E. VIGEVANI, *La responsabilità del direttore del periodico telematico, tra facili equiparazioni e specificità di* Internet, in *Diritto dell'informazione e dell'informatica*, 2010, 91 ss.; S. SEMINARA, Internet *(diritto penale)*, in *Enciclopedia del Diritto, Annali*, VII, Milano, 2014, 570, 584 ss.; D. PETRINI, *Diffamazione* online: *offesa recata con "altro mezzo di pubblicità" o col mezzo della stampa?,* in *Dir. pen. proc.,* 2017, 1485 ss. Di recente, F. GIUNTA, *Il linguaggio del "penale" e il garantismo della norma,* in *Criminalia* 2024, 320.

[76] Cass. pen., sez. un., 29 gennaio 2015, n. 31022, Rv. 264089. in *Giur. cost*., 2015, 1055 ss., con nota critica di L. DIOTALLEVI, *La Corte di cassazione sancisce l'"equiparazione" tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di "scivolamento" dalla "nomofilachia" alla "nomopoiesi"*?, ivi, 1062 ss., ad avviso del quale ricorre «con sempre maggiore frequenza, nell'ambito della giurisprudenza di legittimità,

dificato la precedente impostazione[77], evidenziando che al concetto di stampa debba attribuirsi un significato evolutivo, coerente tanto con il progresso tecnologico quanto con l'ordinamento giuridico considerato nel suo complesso. Si verrebbe, infatti, a determinare un'evidente situazione di tensione con il principio di uguaglianza di cui all'art. 3 Cost. allorché si legittimasse «un irragionevole trattamento differenziato dell'informazione giornalistica veicolata su carta rispetto a quella diffusa in rete»[78].

Tanto premesso, le Sezioni unite affermano la necessità di discostarsi dall'esegesi letterale del dettato normativo per privilegiare «una interpretazione estensiva dello stesso, sì da attribuire al termine "stampa" un significato evolutivo». Invero, detta interpretazione estensiva consentirebbe di assegnare al dato normativo «un senso e una portata corrispondenti alla coscienza giuridica e alle necessità sociali del momento attuale»[79].

Nondimeno, in tale prospettiva, sarebbe comunque necessario tenere ben distinta l'area dell'informazione di tipo professionale, veicolata per il tramite di una testata giornalistica *on line*, dal vasto ed eterogeneo ambito della diffusione di notizie ed informazioni effettuata da singoli soggetti in modo spontaneo[80]. Sicché, l'esito di un'operazione ermeneutica estensiva non potrebbe comunque riguardare tutti in blocco i nuovi mezzi, informatici e telematici, di manifestazione del pensiero (*forum*, *blog*, *newsletter*,

la scelta di avallare opzioni interpretative che, risolvendosi in una "forzatura" della naturale portata semantica delle proposizioni legislative, finiscono - in concreto - per assumere una valenza "creativa" e, in questo senso, "normativa"» (ivi, 1070).

77 Il *leading case* in tal senso fu rappresentato da Cass. pen., sez. V, 16 luglio 2010, n. 35511, Rv. 248507. Sulla pronuncia *de qua*, C. MELZI D'ERIL, Roma locuta: *la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line, in *Diritto dell'informazione e dell'informatica*, 2010, 895 ss.; I. SALVADORI, *La normativa penale sulla stampa non si applica,* de jure condito*, ai giornali telematici*, in *Cass. pen*., 2011, 2982 ss.; I. PISA, *Profili di responsabilità penale del direttore di periodici telematici*, in *Dir. pen. proc.*, 2011, 455 ss. Nella giurisprudenza successiva, in senso conforme, Cass. pen., sez. V, 28 ottobre 2011, n. 44126, Rv. 251132, con note di G. E. VIGEVANI, *La "sentenza figlia" sul direttore del giornale telematico: il caso Hamaui*, in *Diritto dell'informazione e dell'informatica*, 2011, 795 ss., e di G. CORRIAS LUCENTE, *Al direttore responsabile di un periodico* on line *non si applica il reato previsto dall'art. 57 del codice penale*, in *Diritto dell'informazione e dell'informatica*, 2012, 82 ss. Su entrambe le importanti citate pronunce, D. PETRINI, *Il direttore della testata telematica, tra* horror vacui e *prospettive di riforma; sperando che nulla cambi*, in *Riv. it. dir. proc. pen.*, 2012, 1611 ss.

78 Cass. pen., sez. un., 29 gennaio 2015, n. 31022, cit., punto n. 17 del Considerato in diritto.

79 Cass. pen., sez. un., 29 gennaio 2015, n. 31022, cit. punto n. 17 del Considerato in diritto.

80 Cass. pen., sez. un., 29 gennaio 2015, n. 31022, cit., punto n. 18 del Considerato in diritto.

newsgroup, *mailing list*, pagine *Facebook*), a prescindere dalle caratteristiche specifiche di ciascuno di essi, ma dovrebbe rimanere circoscritto a quei soli casi che, per i profili strutturale e finalistico che li connotano, siano riconducibili al concetto di stampa inteso in senso più ampio[81].

Quest'ultimo sarebbe, in sintesi, ravvisabile nel prodotto editoriale che presenti gli specifici requisiti ontologici (struttura) e teleologici (scopi della pubblicazione) propri di un giornale. La struttura di questo sarebbe costituita «dalla "testata", che è l'elemento che lo identifica, e dalla periodicità regolare delle pubblicazioni (quotidiano, settimanale, mensile); la finalità si concretizza nella raccolta, nel commento e nell'analisi critica di notizie legate all'attualità (cronaca, economia, costume, politica) e dirette al pubblico, perché ne abbia conoscenza e ne assuma consapevolezza nella libera formazione della propria opinione»[82].

Ne conseguirebbe che il giornale telematico, così individuato, sia se riproduzione di quello cartaceo, sia se unica e autonoma fonte di informazione professionale, dovrebbe soggiacere alla normativa sulla stampa, perché ontologicamente e funzionalmente assimilabile alla pubblicazione cartacea[83]. Talché, la stampa telematica, al pari di quella tradizionale, in quanto emancipata da qualsiasi forma di censura, non potrebbe essere sottoposta a sequestro preventivo, se non nei casi eccezionali espressamente previsti dalla legge, e dovrebbe soggiacere alle norme che disciplinano la responsabilità per gli illeciti commessi[84].

I principi affermati dalle sezioni unite attraverso il predetto percorso argomentativo sono stati successivamente ribaditi da più recenti pronunce della Cassazione[85], con la conseguenza però che la nuova nozione estesa di stampa, plasmata nel 2015 con indubbi effetti *in bonam partem,* è stata ritenuta utilizzabile anche in ambiti ulteriori e completamente diversi rispetto a quello in cui era "nata"[86]. Ne è in tal modo derivata l'estensione agli illeciti commessi

[81] Sul punto, M. MIGLIO, *La responsabilità dell'amministratore di un gruppo* Facebook *per i commenti offensivi pubblicati da altri utenti: un travagliato percorso giurisprudenziale,* cit.

[82] Cass. pen., sez. un., 29 gennaio 2015, n. 31022, punto n. 20 del Considerato in diritto.

[83] Cass. pen., sez. un., 29 gennaio 2015, n. 31022, punto n. 22 del Considerato in diritto.

[84] Cass. pen., sez. un., 29 gennaio 2015, n. 31022, punto n. 22 del Considerato in diritto.

[85] Cass. pen., sez. V, 11 dicembre 2017, n. 13398, in *Dejure*; Cass. pen., sez. V, 23 ottobre 2018, n. 1275, Rv. 274385.

[86] C. MELZI D'ERIL, *L'applicabilità della disciplina prevista per la stampa a* Internet: *l'ultima*

attraverso testate digitali di tutta la disciplina concernente i reati a mezzo stampa, compreso, paradossalmente, l'art. 57 c.p., ferma restando, invece, l'esclusione da tale applicabilità per gli altri mezzi informatici di manifestazione del pensiero non assimilabili alla nozione di stampa[87]. Infatti, anche per la giurisprudenza successiva, solo la testata giornalistica telematica, funzionalmente assimilabile a quella tradizionale in formato cartaceo, sarebbe da ricondurre nel concetto di stampa di cui all'art. 1 della legge 8 febbraio 1948 n. 47[88].

Sennonché, se anche in relazione alle testate giornalistiche *online* sembra giustificata un'estensione della disciplina tradizionale in tema di stampa in relazione ai profili extrapenali (primi tra tutti, le garanzie costituzionali), non parrebbero viceversa dilatabili in via interpretativa le disposizioni in materia penale[89].

In altre parole, se le sezioni unite avevano esteso il concetto di stampa con finalità di tutela del tutto condivisibili, la giurisprudenza successiva delle sezioni semplici, sulla base di una totale eterogenesi dei fini, ha iniziato a far propria la nuova nozione di stampa per estendere la portata dell'art. 57 c.p. e colmare in tal modo una presunta lacuna che, quand'anche ritenuta effettivamente esistente, andrebbe comunque "gestita" dal legislatore, sulla base dei principi cardine del nostro ordinamento penale[90].

puntata di una lunga storia, tra legislatore assente e giurisprudenza (molto) creativa, in *Media-Laws*, 5 novembre 2024, 12, 13.

[87] Cass. pen., sez. V, 19 febbraio 2018, n. 16751, Rv. 272685; Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995; Cass. pen, sez. V, 23 ottobre 2018, n. 1275 (con nota di F. LOMBARDI, *La responsabilità del direttore del periodico telematico ex art. 57 c.p. tra interpretazione estensivo-evolutiva e analogia* in malam partem, in *www.giurisprudenzapenale.com,* 11 gennaio 2019), ad avviso della quale in «tema di diffamazione, l'amministratore di un sito *internet* non è responsabile ai sensi dell'art. 57 c.p., in quanto tale norma è applicabile alle sole testate giornalistiche telematiche e non anche ai diversi mezzi informatici di manifestazione del pensiero (*forum, blog, newsletter, newsgroup, mailing list, facebook*)». Sulla pronuncia *de qua* v. anche F. G. CATULLO, *La responsabilità penale del direttore del giornale telematico tra legislatore pigro e giudice intraprendente,* in *Diritto di Internet*, 2019, 173 ss.

[88] Cass. pen., sez. V, 11 dicembre 2017, n. 13398, in *deJure.*

[89] In questo senso, tra gli altri, F. CECCHINI, *La responsabilità del direttore di periodico telematico ex art. 57 c.p. tra divieto di analogia, "esigibilità" del controllo e prevedibilità dell'esito giudiziario*, in *Archivio penale web*, n. 2 del 2019, 3 ss., con ampie argomentazioni in merito alla distinzione tra *Internet* e stampa.

[90] In tale prospettiva si ricorda il disegno di legge (d.d.l. Costa, C-925B), approvato dalla Camera dei Deputati e trasmesso al Senato il 25 giugno 2015, che proponeva l'estensione alle testate *online* di tutte le norme sulla stampa tradizionale, compresa la circostanza aggravante

Si deve, comunque, segnalare un ritorno della recente giurisprudenza di merito ad un orientamento più in linea con il principio di legalità e propenso ad escludere in termini netti l'applicabilità dell'art. 57 c.p. ai giornali telematici.

La definizione di stampa – si legge in una pronuncia del Tribunale di Milano[91] – «è del tutto incompatibile con la funzionalità della testata giornalistica *online* e l'applicazione della prima a quest'ultima deve necessariamente passare per un'operazione analogica – preclusa in ambito penale – giacché il senso letterale di "riproduzioni tipografiche" non può certo essere esteso fino a ricomprendere la veicolazione di contenuti di tipo multimediale».

Nello stesso senso, in termini ancora più espliciti, si è espressa altresì la Corte d'appello di Milano[92], secondo la quale – vale la pena metterlo in evidenza - l'estensione di una garanzia, quale è quella del divieto di sequestro preventivo, da parte della giurisprudenza delle sezioni unite «non può e non deve consentire l'automatica estensione della responsabilità penale per casi non disciplinati dalla legge. Interpretare evolutivamente il concetto di stampa, in assenza di un intervento legislativo, è ammissibile se comporta un trattamento di favore nei confronti del cittadino, ma non se comporta la creazione di nuove fattispecie incriminatrici, agendo in suo svantaggio, perché l'interprete non ha il potere, nell'ambito del diritto penale, di colmare i vuoti normativi lasciati dal legislatore, creando di fatto nuove fattispecie incriminatrici». Sicché -si prosegue - «se davvero un'esigenza di responsabilizzazione per omesso controllo esiste, anche nel settore telematico, è solo il legislatore che può legittimamente farsene carico»[93].

prevista dall'art. 13, l. n. 47 del 1948 e la responsabilità colposa del direttore responsabile per omesso controllo delle pubblicazioni di altri, ai sensi dell'art. 57 c.p.

[91] Tribunale di Milano, sezione Giudice per le Indagini preliminari, 14 ottobre 2021, nell'ambito del proc. pen. n. 21763 del 2019 R.G.G.I.P. Nello stesso senso, altresì, Tribunale di Milano, sez. V penale, 15 marzo 2024, n. 3825.

[92] Corte d'appello di Milano, sez. III penale, 24 novembre 2022, § 4, punto n. 4.2.4. Sulla pronuncia *de qua,* S. VIMERCATI, Revirement *dei giudici di merito: il direttore della testata telematica non risponde del reato di omesso controllo. Verso due nozioni di "stampa"?,* in *MediaLaws,* n. 2, 2023, 382 ss.

[93] Corte d'Appello di Milano, sez. III penale, 24 novembre 2022, § 4, punto n. 4.2.4.

8. *Il* web *come "luogo pubblico" o "aperto al pubblico"*

Spesso il *web* e i social *network* in particolare vengono equiparati ad un'*agorà* virtuale, un luogo, dunque, assimilabile ad uno spazio aperto al pubblico. Da qui la convinzione, emersa nella prassi, che possa, per esempio, configurarsi il reato di molestie contemplato dall'art. 660 c.p. anche tramite l'utilizzo di *Facebook*. Quest'ultimo, infatti, si presenterebbe come un luogo aperto all'accesso di chiunque utilizzi la rete, dunque come una "piazza immateriale", che consente un numero indeterminato di accessi, «resa possibile da un'evoluzione scientifica, che certo il legislatore non era arrivato ad immaginare»[94].

Sennonché, anche siffatta equiparazione non è esente da profili problematici, segnatamente nel momento in cui si voglia far discendere da detta equiparazione l'integrazione di un elemento di fattispecie.

Ebbene, il discorso si atteggia in termini diversi rispetto ad altre situazioni, già da tempo oggetto di attenzione, in cui *Facebook* è venuto in rilevo come mezzo di commissione del reato. Si pensi, come già anticipato, all'ipotesi della diffamazione, per lo più ritenuta aggravata allorché realizzata per il tramite dei nuovi mezzi di comunicazione digitali[95].

Nel caso delle molestie, viceversa, *Facebook* sarebbe chiamato in causa non come mezzo attraverso il quale commettere il reato, bensì come *locus* nel quale la fattispecie viene ad esistenza[96]. Si tratterebbe, dunque, di un'interpretazione del sintagma "luogo pubblico o aperto al pubblico" smaterializzata[97]. Da qui l'emergere della questione se detta interpretazione possa effettivamente considerarsi compatibile con il principio di tassatività e il correlato divieto di analogia.

Invero, ad avviso di una parte della dottrina, i luoghi virtuali parrebbero

[94] Cass. pen., sez. I, 11 luglio 2014, n. 37596, in *Dejure*. Sulla pronuncia *de qua* L. Diotallevi, *Reato di molestia e* Facebook *tra divieto di analogia in materia penale, (presunta) interpretazione "evolutiva" dell'art. 17 Cost. e configurabilità di un diritto di accesso ad* Internet, in *Giur. cost.*, 2014, 4104 ss.; M. C. Ubiali, *Molestie via* Facebook*: tra divieto di analogia ed esigenze di adeguamento alle nuove tecnologie,* in *www.penalecontemporaneo.it,* 5 marzo 2015.

[95] Sul punto v. *supra* paragrafo 6.

[96] G. Checcacci, Facebook *come un luogo pubblico: un caso di "analogia digitale"* in malam partem*,* in *Criminalia* 2014, 505.

[97] G. Checcacci, Facebook *come un luogo pubblico: un caso di "analogia digitale"* in malam partem*,* cit., 504.

appartenere «quantomeno alla penombra del significato di "luogo" nella lingua corrente», al punto che, pur collocandosi oltre il significato letterale standard del termine, non si troverebbero «tanto lontano da esso da richiedere la creazione di nuovo diritto per via analogica»[98].

Sicché, posto che le condotte realizzate nello spazio virtuale hanno un'offensività superiore date le caratteristiche di detto spazio (raggiungibilità di un più ampio numero di persone, minor costo per il molestatore, maggiore diffusione, ecc.), non vi sarebbero ostacoli alla riconducibilità delle molestie realizzate sul *web* alla citata fattispecie incriminatrice[99].

Nondimeno, al di là delle questioni legate – come già anticipato – alla non scontata natura "aperta" di ogni profilo *Facebook*[100], la tesi esposta (e per lo più recepita dalla giurisprudenza) parrebbe scontrarsi con (almeno) due diversi ordini di argomentazioni.

Da un lato, infatti, già il ricondurre *Fecebook* (ma, altresì, la rete in generale) – per definizione privo di ogni riferimento di ordine spaziale – al concetto di "luogo" integra un'operazione che finisce per travalicare quel limite di "compatibilità" semantica sotteso ad ogni operazione di interpretazione, sia pure estensiva[101].

Dall'altro lato, anche ammesso di poter (difficilmente) superare siffatta prima obiezione, occorrerebbe comunque verificare la tenuta della prospettata interpretazione sotto il profilo logico, con specifico riferimento al reato di molestia, il quale, in virtù del peculiare oggetto di tutela, sembrerebbe, invero, riconducibile alla categoria di reati ad ambientazione materiale vincolata, ovvero destinati a realizzarsi necessariamente in uno spazio fisico concreto[102].

Infatti, la fattispecie in oggetto integra una contravvenzione posta a tutela dell'ordine pubblico, inteso nella più specifica prospettiva della pubblica tranquillità, vale a dire dell'esigenza di evitare fatti e/o reazioni pericolose per la collettività. Ed anche là dove si preferisse, invece, attribuire al reato –

98 G. TUZET, *Luoghi, siti, bacheche. Un caso di interpretazione estensiva,* in *Criminalia* 2014, 517.

99 G. TUZET, *Luoghi, siti, bacheche. Un caso di interpretazione estensiva,* cit., 517, 518.

100 Sul punto v. già *supra* paragrafo 6.

101 Così, L. DIOTALLEVI, *Reato di molestia e* Facebook *tra divieto di analogia in materia penale, (presunta) interpretazione "evolutiva" dell'art. 17 Cost. e configurabilità di un diritto di accesso ad* Internet, cit., 4105.

102 La definizione è di G. CHECCACCI, Facebook *come un luogo pubblico: un caso di "analogia digitale"* in malam partem*,* cit., 507.

nella sua complessiva struttura – una vocazione plurioffensiva, rivolta altresì nei confronti della tranquillità personale, intesa come bene di natura individuale[103], non parrebbe revocabile in dubbio che, nella parte in cui la norma richiede la realizzazione del fatto in luogo pubblico, la tranquillità del singolo verrebbe, invero, a ricevere una tutela giuridica soltanto riflessa, nella misura in cui la sua protezione coincida con quella del bene collettivo[104].

Tanto premesso, l'estensione della fattispecie di molestie al mondo virtuale, del quale l'immaterialità costituisce il dato strutturale qualificante, parrebbe comportare uno snaturamento della norma, non giustificato da alcuna istanza di tutela. In tal modo, infatti, la disposizione in oggetto verrebbe «piegata al raggiungimento di un fine totalmente diverso, anche se evolutivamente interpretato, rispetto all'originaria area di protezione designata dal legislatore, attraverso un'operazione analogica, vietata nel campo del diritto penale»[105].

Per quanto, dunque, il *web* in generale e i *social network* in particolare costituiscano indubbiamente – come detto in apertura di queste riflessioni - la nuova *agorà*, ciò non significa che si possa effettuare il "trapianto" *tout court* di qualunque forma di tutela penale dallo spazio pubblico materiale a quello virtuale. Siffatta traslazione, infatti, deve essere di volta in volta attentamente vagliata sia alla luce della stretta tipicità della singola fattispecie, sia alla luce dell'interesse protetto dalla norma[106].

D'altra parte, quando il legislatore ha inteso dare rilievo (e tutela) a luoghi informatici virtuali, lo ha fatto espressamente. Il riferimento è, per esempio, al c.d. domicilio informatico, divenuto oggetto di specifica protezione in virtù dell'ingresso nel nostro ordinamento del reato che incrimina l'accesso abusivo a un sistema informatico o telematico[107].

[103] In questo senso *amplius* F. BASILE, *Art. 660,* in *Codice penale commentato,* fondato da E. DOLCINI, G. MARINUCCI, diretto da E. DOLCINI, G.L. GATTA, Tomo, III, Milano, 2025, 1258, 1259.

[104] Sul tema cfr., M. BOTTO, *Le molestie sessuali nell'universo digitale. Riflessioni sulla dimensione "non fisica" della libertà sessuale,* in K. SUMMERER, M.L. MATTHEUDAKIS, G. M. CALETTI, *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea,* Pisa, 2025, 185 ss.

[105] G. CHECCACCI, Facebook *come un luogo pubblico: un caso di "analogia digitale"* in malam partem*,* cit., 511.

[106] G. CHECCACCI, Facebook *come un luogo pubblico: un caso di "analogia digitale"* in malam partem*,* cit., 512.

[107] M. C. UBIALI, *Molestie via* Facebook*: tra divieto di analogia ed esigenze di adeguamento*

9. *Molestia "col mezzo del telefono" e nuove modalità di intrusione tecnologica non gradita*

La fattispecie di molestie ha sollevato un ulteriore problema interpretativo, concernente la possibilità di ritenere configurabile il reato nel caso di ripetuto invio non gradito di *sms* o di messaggi di posta elettronica[108].

Come ricordato anche dalla giurisprudenza, la *quaestio iuris* sul significato da attribuire alla locuzione "col mezzo del telefono", utilizzata dal legislatore del 1930, si è posta nel momento in cui si è reso necessario verificare la riconducibilità o meno alla previsione normativa di innovative modalità di interferenza, non gradita, nella vita altrui create dallo sviluppo tecnologico e non immaginate dal legislatore nel momento in cui è stata scritta la norma[109].

Ebbene, anche in relazione a tale questione le posizioni di dottrina e giurisprudenza sono piuttosto articolate.

Una pronuncia della Cassazione[110], che si è occupata, in particolare, della rilevanza penale della molestia arrecata mediante *sms*, ha ritenuto integrabile la fattispecie di cui all'art. 660, posto che tale tipologia di messaggi è trasmessa attraverso sistemi telefonici e dunque il destinatario di essi sarebbe costretto, sia *de auditu* che *de visu*, a percepirli, con corrispondente turbamento della quiete e tranquillità psichica. Sul piano del rispetto del principio di tipicità della fattispecie penale, detta pronuncia non ravvisa particolari motivi di tensione, ritenendo che la soluzione prospettata si muova ancora in un sistema di comunicazioni che è caratterizzato dall'utilizzo di un apparecchio telefonico.

Una differente presa di posizione della giurisprudenza di legittimità, si è, invece, occupata della rilevanza penale delle molestie perpetrate mediante messaggi di posta elettronica, introducendo, invero, una prima limitazione

alle nuove tecnologie, cit., 10.

[108] In argomento, per tutti, G. MARTIELLO, *Il caso della molestia "telefonica" tra evoluzione tecnologica e primato della legalità,* in *Gius. pen.*, 2011, II 47 ss. In termini generali, sulle interazioni tra testo e contesto nell'interpretazione delle norme penali, F. VITARELLI, *Il disvalore penale tra testo e contesto,* Torino, 2025, in particolare 27 ss., là dove si evoca, altresì, il caso delle molestie telefoniche.

[109] Cass. pen., sez. I, 18 marzo 2021, n. 37974, Rv. 282045, punto n. 2.3 del Considerato in diritto; Cass. pen., sez. I, 6 giugno 2023, n. 40033, Rv. 285371, punto n. 1 del Considerato in diritto.

[110] Cass. pen., sez. III, 26 marzo 2004, 28680, Rv. 229464.

alla possibilità di sussumere nell'ambito della previsione di cui all'art. 660 c.p. anche questa tipologia di comunicazione a distanza.

Si muove, infatti, dalla premessa che la sentita esigenza di espandere la tutela della tranquillità individuale incontri il limite coessenziale della legge penale costituito dal "principio di stretta legalità" e di tipizzazione delle condotte illecite, sanciti dall'art. 25, secondo comma, Cost., e dall'art. 1 c.p.[111], il quale impedirebbe di dilatare l'espressione "col mezzo del telefono" sino a comprendere anche le modalità di comunicazione asincrone, quali l'invio di messaggi di posta elettronica, che pure utilizzano la rete telefonica e la rete cellulare delle bande di frequenza.

Occorrerebbe, infatti, muovere dal presupposto che il mezzo telefonico assunse rilievo ai fini dell'ampliamento della tutela penale (altrimenti limitata alle molestie arrecate in luogo pubblico o aperto al pubblico) proprio per il carattere invasivo della comunicazione alla quale il destinatario non può sottrarsi, se non disattivando l'apparecchio telefonico medesimo[112]. La comunicazione telefonica implicherebbe, in altre parole, un'immediata interazione tra il chiamante e il chiamato e una diretta intrusione del primo nella sfera delle attività del secondo.

Viceversa, l'invio di un messaggio di posta elettronica, – esattamente come una lettera spedita tramite il servizio postale – non comporterebbe (a differenza della telefonata) nessuna immediata interazione tra il mittente e il destinatario, in quanto «l'azione del mittente si esaurisce nella memorizzazione di un documento di testo (colla possibilità di allegare immagini, suoni o sequenze audiovisive) in una determinata locazione della memoria dell'elaboratore del gestore del servizio, accessibile dal destinatario» e «la comunicazione si perfeziona, se e quando il destinatario, connettendosi, a sua volta, all'elaboratore e accedendo al servizio, attivi una sessione di consultazione della propria casella di posta elettronica e proceda alla lettura del messaggio»[113].

[111] Cass. pen., sez. I, 17 giugno 2010, n. 24510, Rv. 247558, punto n. 4 della parte argomentativa. Sulla pronuncia *de qua*, F. G. CATULLO, *Sulle molestie via* e- mail*,* in *Cass. pen.,* 2011, 1039 ss.

[112] Cass. pen., sez. I, 18 marzo 2021, n. 37974, Rv. 282045, punto n. 2.3 del Considerato in diritto. In dottrina, *amplius,* G. MARTIELLO, *Il caso della molestia "telefonica" tra evoluzione tecnologica e primato della legalità,* cit., 47 ss.

[113] Cass. pen., sez. I, 17 giugno 2010, n. 24510, Rv. 247558, punto n. 4 della parte argomentativa. Sostanzialmente nello stesso senso, Cass. pen., sez. fer., 6 settembre 2012, 44855,

Secondo tale orientamento, dunque, nella locuzione "col mezzo del telefono" rientrerebbero solo le comunicazioni che avvengono con modalità sincrona, dando luogo ad una immediata interazione tra soggetto agente e destinatario della comunicazione, anche se effettuate non propriamente con il mezzo del telefono, ma con altri analoghi mezzi di comunicazione a distanza.

Nondimeno, poco tempo dopo siffatta presa di posizione, la giurisprudenza[114], ritornando sul tema della configurabilità del reato di molestie con lo strumento della posta elettronica e muovendo dal rilievo che i risultati dell'innovazione tecnologica consentono di inviare *e–mail*, in entrata e in uscita, attraverso i normali apparecchi telefonici, ha precisato che «al termine telefono, espressivo "dell'*instrumentum* della contravvenzione *de qua*", va equiparato, senza esondare dal perimetro dei possibili significati della formulazione letterale impiegata dal legislatore, qualsiasi mezzo di trasmissione, tramite rete telefonica e rete cellulare delle bande di frequenza, di voci e di suoni imposti al destinatario, senza possibilità per lo stesso di sottrarsi alla "immediata" interazione con il mittente. Si è rimarcato, infatti, come non possa essere considerato dirimente il criterio incentrato sul carattere sincronico o asincronico del contenuto della comunicazione»[115].

Sicché, muovendo da tali spunti, si è riconosciuto che la posta elettronica, quando la comunicazione sia accompagnata da un avvertimento acustico che ne indichi l'arrivo, possa rivelarsi molesta, proprio come l'invio ripetuto di squilli telefonici, in considerazione dell'idoneità a determinare una significativa intrusione nell'altrui sfera personale. Situazione, questa, che risulterebbe diversa da quella in cui il destinatario dei messaggi di posta elettronica, senza essere avvertito dell'arrivo degli stessi, decida di aprirli, così volontariamente accedendo al loro contenuto, come accade per la corrispondenza epistolare, senza subire alcun condizionamento costituito "da segni o rumori premonitori"[116].

in *Giur. it.,* 2013, 1169, con osservazioni di M. A. Federici, *In tema di molestie mediante posta elettronica.*

[114] Cass. pen., sez. I, 27 settembre 2011, n. 36779, Rv. 250807. Sulla pronuncia, E. Lo Monte, *Una riflessione su* spamming *e molestie: la problematica configurabilità della fattispecie incriminatrice di cui all'art. 660 c.p.,* in *Cass. pen.,* 2012, 2113 ss.

[115] Cass. pen., sez. I, 27 settembre 2011, n. 36779, Rv. 250807, punto 3 della parte argomentativa.

[116] Cass. pen., sez. I, 18 marzo 2021, n. 37974, Rv. 282045, punto n. 2.3 del Considerato in diritto.

In un'ulteriore circostanza[117], la giurisprudenza ha nuovamente affrontato la questione relativa alle molestie arrecate tramite messaggistica istantanea *sms* e *whatsapp*, precisando che l'interazione immediata, e non gradita, del destinatario con il mittente può consistere non soltanto nell'avvertimento acustico che indica l'arrivo del messaggio, ma anche nella percezione immediata e diretta del contenuto del messaggio attraverso l'anteprima di testo che compare sulla schermata di blocco.

Infine, una pronuncia di poco successiva[118], è tornata sul tema delle comunicazioni che avvengono mediante posta elettronica, escludendo la rilevanza penale delle stesse ai sensi dell'art. 660 c.p., a causa della minore invasività della modalità asincrona attraverso cui avviene la comunicazione, sempre che, però, detta comunicazione tramite posta elettronica non avvenga con un telefono "attrezzato", che permetta «la trasmissione di voci e di suoni in modalità sincrona, che avvertono non solo l'invio e la contestuale ricezione di *sms*, ma anche l'invio e la ricezione di posta elettronica».

Tanto premesso, appare evidente come le conclusioni in merito alla possibile estensione della fattispecie di cui all'art. 660 c.p. alle nuove forme di intrusione tecnologica non gradita siano mutevoli, in larga misura legate ad un approccio casistico e ad un apporto creativo ad opera dell'interprete[119].

L'impressione è che si sia tacitamente fatta strada l'idea della generalizzata punibilità, ai sensi dell'art. 660 c.p., della molestia e del disturbo arrecati con qualunque modalità di comunicazione che presenti il carattere dell'invasività. Sennonché, si tratterebbe un'interpretazione compiuta sulla base di valutazioni teleologiche riguardanti l'offensività del comportamento tenuto che non trova, però, riscontro nella lettera della norma.

Anche la giurisprudenza più recente ha ravvisato il comune denominatore delle diverse pronunce che hanno ritenuto possibile l'integrazione della fattispecie in una invasività della comunicazione assimilabile a quella della chiamata telefonica molesta.

Nondimeno, si è, poi, da ultimo osservato che «se sono i sistemi di *alert*

[117] Cass. pen., sez. I, 18 marzo 2021, n. 37974, Rv. 282045.

[118] Cass. pen., sez. I, 4 maggio 2021, n. 28959, Rv. 281755.

[119] In argomento, con specifico riferimento alla questione qui oggetto di attenzione, S. LEUCCI, *Appunti sul difficile rapporto tra linguaggio, diritto penale e tecnologia,* in *Informatica e diritto,* 2013, n. 2, in particolare 158 ss.

o *preview* che affiancano la forma di comunicazione a distanza a rendere la stessa sufficientemente invasiva da dover essere considerata molesta nel significato dell'art. 660 c.p., deve essere a questo punto osservato che la esistenza o meno di un sistema di *alert* o *preview* dipende, in realtà, non dal soggetto che invia, ma da quello che riceve, che può decidere liberamente se consentire all'applicazione di messaggistica telematica di inviargli la notifica della ricezione di un messaggio»[120].

Sicché – il passaggio merita di essere sottolineato – «in un sistema di messaggistica telematica che ormai, per effetto dell'ulteriore progresso delle telecomunicazioni, permette al destinatario di sottrarsi sempre all'interazione immediata con il mittente ponendo un filtro al rapporto con il soggetto che invia il messaggio molesto, la equiparazione tra l'invasività delle comunicazioni moleste effettuate tramite sistemi di messaggistica telematica e quella delle comunicazioni tradizionali effettuate con il mezzo del telefono non si giustifica più»[121].

10. *Lo sfruttamento sessuale* online

Il settore dei reati sessualmente connotati costituisce uno straordinario banco di prova per verificare la tenuta del principio di legalità allorché vengano in considerazione comportamenti realizzati nella dimensione digitale e qui destinati ad esaurirsi interamente[122].

In particolare ci si chiede se, ed eventualmente fino a che punto, possa dirsi superabile il requisito della contemporanea presenza e interazione fisica tra soggetto attivo e soggetto passivo che parrebbero connotare diversi paradigmi punitivi, *ab origine* concepiti a prescindere delle nuove e sempre più sofisticate modalità di comunicazione interpersonale.

[120] Cass. pen., sez. I, 3 ottobre 2023, n. 40033, in *deJure*, punto n. 1.6.3 del Considerato in diritto.

[121] Cass. pen., sez. I, 3 ottobre 2023, n. 40033, in *deJure*, punto n. 1.6.3 del Considerato in diritto.

[122] In argomento, con specifico riferimento alle forme di aggressione della sfera sessuale, B. PANATTONI, *Violazioni "incorporee" della sfera sessuale. Possibili evoluzioni ed insidie nell'ambito dei reati sessualmente connotati*, in *www.archiviopenale.it*, 2 dicembre 2022; G. FIORINELLI, *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Torino, 2024, in particolare 143 ss.

Come già anticipato, attualmente numerose manifestazioni dell'affettività e della sessualità si realizzano *online*. Di pari passo, però, anche le condotte illecite che coinvolgono dette sfere della persona si sono trasferite nella realtà digitale, poiché *Internet* permette di nascondere facilmente la propria identità e consente di raggiungere un numero molto più ampio di potenziali vittime, facilitandone la selezione.

La rete, in aggiunta, oltre a rendere più agevole la commissione del reato, può indurre all'azione anche persone che, in assenza delle caratteristiche dello spazio digitale non avrebbero mai manifestato un istinto predatorio[123].

La consapevolezza del legislatore in merito alla possibile realizzazione attraverso *Internet* di reati che coinvolgano direttamente e primariamente la sfera sessuale è crescente e ha già portato, nel corso del tempo, ad opportuni adeguamenti del diritto vigente alle nuove tecnologie. E' il caso, solo per fare un esempio, del delitto di *Adescamento di minorenni*, introdotto nel nostro ordinamento dalla l. 1° ottobre 2012, n. 172, in attuazione della Convenzione di Lanzarote. Ma ulteriori e plurimi espressi riferimenti all'utilizzo delle nuove tecnologie sono altresì contenuti nell'articolata disciplina in tema di pornografia minorile.

Nondimeno, persiste il problema della corretta interpretazione e applicazione di altre ipotesi di reato forgiate in tempi in cui non erano neppure immaginabili le attuali dinamiche relazionali. In particolare, ci si chiede se si possano ritenere integrati i reati di prostituzione o di violenza sessuale *online,* nonché di corruzione di minorenne allorché il concetto di "presenza" contenuto nella formulazione della norma assuma natura smaterializzata.

In merito alla possibilità di ricondurre alla nozione di prostituzione, e alle relative fattispecie previste nella l. n. 75 del 1958, anche le prestazioni sessuali a pagamento effettuate *on line* – che prescindono, dunque, da qualsiasi contatto fisico tra la persona che compie l'atto e quella che ne "fruisce" – mentre la dottrina ha espresso posizioni divergenti, la giurisprudenza parrebbe, invece, ad oggi essersi assestata su un indirizzo pressoché consolidato.

Quest'ultima, infatti, è decisamente orientata nel senso di ritenere che l'atto di prostituzione non debba necessariamente essere costituito dal contatto fisico tra i soggetti, ma possa consistere in qualsiasi atto sessuale che venga compiuto dietro pagamento di un corrispettivo e risulti finalizzato, in

[123] Sul punto, *amplius supra* capitolo primo.

via diretta ed immediata, a soddisfare la libidine di colui che ha chiesto o che è destinatario della prestazione[124].

Pertanto – venendo alla questione specifica qui oggetto di interesse – sarebbe «irrilevante il fatto che chi si prostituisce e il fruitore della prestazione si trovino in luoghi diversi, allorché gli stessi risultino collegati, tramite *Internet*, in videoconferenza», la quale consentirebbe «all'utente della prestazione, non diversamente da quanto potrebbe verificarsi nell'ipotesi di contemporanea presenza nello stesso luogo, di interagire con chi si prostituisce, in modo da poter chiedere a questo il compimento di atti determinati, che vengono effettivamente eseguiti e immediatamente percepiti da colui che ordina la prestazione sessuale a pagamento»[125].

In altre parole, sarebbe l'elemento della interazione a distinguere il fenomeno della prostituzione, anche se virtuale o a distanza, da quello della mera esibizione del proprio corpo[126].

Nondimeno, sul punto la dottrina appare a tutt'oggi divisa.

Ad avviso di alcuni Autori, infatti, l'estensione della disciplina in tema di prostituzione anche alle prestazioni di natura meramente telematica non comporterebbe alcuna violazione del divieto di analogia, posto che il nucleo concettuale della prostituzione consisterebbe «da sempre nel mercimonio della propria sessualità, e cioè nel sinallagma tra sesso ed utilità economica corrisposta in suo cambio»[127].

Sicché, «il resettaggio della fattispecie di sfruttamento della prostituzio-

[124] Cass. pen., sez. III, 22 aprile 2004, n. 25464, Rv. 228692; Cass. pen., sez. III, 21 marzo 2006, n. 15158, Rv. 233929. Siffatta impostazione è stata successivamente ribadita anche da Cass. pen., sez. un., 19 dicembre 2013, n. 16207, Rv. 258757, in relazione ad un'ipotesi di prostituzione minorile. Sennonché, anche con riguardo alla prostituzione minorile, attenta dottrina sottolinea come «gli atti sessuali incriminati dal comma 2 dell'art. 600 *bis* sono quelli che presentano una interrelazione sessuale tra due soggetti (…). Inoltre, non sembra che l'attuale versione della norma possa permettere di colpire anche gli atti "che il minore compia su se stesso" o, all'opposto, che il cliente esibizionista mostri al minore. Diversamente opinando, pur nel trasparente (e, in linea di principio, apprezzabile) intento di estendere la tutela penale del minore, si finisce per dar vita ad una incriminazione *in malam partem*» (così, B. ROMANO, *Delitti contro la sfera sessuale della persona,* Milano, 2022, 196).

[125] Così Cass. pen., sez. III, 22 aprile 2004, n. 25464, Rv. 228692. Nello stesso senso, Cass. pen., sez. III, 9 aprile 2015, n. 17394, Rv. 263358.

[126] Cass. pen., sez. III, 21 marzo 2006, n. 15158, Rv. 233929; Cass. pen., sez. III, 18 gennaio 2012, n. 7368, Rv. 252133, relativa ad un'ipotesi di prostituzione minorile.

[127] O. DI GIOVINE, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla recente giurisprudenza. Opinioni a confronto*, in *Criminalia* 2010, 363.

ne, nel momento in cui ne aggiorna il contenuto», non ne modificherebbe «la *ratio*, che continua ad essere colta nella tutela della persona e della sua libera determinazione»[128].

Tuttavia, secondo un differente indirizzo, invece, una nozione di prostituzione suscettibile di abbracciare anche le prestazioni *on line* costituirebbe una generalizzazione che non troverebbe alcun riscontro nel contesto legislativo, e risulterebbe perciò legata a un indebito ampliamento della *ratio* della disciplina[129].

Ad orientare verso questa diversa posizione deporrebbe in particolare la stessa tipologia del mezzo telematico, il quale impedisce radicalmente il compimento di atti sessuali, rendendo al massimo possibile al fruitore della prestazione a distanza intervenire sui "contenuti" della stessa[130]. Ma, in tale prospettiva, risulterebbero del tutto evidenti i potenziali rischi connessi alla riconduzione di siffatti casi al concetto di prostituzione; per tale via, infatti, si potrebbero considerare "prostituzione" anche comportamenti di *lap–dance,* di *strip–tease* «particolarmente accondiscendente (interattivo?) verso gli incitamenti del pubblico»[131], nonché, financo, le c.d. *chat lines*, le quali

[128] O. Di Giovine, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla recente giurisprudenza. Opinioni a confronto*, cit., 363.

[129] G. Carcaterra, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla recente giurisprudenza. Opinioni a confronto*, in *Criminalia* 2010, 354 ss., ad avviso del quale «l'estensione del significato di "prostituzione" al caso delle esibizioni sessuali *on line* appare (….) distante dal significato proprio e prevalente del termine, non documentata nel contesto legislativo, non coerente nei parametri di riferimento e fondata su una generalizzazione di eccessiva latitudine: cosicché rimane non vinto (….) il dubbio che si tratti di una estensione non compiuta per via di interpretazione ma di natura sostanzialmente analogica» (ivi, 355). Ritiene che la prostituzione "virtuale" costituisca un esito interpretativo giurisprudenziale *in malam partem,* altresì, A. di Martino, *Una legalità per due? Riserva di legge, legalità CEDU e giudice-fonte,* in *Criminalia* 2014, 111.

[130] R. Borgogno, *La prostituzione 'a distanza' in due recenti pronunce della giurisprudenza di legittimità*, in *Cass. pen.,* 2005, 3501. Nello stesso senso, S. Seminara, *Delitti contro la persona,* in R. Bartoli, M. Pelissero, S. Seminara, *Diritto penale. Lineamenti di parte speciale*, Torino, 2021, 188, il quale – a proposito della prostituzione minorile – ritiene che l'interpretazione giurisprudenziale secondo la quale non sarebbe necessario il contatto fisico ai fini della configurabilità dell'art. 600 *bis* c.p. «trasforma in atto prostitutivo quella che è una "esibizione" tipizzata dall'art. 600 *ter,* trascurando che nell'art. 600 *bis* il cliente "compie atti sessuali con un minore", dunque attraverso un contatto fisico».

[131] F. C. Palazzo, T*esto, contesto e sistema nell'interpretazione penalistica,* in *Studi in onore di Marinucci,* a cura di E. Dolcini, C.E. Paliero, vol. I. *Teoria del diritto penale, criminologi e politica criminale*, Milano, 2006, 532.

offrono un servizio a pagamento, fruibile senza restrizioni da chiunque vi abbia interesse e finalizzato a soddisfare la libidine del cliente mediante colloqui verbali a carattere erotico[132].

Tanto è vero che il confine tra quest'ultimo fenomeno e talune ritenute ipotesi di prostituzione da parte della giurisprudenza è labilissimo. Il riferimento è, per esempio, al caso in cui è stata ravvisata siffatta tipologia criminosa nel fatto di aver elargito ricariche telefoniche per ricevere telefonate erotiche. In tale occasione si è, infatti, precisato che «la possibilità di interagire non è esclusa dal ricorso al solo collegamento telefonico»[133].

In realtà, a sollevare ulteriori perplessità in merito ad un'estensione del concetto di prostituzione, tale da ricomprendervi le ipotesi in cui è esclusa in radice la possibilità per il cliente di compiere atti sessuali con la controparte, vi sarebbe il dato sistematico rappresentato dalla compresenza della fattispecie di cui all'art. 528 c.p. (in tema di spettacoli osceni), la cui applicazione ben potrebbe essere invocata anche nei casi esaminati[134].

Sicché, la scelta di ricondurre la cd. prostituzione *on line* nell'ambito applicativo della disciplina prevista dalla l. n. 75 del 1958 sarebbe il frutto di una scelta di politica criminale compiuta dalla giurisprudenza, che – a fronte della una ritenuta obsoloscenza della normativa vigente – conferisce rilevanza penale ad una modalità di offesa del tutto nuova, realizzata mediante la rete[135].

Sennonché è difficile sostenere che l'esercizio "a distanza" della prostituzione rivesta lo «specifico contenuto di disvalore omogeneo a quello espresso dalla fattispecie legale»[136]. L'equiparazione (analogica) della prostituzione telematica a quella tradizionale parrebbe, infatti, tradire completamente lo

[132] R. BORGOGNO, *La prostituzione 'a distanza' in due recenti pronunce della giurisprudenza di legittimità*, cit., 3501. Nello stesso senso, F. C. CATULLO, *Sullo sfruttamento della prostituzione* on line, in *Cass. pen.,* 2004, 3582, 3583.

[133] Cass. pen., sez. III, 18 gennaio 2012, n. 7368, Rv. 25133.

[134] Così N. MAZZACUVA, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla recente giurisprudenza. Opinioni a confronto*, in *Criminalia* 2010, 374. Nello stesso senso R. BORGOGNO, *La prostituzione 'a distanza' in due recenti pronunce della giurisprudenza di legittimità*, cit., 3503.

[135] A. INGRASSIA, *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine*?, in *www.penalecontemporaneo.it,* 2012, 13.

[136] F. C. PALAZZO, *Legalità penale, interpretazione ed etica del giudice,* in *Riv. it. dir., proc. pen.,* 2020, 1262.

spirito e l'originaria prospettiva assunta dalla l. n. 75 del 1978[137]. Ebbene, se il significato linguistico della parola "prostituzione" da solo non può costituire un limite, detto limite deve essere ricercato nel "tipo" criminoso quale criterio utile delimitare la naturale propensione del giudice a farsi artefice di una tutela ad ogni costo[138].

Analoghi problemi interpretativi sono emersi, nel corso del tempo, in relazione alle diverse fattispecie di violenza sessuale.

La prassi meno recente era solita ritenere necessario, ai fini della configurabilità dei reati sessuali, il coinvolgimento della corporeità della vittima come elemento tipico[139]. «Nessun criterio ermeneutico – precisava fermamente la giurisprudenza – può giustificare un'interpretazione allargata del concetto di atti sessuali (…) che prescinda dal coinvolgimento della corporeità sessuale della persona offesa»[140]. Risulterebbe, infatti, «aberrante» e «chiaramente contrastante con la giurisprudenza elaborata in materia da questa corte» il tentativo di qualificare come atti sessuali quelli che non si concretizzino in un contatto fisico diretto con il soggetto passivo, in un rapporto *corpore corpori*[141].

Sicché, si riteneva che la mancanza di contatto fisico tra le parti potesse, piuttosto, integrare un'offesa alla libertà morale quale bene giuridico tutelato dalla fattispecie di violenza privata di cui all'articolo 610 ovvero il reato di atti osceni di cui all'articolo 527, non risultando invece idonea ad compromettere la libertà di autodeterminazione sessuale[142].

[137] Così e *amplius,* F. C. PALAZZO, T*esto, contesto e sistema nell'interpretazione penalistica,* cit., 530 ss.

[138] F. C. PALAZZO, *Legalità penale, interpretazione ed etica del giudice,* cit., 1261, 1261.

[139] Cass. pen., sez. III, 28 settembre 1999, n. 2941, Rv. 215100, in *deJure,;* Cass. pen., sez., III, 15 giugno 2006, n. n. 33464, Rv. 234786. Sul punto *amplius* M. PICCARDI, *Il necessario coinvolgimento della corporeità sessuale della vittima nel reato di violenza sessuale*, in *Cass. pen.*, 2008, 3293 e ss.; M. CAPPAI, *La qualificazione delle "violenze" prive di un contatto* corpore corpori *alla prova della recente giurisprudenza in tema di atti sessuali*, in *www.penalecontemporaneo.it*, *Riv. trim.*, n. 2 del 2017, in particolare 50 ss.

[140] Cass. pen., sez. III, 28 settembre 1999, n. 2941, Rv. 215100, in *deJure,* punto n. 4 della parte argomentativa.

[141] Ancora Cass. pen., sez. III, 28 settembre 1999, n. 2941, Rv. 215100, in *deJure,* punto n. 4 della parte argomentativa.

[142] Cass. pen., sez. III, 28 settembre 1999, n. 2941, Rv. 215100, ad avviso della quale «la nozione di "atti sessuali" cui fa riferimento l'art. 609 *bis* c. p., nasce dalla semplice somma delle due nozioni di congiunzione carnale e di atti di libidine che la legislazione previgente considerava e disciplinava separatamente. Ne consegue che essa non può non comportare - così

Successivamente, però, la prassi ha cominciato ad allontanarsi da tale linea di pensiero, annoverando tra le ipotesi di abuso sessuale anche le condotte, connotate da costrizione, realizzate tuttavia in assenza di un concreto contatto corporeo. Tra queste potrebbero, per esempio, rientrare le condotte di "autoerotismo indotto", consistenti nella costrizione, da parte dell'agente nei confronti della vittima, a compiere atti sessuali su sé stessa.

A sostegno di tale indirizzo, la Cassazione ha evidenziato che un'interpretazione in senso restrittivo della locuzione di atti sessuali sarebbe incompatibile con la *ratio* di tutela degli interessi protetti. Sicché, prendendo atto che le relazioni intime interpersonali si intrattengono sempre più spesso nel *cyberspace*, ha ricondotto diverse tipologie di comportamenti nell'ambito delle condotte tipizzate dagli articoli 609 *bis* e 609 *quater*, segnatamente allorché le vittime siano minori[143].

A titolo meramente esemplificativo, è stata considerata idonea ad integrare il reato di cui all' art. 609 *quater* c.p. la condotta consistente nel richiedere ad un minorenne, nel corso di una conversazione telefonica, di compiere atti sessuali, di filmarli e di inviare immediatamente i video all'interlocutore, non distinguendosi tale fattispecie da quella del minore che compia atti sessuali durante una video–chiamata o una video–conversazione[144]. Il delitto di cui all'art. 609 *quater* c.p. – si precisa infatti – non sarebbe necessariamente caratterizzato dal contatto fisico fra l'agente e la vittima, risultando configurabile anche nel caso in cui l'uno trovi soddisfacimento sessuale dal fatto di assistere, anche per via telematica, all'esecuzione di atti sessuali di auto-

come la comportavano le due distinte nozioni preesistenti - un coinvolgimento della corporeità sessuale della persona offesa. Non possono, pertanto, qualificarsi come "atti sessuali", nel senso richiesto dalla suddetta norma incriminatrice, tutti quegli atti, i quali, pur essendo espressivi di concupiscenza sessuale, siano però inidonei (come nel caso dell'esibizionismo, dell'autoerotismo praticato in presenza di altri costretti ad assistervi o del "voyeurismo"), ad intaccare la sfera della sessualità fisica della vittima, comportando essi soltanto offesa alla libertà morale di quest'ultima o al sentimento pubblico del pudore». Nello stesso senso, Cass. pen., sez. III, 11 maggio 2011, n. 23094, Rv. 250654.

[143] Cass. pen., sez. III, 26 marzo 2013, n. 19033, Rv. 255295, ha ravvisato l'integrazione del reato nel fatto di aver contattato via *Internet* minori infra-quattordicenni, costringendole con minacce ad inviare foto e video che le ritraevano nude ed in pose oscene. In tale occasione si è, peraltro, escluso che il mezzo utilizzato per realizzare il reato dovesse ritenersi scarsamente offensivo come invece prospettato dalla linea difensiva.

[144] Cass. pen., sez. III, 30 ottobre 2018, n. 17509, in *deJure*.

erotismo da parte dell'altra, sempre che vi sia la possibilità di interagire[145].

In termini ancora più "evolutivi", in tempi relativamente recenti, si è ritenuto configurato il reato di violenza sessuale nella condotta consistente nell'invio di una serie di messaggi *Whatsapp* "allusivi e sessualmente espliciti" ad una minorenne, costringendola a scattarsi fotografie da inviare al soggetto agente, con la minaccia di pubblicare la *chat* su un altro *social network*[146].

Vale la pena sottolineare che in siffatta presa di posizione la Cassazione giunge a dilatare il significato della nozione di "atti sessuali" fino a ricondurvi non solo situazioni nelle quali non si è avuto alcun contatto fisico fra autore e vittima – come già in altre occasioni – ma anche un'ipotesi in cui né l'autore, né la vittima hanno compiuto atti materiali di natura sessuale su se stessi o su terzi, essendo state oggetto di scambio via *Whatsapp* soltanto immagini e messaggi di contenuto erotico, in un contesto di coercizione della persona offesa minorenne.

In altra occasione, è stato ritenuto integrato il reato di violenza sessuale in quanto la vittima era stata costretta a compiere atti di autoerotismo da lei stessa ripresi in un video inviato poi all'autore della condotta costrittiva. Si è, infatti, anche qui ribadito che il reato può configurarsi indipendentemente da un contatto fisico tra l'agente e la vittima allorquando venga lesa la capacità di autodeterminazione di quest'ultima per essere stata costretta, mediante violenza o minaccia, ovvero indotta, alla profanazione della sua sfera sessuale[147]. Invero, ai fini del compimento di un atto sessuale, la presenza fisica dell'agente integrerebbe un elemento «non solo non richiesto dalla *littera legis*, ma configurante una connotazione quanto meno anacronistica in una realtà quale quella attuale sempre più improntata a relazioni di natura virtuale legate all'interconnessione telematica universalmente apprestata dalla rete che consente la presenza degli interlocutori indipendentemente dalle distanze fisiche o geografiche»; sicché, «diventa un fuor d'opera esigerne la compresenza anche solo telematica al compimento dell'atto, rivolto

[145] Cass. pen., sez. III, 4 aprile 2023, n. 26809, Rv. 285060.

[146] Cass. pen., sez. III, 2 luglio 2020, n. 25266, in *deJure*. Sulla pronuncia *de qua,* L. Picotti, *La violenza sessuale via* Whats App, in *Diritto di Internet,* 2020, 685 ss.; F. Parisi, *Violenza sessuale via* Whatsapp*? L'estensione della nozione di atto sessuale in una sentenza della Cassazione*, in *Il Foro Italiano*, 2021, II, 268 ss.

[147] Cass. pen., sez. III, 18 settembre 2024, n. 5688, Rv. 287433. Sulla pronuncia *de qua* A. Piccaluga, *L'art. 609-bis c.p. dai mille volti: il caso della violenza sessuale "a distanza" e "in differita"*, in *Dir. pen. proc.*, 2025, 1041 ss.

nei confronti della sua stessa persona da parte della vittima allorquando sia accertato che il suo verificarsi, lungi dal rispondere ad una volizione spontanea del suo autore, sia l'effetto della costrizione ovvero dell'induzione posta in essere nei suoi confronti dal suo interlocutore»[148].

Sennonché, come è facile intuire, l'evaporazione dei connotati strutturali del reato di violenza sessuale, originariamente richiesti da dottrina e giurisprudenza alla stregua del vigente dettato normativo, si fa sempre più evidente. Da un lato, infatti, nella penultima pronuncia qui richiamata gli atti sessuali coartati sono stati ravvisati nel mero scambio di *selfie* e di messaggi sessualmente espliciti via *Whatsapp*. Dall'altro lato e sotto diverso aspetto, nell'ultima citata presa di posizione si sgretola anche uno dei capisaldi su cui si pareva fondata l'interpretazione "digitalmente orientata", progressivamente affermatasi negli ultimi anni, posto che nel caso affrontato difettava altresì l'immediatezza dell'interazione (sia pure telematica) tra la condotta del reo e quella della persona offesa per essere stato il video realizzato da quest'ultima senza la presenza del primo, in un momento successivo alla sua richiesta. «L'interazione tra il comportamento coercitivo dell'agente e il fatto delittuoso compiuto a seguito di esso dalla vittima – si legge nella pronuncia – non è affatto richiesto in termini di contestualità, essendo sufficiente che sussista tra la condotta intimidatoria dell'agente e l'atto sessuale ricadente sulla vittima il rapporto di causa–effetto, ben potendo quindi l'atto involgente la corporeità sessuale di quest'ultima svolgersi anche in un momento successivo, in assenza di colui che mediante la prospettazione delle nefaste conseguenze che si sarebbero verificate ove la ragazza non avesse assecondato le sue richieste, la aveva comunque compulsata ad un atto sessuale del tutto contrario alla sua volontà»[149].

La Corte, dunque, valorizza un nuovo ed ulteriore criterio evolutivo per ampliare lo spettro applicativo della norma: una volta ammessa la configurabilità del reato quando vi sia una presenza meramente virtuale delle parti, non esisterebbe alcun impedimento a riconoscere la sussistenza del reato anche quando i due soggetti non siano neppure contestualmente collegati in via telematica.

Il limite di siffatte operazioni interpretative, però, è da ravvisare nel ri-

[148] Cass. pen., sez. III, 18 settembre 2024, n. 5688, Rv. 287433, punto n. 1 del Considerato in diritto.

[149] Cass. pen., sez. III, 18 settembre 2024, n. 5688, Rv. 287433, punto n. 1 del Considerato in diritto.

schio che «di analogia in analogia» il diritto penale finisca per «estendere la sua ragnatela, anzi la sua pesante cappa di piombo»[150], in termini non corrispondenti a quanto previsto dal legislatore.

Diventa, peraltro, a questo punto davvero difficile distinguere, nei contesti nei quali la parte coinvolta sia un minore, le ipotesi di violenza sessuale da quelle di pornografia minorile. E siffatta difficoltà trapela anche dall'argomentare della giurisprudenza là dove si afferma (addirittura) che «ove l'atto involgente la corporeità del soggetto passivo, *id est* sessuale, sia compiuto sulla sua persona da un minorenne dietro la *vis* compulsiva (….) possa configurarsi altresì, in concorso con il reato ex art. 609 *bis* c.p., il delitto, in presenza dei necessari elementi costitutivi, di pornografia minorile di cui all'art. 600 *ter* c.p.»[151].

Ebbene, l'impressione che si trae è che le condivisibili istanze di tutela prevarichino il vincolo legale della tipicità del fatto costitutivo del reato, con il pericolo di equiparare, sotto la medesima pena edittale della violenza sessuale, fatti strutturalmente disomogenei, astrattamente idonei ad attingere la libertà di autodeterminazione nella sfera sessuale con modalità e gradi di offensività profondamente diversi[152]. All'inadeguatezza dell'attuale quadro normativo in materia di delitti sessuali, tuttavia, non può, rimediare la prassi applicativa.

Un monito in tale senso è stato di recente ribadito, in termini generali, anche dalla Corte costituzionale, la quale, con la sentenza n. 98 del 2021, ha ricordato che «il divieto di analogia non consente di riferire la norma incriminatrice a situazioni non ascrivibili ad alcuno dei suoi possibili significati letterali, e costituisce così un limite insuperabile rispetto alle opzioni interpretative a disposizione del giudice di fronte al testo legislativo. E ciò in quanto, nella prospettiva culturale nel cui seno è germogliato lo stesso principio di legalità in materia penale, è il testo della legge – non già la sua successiva interpretazione ad opera della giurisprudenza – che deve fornire al

[150] F. C. PALAZZO, T*esto, contesto e sistema nell'interpretazione penalistica,* cit., 534.

[151] Cass. pen., sez. III, 18 settembre 2024, n. 5688, Rv. 287433, punto n. 1 del Considerato in diritto.

[152] Critico nei confronti dell'orientamento espansivo fatto proprio dalla giurisprudenza anche V. PLANTAMURA, Internet*, sesso e minori tra rapporti virtuali e adescamento*, in *www.archivio.penale.it,* 2015, n. 1, 19, il quale formula, provocatoriamente, il seguente quesito: «Insomma, la conclusione della giurisprudenza è che costringere una persona a subire una congiunzione carnale, e costringerla, invece, ad inviare *on–line* foto/filmati osceni sarebbe ugualmente grave. Ma è veramente così? Ovviamente, no».

consociato un chiaro avvertimento circa le conseguenze sanzionatorie delle proprie condotte; sicché non è tollerabile che la sanzione possa colpirlo per fatti che il linguaggio comune non consente di ricondurre al significato letterale delle espressioni utilizzate dal legislatore»[153].

Analoghi problemi di dilatazione interpretativa si pongono in relazione alla fattispecie di corruzione di minorenne disciplinata dal primo comma dell'art. 609 *quinquies* c.p. Anche in questo caso ci si chiede se sia possibile assegnare un nuovo, più esteso, significato al concetto di "presenza" contenuto nella formulazione della norma, scollegandolo dalla fisicità della stessa, nel senso di identità di tempo e di luogo.

La giurisprudenza ha per lo più – ancora una volta – risposto affermativamente[154], ritenendo che il concetto di "presenza" possa estendersi a ricomprendere anche atti compiuti nella dimensione virtuale e non fisica. Sicché, nella nozione di atti sessuali commessi in presenza di un minore potrebbero essere inclusi, «senza far ricorso alla analogia, ma sulla base di una interpretazione della disposizione che tenga conto dei mezzi di comunicazione attualmente esistenti e delle possibilità dagli stessi offerte, anche quelli realizzati a distanza ma condivisi in tempo reale mediante mezzi di comunicazione telematica (come nel caso in esame mediante la cosiddetta "diretta" *Instagram*), posto che attraverso detti mezzi si ottiene il medesimo risultato di far assistere un minore al compimento di atti sessuali nel corso della loro realizzazione»[155]. In tale modo si realizzerebbe una situazione in tutto assimilabile a quella che si avrebbe se il soggetto passivo fosse presente fisicamente. Del resto, si aggiunge, anche le condotte realizzate a distanza, ma condivise con mezzi telematici, risultereb-

[153] Corte cost. n. 98 del 2021, punto n. 2.4 del Considerato in diritto. Sulla pronuncia *de qua,* L. RISICATO, *Argini e derive della tassatività. Una riflessione a margine della sentenza costituzionale n. 98/2021*, in *disCrimen*, 16.7.2021; C. CUPELLI, *Divieto di analogia* in malam partem *e limiti dell'interpretazione in materia penale: spunti dalla sentenza n. 98 del 2021*, in *Giur. cost.,* 2021, 1807 ss.

[154] Cass. pen., sez. III, 23 marzo 2023, n. 15261, Rv. 284492. Sulla pronuncia *de qua* M. GRANDE, *Atti sessuali condivisi con minorenne mediante* videochat*,* in *Cass. pen.,* 2023, 3141 ss. M. E. PASQUIN, *Atti sessuali in videochiamata su Instagram e "presenza" del minore: la linea di confine tra interpretazione estensiva e analogia in una recente sentenza della Cassazione in tema di corruzione di minorenne ex art. 609 quinquies, co 2 c.p.,* in *www.sistemapenale.it,* 2 maggio 2023.

[155] Cass. pen., sez. III, 23 marzo 2023, n. 15261, Rv. 284492, punto n. 3 del Considerato in diritto.

bero idonee «a pregiudicare l'interesse protetto dalla disposizione, ossia a compromettere il sereno sviluppo della sfera sessuale di soggetti minori di quattordici anni»[156].

Ad ulteriore sostegno di siffatta interpretazione del concetto di "presenza", la Cassazione richiama altresì l'orientamento in tema di ingiuria[157], ricordando come fosse stato ritenuto integrato detto reato nella sua forma aggravata dalla presenza di più persone (e non quello di diffamazione) nell'ipotesi di persona che avesse pronunciato «espressioni offensive mediante comunicazioni telematiche dirette alla persona offesa attraverso una video *chat*, alla presenza di altre persone invitate nella *chat*, in condizione di interloquire con l'offensore»[158].

Tanto premesso, è evidente come a siffatta conclusione la giurisprudenza pervenga, in realtà, alla luce di un assorbente criterio teleologico: la (ritenuta) sostanziale identità di offesa per l'interesse protetto (lo sviluppo psichico della sua sfera sessuale) che si manifesterebbe allorché il minore di quattordici anni assistesse al compimento di atti sessuali per il tramite del *medium* digitale rispetto alle ipotesi nelle quali egli sia presente fisicamente nel luogo in cui detti atti si realizzano.

Nondimeno, la formulazione letterale della norma incriminatrice in oggetto, quantomeno nella previsione del primo comma, non sembra poter abbracciare anche la trasmissione virtuale degli atti sessuali, neppure se realizzata in diretta[159].

A riprova di siffatta conclusione si ricorda come una precedente pronuncia, richiamata dalla stessa Cassazione a sostegno della propria interpretazione "evolutiva", si fosse occupata, invero, della fattispecie contemplata dal

[156] Cass. pen., sez. III, 23 marzo 2023, n. 15261, Rv. 284492, punto n. 3 del Considerato in diritto.

[157] Cass. pen., sez. V, 25 febbraio 2020, n. 10905, Rv. 278742, commentata da E. La Rosa, *Offese in* videochat. *La Corte di Cassazione si pronuncia sui rapporti tra ingiuria e diffamazione*, in *Giur. it.,* 2020, 1750 ss. In argomento v., altresì, A. Visconti, *La repressione delle offese* online *alla reputazione: tra anomia di contesto e anomia normativa,* in K. Summerer, M. L. Matheudakis, G. M. Caletti, *La nozione di contenuto illecito* online. *Fattispecie e responsabilità penale nella prospettiva europea,* Pisa, 2025, 203 ss.

[158] Cass. pen., sez. III, 23 marzo 2023, n. 15261, Rv. 284492, punto n. 3 del Considerato in diritto.

[159] Così, M. E. Pasquin, *Atti sessuali in videochiamata su* Instagram *e "presenza" del minore: la linea di confine tra interpretazione estensiva e analogia in una recente sentenza della Cassazione in tema di corruzione di minorenne ex art. 609 quinquies, co 2 c.p.,* cit..

secondo comma dell'art. 609 *quinquies*[160], la quale parrebbe effettivamente compatibile anche con modalità di realizzazione della fattispecie a distanza, ad esempio con l'utilizzo di una *webcam*, o con l'invio via *sms* di immagini e video pornografici. Viceversa, l'ipotesi descritta nel primo comma del medesimo articolo parrebbe distinguersi proprio per il fatto di richiedere la necessaria compresenza fisica dell'agente e della vittima, nel medesimo luogo e al momento del fatto.

[160] Cass. pen., sez. III, 30 ottobre 2019, n. 14210, in *deJure*.

Capitolo terzo

IL FATTO DIGITALE NELLA TEORIA DEL REATO

SOMMARIO: 1. Il fatto di reato nel contesto digitale. – 2. Il soggetto attivo del reato. – 3. I beni giuridici digitali. – 4. La natura ibrida della condotta. – 5. La smaterializzazione dell'evento e del nesso di causalità. – 6. Il poliedrico volto dell'offesa nel mondo digitale. – 7. La natura permanente dell'offesa. – 8. Complessità della rete e volontà del fatto. – 9. Il caso del *trading* algoritmico. – 10. Ubiquità del fatto e *locus commissi delicti.* – 10.1. L'accesso abusivo ad un sistema informatico. – 10.2. La diffamazione *online.*

«*Cambiare il mondo non basta. Lo facciamo comunque.*
E in larga misura questo cambiamento avviene persino senza
la nostra collaborazione. Nostro compito è anche d'interpretarlo.
E ciò, precisamente, per cambiare il cambiamento. Affinché
il mondo non continui a cambiare senza di noi. E, alla fine,
non si cambi in un mondo senza di noi».
[G. ANDERS, *L'uomo è antiquato,* vol. II, *Sulla distruzione della Vita nell'epoca della terza rivoluzione industriale,* Torino, 1992, 1]

1. *Il fatto di reato nel contesto digitale.*

Il fatto di reato assume nella realtà digitale una fisionomia originale per una pluralità di fattori.

Si tratta, infatti, di illeciti il cui elemento caratterizzante è costituito dalla diretta realizzazione o proiezione del fatto tipico in rete, con una costante osmosi – però – tra dimensione fisica e dimensione virtuale. Sicché, in buona sostanza tutti gli elementi del fatto tipico assumono tratti inediti se confrontati con quanto accade nella realtà interamente analogica.

Come è stato di recente osservato, il «primo prodotto del *Cyberspace* è il *phygital* – acronimo formato dalle parole *physical* e *digital* – che indica la fusione tra fisico e digitale. (……) Materiale e immateriale, tangibile e virtuale, non possono essere più concepiti in opposizione tra loro. (…) L'avvento del digitale ha secolarizzato l'immateriale»[1].

[1] L. VIOLANTE, *Diritto e potere nell'era digitale.* Cybersociety*,* cybercommunity*,* cyberstate*,* cyberspace*: tredici tesi,* in *Rivista di BioDiritto,* 2022, 146.

In breve: le interazioni umane nel mondo digitale assumono sempre natura ibrida[2].

2. *Il soggetto attivo del reato*

Nello spazio digitale già la fisionomia del soggetto attivo del reato presenta caratteristiche in parte inedite[3].

Innanzitutto, l'avvento delle nuove tecnologie ha condotto ad una sorta di "democratizzazione" del crimine, dal momento che non servono particolari competenze per poter sfruttare abusivamente le potenzialità del *web* (e dell'intelligenza artificiale).

Sicché, lo spettro dei profili soggettivi dei potenziali autori di reato è ora molto ampio: si va dagli adolescenti che giocano (o pensano di giocare) con i loro *computer* e altri dispositivi digitali, ai criminali estremamente pericolosi e altamente qualificati che si introducono nelle reti pubbliche e private per vari scopi *ab origine* manifestamente illeciti. Nella zona intermedia si trovano persone, dalle caratteristiche più diverse, che decidono di abusare in vario modo delle nuove tecnologie.

Non solo. La potenzialità criminogena insita nel *medium* digitale ha, addirittura, trasformato alcuni comportamenti illeciti (come, ad esempio, la diffamazione e la diffusione di materiale coperto dal diritto d'autore) in veri e propri *reati di massa*[4].

Un altro elemento peculiare messo in luce dagli studi in materia è rappresentato dalla circostanza che non di rado, le persone che presentano un comportamento criminale represso all'interno dello spazio fisico dimostrano una «propensione a commettere azioni criminali nel ciberspazio, azioni

[2] In argomento, J. R. Agustina Sanllehí, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?,* in *Estudios penales y criminológicos*, 2021, vol. 41, 705 ss.

[3] Per uno studio interdisciplinare sulle possibili caratteristiche della personalità dei criminali informatici, M. Weulen Kranenbarg, J. L. van Gelder, A. J. Barends, R. E. de Vries, *Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets,* in *Computers in Human Behavior,* 140, 2023.

[4] Così A. Ingrassia, *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine*?, in *www.penalecontemporaneo.it,* 2012, 4.

che non avrebbero commesso nel mondo reale a causa del loro *status* o della loro posizione sociale»[5].

Si introduce così il concetto di «*Identity Flexibility*», identità flessibile, inteso come un anonimato dissociativo tipico del *cyberspace*, che comporta una mancanza di deterrenza nel passaggio tra lo spazio fisico e lo spazio virtuale, con conseguente propensione alla commissione di azioni devianti[6].

Inoltre, il *cyberspace,* in quanto non luogo, prescinde dal contatto personale e fisico tra soggetti. L'autore del reato è, dunque, sempre un soggetto che agisce in qualità di utente di un sistema informatico e che utilizza la propria identità digitale. Sicché, uno dei problemi principali che coinvolge la realizzazione digitale del reato è proprio quello relativo all'esatta riconducibilità della condotta alla vera identità del soggetto attivo[7].

Gli attori che si muovono nello spazio virtuale sono, infatti, persone, ma la loro condotta è inevitabilmente filtrata da dispositivi con numeri identificativi dai quali non è sempre possibile risalire all'operatore. A questo si aggiunga la proliferazione nello spazio digitale di identità false o "rubate".

3. *I beni giuridici digitali*

Lo sviluppo delle nuove tecnologie, così come ha modificato le classiche fenomenologie criminali, del pari ha reso necessario non solo ripensare e rimodulare la tutela di alcuni beni tradizionali, declinandoli secondo le peculiarità della rete, ma anche perimetrare nuovi interessi meritevoli di tutela, frutto essi stessi dello sviluppo informatico e neppure immaginabili fino a pochi decenni fa[8]. Si pensi, solo per fare alcuni esempi e senza alcu-

[5] M. Tonellotto, *Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità*, in *Riv. vitt. crim. sic.*, vol. XVI (2022), 10.

[6] In argomento, J. Suler, *The Online Disinhibition Effect*, in *Cyberpsychology & Behavior*, 2004, Vol. VII, n. 3, 321 ss.

[7] Sul punto v. anche *supra* capitolo primo, paragrafo 3.

[8] In argomento, tra gli altri, D. Fondaroli, *La tutela penale dei «beni informatici»*, in *Diritto dell'informazione e dell'informatica*, 1996, n. 2, 291 ss.; R. Flor, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *www.archiviodpc.dirittopenaleuomo.org*, 20.9.2012; S. Scagliarini, *I diritti costituzionali nell'era di* Internet*: cittadinanza digitale, accesso alla rete e* net neutrality, in *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali,*

na pretesa di completezza, all'identità digitale, alla riservatezza informatica, alla sicurezza informatica, al diritto a non essere ingannati o condizionati sfavorevolmente dall'intelligenza artificiale.

Sennonché, il quadro degli interessi emergenti è oltremodo complesso, posto che la rivoluzione tecnologica ha messo in luce inediti profili di vulnerabilità e debolezza di taluni diritti fondamentali, e conseguentemente specifiche esigenze di tutela, ma altresì, e per converso, nuovi ambiti di libertà e di autonomia del singolo da salvaguardare rispetto all'intervento penale. Sicché, è divenuto sempre più evidente il difficile equilibrio e bilanciamento tra interessi che possono risultare contrapposti[9], dal momento che «la libertà *della* rete e la libertà *dalla* rete sembrano rincorrersi, contraddirsi, sovrapporsi»[10].

A questo si aggiunga che in relazione ai nuovi beni giuridici digitali manca ancora una precisa concettualizzazione.

Di più: gli stessi parrebbero presentare rilevanti profili di reciproca intersezione che complicano l'individuazione dell'esatta fisionomia degli stessi, anche al fine di predisporre o applicare adeguate e specifiche forme di tutela. I nuovi interessi emergenti nello spazio digitale, infatti, presentano come comune denominatore il fatto di afferire per lo più a dati. Del resto, come è stato evidenziato, la rivoluzione digitale ha portato «alla luce la natura intrinsecamente informazionale dell'identità umana»[11]. Gli individui, *disindividualizzati* e *reidentificati* «possono essere trattati come beni da vendere e acquistare sul mercato della pubblicità (….) Il nostro valore dipende dal potere di acquisto che abbiamo come membri di un gruppo di consumo, che si trova ad un solo *click* di distanza»[12].

Non deve, dunque, sorprendere che molti dei comportamenti illeciti nel-

a cura di T. Casadei, S. Pietropaoli, Milano, 2021, 3 ss.

[9] In argomento, tra gli altri, M. Lamanuzzi, *Il "lato oscuro della rete": odio e pornografia non consensuale. Ruolo e responsabilità dei gestori delle piattaforme* social *oltre la* net neutrality, in *www.lalegislazionepenale.eu,* 25.5.2021, in particolare 10 ss.

[10] A. C. Amato Mangiameli, G. Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose,* Torino, 2015, 26. In argomento, altresì, S. Rodotà, *Una costituzione per* Internet*?,* in *Politica del diritto*, n. 3, settembre 2010, 337 ss.

[11] L. Floridi, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, trad. it. a cura di M. Durante, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo,* Milano, 2017, 109

[12] L. Floridi, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, cit., 111, 112.

la nuova realtà muovano proprio da un'abusiva raccolta o indebito utilizzo, a vario titolo e con differenti finalità, di dati[13].

Il *cyberspace* ha progressivamente assunto le sembianze di un'enorme banca di dati, i quali, da un lato, integrano una componente fondamentale per la costruzione della personalità digitale dell'individuo, e, dall'altro lato, assumono un enorme valore immateriale di scambio.

Nella dimensione digitale gli utenti sono non solo i creatori e diffusori di informazioni e contenuti, ma anche la fonte inesauribile di quelli che vengono sistematicamente estrapolati da tutte le loro attività *online*, grazie a configurazioni appositamente finalizzate degli spazi, dei servizi, delle *app*[14], e che rendono possibile in tal modo la sistematica "profilazione" di chiunque vi operi[15].

Generalmente, tra il gestore della struttura informatica e gli utenti si realizza una sorta di "implicito baratto"[16]: l'utente che vuole utilizzare una piattaforma e creare uno spazio virtuale deve "consensualmente" cedere i propri dati al *provider* proprietario della suddetta piattaforma.

La facilità con cui le informazioni possono essere raccolte ed elaborate in massa e, di conseguenza, la facilità di sorveglianza e tracciamento onnipresente degli individui è direttamente proporzionale alla dipendenza della nostra società dalle infrastrutture tecnologiche.

Da qui deriva, dunque, la necessità di ridefinire il concetto di *privacy*[17], come esigenza peraltro strettamente connessa, altresì, alla tutela dell'identità digitale.

[13] Come è noto, la tecnica maggiormente utilizzata e conosciuta di aggressione è sicuramente il c.d. *phishing*, che consiste nell'invio di *e-mail* o *sms* abilmente contraffatti, che segnalano all'utente la necessità di aggiornare i propri dati per le ragioni più varie, inducendo l'utente medesimo a cliccare su un apposito *link,* che generalmente rinvia ad un sito "clone" di quello ufficiale. Sul tema, per tutti, R. FLOR, Phishing*,* identity theft*, e* identity abuse*. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 899 ss.

[14] L. PICOTTI, *Cybercrime e diritto penale,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. PARODI, V. SELLAROLI, Milano, 2020, 717.

[15] *Amplius* L. FLORIDI, *La differenza fondamentale,* eBook, Mondadori, 2025, Parte Prima, par. 1.

[16] Così E. MAESTRI, *Stupri digitali: una questione di* governance *del cyberspazio,* in *Annali online della Didattica e della Formazione Docente,* vol. 16, n. 27/2024, 32.

[17] N. J. DE LA MATA BARRANCO, *Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 197 bis CP) El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación,* en *Cudernos de poliica criminal,* n. 118, Mayo 2016, in particolare 62 ss.

Il concetto di identità digitale è entrato nel lessico del diritto positivo con il Codice dell'amministrazione digitale (d.lgs. n. 82 del 2005), il quale, all'art. 1, comma 1, lett. u *quater*), la definisce come la «rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64».

Sennonché, sarebbe erroneo limitare la tutela dell'identità digitale a quella tipizzata dal citato Codice[18]. Nella dimensione digitale, infatti, tale interesse deve essere inteso in una più ampia accezione, includendo due diversi aspetti: il diritto all'utilizzo esclusivo delle proprie generalità ed attributi nei sistemi informatici, da un lato, e il diritto alla tutela dei dati personali, intesi come le forme con cui il soggetto proietta se stesso (più o meno volontariamente) nel mondo digitale, dall'altro lato[19].

Per quanto l'interesse all'identità digitale sia sempre più frequentemente esposto a minacce arrecate con modalità variamente congegnate, non esiste una specifica fattispecie incriminatrice volta a predisporre tutela allo stesso[20]. Nel corso del tempo si è cercato di ricondurre talune tipologie criminose coinvolgenti l'identità digitale a fattispecie esistenti, utilizzando un'asserita (ancora una volta, non poco problematica) interpretazione estensiva delle stesse.

Un primo orientamento giurisprudenziale, ritenendo che questo fenomeno ledesse il diritto alla riservatezza, ha tentato di ricondurre lo stesso al reato di trattamento illecito di dati personali[21]. In tempi più recenti, le nuove

[18] C. Parodi, *I reati patrimoniali,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. Parodi, V. Sellaroli, Milano, 2020, 166.

[19] Così, G. Malgieri, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *www.penalecontemporaneo.it, Riv. trim.*, n. 2, 2015, 144.

[20] Nondimeno, il legislatore sembra aver implicitamente riconosciuto dignità di autonomo bene giuridico all'identità digitale, ma pur sempre solo nell'ambito della previsione di una circostanza aggravante. Il riferimento è alla l. n. 119 del 15 ottobre 2013 (di conversione del d.l. n. 93 del 14 agosto 2013), che ha aggiunto un nuovo comma all'art. 640 *ter* (l'attuale comma 3), il quale contempla un inasprimento sanzionatorio là dove il fatto sia commesso "con furto o indebito utilizzo dell'identità digitale". In argomento, F. Cajani, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119),* in *Cass. pen.,* 2014, 1094 ss.; M. Maraffino, *La sostituzione di persona mediante furto di identità digitale,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, in particolare 319 ss.

[21] Tra le altre, Cass. pen., sez. III, 17 novembre 2004, n. 5728, che, tuttavia, non ha condi-

forme di aggressione dell'identità digitale sono state, per lo più, ricondotte alla fattispecie di sostituzione di persona di cui all'art. 494 c.p.[22].

Tanto premesso, occorre altresì rilevare come i citati dati personali con cui il soggetto proietta se stesso nel mondo digitale, che danno corpo all'identità digitale, costituiscono altresì l'oggetto, come anticipato, di un altro importante interesse meritevole di protezione. Il riferimento è alla riservatezza informatica[23].

Originariamente, si riteneva che tale interesse dovesse essere inteso come mera proiezione digitale della tutela del domicilio. In realtà, esso assume una sua propria autonomia[24], non foss'altro perché in ambito digitale non esistono luoghi fisici e confini che possano riflettere il carattere riservato delle attività che ivi si svolgano. Infatti, se il concetto di domicilio, prima della rivoluzione tecnologia, era chiaramente identificabile in un ambito territoriale definito, di esclusiva pertinenza di un titolare, viceversa, oggi, ogni volta che una persona si connette a *Internet*, i muri fisici scompaiono.

Non solo: lo schermo davanti a noi è in realtà «una finestra spalancata sulle nostre vite *online*», e il «monitor e sta monitorando proprio noi»[25]. L'esigenza di riservatezza si è, dunque, evoluta, posto che occorre tutelare

viso la posizione dei giudici di merito, escludendo dunque la rilevanza penale del fatto. Il caso affrontato riguardava la condotta di un uomo che, senza il consenso dell'interessata ed al fine di procurarle un danno, aveva comunicato i dati personali di una giocatrice della nazionale di pallacanestro (generalità, indirizzo, recapiti telefonici e di posta elettronica, numero di codice fiscale) a soggetti terzi, aprendo a suo nome un sito internet ed iscrivendola ad un sito di messaggeria erotica. Per alcune osservazioni critiche sulla pronuncia *de qua*, I. SALVADORI, *Il trattamento senza consenso di dati personali altrui reperibili su* Internet *costituisce reato?,* in *Dir. pen. proc.,* 2006, 467 ss.

[22] Tra le altre, Cass. pen., sez. V, 14 ottobre 2021, n. 323, Rv. 282768; Cass. pen., sez. V, 13 luglio 2020, n. 5215, Rv. 279450; Cass. pen., sez. V, 6 luglio 2000, n. 22049, Rv. 279358; Cass. pen., sez. V, 23 aprile 2014, n. 25774, Rv. 259303; Cass. pen., sez. V, 28 novembre 2012, n.18826, Rv. 255086, con nota di E. MENGONI, *Chattare con un* nickname *riconducibile ad altri (e comunicare il loro numero telefonico) integra il reato di sostituzione di persona*, in *Cass. pen.*, 2014, 148 ss. In argomento, altresì, C. FLICK, *Falsa identità su* internet *e tutela penale della fede pubblica degli utenti e della persona,* in *Diritto dell'informazione e dell'informatica,* 2008, 526 ss.

[23] Per tutti, P. VENEZIANI, *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in *Ind. pen*., 2000, 139 ss.

[24] Sul punto, *amplius* e per tutti, I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in *Tutela penale della persona e nuove tecnologie*, a cura di L. PICOTTI, Padova, 2013, in particolare 149 ss.

[25] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, cit., 125.

la spazio digitale privato (anche) rispetto al rischio di una esposizione continua e onnipresente. Sicché, dalla tutela della *privacy* in termini per così dire statici, si è passati ad un'esigenza di protezione dinamica dei dati personali.

Il concetto di riservatezza informatica si sta, dunque, progressivamente arricchendo di ulteriori contenuti, assumendo la natura di «interesse al godimento e controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento»[26].

Tant'è che talora si preferisce parlare, anziché di riservatezza informatica, di autodeterminazione informativa, mutuando in tal modo un concetto già emerso nel diritto penale tedesco[27]. Si tratterebbe del diritto che conferisce ad ogni persona «il potere di determinare, in sé, la divulgazione e l'utilizzo dei suoi dati personali, ampliando la tutela della libertà della vita privata in termini di diritti fondamentali»[28].

Emerge, dunque, il concetto di *habeas data* inteso come moderno sviluppo dell'*habeas corpus*[29]. In altre parole, il diritto individuale che dovrebbe essere riconosciuto e tutelato nello spazio digitale presenterebbe diverse articolazioni, concretizzandosi nella possibilità di mantenere il controllo dei frammenti della personalità, «di consentire consapevolmente che altri ne facciano un uso conforme alla nostra volontà, di opporci ai trattamenti indesiderati, di poter cancellare le tracce digitali che riteniamo non ci rappresentino più correttamente o che semplicemente desideriamo mantenere nascoste a tutti o ad alcuni, di avere la garanzia che dalla riaggregazione dei frammenti non emerga una rappresentazione falsa o distorta della nostra identità o della nostra personalità[30]».

[26] Così, L. Picotti, *Reati informatici*, in *Enc. giur. Treccani*, XXIX, Roma, 1993, 21.

[27] Si tratta del *Recht auf informationelle Selbstbestimmung*. Per la definizione giurisprudenziale di «autodeterminazione informativa», cfr. BdVerfG, sent. 27.2.2008, 370/07 – 595/07. Sul punto cfr. R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung,* in *Riv. trim. dir. pen. econ.,* 2009, 705.

[28] Così R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung,* cit., 702, riprendendo le parole della Corte costituzionale tedesca.

[29] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli,* Bari, 2014, 30 ss.; G. Scotti, *Dall'*habeas corpus *all'*habeas data*: il diritto all'oblio e il diritto all'anonimato nella loro dimensione costituzionale*, in *Diritto.it*, 7 settembre 2015, 1 ss.

[30] M. R. Allegri, Ubi social, ibi ius*. Fondamenti costituzionali dei social networkeprofili giuridici della responsabilità dei provider,* Milano, 2018, 76.

Strettamente collegato ai predetti interessi è, come facile intuire, anche il bene della sicurezza informatica[31], la quale assurge a funzione di garanzia preventiva di tutti gli altri diritti che si possono esercitare nella dimensione digitale[32].

La sicurezza informatica, peraltro, non riguarda solo i singoli utenti ma coinvolge anche la sicurezza nazionale, vale a dire la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche dal cui malfunzionamento, interruzione o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale[33].

La sicurezza dello spazio cibernetico ha raggiunto una connotazione strategica assolutamente comparabile a quella della protezione dello spazio fisico[34]. Basti pensare alle possibili devastanti ripercussioni che potrebbero avere attacchi cibernetici sferrati nei confronti dei sistemi di fornitura energetica di un paese, dei sistemi di controllo del traffico aereo, di strutture finanziarie, di banche dati delle più diversa natura.

Del resto, il *cyberspace* non è stato «disegnato o ingegnerizzato per essere un posto sicuro ma, al contrario, per trasmettere informazioni. Da ciò ne consegue un deficit intrinseco di sicurezza, che lo rende un ambiente a "offesa persistente". Se, infatti, le interconnessioni sono di grande utilità in tempo di pace, in tempo di guerra "interconnettività" significa che tutto ciò che ha un'interfaccia in *Internet* può divenire oggetto di aggressione da qualsiasi parte del mondo»[35].

[31] Per tutti, L. PICOTTI, *Sicurezza informatica e diritto penale*, in *Sicurezza e diritto penale*, a cura di M. DONINI, M. PAVARINI, Bologna, 2011, 217 ss.

[32] Sul tema, S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli,* cit.

[33] In argomento *amplius* R. BRIGHI, P. G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* in *www.federalismi.it.,* n. 21, 8.9.2021.

[34] In argomento, *amplius,* R. ZAMPETTI, *Sicurezza nazionale e spazio cibernetico. Una minaccia "invisibile" nell'era digitale,* in *Istituto di Ricerche Internazionali Archivio Disarmo,* n. 1/2015, gennaio 2015, 3 ss.

[35] F. VIGNERI, *Brevi considerazioni sulla natura e sulle caratteristiche dello spazio cibernetico*, in *SalvisJuribus*, 10.10.2019, par. V, disponibile al link: *http://www.salvisjuribus.it/brevi-considerazioni-sulla-natura-e-sulle-caratteristiche-dello-spazio-cibernetico/*

4. *La natura ibrida della condotta*

Anche la condotta suscettibile di integrare gran pare dei reati digitalmente connotati presenta caratteristiche un tempo non immaginabili.

Innanzitutto, si tratta, come anticipato, di condotte realizzate attraverso l'utilizzo di strumenti tecnologici e/o nell'ambito di una realtà virtuale. Sicché, l'integrazione del reato non è frutto della sola azione umana materialmente intesa, vale a dire quella dell'operatore che agisce dinanzi al dispositivo digitando dati. Siffatta azione costituisce, infatti, solo un segmento che si salda con una trasformazione automatica di quella medesima condotta.

In altre parole, i comportamenti digitali, sebbene abbiano un'origine fisica in un'azione-decisione umana (che si traduce in quello che un tempo si poteva definire *click*), producono risultati solo attraverso l'elaborazione, la manipolazione e l'archiviazione di dati informatici[36].

Si pensi ancora una volta, per esemplificare, alla fattispecie di accesso abusivo ad un sistema informatico, la cui condotta tipica è, come detto, inevitabilmente veicolata dal sistema informatico[37]. Sicché, il fatto di "accesso", che nella realtà materiale evoca il comportamento di chi fisicamente oltrepassa uno spazio delimitato, va in realtà reinterpretato. In altre parole, nella dimensione digitale, l'accesso non coincide puramente e semplicemente con collegamento fisico, ovvero l'accensione del *computer* che viene utilizzato per commettere il reato e l'invio delle credenziali, bensì con quello logico, ovvero con il superamento della barriera di protezione del sistema, che renda possibile il dialogo con il medesimo, in modo tale che l'agente venga poi a trovarsi nella condizione di conoscere dati, informazioni e programmi[38].

Di siffatta metamorfosi della condotta digitale ha da tempo preso atto anche la prassi applicativa, nella misura in cui si riconosce che «la condotta illecita commessa in un ambiente informatico o telematico assume delle specifiche peculiarità per cui la tradizionale nozione – elaborata per una realtà fisica nella quale le conseguenze sono percepibili e verificabili con immedia-

[36] *Amplius* L. Picotti, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 2011, 842, 843.

[37] *Amplius* L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 46.

[38] Cass. pen., sez. V, 8 luglio 2008, n. 37322, Rv. 241201.

tezza – deve essere rivisitata e adeguata alla dimensione virtuale. In altre parole, il concetto di azione penalmente rilevante subisce nella realtà virtuale una accentuata modificazione fino a sfumare in impulsi elettronici; *l'input* rivolto al computer da un atto umano consapevole e volontario si traduce in un trasferimento sotto forma di energie o *bit* della volontà dall'operatore all'elaboratore elettronico, il quale procede automaticamente alle operazioni di codificazione, di decodificazione, di trattamento, di trasmissione o di memorizzazione di informazioni. L'azione telematica viene realizzata attraverso una connessione tra sistemi informatici distanti tra loro, cosicché gli effetti della condotta possono esplicarsi in un luogo diverso da quello in cui l'agente si trova; inoltre, l'operatore, sfruttando le reti di trasporto delle informazioni, è in grado di interagire contemporaneamente sia sul *computer* di partenza sia su quello di destinazione»[39].

Dunque, il concetto penalistico di "azione" non può più essere inteso nell'originaria accezione puramente naturalistica e causale, legata esclusivamente al movimento corporeo dell'uomo capace di modificare il mondo esterno, ma deve tenere conto dell'apporto delle nuove tecnologie, che in misura sempre più rilevante giungono a supportare ed anche a sostituire atti significativi dell'uomo, produttivi di effetti giuridicamente rilevanti[40].

Si pensi ai pericolosi *malware*, che, una volta "attivati", producono autonomamente loro effetti pregiudizievoli, peraltro difficilmente arrestabili, in un brevissimo arco temporale, colpendo, spesso in modo indiscriminato, gli utenti connessi alla rete[41]. Un esempio a tutti noto è quello dei programmi (c.d. *redirector*) che reindirizzano il traffico *Internet* del sistema informatico infettato verso pagine *web* apparentemente uguali a quelle che l'utente avrebbe voluto consultare (*Home banking*, siti di *e–commerce*, ecc.). Sennonché, nel momento in cui l'utente digita i suoi dati personali sul sito "clonato" essi vengono automaticamente salvati sul *server* che lo ospita e al quale accedono i criminali informatici[42].

Nella realtà digitale il *medium* informatico funge, dunque, da ponte tra

[39] Cass. pen., sez. un., 26 marzo 2015, n. 17325, Rv. 263020, punto n. 3 del Considerato in diritto.

[40] L. PICOTTI, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi?,* in *www.sistemapenale.it,* 31 luglio 2024, 4. Analogamente, I. SALVADORI, *Il diritto penale dei software "a duplice uso",* in *Quaderno della Facoltà di Giurisprudenza di Trento,* 2017, 422 ss.

[41] I. SALVADORI, *Il diritto penale dei software "a duplice uso",* cit., 422.

[42] Ancora I. SALVADORI, *Il diritto penale dei software "a duplice uso",* cit., 423.

la tra il mondo fisico e la realtà virtuale. Sicché, bisogna valutare con cura in che modo la dimensione tecnica e i processi di automazione incidano sul significato giuridico dell'azione[43].

In alcuni casi può addirittura essere difficile individuare la consistenza della condotta fisica e separarla dalla componente tecnologica. Si pensi al problema che si può porre – e si poneva in particolare prima dell'avvenuta riforma dell'art. 600 *quater* c.p. che attribuisce oggi rilievo anche alla condotta del mero accesso[44] – in relazione alla condotta di detenzione di materiale pedopornografico. Ci si chiedeva, infatti, se il rinvenimento di immagini pedopornografiche registrate automaticamente ed involontariamente nella memoria del *computer* durante la navigazione e la visita ad un sito potesse integrare una condotta di detenzione.

Ebbene, la giurisprudenza sul punto ha per lo più ritenuto non sussistente un possesso penalmente rilevante di *files* scaricati automaticamente sul computer per mancanza del richiesto elemento soggettivo doloso[45]. Ma forse, alla medesima conclusione si sarebbe potuti giungere argomentando sull'impossibilità di riferire il segmento automatizzato (e, dunque, inconsapevole) della condotta al soggetto agente già sul piano oggettivo.

Nella dimensione digitale, inoltre, è possibile impostare la detemporalizzazione delle azioni, nel senso che attraverso gli strumenti tecnologici si possono programmare e automatizzare operazioni che, poi, non richiedono più l'intervento diretto e immediato dell'uomo. Si pensi all'utilizzo di codici informatici progettati per attivare automaticamente condotte illecite al verificarsi di condizioni predefinite. In tali contesti, il soggetto agente non partecipa direttamente alla fase esecutiva del reato: egli si limita a predisporre il programma in anticipo, impostando le variabili che ne determineranno l'attivazione, con margini di tracciabilità estremamente ridotti.

[43] *Amplius* T. Pietrella, *Reati informatici e concorso di norme: l'evoluzione tecnologica informa il diritto penale,* in *disCrimen* 2.12.2021, in particolare 15 ss.

[44] Sul tema *amplius* P. Caroli, *Quando guardare è un reato. Accesso intenzionale a materiale pedopornografico e novità in materia di reati sessuali nei confronti di minori,* in *Dir. pen. proc.,* 2022, 973 ss.

[45] Cass. pen., sez. III, 16 ottobre 2008, n. 3194, in *deJure.*

5. *La smaterializzazione dell'evento e del nesso di causalità*

Tanto premesso, è facile intuire come anche l'accezione naturalistica di evento subisca nel mondo digitale una metamorfosi, in considerazione della natura per lo più immateriale e frequentemente ubiquitaria dello stesso[46]. Si pensi alla diffusione di determinati contenuti riservati o offensivi, che possono essere resi disponibili simultaneamente ad una pluralità di utenti, in diverse parti del mondo, nonché, come già anticipato, alla diffusione di *virus* malevoli capaci di compromettere contemporaneamente infrastrutture dislocate in differenti località.

Conseguentemente, un ulteriore aspetto meritevole di attenzione è rappresentato dalla possibile evoluzione delle dinamiche causali nella dimensione digitale. Occorre, infatti, comprendere i presupposti ed i limiti in relazione ai quali può dirsi esercitato e mantenuto, ai fini della responsabilità penale, il "dominio" dell'agente su tutti i risultati che conseguono da una determinata condotta.

Innanzitutto, può essere utile ricordare come, se in alcuni casi l'effetto del reato digitale si materializza anche nella realtà *offline*, in altre ipotesi, viceversa, detto effetto può esaurirsi interamente all'interno del *cyberspace* e non integrare una conseguenza naturalistica della condotta[47]. L'evento in altre parole può assumere una natura squisitamente tecnologica[48].

In entrambi i casi, tuttavia, il nesso di causalità non presenta una natura meramente e interamente fisica, ma anche logica, presupponendo – come detto – un processo di elaborazione delle informazioni che producono il risultato immateriale.

Sicché, la ricostruzione del rapporto causativo di un evento lesivo, sempre complessa anche in relazione alle tradizionali dinamiche criminose della realtà materiale, si complica ulteriormente in presenza di un'interazione necessaria tra condotta umana e sistema tecnologico. A questo si aggiun-

[46] In argomento L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee,* in *Riv. trim. dir. pen. econ.,* 2011, 841.

[47] *Amplius* L. PICOTTI, Cybercrime *e diritto penale,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. PARODI, V. SELLAROLI, Milano, 2020, 721.

[48] In tal senso L. PICOTTI, Cybercrime *e diritto penale,* cit. 721, ad avviso del quale nei reati commessi nel *cyberspace* «l'evento stesso, consumativo del reato (…) può presentarsi altresì di natura esclusivamente tecnologica, come nel caso di interferenze e danneggiamenti informatici pur solo funzionali, che riguardino sistemi, programmi o dati».

ga – è facile intuirlo – la variabile collegata alla crescente autonomia degli algoritmi di intelligenza artificiale, che sempre più frequentemente porrà la sfida di discernere tra azioni ed omissioni umane e fattori strettamente tecnologici[49].

Con l'espressione *black box,* da tempo invalsa tra gli addetti ai lavori, si vuole infatti proprio indicare quel fenomeno per il quale è possibile individuare *input* e *output* all'interno di un sistema, ma non è invece possibile ricostruire cosa accade all'interno della scatola nera, ovverosia la catena causale che ha determinato il passaggio dagli *input* agli *output*[50].

A queste peculiarità si aggiunga che, nella gamma delle possibili cause di un evento possono rientrare anche fattori esterni rispetto alla naturale interazione uomo-sistema digitale, afferenti, per esempio, all'infrastruttura tecnologica che rende possibile il funzionamento del sistema medesimo[51].

Sicché, un'ulteriore sfida posta dal reato cibernetico consisterà nel comprendere se, ed eventualmente in presenza di quali presupposti, sia possibile immaginare un'interruzione del nesso eziologico dovuta ad un coefficiente interamente tecnico.

6. *Il poliedrico volto dell'offesa nel mondo digitale*

L'offesa nello spazio digitale sollecita riflessioni apparentemente contraddittorie.

Da un lato, infatti, si è portati a ritenere che il peculiare *medium* in oggetto sia generalmente in grado di comportare una diffusività (e in taluni casi, permanenza[52]) delle conseguenze pregiudizievoli sconosciuta ai fatti realizzati nella dimensione materiale, anche in considerazione – almeno in taluni casi – del contributo offerto dal funzionamento algoritmico delle realtà virtuali.

Dall'altro lato, però, è altresì necessario riflettere sulla circostanza che

[49] In argomento, L. D'Amico, *La misura della (im)prevedibilità. Modelli d'imputazione della responsabilità al tempo dell'intelligenza artificiale*, Napoli, 2025, in particolare 40 ss.

[50] Sul punto, B. Fragasso, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, Torino, 2025, 56 ss.

[51] B. Fragasso, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., 63.

[52] Sul punto specifico v. *infra* paragrafo 7.

un medesimo comportamento potrebbe essere percepito diversamente dalla collettività a seconda che esso sia realizzato nella dimensione digitale o, piuttosto, analogica; e questo in forza della normalizzazione di talune modalità di agire "tossiche" proprie dell'*online*[53].

Il riferimento è, per esempio, alla frequente condivisione di immagini pornografiche, nonché – sotto diverso profilo – alla diffusione tra gli utenti del *web* – specie su *blog*, *forum, social network* – di un registro linguistico alternativo, spesso contraddistinto da basso livello culturale e da espressioni forti, virulente e offensive[54].

In altre parole, occorre considerare che nello spazio digitale può risultare più difficile qualificare come illeciti taluni comportamenti che potrebbero "confondersi" con nuove forme comunicative socialmente tollerate.

Si pensi emblematicamente al fenomeno del c.d. *sexting*. La straordinaria capacità dello strumento telematico di restituire l'illusione della vicinanza fisica replicandone, in parte, le dinamiche, è la ragione del successo e della diffusione del *sexting* nel tessuto sociale[55].

Sennonché, il *sexting* – come è noto – può assumere le vesti della pedopornografia, allorché le immagini realizzate e condivise coinvolgano minori. Tuttavia, a fronte di siffatto comportamento, frequentissimo tra i giovani, occorre ritagliare con precisione chirurgica, da un lato, le condotte effettivamente riconducibili alle gravissime fattispecie predisposte dal nostro ordinamento per contrastare l'aberrate sfruttamento sessuale dei minori e, dall'altro lato, le condotte che, viceversa, costituiscono solo nuove forme comunicative e relazionali diffuse nella società contemporanea, segnatamente tra i giovani della c.d. Generazione Z.

Tanto che, proprio in relazione a queste ultime tipologie comportamentali (la c.d. pornografia domestica), «al fine di evitare "ipercriminalizza-

[53] Su questi aspetti, T. PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante* online *nel reato di diffamazione*, in *www.sistemapenale,it,* ottobre 2023, in particolare 17 ss.

[54] T. PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante* online *nel reato di diffamazione*, cit., 19. Analogamente, M. LAMANUZZI, *Il "lato oscuro della rete": odio e pornografia non consensuale. Ruolo e responsabilità dei gestori delle piattaforme* social *oltre la* net neutrality, cit., in particolare 6 ss.

[55] Così G. BEGUINOT, *I reati contro la sfera sessuale della persona al tempo di* internet*, tra criticità tradizionali ed esigenze di prevenzione*, in *Riv. it. dir. proc. pen.*, 2023, 1005.

zioni" non coerenti con le finalità proprie del diritto penale»[56], anche alla luce di quanto previsto dalle fonti internazionali e sovranazionali[57], si ritiene che debba essere valorizzato «il dato dell'appartenenza di tali condotte all'ambito "dell'autonomia privata sessuale"»[58]. Sicché, si dovrebbero distinguere le «condotte di produzione aventi un carattere abusivo, per la posizione di supremazia rivestita dal soggetto agente nei confronti del minore o per modalità con le quali il materiale pornografico viene prodotto (ad esempio, minaccia, violenza, inganno) o per il fine commerciale che sottende la produzione, o per l'età dei minori coinvolti, qualora questa sia inferiore a quella del consenso sessuale», dalle ipotesi in cui le immagini o i video abbiano, invece, «per oggetto la vita privata sessuale nell'ambito di un rapporto che, valutate le circostanze del caso, non sia ca-

[56] Cass. pen., sez. un., 31 maggio 2018, n. 51815, Rv. 274087, punto n. 4.1.1 del Considerato in diritto.

[57] L'art. 3, comma 2, della Decisione Quadro del Consiglio n. 2004/68/GAI del 22 dicembre 2003 (relativa alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile) così dispone: «2. Uno Stato membro può prevedere che esulino dalla responsabilità penale le condotte connesse con la pornografia infantile: (...) b) di cui all'articolo 1, lettera b), punti i) e ii), in cui, trattandosi di produzione e possesso, immagini di bambini che abbiano raggiunto l'età del consenso sessuale siano prodotte e detenute con il loro consenso e unicamente a loro uso privato. Anche nei casi in cui sia stata stabilita l'esistenza del consenso, questo non può essere considerato valido se, ad esempio, l'autore del reato l'ha ottenuto avvalendosi della sua superiorità in termini di età, maturità, stato sociale, posizione, esperienza, ovvero abusando dello stato di dipendenza della vittima dall'autore». Analoghe previsioni sono contenute nell'articolo 20, comma 3, della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e gli abusi sessuali del 25 ottobre 2012 (c.d. Convenzione di Lanzarote), là dove si prevede che ogni Parte potrà riservarsi il diritto di escludere la rilevanza penale della produzione e del possesso di materiale pornografico in cui siano coinvolti minori che abbiano raggiunto l'età del consenso sessuale, «quando tali immagini sono prodotte o detenute da questi ultimi con il loro consenso e unicamente a loro uso privato». Sulla stessa linea si colloca la Direttiva dell'Unione europea 2011/93 (UE) contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che ha sostituito la precedente Decisione Quadro del Consiglio n. 2004/68/GAI , la quale, all'art. 8, comma 3, attribuisce alla discrezionalità degli Stati membri decidere se attribuire o meno rilevanza penale alla «produzione, all'acquisto o al possesso di materiale pedopornografico in cui sono coinvolti minori che abbiano raggiunto l'età del consenso sessuale nei casi in cui tale materiale è prodotto e posseduto con il consenso di tali minori e unicamente a uso privato delle persone coinvolte, purché l'atto non implichi alcun abuso».

[58] Cass. pen., sez. un., 31 maggio 2018, n. 51815, Rv. 274087, punto n. 4.1.1. del Considerato in diritto. Sulla pronuncia *de qua*, L. Picotti, *La pedopornografia nel* Cyberspace*: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa,* in *Diritto di Internet,* 2019, n. 1, 187 ss.

ratterizzato da condizionamenti derivanti dalla posizione dell'autore, ma siano frutto di una libera scelta – come avviene, per esempio, nell'ambito di una relazione paritaria tra minorenni ultraquattordicenni – e siano destinate ad un uso strettamente privato»[59].

7. *La natura permanente dell'offesa*

Tra i comportamenti più frequentemente realizzati nello spazio digitale rientrano senza dubbio quelli di caricamento e di diffusione di contenuti della più varia natura, molti dei quali si sostanziano in diversificate forme di espressione del diritto alla libera manifestazione del pensiero. Nondimeno, in alcuni casi, dette manifestazioni del pensiero possono altresì comportare il pregiudizio di altri interessi, parimenti rilevanti, integrando ipotesi di reato (c.d. *content related offences*).

La nuova dimensione digitale, peraltro, ha comportato una profonda ridefinizione delle modalità comunicative, oltre che ad un ripensamento del concetto di "spazio pubblico"[60]: il ciberspazio, infatti, si presenta come uno luogo «privo di confini, accessibile a tutti, con grandi potenzialità diffusive e sfuggente ai condizionamenti che tradizionalmente hanno vincolato od incanalato le relazioni sociali e politiche»[61]. La stessa giurisprudenza ha recentemente definito il *cyberspace* come una "piazza telematica" aperta, idonea a diffondere tutto quanto gli utenti vi versino[62].

Siffatto peculiare scenario, sia pure portatore di inedite opportunità, ha creato anche nuovi spazi di vulnerabilità e inedite forme di violazione dei diritti. Basti pensare alla circostanza che le condotte realizzate nel *cyberspace*, come anticipato, si caratterizzano, tra le altre cose, per la loro attitudine a determinare una permanenza dell'offesa arrecata; infatti, un contenuto

[59] Cass. pen., sez. un., 31 maggio 2018, n. 51815, Rv. 274087, punto n. 4.1.2. del Considerato in diritto.

[60] Sul tema, per tutti, A. Spena, *La parola(-)odio. Sovraesposizione, criminalizzazione e interpretazione dello* hate speech*,* in *Criminalia* 2016, 577 ss.

[61] Così, B. Panattoni, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel* Cyberspace*,* in *www.sistemapenale.it,* 22.5.2020, 306.

[62] Cass. pen., sez. un., 31 maggio 2018, n. 51815, Rv. 274087, punto n. 2.4.2 del Considerato in diritto. Sulla pronuncia *de qua* L. Picotti, *La pedopornografia nel* Cyberspace*: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa,* cit., 177 ss.

lesivo, una volta immesso nello spazio *online,* può diffondersi in modo incontrollabile e restare accessibile per anni. Senza trascurare che gli effetti della condotta dell'agente si possono protrarre nel *cyberspace* in modo non più (o non più interamente) dominabile dal soggetto[63].

Il problema si è posto in termini particolarmente evidenti in relazione al reato di diffamazione.

Come osservato anche dalla giurisprudenza, le condotte di diffamazione sono state facilitate dalla possibilità di un numero esponenziale di fruitori della rete *internet* di esprimere giudizi su tutti gli argomenti trattati, per cui alla «schiera di "opinionisti social" spesso si associano i cosiddetti "odiatori sul *web*", che non esitano – spesso dietro l'anonimato – ad esprimere giudizi con eloquio volgare e offensivo»[64].

Al contempo, una volta che i contenuti diffamatori siano stati immessi in rete, essi iniziano circolare e a diffondersi con una velocità sconosciuta agli altri *media,* divenendo fruibili da parte di un numero indeterminato di persone e per un tempo potenzialmente illimitato (c.d. eternità mediatica)[65].

Si tratta dunque di comprendere se sia possibile, ed eventualmente in quale forma, attribuire autonomo rilievo giuridico al periodo successivo a quello in cui il contenuto illecito viene caricato nel *cyberspace*, rimanendo tuttavia accessibile e produttivo di effetti lesivi.

Siffatta questione è stata affrontata dalla prassi applicativa soprattutto al fine di verificare se, per tale via, vi sia la possibilità di configurare un'eventuale responsabilità in capo al *provider* che ometta di rimuovere i predetti contenuti illeciti presenti sugli spazi dallo stesso gestiti[66].

Infatti, la ricostruzione che consentirebbe di configurare una responsabilità, a titolo di concorso nel reato, per la mancata rimozione dei contenuti diffamatori, richiede che venga compresa all'interno dei confini del fatto tipico anche la fase di perdurante disponibilità dei contenuti medesimi sul *web*. Da tale impostazione, infatti, deriverebbe l'effetto di non considerare il reato di diffamazione *online* sostanzialmente "esaurito" con il solo caricamento (e prima conoscenza da parte di una pluralità di destinatari) dell'informazione in rete.

[63] In argomento v, anche *supra* capitolo primo, paragrafo 3.

[64] Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, punto n. 2.1 del Considerato in diritto.

[65] In argomento v. anche *supra* capitolo primo, paragrafo 3.

[66] Sul punto v. *amplius infra* capitolo quarto.

Ebbene, muovendo da tale dato di partenza, si è ritenuto che con la condotta di mantenimento del contenuto illecito, successiva all'acquisizione dell'effettiva sua conoscenza, il gestore di un sito *Internet,* di fatto, farebbe proprio quello stesso contenuto e si renderebbe anch'egli colpevole del reato di diffamazione[67].

Infatti – si legge in una recente pronuncia della Cassazione – la non tempestiva attivazione da parte del gestore al fine di rimuovere i commenti offensivi pubblicati da soggetti terzi equivarrebbe, non al mancato impedimento dell'evento diffamatorio (rilevante ex art. 40, secondo comma, c.p.), bensì alla consapevole condivisione del contenuto lesivo dell'altrui reputazione, con ulteriore replica della offensività dei contenuti medesimi[68]. Sicché – si prosegue – per superare le perplessità da più parti manifestate sulla configurabilità di una responsabilità in concorso ex artt. 40 e 110 c.p. del *blogger*, si potrebbe «fare ricorso alla figura della pluralità di reati, integrati dalla ripetuta trasmissione del dato denigratorio. In altri termini, se – come è accaduto nella specie – il gestore del sito apprende che sono stati pubblicati da terzi contenuti obiettivamente denigratori e non si attiva tempestivamente a rimuovere tali contenuti, finisce per farli propri e quindi per porre in essere ulteriori condotte di diffamazione, che si sostanziano nell'aver consentito, proprio utilizzando il suo *web-log*, l'ulteriore divulgazione delle stesse notizie diffamatorie»[69].

Invero, siffatta ricostruzione giurisprudenziale solleva non pochi dubbi, non foss'altro perché risulta difficoltoso individuare, a livello fenomenologico, nel caso di specie, diverse condotte, posto che la continua trasmissione dei dati è riconducibile solamente all'azione dei *software* che contribuiscono al funzionamento tecnico della rete[70]. In altre parole, «tutto ciò che succede dopo l'"azione" della «messa a disposizione» (la digitalizzazione

[67] Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, punto 4.3 del Considerato in diritto.

[68] Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, punto n. 3.3.b del Considerato in diritto. Sulla pronuncia *de qua* C. PAGELLA, *La Cassazione sulla responsabilità del* blogger *per contenuti diffamatori (commenti) pubblicati da terzi,* in *www.penalecontemporaneo.it,* 17 maggio 2019.

[69] Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, punto n. 4.3 del Considerato in diritto.

[70] Così, B. PANATTONI, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel Cyberspace*, cit., 316.

del contenuto e il "*click*") è (…) riconducibile ad una automatica, automatizzata (nonché autonoma) azione dei sistemi informatici che costituiscono il *Cyberspace*»[71].

Una diversa ipotesi interpretativa configura, invece, l'illecito che avviene su *Internet* quale reato permanente[72], in considerazione della protratta ritrasmissione del dato[73]. Siffatta ricostruzione comporterebbe la possibilità di configurare un'autonoma responsabilità anche del *provider* in capo al quale sussisterebbe un obbligo giuridico, non di evitare l'evento in senso stretto, ma di eliminarne le conseguenze. Sicché, se l'evento non può dirsi esaurito con la prima comunicazione, sarebbe possibile configurare un'ipotesi di diffamazione omissiva (commissiva mediante omissione)[74]. In altre parole, nel momento in cui il *provider* viene a conoscenza che attraverso il suo *server* si sta realizzando un comportamento lesivo permanente, egli concorrerebbe nel fatto altrui se non provvedesse ad interrompere la visibilità del messaggio illecito, rimuovendo il dato informatico in questione o bloccando l'accesso allo stesso[75].

[71] B. Panatton, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel Cyberspace,* cit., 316.

[72] Invero, il richiamo alla categoria del reato permanente era stato utilizzato dalla giurisprudenza anche in altri ambiti, sempre concernenti la diffusione di dati e/o contenuti nel *web*. Così, per esempio, secondo Cass. pen., sez. III, 28 maggio 2019, n. 42565, Rv. 276830, «il reato di illecito trattamento dei dati personali, di cui all'art. 167 del d.lgs. 30 giugno 2003, n. 196, realizzato con la diffusione dei dati medesimi, ha natura di reato permanente, caratterizzandosi per la continuità dell'offesa arrecata dalla condotta volontaria dell'agente, il quale ha la possibilità di far cessare in ogni momento la propagazione lesiva dei dati medesimi». Nondimeno, in siffatta pronuncia la natura del reato permanente è stata ritenuta sussistente agli esclusivi fini della individuazione del *dies a quo* per il decorso del termine prescrizionale. Analogo iter argomentativo è stato condotto da Cass. pen., sez. I, 19 dicembre 2017, n. 21948, Rv. 273136, in relazione al reato di cui all'art. 2 *bis* l. n. 895 del 1967, per avere il soggetto reso disponibili, sulle pagine di un sito da lui attivato, istruzioni dettagliate per la preparazione e l'uso di materiali esplosivi ed aggressivi chimici pericolosi, individuando il *dies a quo* del termine prescrizionale non già nel momento in cui la fattispecie si era perfezionata (vale a dire la data della immissione delle istruzioni sul sito *web*), bensì nell'ultimo momento, successivo alla pubblicazione del dato, in cui si era avuta conoscenza del fatto che le istruzioni *de quibus* fossero ancora visibili (punto n. 3.1 del Considerato in diritto).

[73] F. Buffa, *Responsabilità del gestore di sito internet. Nota a margine della sentenza di Cassazione n. 54946 del 27 dicembre 2016*, in *Questione Giustizia,* 9 gennaio 2017.

[74] M. Fumo, *La condotta nei reati informatici,* in *Arch. Pen.,* 2013, 779.

[75] F. Buffa, *Responsabilità del gestore di sito internet. Nota a margine della sentenza di Cassazione n. 54946 del 27 dicembre 2016*, cit.

In senso contrario, tuttavia, si è evidenziato come, collocandosi dopo la consumazione del reato, la perdurante accessibilità del contenuto illecito in rete dovrebbe essere qualificata quale postfatto non punibile; oppure, nel caso in cui non venga attribuita alcuna autonomia concettuale a tale fase, essa andrebbe a coincidere semplicemente con gli effetti "materiali" del reato consumato. Infatti, l'obbligo di impedimento, sul quale si vorrebbe fondare il giudizio di responsabilità concorsuale, verrebbe in essere in un momento successivo a quello della consumazione del reato che sarebbe diretto ad impedire, in palese contrasto con la struttura della fattispecie[76].

Tanto considerato, parrebbero sussistere elementi sufficienti per ritenere che gli illeciti di comunicazione e diffusione del pensiero non si prestano a un inquadramento nello schema della permanenza: infatti, «i perduranti effetti che ne derivano non influiscono sul *tempus commissi delicti*, allo stesso modo in cui non è ritenuta permanente la diffamazione compiuta su un supporto cartaceo rimasto in circolazione dopo la sua pubblicazione»[77].

In breve: allo stato non parrebbe possibile attribuire un autonomo rilievo alla protrazione degli effetti del reato digitale. Allorché si ritenga che siffatta peculiare dinamica del *cyberspace* sia meritevole di una peculiare considerazione, ci si dovrebbe interrogare circa la previsione di una nuova categoria dogmatica, volta a precisare se e fino a che punto sia possibile imputare all'agente la circolazione e la riproduzione, in forza delle funzioni automatizzate, di contenuti illeciti dallo stesso prodotti o immessi nello spazio digitale oppure, più semplicemente, sulla previsione di autonomi illeciti omissivi propri volti a sanzionare la violazione di obblighi di rimozione.

8. *Complessità della rete e volontà del fatto*

La complessità di funzionamento della rete può, altresì, condizionare la configurabilità dell'imputazione soggettiva del reato, che – di regola – nei reati digitali – assume la forma dolosa.

Innanzitutto, la fisionomia dell'elemento soggettivo deve misurarsi, an-

[76] Così A. Ingrassia, *Responsabilità penale degli internet service provider: attualità e prospettive*, in *Dir. pen. proc.*, 2017, 1625.

[77] S. Seminara, *Internet (diritto penale)*, in *Enciclopedia del diritto, Annali,* VII, Milano 2014, 597.

cora una volta, con la dimensione virtuale. Non si deve, infatti, trascurare la circostanza che nel *cyberspace* si può determinare in capo all'agente una sovrapposizione di piani: quello reale e quello virtuale, appunto.

Questo significa che il soggetto che opera nel mondo digitale, almeno in alcuni casi, può non avere piena consapevolezza degli effetti della propria condotta o, quantomeno, della portata degli stessi, i quali potrebbero andare ben oltre quelli preventivati e desiderati. Tanto che parte della dottrina, nel descrivere una "scissione" tra le nostre pratiche quotidiane nel mondo digitale e i loro effetti, si chiede se questo dato non possa in un qualche modo incidere sui «presupposti della colpevolezza, lasciando dolo e colpa integri, ma svuotati»[78].

Inoltre, nei processi di imputazione non si può prescindere – ancora una volta – dal ruolo e dalla rilevanza che assumono, nella configurazione o realizzazione della fattispecie criminosa, le componenti tecnico-informatiche[79].

Si pensi, in tale prospettiva, alle già citate pronunce, in tema di pornografia minorile, con le quali si è, per esempio, precisato che, presupponendo la condotta di divulgazione e diffusione nella rete *Internet* di materiale pornografico la consapevole detenzione del materiale stesso, non possa considerarsi volontaria la divulgazione e diffusione di *files* pedopornografici compiute automaticamente dal programma di condivisione installato sul *computer* dell'agente[80].

Del pari, è stata ritenuta involontaria la condivisione di un solo *file* temporaneo generato automaticamente dalla visione di un sito e registrato, altrettanto automaticamente, dal *browser* di navigazione, non essendo possibile ravvisare in detta condotta una intenzionale detenzione del materiale

[78] P. Caroli, *Dei post e delle pene. Considerazioni su eguaglianza,* social network *e giustizia penale*, in *La giustizia penale tra ragione e prevaricazione. Dialogando con Gaetano Insolera*, Roma, 2021, 87.

[79] In argomento, R. Posada Maya, *El cibercrimen y sus efectos en la teoria de la tipicidad: de una realidad fisica a una realidad virtual*, *Revista Nuevo Foro Penal*, vol. 13, n.88, 2017, 102.

[80] Cass. pen., sez. III, 16 ottobre 2008, n. 3194, Rv. 242172, secondo la quale «in tema di pornografia minorile, la condotta di divulgazione e diffusione nella rete *Internet* di materiale pornografico presuppone la consapevole detenzione del materiale stesso (fattispecie nella quale è stata ritenuta involontaria la divulgazione e diffusione via internet di *files* pedopornografici compiute automaticamente dal programma di condivisione dati installato sul computer dell'indagato, in quanto tali *files* erano stati rinvenuti nella memoria *cache* e non all'interno di una cartella)».

illecito, necessario presupposto di una condivisione penalmente rilevante[81].

Un'attenzione peculiare è stata, inoltre, dedicata, soprattutto in tempi recenti, alle ipotesi nelle quali il soggetto agente si avvalga per la realizzazione di comportamenti illeciti nello spazio digitale di strumenti di IA[82], peraltro, sempre più connotati da un elevato grado di autonomia, automazione ed opacità[83].

Come è noto, solitamente si distinguono le ipotesi in cui i sistemi IA siano utilizzati in attività di per sé illecite ed ipotesi in cui siano invece utilizzati in attività di per sé lecite, ma da cui possano scaturire rischi od offese.

Nel primo ambito si tratta principalmente di condotte dolose, che parrebbero porre meno problemi di attribuzione della responsabilità penale, dato che il ricorso a sistemi IA per commettere un reato non appare concettualmente diverso dall'utilizzo di altri mezzi di realizzazione di un fine delittuoso[84].

In altre parole, la responsabilità penale dell'operatore non presenta particolari problemi se egli intenzionalmente e consapevolmente programma l'agente intelligente in modo che questo cooperi alla realizzazione di reati, come sua *longa manus*[85].

[81] Cass. pen., sez. III, 25 ottobre 2012, n. 44914, Rv. 253558, ad avviso della quale «non integra il reato di pornografia minorile la divulgazione nella rete *Internet*, attraverso programmi di *file-sharing*, di materiale pedopornografico non intenzionalmente detenuto o consapevolmente procurato dall'utente (fattispecie nella quale è stata ritenuta involontaria la condivisione di un solo *file* "temporaneo" generato dalla visione di un sito, che è automaticamente registrato dal *browser* di navigazione ed archiviato nella memoria del sistema informatico senza intervento dell'utilizzatore)».

[82] Per tutti, F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *www.dirittopenaleuomo.org*, n. 10, 2019, in particolare 25 ss.; G. P. Demuro, *Dai big data all'intelligenza artificial*e. *Alla ricerca di principi,* in *Diritto @ Storia,* n. 19, 2022.

[83] L'autonomia può essere intesa come «la capacita dell'algoritmo di agire in situazioni di incertezza e l'automazione come la capacita di raggiungere un determinato obiettivo in assenza di intervento umano». L'opacità «è l'altra faccia dell'autonomia dei sistemi di i.a., e indica l'impossibilita di comprendere precisamente, a posteriori, i nessi causa-effetto che hanno portato l'algoritmo ad assumere una determinata decisione». Così B. Fragasso, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., 48. Sul punto, altresì, M. Simmler, R. Frischknecht, *A taxonomy of human–machine collaboration: capturing automation and technical autonomy,* in *AI & Society,* 36, 2021, 239 ss.

[84] L. Picotti, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi?,* in *www.sistemapenale.it,* 31 luglio 2024, 10; L. D'Amico, *La misura della (im)prevedibilità. Modelli d'imputazione della responsabilità al tempo dell'intelligenza artificiale*, cit., in particolare 178 ss.; B. Fragasso, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., 549 ss.

[85] B. Magro, Robot*,* cyborg *e intelligenze artificiali,* in *Trattati giuridici.* Cybercrime*,* di-

Si pensi all'ipotesi in cui il soggetto agente deliberatamente deleghi ad un algoritmo l'identificazione dei sistemi informatici vulnerabili al fine di commettere un accesso abusivo. O ancora, si pensi alla capillare diffusione sui *social network* di contenuti diffamatori o di istigazione all'odio, attraverso meccanismi di ripubblicazione automatica di *post* che contengano determinate parole o *hashtag*.

Senza dubbio più complesse si sono, invece, dimostrate le questioni relative ai reati colposi, che possono essere commessi *offline* nell'esercizio di molteplici e tendenzialmente sempre più numerose attività lecite di base (quali la circolazione di veicoli a guida autonoma o l'uso di sistemi intelligenti e robotici nella diagnosi e nel trattamento medico–chirurgico). Ma siffatto ambito esula dall'oggetto di questo studio.

Nondimeno, tornando alle ipotesi più direttamente coinvolte dalla presente indagine, non si può escludere a priori che l'imprevedibilità e l'autonomia che può connotare i sistemi di IA anche nella dimensione digitale possano comunque influire, sia pure in termini meno incisi, sull'attribuzione del fatto all'agente[86]. E' facile intuire, infatti, che in tutte le ipotesi in cui l'agire umano interseca fattori riconducibili a sistemi di IA il percorso di attribuzione della responsabilità si complica.

Si tenterà di mettere meglio a fuoco la problematica attraverso un'esemplificazione.

9. *Il caso del* trading *algoritmico*

Vi sono alcuni ambiti nei quali risulta particolarmente arduo distinguere esiti direttamente imputabili all'azione umana da quelli riferibili, invece,

retto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, in particolare 1206 ss.; F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, cit., in particolare 24 ss.; A. Cappellini, Machina delinquere non potest*? Brevi appunti su Intelligenza artificiale e responsabilità penale*, in *Criminalia* 2018, in particolare 503 ss.

[86] B. Fragasso, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., 112. Su questi e altri problemi connessi allo sviluppo dei sistemi di AI, *amplius* B. Magro, Robot*,* cyborg *e intelligenze artificiali,* cit., in particolare 1206 ss.; I. Salvadori, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen*., 2021, 83 ss.; T. C. King, N. Aggarwal, M. Taddeo, L. Floridi, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions,* in *Science and Engineering Ethics*, 2020, vol. 26, 89 ss.

all'autonoma operatività del sistema informatico. Uno di questi è il contesto finanziario nel quale sempre più frequentemente operano programmi che investono nel mercato anche con rilevanti margini di indipendenza ed autonomia rispetto alle istruzioni impartite da persone fisiche[87].

Già da tempo, invero, il mondo della finanza è stato caratterizzato da un'influenza sempre più pervasiva della tecnica, tanto che con il termine *Fintech* si intende oggi la tecnologia applicata alla finanza, la quale ha reso possibile importanti innovazioni sia nell'offerta di servizi agli utenti finali sia nei processi produttivi interni agli operatori finanziari[88].

Come è stato, infatti, osservato «il mercato finanziario non è più da tempo un luogo *fisico* e molti dei soggetti che vi operano hanno abbandonato l'immane concretezza dei connotati umani, per assumere vieppiù i caratteri della virtualità e immaterialità»[89].

Sicché, in questo contesto si è determinato un progressivo cambio di paradigma, per cui appare sempre più difficile distinguere l'azione umana da quella di elaboratori e programmi informatici che investono nel mercato in modo vieppiù indipendente ed autonomo rispetto alle eventuali istruzioni impartite dai soggetti-persone fisiche[90].

I sistemi di *trading* algoritmico sono, infatti, in grado di effettuare autonomamente ordini di acquisto[91]: l'algoritmo decide la tempistica, il prezzo e

[87] F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato,* in *Banca, borsa, titoli di credito*, 2018, 196; M. Palmisano, *L'abuso di mercato nell'era delle nuove tecnologie.* Trading *algoritmico e principio di personalità dell'illecito penale*, in *www.penalecontemporaneo.it, Riv. trim.* n. 2 del 2019, 130; F. Consulich, Flash offenders. *Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. proc. pen.*, 2022, 1015 ss.

[88] G. Ruta, *I.A. nei reati economici e finanziari*, in *Intelligenza artificiale e giurisdizione penale*, *Atti del* workshop *organizzato dalla Fondazione Occorsio* il 19 novembre 2021, in *www.sistemapenale.it*, 13 giugno 2022, 59.

[89] F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., 196.

[90] M. Palmisano, *L'abuso di mercato nell'era delle nuove tecnologie. Trading algoritmico e principio di personalità dell'illecito penale*, cit., 130.

[91] Una definizione normativa di negoziazione algoritmica si rinviene nella direttiva 2014/65/UE del 15 maggio 2014 (relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE). All'art. 4, §1, n. 39, si precisa che per negoziazione algoritmica si intende la «negoziazione di strumenti finanziari in cui un algoritmo informatizzato determina automaticamente i parametri individuali degli ordini, come ad esempio se avviare l'ordine, i tempi, il prezzo o la quantità dell'ordine o come gestire l'ordine dopo la sua presenta-

la quantità dell'ordine; nella maggior parte dei casi, può addirittura avviare l'ordine in assenza di intervento umano[92].

Una categoria particolare di *automated trading* sono i c.d. *High Frequency Trading (HFT)*[93], che consentono di effettuare negoziazioni ad altissima velocità, rendendo possibile perfezionare migliaia di ordini al secondo[94]. Inoltre, diversamente dagli algoritmi di prima generazione, quelli ad alta frequenza sono in grado di apprendere dal contesto in cui operano e modificare le proprie strategie operative. Tanto che, ancora una volta, si parla di *black box algorithms* per indicare quel cono di opacità che si registra tra i dati di *input* e quelli comportamentali di *output*[95].

Siffatti strumenti algoritmici presentano, dunque, una qualità particolare: «sono progettati per reagire al mutamento del contesto in cui operano, senza alcuna istruzione umana, diversa ed aggiuntiva a quelle iniziali fornite dal programmatore»[96]. Sfruttando tecniche di *machine learning* capaci di apprendere dall'ambiente in cui operano e modificare le proprie strategie operative, l'*HFT* risulta in grado di effettuare una scelta di investimento che

zione, con intervento umano minimo o nullo (…)», specificando altresì, al n. 40, che la tecnica di negoziazione algoritmica ad alta frequenza si identifica in «qualsiasi tecnica di negoziazione algoritmica caratterizzata da: a) infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere, compresa almeno una delle strutture per l'inserimento algoritmico dell'ordine: co-ubicazione, *hosting* di prossimità o accesso elettronico diretto a velocità elevata; b) determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine senza intervento umano per il singolo ordine o negoziazione, e c) elevato traffico infragiornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni».

92 F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit. 198, 199; F. Consulich., Flash offenders. *Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*, cit., 1015 ss.; A.F. Tripodi, *Abusi di mercato e* trading *algoritmico*, in Il *diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, a cura di R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto, Milano, 2022, 745 ss.

93 *Amplius* G. Ruta, *I.A. nei reati economici e finanziari*, in *Intelligenza artificiale e giurisdizione penale*, cit., in particolare 60 ss.; F. Consulich, M. Maugeri, C. Milia, T. N. Poli, G. Trovatore, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?,* in *Quaderni giuridici Consob,* n. 29, maggio 2023, 7 ss.

94 B. Fragasso, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., 114,115.

95 Così A. Tripodi, *Uomo, societas, machina*, in *www.lalegislazionepenale.eu*, 10 maggio 2023, 11 e bibliografia ivi riportata.

96 F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., 207.

potrebbe non essere prevedibile dal programmatore al momento del suo utilizzo.

É, dunque, facile intuire come gli operatori algoritmici dispongano di «un colossale vantaggio competitivo di carattere conoscitivo, generato dalla loro superiorità in termini di velocità operativa; prima che un operatore umano abbia eseguito una singola operazione, il *trader* algoritmico ha già elaborato migliaia di informazioni e conseguentemente effettuato un investimento compiuto e definito»[97].

Tanto premesso, non è difficile immaginare che gli algoritmi di *trading* possano realizzare anche comportamenti distorsivi del mercato[98], in particolare nelle forme dell'abuso di informazioni privilegiate (*Insider trading*)[99] o della manipolazione del mercato[100]. Peraltro, proprio la velocità operativa degli *High Frequency Trading* ha determinato l'emergere di nuovi schemi di turbativa, quali, ad esempio, il *pump and dump,* il *pinging*, il *quote suffing,* lo *smoking*, il *layering*, lo *spoofing*, il *front running,* il cui comune denominatore è costituito, in buona sostanza, dall'utilizzo di informazioni acquisite sulla base di analisi automatizzate del mercato nella immissione e nella contestuale cancellazione di migliaia di ordini, al fine di far apparire le condizioni di mercato differenti da quelle effettive[101].

A fronte di questo quadro, ci si chiede dunque se i delitti tradizionalmente previsti in materia di abuso di mercato possano oggi ritenersi applicabili anche alle nuove configurazioni digitali di detto fenomeno, nonostante le torsioni ingenerate dall'operatività dei nuovi soggetti economici algoritmici. Come è facile intuire, infatti, anche se il comportamento dell'algoritmo è certamente *ab origine* condizionato dalle istruzioni impartite dall'utilizzatore, in realtà dall'autonoma interazione tra l'algoritmo medesimo e il conte-

[97] F. CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., 199, 200. Analogamente, M. PALMISANO, *L'abuso di mercato nell'era delle nuove tecnologie. Trading algoritmico e principio di personalita dell'illecito penale*, cit., 129.

[98] *Amplius* G. RUTA, *I.A. nei reati economici e finanziari*, in *Intelligenza artificiale e giurisdizione penale*, cit., 65 ss.

[99] Ai sensi dell'art. 184 TUF.

[100] Ai sensi degli artt. 185 TUF, 501 c.p. e 2637 c.c.

[101] In argomento, G. RUTA, *I.A. nei reati economici e finanziari*, cit., 66 ss.; B. FRAGASSO, I*ntelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, cit., 116; F. CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., 209 ss.

sto economico mutevole, in cui esso opera, potrebbe scaturire una decisione di investimento assolutamente "imprevedibile". Conseguentemente, non è da escludere una sorta di «rottura del rapporto di "autoria" tra operazione finanziaria e soggetto agente, potendosi riferire la prima al secondo solo in via "tendenziale"»[102].

In effetti, là dove l'abuso di mercato consegua a scelte autonome dell'algoritmo ad alta frequenza, potrebbe mancare in capo alla persona fisica il dolo, correttamente inteso quale specchio del fatto nei suoi snodi storici essenziali, con conseguente impossibilità di un'imputazione penalistica in capo all'operatore[103]. Sicché, nel momento in cui ci si interroga sulle condizioni di responsabilità dell'agente che si avvalga di siffatti strumenti appare sempre più impervio il percorso logico che si avvale dei modelli imputativi "classici"[104].

Pertanto, pur a fronte delle argute soluzioni prospettate in via interpretativa da attenta dottrina[105], parrebbe più che mai opportuna, *de iure condendo,* la predisposizione di una normativa specificamente diretta a disciplinare l'operatività di siffatti meccanismi finanziari, nonché a regolare i criteri di imputazione delle responsabilità derivanti dall'impiego degli stessi[106].

Peraltro, la recente legge 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale)[107], ha introdotto, nella

[102] M. Palmisano, *L'abuso di mercato nell'era delle nuove tecnologie.* Trading *algoritmico e principio di personalità dell'illecito penale*, cit., 138

[103] Così, F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., 223. Cfr., altresì, F. Consulich., Flash offenders. *Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*, cit., 1035, ove l'Autore propone di coniare «il concetto di *imputazione mediata*, per indicare tutti i casi in cui lo strumento abbia una quota parte di autonomia nel concretizzare il progetto illecito dell'unico soggetto perseguibile, la persona fisica che se ne avvalga. È evidente che si tratta di un concetto 'critico', poiché la sua legittimità dipende dal *quantum* di fatto tipico compiuto dall'agente artificiale senza la copertura dell'elemento soggettivo dell'individuo. Ove, per ipotesi, quest'ultimo determinasse solo il *genus* del reato, senza definire il *tempus* e il *modus* dell'illecito, non vi sarebbe modo di configurare una responsabilità dolosa a suo carico».

[104] A. Tripodi, *Uomo, societas, machina*, cit., 10 maggio 2023, 12 ss.

[105] *Amplius* F. Consulich, M. Maugeri, C. Milia, T. N. Poli, G. Trovatore, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?,* cit., in particolare 29 ss.

[106] Ancora F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, cit., 199, 217.

[107] In argomento, per tutti, L. Picotti, *I contenuti penali della legge sull'intelligenza artificiale,* in *www.sistemapenale.it,* 2 dicembre 2025; B. Fragasso, *Profili penalistici del-*

materia qui considerata, due circostanze aggravanti per le ipotesi contemplate, rispettivamente, dagli artt. 2637 c.c. e 185 TUF[108], proprio in considerazione dell'esigenza di rafforzare la tutela penale del regolare andamento del mercato di fronte all'utilizzo sempre più diffuso di sistemi di intelligenza artificiale[109].

10. *Ubiquità del fatto e* locus commissi delicti

Sicuramente una delle questioni più complesse evidenziate dalla dimensione digitale del reato è rappresentata dal fatto che le nuove fenomenologie criminose si muovono in uno spazio fluido, invisibile, intangibile: un "non luogo" «la cui consistenza fisica è, per definizione, evanescente»[110], in cui non ci sono confini e distanze.

Internet presenta, infatti, uno spazio di operatività geografica preventivamente non delimitabile, una struttura aperta ad uno sterminato numero di connessioni[111]. Sicché, la c.d. *digital disruption* obbliga l'odierno giurista ad ammettere che «esistano un altro spazio e un altro tempo oltre a quelli che considerava "naturali"»[112].

Il diritto penale dello Stato moderno fu, infatti, configurato come un diritto essenzialmente territoriale, allo stesso modo della moneta nazionale.

la legge sull'intelligenza artificiale: osservazioni a prima lettura, in *www.sistemapenale.it,* n. 10, 2025, 157 ss.

[108] L'ultimo periodo dell'art. 2637 c.c. prevede ora che la pena sia della reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale. Analogamente, il primo comma, parte seconda, dell'art. 185 TUF prevede che la pena sia inasprita rispetto a quella contemplata per l'ipotesi base (reclusione da due a sette anni e multa da euro venticinquemila a euro sei milioni) se la manipolazione del mercato è commessa mediante l'impiego di sistemi di intelligenza artificiale.

[109] In argomento F. MUCCIARELLI, *Intelligenza artificiale e condotte manipolative su strumenti finanziari: una nuova aggravante con effetto attenuante,* in *www.sistemapenale.it,* 17 ottobre 2025.

[110] F. CAMPLANI, Locus commissi delicti*, norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Archivio penale*, 2020, n. 2, 2.

[111] *Amplius* F. RUGGIERO, *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002, 254 ss. In argomento v., altresì, S. SEMINARA, *La pirateria su Internet e il diritto penale,* in *Riv. trim. dir. pen. econ.*, 1997, in particolare 102 ss.

[112] A. GARAPON, J. LASSÈGUE, *La giustizia digitale. Determinismo tecnologico e libertà,* trad. it. a cura di F. Morini, Bologna, 2021, 99.

Però, già a partire dall'inizio del XX secolo si sono sviluppati molteplici fattori di internazionalizzazione e globalizzazione che hanno evidenziato peculiarità ed esigenze di armonizzazione prima sconosciute[113]. L'era digitale ha enormemente alimentato siffatto declino della sovranità statale.

Come è stato ben evidenziato, «nel *cyberspace* i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio). Pertanto non è sempre agevole individuare con certezza una sfera spaziale suscettibile di tutela in un sistema telematico, che opera e si connette ad altri terminali mediante reti e protocolli di comunicazione. Del resto, la dimensione aterittoriale si è incrementata da ultimo con la diffusione dei dispositivi mobili (*tablet*, *smartphone*, sistemi portatili) e del *cloud computing*, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate dalle quali è possibile accedere da qualunque parte del globo. Va comunque precisato che, se i dati oggetto di accesso abusivo sono archiviati su *cloud computing* o resi disponibili da *server* che sfruttano tali servizi, potrebbe risultare estremamente difficile individuare il luogo nel quale le informazioni sono collocate»[114].

Lo spazio cibernetico è, dunque, un ambiente ubiquo e ibrido, costituito da elementi fisici e digitali che concorrono a renderlo al contempo reale e virtuale[115].

A questo si aggiunga che le nuove tecnologie rendono più evidente «la distinzione tra presenza e localizzazione del sé», nel senso che esse possono fare in modo che «trascorriamo una parte consistente del nostro tempo cosciente in un luogo diverso rispetto a quello in cui siamo fisicamente collocati»[116].

[113] Così e *amplius,* A. ZAPATERO, *La armonizacíon internacional del derecho penal,* in *Piratas, mercenarios, soldados, jueces y policías: nuevos desafios del derecho penal europeo y internacional,* a cura di A. ZAPATERO, N. MARTIN, Castilla-La Mancha, 2010, 29.

[114] Cass. pen., sez. un. 26 marzo 2015, n. 17325, Rv. 263020, punto n. 3 del Considerato in diritto.

[115] F. VIGNERI, *Brevi considerazioni sulla natura e sulle caratteristiche dello spazio cibernetico*, in *SalvisJuribus*, 10.10.2019, par. III.

[116] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, trad. it. a cura di M. Durante, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo,* Milano, 2017, 81.

Ebbene, tanto premesso, non sorprende che in diverse occasioni la prassi applicativa abbia incontrato difficoltà ed evidenziato criticità nella soluzione di questioni attinenti all'individuazione del *locs commissi delicti,* segnatamente al fine di radicare la giurisdizione e individuare la competenza territoriale nel *cyberspace*[117].

Come è stato di recente ricordato, «il *nomos* è sempre stato (……) "*nomos* della terra" (…) il diritto fatica a riconoscere la sua esistenza senza la terra. Subisce letteralmente uno scacco». (…) Il reato diventa, in breve, letteralmente "*u*–topico", ossia reato di un luogo che non c'è»[118].

La complessità del tema è, del resto, ben evidenziato dalla giurisprudenza che si è trovata ad affrontare le predette questioni in relazione a diverse fattispecie incriminatrici, alimentando, invero, la sensazione che le problematiche evidenziate siano state affrontate, non di rado, in modo casistico.

Si prenderanno in esame, a titolo esemplificativo, due differenti tipologie delittuose: l'accesso abusivo a sistema informatico e la diffamazione *online*.

10.1. *L' accesso abusivo ad un sistema informatico*

In relazione al reato di accesso abusivo a sistema informatico, per un certo periodo di tempo la prassi applicativa aveva messo in luce due soluzioni differenti nel modo di intenderne la spazialità.

Per un primo orientamento, infatti, il *locus commissi delicti* avrebbe dovuto essere individuato nel luogo nel quale il soggetto si è connesso alla rete effettuando il collegamento abusivo, mentre per una diversa opzione interpretativa, nel luogo ove è fisicamente allocata la banca-dati che costituisce l'oggetto dell'intrusione. Una contrapposizione, questa, che ad avviso della dottrina scontava, invero, il modo inadeguato con il quale il legislatore italiano, nel 1993, aveva costruito i reati informatici sulla falsariga dei, corrispondenti, reati non informatici (nel caso di specie, la violazione di domicilio), anziché prestando attenzione alle specifiche caratteristiche della nuova realtà che si accingeva a disciplinare[119].

[117] *Amplius* R. Flor, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative,* in *Trattati giuridici. Cybercrime,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 141 ss.

[118] A. Incampo, *Metaverso. Come del mondo (o del diritto o dell'economia) fin dalla sua origine*, in *Riv. fil. dir.*, 2025, n. 1, 59.

[119] Così, C.F. Grosso, *Su di un'interessante controversia interpretativa in tema di luogo del*

Inizialmente la giurisprudenza sembrava prevalentemente aver recepito la seconda tra le soluzioni prospettate, ritenendo che il *locus commissi delicti* corrispondesse a quello ove fosse materialmente collocato l'oggetto materiale della condotta criminosa, ovvero il *server* (o comunque il sistema informatico) violato[120]. Posta la centralità dello *jus excludendi* – si leggerà poi in un'importante pronuncia delle sezioni unite sulla questione – la fattispecie si riteneva perfezionata nel momento in cui il soggetto agente fosse entrato nel sistema altrui, oltrepassandone le barriere logiche protettive[121].

Il criterio adottato era dunque mutuato dagli abituali schemi concettuali del mondo materiale, adottando, però, un parametro che si è presto rivelato problematico se rapportato alla circolazione dei dati in una rete di comunicazione telematica che ne permette la contemporanea consultazione da parte di una pluralità di utenti, spazialmente diffusi sul territorio. Iniziò dunque ad emergere la convinzione che il luogo e il tempo di perfezione del reato dovesse essere individuato nel momento in cui l'agente si introduce abusivamente nella postazione locale[122].

Tanto che, successivamente, i contrastanti orientamenti giurisprudenziali, registrati sia fra i giudici di merito sia fra quelli di legittimità, portarono la questione dinanzi alle sezioni unite[123], le quali hanno ritenuto preferibile

commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico, in *Riv. it. dir. proc. pen.*, 2014, 1519.

[120] Così Cass. pen., sez. I, 27 maggio 2013, n. 40303, Rv. 257252.

[121] Cass. pen., sez. un., 26 marzo 2015, n. 17325, Rv. 263020, punto n. 1.2 del Considerato in diritto.

[122] Così, per esempio, Tribunale di Roma, Ufficio indagini preliminari, 16 aprile 2014, ad avviso della quale «nel caso di accesso abusivo ad un sistema telematico realizzato da un soggetto che si è collegato alla banca dati da un terminale periferico è competente il giudice del luogo dal quale il soggetto si è collegato e non il giudice del luogo nel quale è fisicamente collocato il sistema informatico, il *server* o la banca dati obiettivo dell'intrusione» (sulla pronuncia, R. ZANNOTTI, *Accesso abusivo ad un sistema telematico: quale il locus commissi delicti?*, in *Diritto dell'informazione e dell'informatica,* 2014, 948 ss.), nonché Cass. pen., sez. I, 15 luglio 2014, n. 34165, che conferma la citata pronuncia del Tribunale di Roma. Sull'ordinanza di rimessione della questione in oggetto alle sezioni unite della Cassazione, M. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *www.penalecontemporaneo.it*, 2015.

[123] Cass. pen., sez. I, ord. 28.10.2014, n. 52575, in cui si legge: «Poiché il reato si perfeziona con l'introduzione abusiva nel sistema, a prescindere dalla effettiva acquisizione dei dati riservati in esso contenuti, si deve ritenere che la condotta materiale si perfeziona nel luogo fisico e nel momento in cui l'agente si introduce abusivamente nella postazione locale (….), la quale

individuare il *locus commissi delicti,* e conseguentemente radicare la competenza per territorio, proprio nel luogo in cui il soggetto agente ha realizzato il comportamento abusivo[124].

In tale prospettiva, infatti, l'accesso avrebbe inizio con l'unica condotta umana di natura materiale, consistente nella digitazione da remoto delle credenziali di autenticazione da parte dell'utente, mentre tutti gli eventi successivi assumerebbero i connotati di comportamenti comunicativi tra il *client* e il *server*. L'introduzione abusiva, allora, verrebbe ad essere integrata nel luogo in cui l'operatore materialmente digita la *password* di accesso o esegue la procedura di *login*, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, realizzando in tal modo l'ingresso non consentito. Sicché, da tale impostazione, volta a confrontarsi con la specificità della realtà telematica, conseguirebbe che il luogo del commesso reato si identifica con quello in cui si trova la postazione remota dalla quale l'agente si interfaccia con l'intero sistema, digitando le credenziali di autenticazione e premendo il testo di avvio[125].

Sennonché – osserva la dottrina – anche siffatto criterio evidenzia comunque profili di criticità, posto che individuando il *locus commissi delicti* nel luogo in cui si trova il soggetto che realizza la condotta, quest'ultimo «potrebbe scegliere territorialmente il Paese da cui far partire l'attacco e, con esso, il luogo dove instaurare il capolinea della tracciabilità del percorso informatico»[126].

non è un mero mezzo di accesso ma, al pari del *computer* denominato *server* ubicato presso la sede centrale, un componente informatico essenziale costituente articolazione territoriale del complessivo sistema informatico nazionale nella disponibilità del Ministero dei Trasporti». Il caso di specie si era concretizzato nell'introduzione abusiva e ripetuta nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti da parte di un'impiegata della motorizzazione civile, in concorso con altri soggetti, al fine di effettuare visure elettroniche che esulavano dalle mansioni della imputata ed interessavano l'amministratore di una agenzia di pratiche automobilistiche.

[124] Cass. pen., sez. un., 26 marzo 2015, n. 17325, in *Cass. pen.*, 2015, 3501 ss., con nota di M. L. Sciuba, *Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico,* ivi, 3507 ss. Sulla pronuncia v., altresì, R. Flor, *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite,* in *Dir. pen. proc.,* 2015, 1296 ss.; A. Leopizzi, *La biblioteca (digitale) di Babele. Condotte umane nel cyberspazio e competenza territoriale per le violazioni del domicilio informatico*, in *La Giustizia penale,* 2015, III, 410 ss.

[125] Cass. pen., sez. un., 26 marzo 2015, n. 17325, punto n. 4.2 del Considerato in diritto.

[126] R. Flor, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative,* cit., 187.

10.2. *La diffamazione* online

Analoghe questioni si sono poste anche in relazione alla diffamazione *online*. Dottrina e giurisprudenza si sono ben presto rese conto della peculiarità dei profili problematici sollevati, in relazione al *locus commissi delicti,* dal reato di diffamazione commesso nello spazio digitale.

Non sorprende, dunque, che in una delle prime pronunce della Cassazione sulla questione, si legga: «allo scopo di decidere correttamente una questione, quale quella prospettata, che presenta, senza dubbio, alcuni caratteri di novità, appare innanzitutto opportuno verificare come si caratterizzi il delitto di diffamazione consumato con quel nuovo mezzo di trasmissione-comunicazione che prende il nome di *internet*. Il legislatore, pur mostrando di aver preso in considerazione la esistenza di nuovi strumenti di comunicazione, telematici ed informatici (si veda, ad esempio, l'art. 623 *bis* c.p. in tema di reati contro la inviolabilità dei segreti), non ha ritenuto di dover mutare o integrare la lettera della legge con riferimento a reati (e, tra questi, certamente quelli contro l'onore), la cui condotta consiste nella (o presuppone la) comunicazione dell'agente con terze persone. E, tuttavia, che i reati previsti dagli artt. 594 e 595 c.p. possano essere commessi anche per via telematica o informatica, è addirittura intuitivo»[127]. Sennonché, «in considerazione della caratterizzazione "transnazionale" dello strumento adoperato, può apparire, in un primo momento, problematica la individuazione del luogo in cui deve ritenersi consumato il delitto commesso "a mezzo *internet*"»[128].

Tanto premesso, dunque, dottrina e giurisprudenza hanno, nel corso del tempo, proposto soluzioni variegate, in taluni casi caratterizzate, invero, da talune forzature ermeneutiche[129], nel tentativo di offrire un criterio soddisfacente di soluzione del problema evidenziato.

Ad avviso di un primo orientamento, in ossequio alla natura del delitto, che – secondo l'opinione dominante – andrebbe ricostruito come reato di evento, il fatto dovrebbe considerarsi consumato nel luogo in cui si trovano i due soggetti terzi che, collegandosi alla rete, per primi percepiscono la

[127] Cass. pen., sez. V, 17 gennaio 2000, n. 4741, Rv. 217745.

[128] Cass. pen., sez. V, 17 gennaio 2000, n. 4741, Rv. 217745.

[129] Così E. Mazzanti, *Il delitto di diffamazione al tempo dei social network: punti fermi e spunti problematici*, in *Nodi virtuali, legami informali: Internet alla ricerca di regole,* a cura di P. Passaglia, D. Poletti, Pisa, 2016, 215.

natura diffamatoria del messaggio. Qui verrebbe conseguentemente a radicarsi la competenza territoriale del giudice[130].

Nondimeno, per taluno, tenendo contro delle specificità del mezzo di comunicazione telematico, il predetto rapporto comunicativo potrebbe dirsi realizzato già con l'immissione dei dati in rete e la loro conseguente messa e tenuta a disposizione di un pubblico indeterminato di navigatori del ciberspazio, sicché il perfezionamento del reato potrebbe prescindere dall'effettiva percezione o lettura del messaggio offensivo ad opera dei destinatari[131]. Così ragionando, tuttavia, sorge il dubbio che, dal punto di vista logico, si determini una sostanziale coincidenza tra condotta ed evento che priverebbe quest'ultimo di ogni autonoma rilevanza, per imporre, appunto, l'individuazione del *locus commissi delicti* nel luogo ove è stata realizzata la condotta.

Ad avviso di un ulteriore orientamento, il *locus commissi delicti,* al fine dell'individuazione del giudice competente, dovrebbe, parimenti, essere individuato nel luogo in cui l'autore ha agito, caricando il contenuto offensivo sul *server,* ma si perverrebbe a siffatto esito interpretativo attraverso un differente percorso argomentativo.

Occorrerebbe, infatti, prendere atto che per i reati di diffamazione commessi a mezzo *internet* sia normalmente impossibile stabilire il luogo in cui il reato deve effettivamente ritenersi "commesso". Infatti – si osserva – vero è che la diffamazione è un reato di evento, destinato, dunque, a consumarsi nel momento e nel luogo in cui i terzi percepiscono l'espressione offensiva; nondimeno, risulterebbe per lo più difficile nello spazio digitale l'individuazione del soggetto che per secondo (così integrando il requisito della comunicazione con più persone) abbia preso cognizione del contenuto diffamatorio, non essendo sufficiente, in tale prospettiva, la mera connessione al

[130] Così, Cass. pen., sez. V, 17 novembre 2000, n. 4741, Rv. 217745, secondo la quale il reato di diffamazione «si consuma non al momento della diffusione del messaggio offensivo, ma al momento della percezione dello stesso da parte di soggetti che siano "terzi" rispetto all'agente ed alla persona offesa». Nello stesso senso, Cass. pen., sez. II, 21 febbraio 2008, n. 36721, Rv. 242085.

[131] Così e *amplius* L. PICOTTI, *Profili penali delle comunicazioni illecite via Internet*, in *Dir. dell'informazione e dell'informatica*, 1999, 295 ss. Per talune osservazioni critiche in merito a siffatta impostazione S. SEMINARA, *Internet (diritto penale)*, in *Enciclopedia del Diritto, Annali*, VII, Milano, 2014, 570, 571.

sito *internet*[132]. Sicché, procedendo a cascata, verrebbe in esame il primo dei momenti di collegamento suppletivi, contemplati dal nostro ordinamento, che radica la competenza nel luogo in cui è avvenuta una parte dell'azione (l'ultima individuabile), ai sensi dell'art. 9, comma 1, c.p.p.[133].

Ebbene, di recente anche la giurisprudenza parrebbe aver recepito siffatta impostazione, tentando una sintesi tra le precedenti prese di posizione che consentisse, però, di tener conto della peculiare struttura del delitto di diffamazione.

Si muove, dunque, dal presupposto che, trattandosi della immissione della notizia in uno spazio *web*, la comunicazione può effettivamente ritenersi indirizzata a tutti i possibili visitatori del sito, ma non per questo l'introduzione nella Rete del messaggio diffamatorio consolida, di per sé sola, l'evento offensivo della reputazione. Quest'ultimo, infatti, si concretizza solo quando i visitatori entrano nel sito e prendono visione del contenuto della comunicazione. Coerentemente, allora, si precisa che, nel caso di offesa arrecata tramite *Internet*, la condotta, cioè l'introduzione nello spazio *web* del messaggio dal contenuto illecito, deve essere tenuta distinta dall'evento, integrato dalla apprensione del messaggio da parte di terzi[134]. Tanto premesso, ne dovrebbe seguire che il luogo nel quale si verifica l'evento della diffamazione andrebbe identificato con quello nel quale almeno due visitatori abbiano preso conoscenza dei contenuti offensivi (e non si siano, cioè, meramente collegati al sito di riferimento, perché il reato si realizza con l'effettività dell'apprensione della notizia). Nondimeno, posto che nel "mondo virtuale di ampiezza planetaria", nella stragrande maggioranza dei casi risulta complicato, se non impossibile, utilizzare detto indicatore oggettivo al fine di radicare la competenza per territorio, in via subordinata si dovrà aver riguardo al luogo in cui è avvenuto il caricamento del dato informatico perché tale segmento comportamentale individua l'ultimo luogo conoscibile in cui è avvenuta una parte dell'azione che incorpora uno degli elementi costitutivi della fattispecie. Allorché, infine, anche siffatto accertamento risulti impraticabile, si dovrà ricorrere, in via gradata, al luogo di residenza,

[132] Cass. pen., sez. V, 19 maggio 2015, n. 31677, Rv. 264521, punto n. 5 del Considerato in diritto.

[133] E. Mazzanti, *Il delitto di diffamazione al tempo dei* social network*: punti fermi e spunti problematici*, cit., 217.

[134] Cass. pen., sez. V, 7 marzo 2025, n. 14204, Rv. 287857, punto n. 1.3 del Considerato in diritto.

domicilio o dimora dell'imputato, in attuazione della regola suppletiva di cui all'art. 9, comma 2, c.p.p.[135].

Un'ultima notazione. Anche in relazione all'applicazione dei criteri di individuazione del *locus commissi delicti* può assumere un rilievo tutt'altro che trascurabile la peculiare tipologia di strumento informatico utilizzato per commettere il reato. Si spiega in tale prospettiva, per esempio, la precisazione in forza della quale allorché il reato di diffamazione venga realizzato attraverso l'invio di *e-mail*, vale a dire comunicazioni dirette a destinatari predefiniti, il requisito della comunicazione con più persone non può presumersi sulla base del mero inserimento del contenuto offensivo nella rete (e cioè, nel caso di specie, della loro spedizione), ma è necessaria quantomeno la prova dell'effettivo recapito degli stessi[136].

[135] Cass. pen., sez. V, 7 marzo 2025, n. 14204, Rv. 287857, punto n. 1.4 del Considerato in diritto. Analogamente, peraltro, già Cass. pen., sez. I, 15 marzo 2011, n. 16307, Rv. 297957, ad avviso della quale «in tema di competenza per territorio nei casi di diffamazione via *Internet*, attesa la difficoltà di utilizzare criteri oggettivi unici, individuati secondo le regole generali dettate dagli art. 8 e 9, comma 1, c.p.p., come quelli di prima pubblicazione, di immissione della notizia nella rete, di accesso del primo visitatore, di collocazione del *server*, il giudice competente potrà essere individuato ai sensi dell'art. 9, comma 2, c.p.p. che lo indica in quello della residenza, della dimora o del domicilio dell'imputato».

[136] Così, Cass. pen., sez. V, 27 giugno 2023, n. 38144, in *deJure.* Sulla pronuncia *de qua,* F. Riboldi, *I criteri per la determinazione della competenza territoriale nella diffamazione telematica: l'accertamento dell'evento tra rigore tecnico e ricorso alle presunzioni,* in *MediaLaws,* n. 3, 2023, 204 ss.

Capitolo quarto

LE PIATTAFORME DIGITALI E I MOTORI DI RICERCA

SOMMARIO: 1. La responsabilità del *provider* per il reato digitale. – 2. Il problema della posizione di garanzia. – 3. L'analogia *in malam partem* della disciplina in tema di stampa. – 4. La mancata rimozione dei contenuti illeciti. – 5. Il *Digital Services Act.*

«*A seguito della rivoluzione digitale, dovremmo riscrivere ancora una volta il principio di sovranità di Schmitt: sovrano è colui che dispone delle shitstorms in rete*».
(B. C. HAN, *Nello sciame. Visioni del digitale,* Milano, 2023, 17)

1. *La responsabilità del* provider *per il reato digitale*

Alla luce delle evidenziate caratteristiche del reato nel mondo digitale, la cui estrinsecazione presuppone una continua sinergia ed osmosi tra realtà analogica e realtà virtuale, ci si chiede quale ruolo vengano ad assumere i gestori delle piattaforme e dei motori di ricerca. Occorre, in altre parole interrogarsi sulla possibile configurazione di una responsabilità degli operatori professionali del settore telematico per i contenuti illeciti immessi negli spazi da loro gestiti.

Con l'acronimo *ISP* si designano convenzionalmente gli "intermediari di connessione", vale a dire i soggetti che forniscono le infrastrutture digitali volte a consentire agli utenti l'accesso ad *Internet* ed eventualmente la memorizzazione di media o lunga durata di dati, nonché gli spazi virtuali nei quali i fruitori dei servizi possono interagire e scambiarsi dati, informazioni, contenuti[1].

La questione relativa ad un loro possibile coinvolgimento nei processi di ascrizione di responsabilità penali per fatti commessi nel *cyberspace* assume particolare rilievo, segnatamente alla luce di due diversi fattori.

[1] Sul tema, M. R. ALLEGRI, Ubi social, ibi ius. *Fondamenti costituzionali dei* social network *e profili giuridici della responsabilità dei* provider*,* Milano, 2018, 53.

Da un lato, l'anonimato (o pseudoanonimato) garantito da *Internet*, l'utilizzo di credenziali false, la non riconducibilità immediata di indirizzi *IP* ad una persona specifica rendono, non di rado, difficile l'identificazione degli autori materiali delle condotte illecite[2]. Sicché, dinanzi alla eventualità che l'autore materiale del reato resti ignoto, il reato impunito e le vittime sprovviste di tutela, da tempo è maturata una riflessione in merito alla possibilità di ravvisare modelli di imputazione del fatto ai gestori delle piattaforme digitali, quali soggetti agevolmente identificabili e potenziali anelli essenziali nella catena funzionale alla realizzazione di illeciti in rete.

Non sorprende, dunque, che tali soggetti non di rado divengano bersaglio di richieste risarcitorie da parte delle vittime e destinatari di addebiti in sede penale, talora sulla base di asserite forme di responsabilità automatica ed accessoria rispetto a quelle proprie dell'autore del reato[3].

Dall'altro lato, ad alimentare siffatta impostazione si adducono anche ragioni legate al mutato ruolo svolto nel corso del tempo dai c.d. giganti del *web*, i quali parrebbero ormai aver assunto un peso decisivo sul piano politico, oltre che di condizionamento nell'esercizio di diritti fondamentali da parte degli utenti (primo fra tutti, quello alla libera manifestazione del pensiero)[4]. Sicché, detto ruolo sempre più performante dei operatori professionali spingerebbe verso una riconsiderazione delle scelte di "immunizzazione" degli *ISP*, al fine di garantire un più adeguato bilanciamento degli interessi da salvaguardare nel *cyberspace*[5].

Sennonché, la responsabilità penale di tali soggetti per gli illeciti commessi da coloro che usufruiscono dei servizi richiamati è stata pressoché costantemente esclusa sulla base di una pluralità di argomentazioni, di natura sia politico-criminale sia giuridica.

Invero, il tema (complesso e delicatissimo) presenta profili problematici in continua evoluzione, in considerazione dei sempre nuovi meccanismi di

[2] Sul punto *supra* capitolo terzo, paragrafo 2.

[3] Così e *amplius* G. Corrias Lucente, *Ma i* network providers*, i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?*, in *Giur. mer.*, 2004, 2524.

[4] Sul tema, in termini generali, M. Bassini, Internet *e libertà di espressione. Prospettive costituzionali e sovranazionali,* Roma, 2019, in particolare 150 ss.

[5] Così L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme,* in *Trattati giuridici.* Cybercrime, diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 87.

operatività della rete e dei servizi offerti. Senza dimenticare che qualunque soluzione si intenda prospettare, essa non può prescindere da un delicato bilanciamento tra tutela dei diritti individuali (in alcuni casi già tra loro antagonisti) degli utenti, da un lato, e diritto d'impresa dei soggetti che operano come intermediari, dall'altro lato[6].

Esemplificando, in estrema sintesi, si pensi all'utilizzo di sistemi automatizzati per finalità preventive. E' facile intuire come qualunque forma di monitoraggio non possa sconfinare in forme di ingerenze indebite nella vita privata degli individui, né costituire uno strumento di sorveglianza di massa o comprimere, oltre la misura strettamente necessaria, la libertà comunicativa degli utenti, nel rispetto della loro libertà di espressione[7].

In tale prospettiva, per esempio, la Corte di Giustizia dell'Unione europea ha affermato che l'ingiunzione diretta, da parte di un giudice ad un *service provider*, di adottare sistemi di filtro per impedire agli utenti di utilizzare sistemi di *file sharing* in violazione delle norme in materia di diritto d'autore, comprime in modo sproporzionato i diritti e le libertà tutelati dagli artt. 8 e 11 della Carta dei diritti fondamentali dell'Unione europea e dai corrispondenti artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, oltre che la libertà di impresa (art. 16 della Carta) [8].

Ebbene, tanto premesso, nella prospettiva penalistica, il paradigma di imputazione che per lo più viene preso in considerazione, al fine di verifi-

[6] Sul punto, tra gli altri, A. SPAGNOLO, *Bilanciamento tra diritto d'autore, libertà d'impresa e libertà fondamentali nella giurisprudenza recente della Corte di Giustizia*, in *Giur. merito*, 2013, 125 ss.; P. M. SABELLA, Il *fenomeno del* cybercrime *nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di* Internet *per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali,* in *Informatica e diritto*, 2017, 139 ss.

[7] A. VALENTI, M. C. CARDARELLI, G. COLAIACOVO, V. V. CUOCCI, G. FONTANA, W. NOCERINO, A. PROCACCINO, F. G. VITERBO, D. CURTOTTI, *Sistemi di monitoraggio algoritmico delle comunicazioni e tutela dei diritti fondamentali: "*cyber social security*"* research project, in *www.sistemapenale.it.*, n. 4 del 2026, 12.

[8] Corte di Giustizia dell'Unione europea, 24 novembre 2011 (C-70/10, caso Scarlet Extended SA v. SABAM); Corte di Giustizia dell'Unione europea, 16 febbraio 2012 (C-360/10, caso SABAM v. Netlog). In quest'ultimo caso i Giudici hanno ribadito che il gestore di *social networks* non può essere costretto a predisporre un sistema di filtraggio generale, riguardante tutti i suoi utenti, per prevenire l'utilizzo illecito di opere musicali e audiovisive. Tale obbligo comporterebbe una invasione sproporzionata nel diritto alla riservatezza degli utenti ed alla libertà di impresa.

care un possibile coinvolgimento degli intermediari, è quello concorsuale.

Vero è che l'*ISP* può anche essere chiamato a rispondere per illeciti realizzati direttamente con la propria condotta (si pensi, per esempio, alla illecita diffusione di dati personali di alcuni utenti registrati presso di lui o al caricamento diretto con successiva diffusione di un contenuto illecito).

Ma i profili più rilevanti (e controversi) attinenti alla responsabilità di tale soggetto riguardano senz'altro la possibilità che allo stesso siano riferibili profili di rimproverabilità in relazione a reati commessi da terzi[9].

Ci si deve, in altre parole, chiedere se l'*ISP* possa essere chiamato a rispondere a titolo di concorso con l'utente della rete che abbia immesso sulla stessa materiale idoneo ad integrare gli estremi di un reato avvalendosi delle infrastrutture di comunicazione gestite dal *provider* medesimo.

Sotto tale angolazione, due sono le forme di responsabilità che si potrebbero astrattamente configurare: una di tipo omissivo e l'altra di tipo commissivo. Quest'ultimo schema di imputazione opera nelle ipotesi in cui sia possibile dimostrare che il *provider* abbia consapevolmente fornito un contributo attivo nell'immissione di dati illeciti sul suo *server*[10].

Pur in tale prospettiva, si ritiene comunque che l'eventuale agevolazione, consapevolmente prestata, debba andare oltre la mera fornitura dell'accesso ovvero il mantenimento del collegamento alla rete (che presenterebbero un contenuto assolutamente neutro ed in sé consentito dall'ordinamento giuridico), dovendo emergere ulteriori connotati d'illiceità nelle modalità di svolgimento del servizio, «assistititi da un dolo di partecipazione particolarmente intenso e da un'oggettiva possibilità d'impedire la commissione del reato»[11].

[9] In argomento, A. BENEVENTO, *L'apposizione di filtri ai commenti degli utenti non esclude il concorso del* blogger *nella diffamazione*, in *Diritto di Internet*, 2019, 157 ss.

[10] Sul tema, Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995. In dottrina, di recente, G. FIORINELLI, *L'attuale ruolo del* provider *nella società digitale: modelli di responsabilità penale,* in *www.lalegislazionepenale.eu,* 27.12.2022, in particolare 7 ss.

[11] S. SEMINARA, *La pirateria su* Internet *e il diritto penale,* in *Riv. trim. dir. pen. econ.*, 1997, 101; S. SEMINARA, Internet *(diritto penale),* in *Enciclopedia del diritto, Annali,* VII, Milano, 2014, 596. Analogamente, V. TORRE, *Sulla responsabilità penale del* service provider *e la definizione del comportamento esigibile alla luce delle norme contro la pedopornografia,* in *Tutela penale della persona e nuove tecnologie*, a cura di L. PICOTTI, Padova, 2013, 175 ss. Sulla fragile linea di confine «tra l'ipotesi di punibilità del *provider* a titolo concorsuale in forma commissiva — in ragione dell'espletamento consapevole, da parte sua, di condotte agevolatorie dell'altrui azione illecita, e sostanziantesi in attività ulteriori rispetto alla mera fornitura dell'accesso ovvero al

Così, per esempio, la giurisprudenza si è soffermata sulla posizione del titolare del sito *web* il quale metta in comunicazione gli utenti che, in via principale, commettono un delitto contro la proprietà intellettuale[12]. In siffatta ipotesi, osserva la Corte, se il sito «si limitasse a mettere a disposizione un protocollo di comunicazione (quale quello *peer–to–peer*) per consentire la condivisione di *files*, contenenti l'opera coperta da diritto d'autore, ed il loro trasferimento tra utenti, il titolare del sito stesso sarebbe in realtà estraneo al reato»[13].

Nondimeno, a diversa conclusione si dovrebbe giungere, allorché il titolare del sito realizzasse attività ulteriori, quali l'indicizzazione delle informazioni provenienti dagli utenti, autori degli *uploadings* illeciti. Sicché, se dette informazioni (*i.e.* le chiavi per accedere al materiale protetto), «essenziali perché gli utenti possano orientarsi chiedendo il *downloading* di quell'opera piuttosto che un'altra, sono in tal modo elaborate e rese disponibili nel sito, ad esempio a mezzo di un motore di ricerca o con delle liste indicizzate, il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati»[14]. Ed allora, benché lo scambio dei *file* avvenga da utente ad utente (*peer–to–peer*), «l'attività del sito *web* (al quale è riferibile il protocollo di trasferimento e l'indicizzazione di dati essenziali) è quella che consente ciò e pertanto c'è un apporto causale a tale condotta che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone ex art. 110 c.p.»[15].

Certo è che la questione si fa ancora più complessa allorché i meccanismi di filtraggio, indicizzazione, selezione o organizzazione dei contenuti siano automatici, affidati cioè ad algoritmi o altri strumenti dotati di intelligenza artificiale. In questi casi, infatti, occorre chiedersi quale componente di rimproverabilità in sede penale potrebbe residuare in capo all'*ISP*[16].

mantenimento del collegamento alla rete (che presenterebbero un «contenuto assolutamente neutro ed in sé consentito dall'ordinamento giuridico») — e la doverosa esclusione di detta punibilità — a fronte di condotte del *provider* limitate alla *mere conduit*», F. RESTA, *La responsabilità penale del* provider*: tra* laissez faire *ed obblighi di controllo*, in *Giur. merito,* 2004, 1728.

[12] Cfr. Cass. pen., sez. III, 29 settembre 2009, n. 49437, in *Diritto dell'informazione e dell'informatica*, 2010, 437, con nota di F. MERLA, *Diffusione abusiva di opere in internet e sequestro preventivo del sito web: il caso "*The Pirate Bay*"*, ivi, 448 ss.

[13] Cass. pen., sez. III, 29 settembre 2009, n. 49437, cit., punto n. 5 del Considerato in diritto.

[14] Cass. pen., sez. III, 29 settembre 2009, n. 49437, cit., punto n. 5 del Considerato in diritto.

[15] Cass. pen., sez. III, 29 settembre 2009, n. 49437, cit., punto n. 5 del Considerato in diritto. Sul punto, nella dottrina, D. COSTA, *La responsabilità dell'*Internet Service Provider *per i reati in materia di diritto d'autore*, in *Giurisprudenza penale web,* n. 2 del 2022, 40.

[16] In argomento S. SEMINARA, Internet *(diritto penale),* cit., 601 ss.; F. BASILE, *Intelligenza*

2. *Il problema della posizione di garanzia*

Al di fuori di siffatta casistica, senz'altro più complessa si rivela la configurabilità di un concorso mediante omissione nel reato da altri realizzato. In tale diversa prospettiva, infatti, da un lato (e innanzitutto), si dovrebbero ritenere superabili le argomentazioni che vorrebbero circoscrivere la responsabilità per omesso impedimento (anche) nella dimensione concorsuale al novero dei reati causali puri[17]. Dall'altro lato, occorrerebbe dimostrare la sussistenza in capo all'agente di una posizione di garanzia, al fine di equiparare il non impedire al cagionare. Si tratta, dunque, di verificare se nel nostro ordinamento si possa individuare la fonte di un siffatto dovere di impedimento[18].

L'analisi di questo profilo impone che, innanzitutto, si prenda in considerazione la normativa che disciplina specifici obblighi dell'*ISP* per comprendere se sia effettivamente possibile radicare in essi un'autentica posizione di garanzia.

La prima fonte cui storicamente si è fatto riferimento per tentare di risolvere il problema della responsabilità dell'*IPS* fu il d. lgs. 9 aprile 2003, n. 70 ("Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico")[19], che conteneva alcune disposizioni (oggi abrogate dal d.lgs. n. 50 del 2024[20]) volte a disciplinare la responsabilità civile del prestatore di un servizio della società dell'informazione[21].

artificiale e diritto penale: quattro possibili percorsi di indagine, in *www.dirittopenaleuomo.org*, n. 10, 2019; A. BACCIN, *Responsabilità penale dell'*Internet service provider *e concorso degli algoritmi negli illeciti* online*: il caso* Force v. Facebook, in *www.sistemapenale.it*, 2020, n. 5, 75 ss.

[17] *Amplius* e per tutti, G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale,* Bologna, 2025, 633, 670 ss.

[18] Per un'analisi di siffatto aspetto problematico nell'ordinamento spagnolo, A. GALÁN MUÑOZ, *Los ciberdelitos en el ordenamiento español*, Barcellona, 2019, 19 ss.

[19] La Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 è relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[20] D. lgs. 25 marzo 2024, n. 50 ("Disposizioni integrative e correttive del decreto legislativo 8 novembre 2021, n. 208, recante il testo unico dei servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato, in attuazione della direttiva (UE) 2018/1808 di modifica della direttiva 2010/13/UE").

[21] Il riferimento è, in particolare, agli artt. 14, 15, 16, 17. L'art. 14 (Responsabilità nell'atti-

Invero, detto decreto legislativo disciplinava la responsabilità degli *ISP* in

vità di semplice trasporto - *Mere conduit*), così recitava: «1. Nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non è responsabile delle informazioni trasmesse a condizione che: a) non dia origine alla trasmissione; b) non selezioni il destinatario della trasmissione; c) non selezioni né modifichi le informazioni trasmesse. 2. Le attività di trasmissione e di fornitura di accesso di cui al comma 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo. 3. L'autorità giudiziaria o quella amministrativa, avente funzioni di vigilanza, può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse».

L'art.15 (Responsabilità nell'attività di memorizzazione temporanea - *Caching*), prevedeva che «1. Nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione. 2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

L'art. 16 (Responsabilità nell'attività di memorizzazione di informazioni - *Hosting*), disponeva che «1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. 2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore. 3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse».

termini "negativi", ovvero prevedendo solo le condizioni per l'esenzione da detta responsabilità.

In tale prospettiva, assumeva particolare rilevanza soprattutto l'art. 17, il quale – sotto la rubrica "Assenza dell'obbligo generale di sorveglianza" – stabiliva: «1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto: a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite. 3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente»[22].

Ebbene, alla luce della disciplina contenuta nei dati normativi richiamati, in modo quasi unanime, nel tempo, si è ritenuto che non fosse configurabile in capo all'*ISP* alcun obbligo di sorveglianza *ex ante*, vale a dire un obbligo di controllo preventivo e generale sulle attività svolte dagli utenti, né tantomeno un obbligo di ricercare attivamente fatti e circostanze idonee ad indicare la presenza di attività illecite negli spazi dallo stesso gestiti[23].

[22] Una disciplina speciale delle responsabilità degli intermediari informatici (era e tuttora) è prevista per alcuni specifici settori, tra i quali, per esempio, la tutela del diritto d'autore, la pedopornografia o il terrorismo. In materia di tutela del diritto d'autore viene in rilievo la disposizione contenuta nell'art. 102 *septies* l. n. 633 del 1941. Per quanto la pedopornografia, il riferimento è alla disciplina dettata dagli artt. 14 *ter* e 14 *quater* l. n. 269 del 1998. Con riferimento, invece, al terrorismo, deve segnalarsi la previsione dell'art. 7 d. lgs. n. 107 del 2023.

[23] In questo senso nella dottrina, per tutti, S. SEMINARA, Internet *(diritto penale),* cit., 597 ss.; A. INGRASSIA, *Il ruolo* dell'Isp *nel ciberspazio: cittadino, controllore o tutore dell'ordine*?, in *www.penalecontemporaneo.it,* 2012, in particolare 25 ss.; R. BARTOLI, *Brevi considerazioni*

Tanto premesso, avrebbe fatto difetto il presupposto fondante una posizione di garanzia in capo agli operatori telematici rispetto ai contenuti da altri prodotti e/o trasmessi[24]. Da un lato, infatti, il legislatore, all'art. 17 del citato d. lgs. n. 70 del 2003, aveva espressamente escluso - come detto - l'esistenza di un obbligo generale di sorveglianza da parte dell'*ISP* sui contenuti caricati dagli utenti, nonché l'onere per lo stesso di ricercare fatti o circostanze sintomatici di attività illecite. Dall'altro lato, anche là dove erano contemplati in capo all'*ISP* specifici obblighi di segnalazione e rimozione di contenuti illeciti, la violazione di detti obblighi comportava esclusivamente conseguenze di natura extrapenale (responsabilità civile o sanzioni di natura amministrativa).

A siffatti argomenti fondati sul diritto positivo, si è inoltre sempre aggiunta un'ulteriore argomentazione di natura sistematica, volta a ribadire come le richiamate previsioni non avrebbero potuto in ogni caso fondare un obbligo di impedimento, in quanto, logicamente, il dovere di segnalazione e/o di rimozione è destinato a sorgere allorquando il reato si è già consumato, mentre quello di impedimento è funzionale, per sua intrinseca natura, proprio alla prevenzione della commissione di illeciti penali, nel senso che la corretta estrinsecazione del potere del garante dovrebbe servire a neu-

*sulla responsabilità penale dell'*internet service provider, in *Dir. pen. proc.*, 2013, 600 ss.; G. P. ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in *w ww.archiviopenale.it*, 2017, n. 2, 1 ss.; S. BRASCHI, Social media *e responsabilità penale dell'*Internet Service Provider, in *MediaLaws*, 2020, 3, 164 s. Nell'ambito della giurisprudenza Cass. pen., sez. V, 8 novembre 2018, n. 12546, punti n. 2.2, 2.3 del Considerato in diritto. Nella giurisprudenza di merito, Tribunale di Milano, 18 marzo 204 (in *Giur. merito*, 2004, 1713, con nota di F. RESTA, *La responsabilità penale del* provider*: tra* laissez faire *ed obblighi di controllo*, *ivi,* 1715 ss.), ad avviso della quale «i proprietari delle infrastrutture di telecomunicazione (*network providers*), i fornitori di accessi (*access providers*) ed i fornitori di servizi (*service providers*) non possono ritenersi corresponsabili dei reati commessi da coloro che utilizzano i loro servizi (*content providers*) per mera omissione di controllo, in quanto, da una parte, non hanno un obbligo giuridico di evitare l'evento e dall'altra, per la struttura stessa della rete, non hanno la possibilità concreta di esercitare un efficace controllo sui messaggi ospitati sul proprio sito. Non può affermarsi una responsabilità dei medesimi soggetti a titolo di dolo eventuale, ogniqualvolta non vi siano specifici elementi che consentano di ricondurre nella loro sfera di conoscibilità una specifica attività illecita commessa per loro tramite e ciò per la struttura aperta di *internet*, che rende in astratto possibile immissioni costanti, autonome e non controllabili sugli spazi gestiti dal *server*».

[24] Tra gli altri, G. STEA, *La diffamazione a mezzo* Internet*,* in *Riv. pen.,* 2008, par. 6.5.

tralizzare il rischio di verificazione dell'evento lesivo per il bene protetto[25].

Anche la giurisprudenza ha generalmente (salvo isolate voci contrarie) escluso, nei casi considerati, la responsabilità penale dell'*ISP* per l'impossibilità di configurare obblighi di impedimento *ex ante*.

In particolare, a partire dalla pronuncia relativa al noto caso *Google* vs. *Vividown*[26], la Cassazione ha condiviso l'idea che l'*ISP* sia tenuto solo ad obblighi di segnalazione e di rimozione di contenuti a seguito dell'intervento dell'autorità. L'insussistenza di una responsabilità per omesso impedimento del reato altrui è stata affermata, innanzitutto, alla luce dei citati artt. 16 e 17 d.lgs. n. 70 del 2003.

3. *L'analogia* in malam partem *della disciplina in tema di stampa*

Muovendo dalla pressoché concorde impossibilità di pervenire ad un'affermazione di responsabilità degli *ISP* sulla base di una supposta peculiare e autonoma posizione di garanzia in capo agli stessi, ci si è chiesti se fosse allora percorribile la strada di una loro sostanziale equiparazione ai direttori di giornale[27].

Invero, anche questo percorso argomentativo ha, per lo più, incontrato un solido sbarramento, in considerazione della ritenuta impossibilità di estendere all'*ISP* la disciplina in tema di stampa, di cui all'art. 57 c.p., alla luce di una pluralità di argomentazioni.

Il primo problema concerne, infatti, la non riconducibilità del concetto di "reati commessi a mezzo *Internet*" a quello di "reati commessi con il mezzo della stampa"[28], nonostante gli indubbi profili di somiglianza, quanto ad ef-

[25] Per tutti, C. PAONESSA, *Obbligo di impedire l'evento e fisiognomica del potere impeditivo*, in *Criminalia* 2012, 655.

[26] Cass. pen., sez. III, 17 dicembre 2013, 5107, Rv. 258520. Sulla pronuncia *de qua,* S. CORBETTA, *Caso "GIoogle": nessuna responsabilità dell'*Host Provider *per l'omesso impedimento di reati realizzati dagli utenti della rete*, in *Dir. pen. proc.,* 2014, 277 ss. Sulla vicenda e sulla pronuncia di merito adottata dal Tribunale di Milano, P. SILVESTRE, *La sempreverde tentazione di sostituirsi al legislatore*, in *Giur. mer.*, 2013, 1577 ss.

[27] *Amplius* e per tutti, S. SEMINARA, *La responsabilità penale degli operatori su* Internet*,* in *Dir dell'informazione e dell'informatica,* 1998, in particolare 750 ss.

[28] Sul punto, *amplius*, C. MELZI D'ERIL, G. E. VIGEVANI, *La responsabilità del direttore del periodico telematico, tra facili equiparazioni e specificità di* Internet, in *Diritto dell'informazione e dell'informatica*, 2010, 91 ss.

fetti, tra i due mezzi di comunicazione. Infatti, un'esegesi rigorosa della disposizione di cui all'art. 1 della l. n. 47 del 1948 porterebbe a ritenere che la telematica non è stampa e ad estromettere, quindi, dalla relativa definizione il mezzo digitale[29]. Con la conseguenza che il divieto di analogia *in malam partem* in materia penale impedirebbe di estendere al *web* i paradigmi imputativi riservati dal legislatore alla stampa, tra i quali, appunto, l'art. 57 c.p.[30].

A questo si aggiunga che la posizione dell'*ISP* non risulterebbe assimilabile a quella del direttore, poiché manca al *provider* una posizione sovraordinata e direzionale, oltre a far comunque difetto quella capacità di controllo dei contenuti che costituisce la ragione della responsabilità dei direttori di stampa periodica. Mentre, infatti, il direttore di stampa periodica può (o si riteneva "potesse", ai tempi dell'entrata in vigore della legge sulla stampa) espletare una capillare verifica del prodotto editoriale, altrettanto non potrebbe dirsi con riferimento ai fornitori di servizi telematici, atteso che i contenuti diffusi *online* sono enormemente più vasti rispetto a quelli stampati; con la conseguenza che il loro omesso controllo non potrebbe essere rimproverato neppure in termini di responsabilità colposa.

In altre parole, il principio d'inesigibilità assurgerebbe alla stregua di criterio guida della soluzione negativa, che peraltro parrebbe escludere, anche in termini di politica criminale, la legittimità costituzionale (in relazione al principio di colpevolezza) dell'introduzione di fattispecie penali proprie degli operatori telematici impositive di obblighi di controllo penalmente sanzionati sui contenuti immessi da terzi[31].

Sostanzialmente in questo senso si è espressa anche la giurisprudenza[32], la quale – almeno per un certo periodo di tempo – aveva per lo più escluso che le comunicazioni telematiche potessero essere riconducibili alla nozione

[29] Così, tra gli altri, C. MELZI D'ERIL, G. E. VIGEVANI, *La responsabilità del direttore del periodico telematico, tra facili equiparazioni e specificità di* Internet*,* cit., 95; D. PETRINI, *Il direttore della testata telematica, tra* horror vacui e prospettive di riforma; sperando che nulla cambi, in *Riv. it. dir. proc. pen.*, 2012, 1611 ss.

[30] C. MELZI D'ERIL, G. E. VIGEVANI, *La responsabilità del direttore del periodico telematico, tra facili equiparazioni e specificità di* Internet*,* cit., 96.

[31] Così G. CORRIAS LUCENTE, *Ma i* network providers*, i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che gestiscono?*, in *Giur. mer.*, 2004, 2526.

[32] Cass. pen., sez. V, 15 maggio 2008, n. 24018, in *deJure,* che evoca il «tentativo infecondo», posto in essere dai giudici di merito, «di estendere, in ambito penale, alle comunicazioni telematiche la normativa sulla stampa».

di stampa e, conseguentemente, che il direttore di un periodico *online* potesse ritenersi responsabile per il reato di omesso controllo, ex art. 57 c.p. A detta conclusione si perveniva anche in considerazione – come anticipato – dell'impossibilità per il direttore della testata *online* di impedire le pubblicazioni di contenuti diffamatori "postati" direttamente dall'utenza[33].

Sennonché, nel 2015 siffatta posizione è stata messa in discussione da un dirompente intervento delle sezioni unite della Cassazione[34], le quali, dovendosi occupare della sequestrabilità di una testata giornalistica telematica, hanno, invece, equiparato quest'ultima a quella tradizionale in formato cartaceo, riconducendola alla nozione di "stampa" di cui all'art. 1 l. n. 47 del 1948. E' stata, nondimeno, mantenuta ferma la distinzione con i nuovi mezzi di manifestazione del pensiero destinati ad essere trasmessi per via telematica (*forum*, *blog*, *newsletter*, *social* network, ecc.), i quali, pur integrando forme di espressione del diritto di cui all'art. 21 Cost., non potrebbero godere delle garanzie previste in tema di sequestro per la stampa. Risulterebbe, in altre parole, fondamentale distinguere l'area dell'informazione di tipo professionale, veicolata per il tramite di una testata *online*, dall'ambito della diffusione spontanea di notizie da parte di singoli utenti.

Tuttavia, tale pronuncia, pur muovendo dall'intento di estendere un profilo di garanzia alla testata giornalistica *online* (inapplicabilità del sequestro preventivo, mediante oscuramento della pagina telematica), producendo un evidente e rilevante *effetto in bonam partem,* ha presto innescato immediate

[33] Così Cass. pen., sez. V, 16 luglio 2010, n. 35511, Rv. 248507. Sulla pronuncia *de qua*, C. MELZI D'ERIL, Roma locuta: *la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line, in *Diritto dell'informazione e dell'informatica*, 2010, 895 ss.; I. SALVADORI, *La normativa penale sulla stampa non si applica,* de jure condito*, ai giornali telematici*, in *Cass. pen.*, 2011, 2982 ss. Successivamente a tale *leading case,* nello stesso senso, Cass. pen., sez. V, 28 ottobre 2011, n. 44126, Rv. 251132, sulla quale G. CORRIAS LUCENTE, *Al direttore di un periodico* on line *non si applica il reato previsto dall'art. 57 c.p.,* in *Diritto dell'informazione e dell'informatica,* 2012, 82 ss.

[34] Cass., sez. un., 29 gennaio 2015, n. 31022, Rv. 264090, in *Giur. cost.*, 2015, 1055 ss., con nota critica di L. DIOTALLEVI, *La Corte di cassazione sancisce l'"equiparazione" tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di "scivolamento" dalla "nomofilachia" alla "nomopoiesi"*?, ivi, 1062 ss., ad avviso del quale , «ricorre, infatti, con sempre maggiore frequenza, nell'ambito della giurisprudenza di legittimità, la scelta di avallare opzioni interpretative che, risolvendosi in una "forzatura" della naturale portata semantica delle proposizioni legislative, finiscono - in concreto - per assumere una valenza "creativa" e, in questo senso, "normativa"» (ivi, 1070).

(preoccupanti) ricadute *in malam partem*, derivanti dalla equiparazione della testata telematica a quella tradizionale[35].

Infatti, la nuova nozione "figurata" di stampa, forgiata dalle sezioni unite con finalità di garanzia, è stata ritenuta utilizzabile anche in ambiti ulteriori rispetto a quello in cui era nata, con conseguente estensione agli illeciti commessi attraverso testate digitali di tutta la disciplina concernente i reati a mezzo stampa, compreso l'art. 57 c.p.[36]. Tanto che diverse pronunce successive, richiamando proprio i principi enunciati dalle sezioni unite, hanno ammesso la possibilità di applicare l'art. 57 c.p. al direttore di una testata telematica[37], ferma, invece, restando – come detto – l'esclusione di siffatta estensione agli altri mezzi informatici di manifestazione del pensiero, considerati non riconducibili alla nozione di stampa[38].

Ebbene, è facile intuire come l'assimilazione per analogia tra periodico telematico e periodico cartaceo cagionerebbe la traslazione, nel mondo del *web*, di un modello di imputazione (quello contemplato dall'art. 57 c.p.) espressamente e storicamente costruito sulla carta stampata. A siffatto risultato, dunque, sarebbe possibile pervenire solo passando per un esplicito intervento del legislatore, senza possibilità alcuna per l'interprete di proporre chiavi di lettura evolutive non in linea con il dettato normativo. Invero, l'immaterialità dei contenuti pubblicati nel *web* impedisce, allo stato delle vigente disciplina, l'assimilazione degli stessi alla stampa tradizionale.

Si deve, comunque, segnalare un (condivisibile) ritorno della recente giu-

[35] Così, tra gli altri, F. G. CATULLO, *La responsabilità penale del direttore del giornale telematico tra legislatore pigro e giudice intraprendente,* in *Diritto di Internet*, 2019, 173 ss.

[36] C. MELZI D'ERIL, *L'applicabilità della disciplina prevista per la stampa a* Internet: *l'ultima puntata di una lunga storia, tra legislatore assente e giurisprudenza (molto) creativa*, in *MediaLaws*, 5 novembre 2024, 12, 13.

[37] Cass. pen., sez. V, 11 dicembre 2017, n. 13398, in *Dejure*; Cass. pen., sez. V, 23 ottobre 2018, n. 1275, Rv. 274385.

[38] Cass. pen., sez. V, 19 febbraio 2018, n. 16751, Rv. 272685; Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995; Cass. pen., sez. V, 23 ottobre 2018, n. 1275 (con nota di F. LOMBARDI, *La responsabilità del direttore del periodico telematico ex art. 57 c.p. tra interpretazione estensivo-evolutiva e analogia* in malam partem*,* in *www.giurisprudenzapenale.com,* 11 gennaio 2019), ad avviso della quale «in tema di diffamazione, l'amministratore di un sito *internet* non è responsabile ai sensi dell'art. 57 c.p., in quanto tale norma è applicabile alle sole testate giornalistiche telematiche e non anche ai diversi mezzi informatici di manifestazione del pensiero (*forum*, *blog*, *newsletter*, *newsgroup*, *mailing list*, *Facebook*)». Sulla pronuncia *de qua* v. anche F. G. CATULLO, *La responsabilità penale del direttore del giornale telematico tra legislatore pigro e giudice intraprendente,* cit., 173 ss.

risprudenza di merito ad un orientamento più in linea con il principio di legalità e propenso ad escludere l'applicabilità dell'art. 57 c.p. ai giornali telematici. Ad avviso, infatti, del Tribunale di Milano[39], la definizione di stampa «è del tutto incompatibile con la funzionalità della testata giornalistica *online* e l'applicazione della prima a quest'ultima deve necessariamente passare per un'operazione analogica – preclusa in ambito penale – giacché il senso letterale di "riproduzioni tipografiche" non può certo essere esteso fino a ricomprendere la veicolazione di contenuti di tipo multimediale».

In termini ancora più netti si è espressa anche la Corte d'appello di Milano[40], secondo la quale l'estensione di una garanzia, quale è quella del divieto di sequestro preventivo, da parte della giurisprudenza delle sezioni unite «non può e non deve consentire l'automatica estensione della responsabilità penale per casi non disciplinati dalla legge. Interpretare evolutivamente il concetto di stampa, in assenza di un intervento legislativo, è ammissibile se comporta un trattamento di favore nei confronti del cittadino, ma non se comporta la creazione di nuove fattispecie incriminatrici, agendo in suo svantaggio, perché l'interprete non ha il potere, nell'ambito del diritto penale, di colmare i vuoti normativi lasciati dal legislatore, creando di fatto nuove fattispecie incriminatrici. La giurisprudenza successiva alle sezioni unite del 2015, invece, ha allargato analogicamente *in malam partem* l'obbligo di controllo – e le conseguenze del colposo omesso impedimento di cui all'art. 57 c.p. – anche al direttore del quotidiano *online* in aperto contrasto con il dettato normativo». Sicché, prosegue la Corte, «se davvero un'esigenza di responsabilizzazione per omesso controllo esiste, anche nel settore telematico, è solo il legislatore che può legittimamente farsene carico. Ad oggi, in assenza di una previsione normativa in questo senso, non è compito del giudice colmare un vuoto normativo con l'applicazione analogica di una previsione punitiva»[41].

Con rigore ermeneutico e forza delle argomentazioni la più recente giuri-

[39] Tribunale di Milano, Sezione Giudice per le Indagini preliminari, 14 ottobre 2021, nell'ambito del proc. pen. n. 21763 del 2019 R.G.G.I.P. Nello stesso senso, altresì, Tribunale di Milano, sez. V penale, 15 marzo 2024, n. 3825.

[40] Corte d'Appello di Milano, sez. III penale, 24 novembre 2022, § 4, punto n. 4.2.4. Sulla pronuncia *de qua,* S. VIMERCATI, Revirement *dei giudici di merito: il direttore della testata telematica non risponde del reato di omesso controllo. Verso due nozioni di "stampa"?,* in *MediaLaws,* n. 2, 2023, 382 ss.

[41] Corte Appello Milano, sez. III penale, 24 novembre 2022, § 4, punto n. 4.2.4.

sprudenza di merito parrebbe, dunque, in tal modo voler riportare la prassi applicativa nell'alveo dei principi fondamentali.

4. *La mancata rimozione di contenuti illeciti*

Tanto premesso, occorre però precisare che se la questione relativa alla insussistenza di una posizione di garanzia dell'*ISP* parrebbe sufficientemente consolidata in relazione all'attività di ingresso dei dati e delle informazioni nella rete, il discorso si fa, invece, enormemente più complicato in relazione al comportamento dei gestori delle infrastrutture telematiche concernente la permanenza di siffatti dati negli spazi da loro gestiti.

Proprio in relazione a questa seconda eventualità, infatti, si è affermato un indirizzo interpretativo, che riconosce la possibilità di configurare una responsabilità penale dell'*hosting provider*, a titolo di concorso omissivo nel reato commesso dall'utente.

Tale impostazione è stata fatta propria da alcune pronunce della Cassazione[42], che hanno attribuito al gestore di un sito *internet* una responsabilità penale concorsuale per non aver rimosso un contenuto diffamatorio, di cui era venuto a conoscenza dopo la pubblicazione. Il gestore del sito che apprenda la pubblicazione da parte di terzi di contenuti obiettivamente denigratori e non si attivi tempestivamente per rimuovere tali contenuti – si legge nella pronuncia – «finisce per farli propri e quindi per porre in essere ulteriori condotte di diffamazione, che si sostanziano nell'aver consentito, proprio utilizzando il suo *web-log*, l'ulteriore divulgazione delle stesse notizie diffamatorie»[43].

Invero, anche siffatta opzione interpretativa solleva non poche perplessità posto che finisce per configurabile una responsabilità a titolo concorsuale in un reato già perfezionatosi[44]. Detta responsabilità, in altre parole, parrebbe fondarsi su un (asserito) obbligo di impedimento non di un reato, ma

[42] Cass. pen., sez. V, 27 dicembre 2016, n. 54946, in *www.giurisprudenzapenale.it*, 3 gennaio 2017, con nota di M. MIGLIO, *I gestori di un sito* internet *rispondono penalmente per i commenti offensivi pubblicati dagli utenti;* nonché, sia pure in relazione alla posizione di un *blogger,* Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, in *www.penalecontemporaneo.it,* 17 maggio 2019, con nota di C. PAGELLA, *La Cassazione sulla responsabilità del* blogger *per contenuti diffamatori (commenti) pubblicati da terzi.*

[43] Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, punto 4.3. del Considerato in diritto.

[44] In argomento v anche *supra* capitolo terzo, paragrafo 7.

degli effetti dello stesso[45], per il fatto di aver mantenuto consapevolmente l'articolo diffamatorio sul sito, consentendo che lo esso protraesse l'efficacia offensiva sua propria[46].

Invero, l'omesso impedimento, *ex post,* della protrazione di un reato non può rientrare nella clausola di equivalenza di cui all'art. 40, comma 2, c.p. e potrebbe, eventualmente, rilevare penalmente solo in quanto espressamente previsto da una norme di legge munita di apposita sanzione, la cui assenza tuttavia non può certo essere colmata attraverso interpretazioni tese a convertire un ordine giudiziale nel presupposto di una responsabilità omissiva impropria[47].

Ci si troverebbe, in altre parole, dinanzi alla creazione giurisprudenziale, ancora una volta *in malam partem,* di un paradigma di responsabilità ignoto al sistema penale, giustificata e camuffata alla luce delle intrinseche peculiarità di funzionamento dei mezzi di comunicazione legati alle nuove tecnologie.

La stessa giurisprudenza parrebbe, del resto, aver colto siffatta difficoltà nel momento in cui si riconosce che evidenti «perplessità in ordine a tale impostazione scaturiscono dal fatto che l'obbligo d'impedimento, sul quale si fonda il giudizio di responsabilità concorsuale, è stato collocato in un momento successivo a quello della consumazione del reato che è diretto ad impedire, facendo così breccia nella possibilità di configurare la fattispecie omissiva impropria di cui al combinato disposto degli artt. 40 e 110 c. p. Invero, è incontroverso che il delitto di diffamazione abbia natura di reato istantaneo in quanto si consuma nel momento della divulgazione della manifestazione lesiva dell'altrui reputazione (…)» vale a dire «nel momento della pubblicazione in rete del contenuto offensivo, per cui un obbligo di rimozione di quello stesso contenuto sarebbe possibile solo dopo la consumazione del reato»[48].

Sennonché – si aggiunge, altresì, in siffatta prospettiva – per superare tali perplessità sulla configurabilità di una responsabilità in concorso ex artt. 40 e 110 c. p. si potrebbe fare ricorso «alla figura della pluralità di reati,

[45] S. Seminara, Internet *(diritto penale),* cit., 600; A. Ingrassia, *Responsabilità penale degli* internet service provider*: attualità e prospettive,* in *Dir. pen. proc.*, 2017, 1624.

[46] Così Cass. pen., sez. V, 27 dicembre 2016, n. 54946, cit., nell'unico punto del Considerato in diritto.

[47] S. Seminara, Internet *(diritto penale),* cit., 600.

[48] Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, punto n. 4.2. del Considerato in diritto.

integrati dalla ripetuta trasmissione del dato denigratorio». In altri termini, se il gestore del sito apprende che sono stati pubblicati da terzi contenuti obiettivamente denigratori e non si attiva tempestivamente a rimuovere tali contenuti, finirebbe per farli propri e quindi «per porre in essere ulteriori condotte di diffamazione, che si sostanziano nell'aver consentito, proprio utilizzando il suo *web-log*, l'ulteriore divulgazione delle stesse notizie diffamatorie»[49].

Invero, neppure siffatta artificiosa ricostruzione riesce a vincere le difficoltà teoriche già evidenziate che si oppongono alla configurabilità di un'automatica autonoma responsabilità penale in capo al *provider* collegata alla mera mancata rimozione dei contenuti illeciti da parte dello stesso. A tale risultato sarebbe possibile pervenire unicamente attraverso l'espressa previsione di reati omissivi propri volti appunto a presidiare penalmente l'adempimento di obblighi di collaborazione e/o rimozione.

Tutt'altro che trascurabile inoltre appare il delicatissimo profilo legato all'individuazione dei limiti di quello che ad avviso di taluno sarebbe equiparabile ad un vero e proprio potere di censura in capo all'*ISP* per conto dell'ordinamento[50], potendo egli disporre dei mezzi tecnici ma non di quelli "culturali" per realizzarla. Con la possibile paradossale conseguenza che, se per evitare in radice eventuali azioni di responsabilità, il *provider* fosse indotto a inibire o cancellare dati e/o contenuti, anche solo potenzialmente, lesivi, la rimozione del suddetto materiale potrebbe luogo ad un obbligo risarcitorio dell'*ISP* nei confronti dell'utente ingiustamente censurato[51].

[49] Cass. pen., sez. V, 8 novembre 2018, n. 12546, Rv. 275995, punto n. 4.3. del Considerato in diritto.

[50] Così L. GUIDOBALDI, You Tube *e la diffusione di opere protette dal diritto d'autore: ancora sulla responsabilità dei* providers*, tra* hoster *attivi, conoscenza dell'illecito e obbligo di sorveglianza,* in *Diritto dell'informazione e dell'informatica*, 2010, 293, ad avviso del quale «sostenere che il D. Lgs. 70/2003 preveda che *l'*host provider debba attivarsi per la rimozione del materiale semplicemente segnalato come illecito dall'avente diritto, senza attendere un provvedimento formale da parte delle autorità procedendovi autonomamente, indipendentemente dall'accertamento del suddetto illecito o da un qualche *fumus boni juris*, e caricandosi di tutti i costi dell'intervento non equivale forse di fatto ad introdurre l'obbligo di un controllo preventivo, incentivando gli operatori a filtrare il più possibile i contenuti che gli pervengono per diminuire il rischio di risarcimenti e sanzioni (anche a scapito della libertà di connessione e di manifestazione del pensiero) tornando così a promuovere la tanto ripudiata figura del censore telematico privato?».

[51] A. INGRASSIA, *Responsabilità penale degli internet service provider: attualità e prospettive,* cit., 1627.

5. *Il Digital Services Act*

Come anticipato, il regime della responsabilità degli *Internet Service Providers* è stato di recente rivisto per effetto dell'entrata in vigore del Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali (c.d. *DSA*)[52].

La Direttiva *e-commerce*[53], attuata nell'ordinamento italiano dal più volte citato d. lgs. n. 70 del 2003, risultava, infatti, ormai inidonea a rispondere alle esigenze di un mercato profondamente mutato. Come si legge nel primo *Considerando* del citato Regolamento, i «servizi della società dell'informazione e in particolare i servizi intermediari sono diventati una componente significativa dell'economia dell'Unione e della vita quotidiana dei suoi cittadini. A vent'anni dall'adozione del quadro giuridico esistente applicabile a tali servizi stabilito nella direttiva 2000/31/CE del Parlamento europeo e del Consiglio, modelli di business e servizi nuovi e innovativi, quali le reti sociali (cosiddetti *social network*) e le piattaforme *online* che consentono ai consumatori di concludere contratti a distanza con operatori commerciali, hanno permesso agli utenti commerciali e ai consumatori di accedere alle informazioni, diffonderle ed effettuare transazioni in modi nuovi. Attualmente la maggior parte dei cittadini dell'Unione utilizza tali servizi quotidianamente. La trasformazione digitale e il maggiore utilizzo di tali servizi hanno tuttavia anche dato origine a nuovi rischi e sfide per i singoli destinatari dei vari servizi, per le imprese e per la società nel suo insieme»[54].

A questo si aggiunga che, nel corso del tempo, gli *ISP*, nati con lo scopo di fornire un accesso alle principali reti di comunicazione elettronica e di consentire la diffusione passiva di contenuti, hanno progressivamente cambiato volto. Così, «abbandonando via via la propria veste di "intermediari neutri" in favore di un ruolo maggiormente attivo, questi soggetti sono diventati dei veri e propri accentratori delle informazioni e dei contenuti scambiati e creati dagli utenti sulla rete»[55], con la sempre più rilevante possibilità in

[52] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

[53] Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico

[54] *Considerando* n. 1 Reg. (UE) 2022/2065, cit.,

[55] D. Costa, *La responsabilità dell'*Internet Service Provider *per i reati in materia di diritto d'autore*, in *Giurisprudenza penale web*, n. 2 del 2022, 5.

capo agli stessi di intervenire direttamente sui contenuti pubblicati dagli utenti medesimi[56].

E, se è vero che la crescita esponenziale del ricorso ai servizi digitali da parte dei fruitori è principalmente volta a soddisfare finalità legittime e socialmente utili di qualsiasi tipo, al tempo stesso, tuttavia, si è anche sviluppato il ruolo degli operatori professionali nell'intermediazione e nella diffusione di informazioni e attività illegali o comunque dannose[57].

Sicché, come anticipato, la disciplina contenuta nella Direttiva *e-commerce* è stata ritenuta anacronistica in quanto tale da garantire un *safe harbour* eccessivamente ampio e ingiustificato rispetto all'attuale potenza economica e tecnologica dei fornitori dei servizi *Internet*.

In tale prospettiva, il *DSA* detta norma armonizzate con l'obiettivo di garantire un ambiente *online* sicuro, prevedibile e affidabile, in cui i diritti fondamentali siano efficacemente tutelati e l'innovazione sia agevolata, contrastando al contempo la diffusione di contenuti illegali e i rischi per la società che la diffusione della disinformazione può generare[58].

Nondimeno, se, per un verso, il *DSA* ha esplicitamente imposto, in modo del tutto condivisibile, nuovi e più stringenti obblighi per i fornitori di servizi digitali (*due diligence obligations*), parametrati alle loro dimensioni, oltre che alla tipologia di attività che questi svolgono[59], e concernenti non solo ciò che viene pubblicato, ma il modo stesso in cui i servizi sono progettati, presentati e gestiti; per altro verso, sotto il profilo dell'eventuale configurabilità di una responsabilità penale dei fornitori dei servizi digitali, il DSA parrebbe aver confermato l'impostazione contenuta nella precedente disciplina[60].

[56] Sul tema L. D'AGOSTINO, *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di* compliance*,* in *www.penalecontemporaneo.it, Riv. Trim.,* 2021, n. 4, 282 ss.; L. VIOLANTE, *Diritto e potere nell'era digitale.* Cybersociety*,* cybercommunity*,* cyberstate*,* cyberspace*: tredici tesi,* in *Rivista di BioDiritto,* 2022, in particolare 147 ss.

[57] Così anche il *Considerando* n. 5 del citato Regolamento.

[58] V. il *Considerando* n. 9, nonché l'art. 1 del citato Regolamento.

[59] In argomento, *amplius*, E. BIRRITTERI, *Contrasto alla disinformazione*, Digital Services Act e *attività* di private enforcement: *fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione degli operatori*, in MediaLaws, n. 2, 2023, 52 ss.; O. MURRO, *Il ruolo delle piattaforme online nella prevenzione della violenza di genere: cosa cambia con il Digital Services Act, in www.penaledp.it*, 19 dicembre 2025.

[60] Sul punto A. GULLO, *Il Digital Services Act e il contrasto alla disinformazione: responsabilità dei provider, obblighi di compliance e modelli di enforcement*, in MediaLaws, n. 2, 2023, 13 ss.; A. VICINANZA, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali:*

L'art. 8 del Regolamento ribadisce, infatti, che «ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono o memorizzano, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali».

Sicché, detta previsione, che in buona sostanza replica quella *ab origine* contenuta nell'art. 15 della Direttiva sul commercio elettronico, parrebbe impedire (ora come allora) l'individuazione di una posizione di garanzia in capo ai *providers* volta a prevenire reati realizzati loro tramite.

Peraltro, come si legge nel *Considerando* n. 17, le norme sulla responsabilità dei prestatori di servizi intermediari previste nel Regolamento «dovrebbero limitarsi a stabilire i casi in cui il prestatore di servizi intermediari interessato non può essere ritenuto responsabile in relazione ai contenuti illegali forniti dai destinatari del servizio. Tali norme non dovrebbero essere intese come una base per stabilire quando un prestatore può essere ritenuto responsabile, circostanza che deve essere determinata in base alle norme applicabili del diritto dell'Unione o nazionale».

La conseguenza di siffatta impostazione è che, da un lato, il *DSA* non può essere utilizzato per fondare una responsabilità penale, e, dall'altro lato, neppure la mancata applicazione delle clausole di esenzione sopra riportate può determinare automaticamente la configurazione di una responsabilità in capo al *provider*. In altre parole, l'operatore dovrebbe rispondere per le violazioni commesse dagli utenti solamente in quanto siano integrati i presupposti di punibilità fissati dal diritto nazionale e non trovino applicazione le ipotesi di esonero da responsabilità previste dal Regolamento[61].

Si precisa, tuttavia, che dette esenzioni da responsabilità «non dovrebbero applicarsi allorché, anziché limitarsi a una fornitura neutra dei servizi mediante un trattamento puramente tecnico e automatico delle informazioni fornite dal destinatario del servizio, il prestatore di servizi intermediari svolga un ruolo attivo atto a conferirgli la conoscenza o il controllo di tali informazioni. Tali esenzioni non dovrebbero di conseguenza essere disponibili per quanto riguarda la responsabilità relativa alle informazioni fornite non dal

dal caso Telegram al Digital Services Act, in *Quaderni AISDUE*, 1/2025, in particolare 10 ss.

[61] S. Braschi, *La responsabilità penale dell'*Internet Service Provider dopo il Digital Services Act, in K. Summerer, M. L. Mattheudakis.,G. M. Caletti, *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea*, Pisa, 2025, 31.

destinatario del servizio ma dallo stesso prestatore del servizio intermediario, anche nel caso di informazioni elaborate sotto la responsabilità editoriale di tale prestatore»[62]. Ed anche tale previsione non farebbe altro che confermare la distinzione tra una eventuale responsabilità commissiva dell'operatore professionale (ben configurabile) rispetto a quella omissiva per mancato impedimento di un illecito altrui (*de iure condito* non configurabile).

Quanto, infine, alla violazione degli obblighi (di trasparenza, di segnalazione e azione, di informazione, di chiarezza, ecc.) rivolti ai prestatori dei servizi digitali, il *DSA* (art. 52) impone agli Stati membri di introdurre norme volte ad applicare sanzioni «effettive, proporzionate e dissuasive», finalizzate ad assicurare il rispetto delle relative prescrizioni.

Il legislatore italiano ha provveduto con d.l. n. 123 del 2023, che all'art. 15 ha stabilito che l'AGCOM, in quanto Coordinatore dei Servizi Digitali, assicura l'effettività dei diritti e l'efficacia degli obblighi stabiliti dal Regolamento, applicando, in caso di loro violazione, sanzioni amministrative pecuniarie fino ad un massimo del 6% del fatturato annuo mondiale, in base a principi di proporzionalità, adeguatezza e rispetto del contraddittorio[63].

Rimane, inoltre, ferma la possibilità per i singoli utenti di chiedere il risarcimento del danno derivante dal mancato adempimento dei predetti obblighi.

A questo si aggiunga che nel nostro ordinamento sono altresì previste, in specifici contesti normativi, fattispecie volte a sanzionare (in via amministrativa o penale, a seconda dei casi), nella forma dell'illecito omissivo proprio, la violazione di obblighi di rimozione, di disabilitazione, di filtraggio. Si pensi, solo a titolo esemplificativo all'art. 174 *sexies* l. 633 del 1941 (sulla protezione del diritto d'autore), all'art. 14 quater d.lgs. n. 269 del 1998 (contro lo sfruttamento della pornografia minorile), all'art. 7 del d.lgs. n. 107 del 2023 (sul contrasto della diffusione di contenuti terroristici *online*).

[62] *Considerando* n. 18 del citato Regolamento.

[63] In argomento, *amplius*, S. BRASCHI, *La responsabilità penale dell'*Internet Service Provider *dopo* il Digital Services Act, cit., 35.

RIFLESSIONI CONCLUSIVE

Il breve percorso ricostruttivo attraverso il "nuovo" mondo digitale ha suscitato molteplici interrogativi che non sarebbe possibile (e non se ne ha la pretesa) soddisfare in questa sede.

Nondimeno, si può tentare l'individuazione di alcuni punti fermi.

I profili di originalità delle fenomenologie criminose rese possibili dalle più recenti tecnologie sono numerosi e sorprendentemente cangianti. Dunque, il primo obiettivo per un corretto approccio alla materia consiste proprio – banalmente – nel saper cogliere tutte le peculiarità delle varie forme offensive, al fine di verificare la riconducibilità delle stesse alle ipotesi di reato esistenti o, piuttosto, la necessità di introdurne di nuove o, quantomeno, di aggiornare in chiave tecnologica paradigmi già consolidati, là dove sia possibile.

Il fine prioritario da perseguire dovrebbe sempre essere quello di garantire una tipicità costruita in modo tale da assicurare all'intervento normativo, al contempo, le condizioni essenziali di efficacia, da un lato, e di garanzia, dall'altro lato.

Nella costruzione di nuove fattispecie incriminatrici, allorché ne emerga la necessità, appare decisamente preferibile un approccio autonomistico, vale a dire il ricorso a modelli di incriminazione dotati di una loro autonomia e specificità, sganciati dunque da una sorta di accessorietà rispetto a soluzioni mutuate "per somiglianza" da ambiti tradizionali. L'opportunità di tecniche di costruzione delle (eventuali) nuove fattispecie incriminatrici che risultino *ab origine* interamente calibrate sulla realtà digitale si ricollega all'esigenza di evitare quell'impostazione insidiosamente metaforica[1], che – come visto – ha caratterizzato le prime fasi di emersione del diritto penale digitale, condizionando, non sempre nella giusta direzione, la messa a fuoco e la soluzione di molteplici questioni.

[1] L'espressione è di G. MORGANTE, *Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del* law enforcement, in *Riv. it. informatica e diritto*, 2025, 105.

Tanto considerato, nonostante il disorientamento (e sotto certi profili) la fascinazione esercitata dal *novum* della realtà digitale, l'impressione è che molti dei problemi posti, sia relativi alla configurazione di nuove ipotesi di reato, sia all'interpretazione di quelle esistenti, possano ancora trovare soluzione attraverso un buon governo delle categorie e dei tradizionali principi penalistici, valorizzando il loro contenuto di garanzia dinamica a fronte di inedite forme di aggressione. La spinta propositiva verso l'introduzione di nuovi paradigmi di responsabilità può forse essere ridimensionata, almeno in un certo numero di casi.

I piani di indagine e di ulteriore futuro approfondimento dovrebbero, dunque, essere due.

Da un lato, si tratterà effettivamente, nel corso del tempo, di sviluppare il tema relativo all'opportunità di modificare la parte generale del diritto penale per tener conto di nuovi (possibili?) modelli di responsabilità, segnatamente nelle ipotesi sempre più frequenti di contributo dei sistemi di intelligenza artificiale autonomi. La discussione sul punto è, come noto, ormai ampia ed estremamente articolata.

In tale prospettiva sarebbe, tuttavia, ingenuo trascurare che la parte generale non presenta, per sua intrinseca natura, una spiccata attitudine ad evolversi attraverso riforme settoriali volte a rinnovarla nelle idee, mantenendone l'originaria coerenza funzionale[2].

L'impatto sulla teoria del reato indotta dalla dimensione digitale è senza dubbio significativo, ma le necessarie elaborazioni teoriche, che dovessero sviluppare e ricondurre a sistema i nuovi concetti, dovranno sempre confrontarsi con la tenuta delle categorie e dei principi.

Del resto, non tutti i cambiamenti del diritto rivestono la medesima portata. Se, infatti, l'introduzione di nuove fattispecie incriminatrici e la modifica di quelle esistenti è fenomeno del tutto fisiologico per assicurare la vitalità dell'ordinamento e il suo aggiornamento al mutare del contesto, il discorso è differente (e molto più delicato) allorché si voglia incidere sull'architettura del sistema penalistico e sui paradigmi giuridici consolidati. A parere di chi scrive è incontestabile che i principi fondativi del nostro sistema debbano trovare comunque applicazione pur a fronte (anzi, a maggior ragione, a fronte) di inedite fenomenologie di criminalità smaterializzata.

[2] Così, F. Giunta, *Ghiribizzi penalistici per colpevoli. Legalità "malalegalità", dintorni,* Pisa, 2019, 52.

Dall'altro lato, più nell'immediato, il problema principale attiene ad un rigoroso confronto tra le scelte politico criminali veicolate dalle fattispecie incriminatrici esistenti e le nuove fenomenologie comportamentali destinate e consumarsi attraverso l'impiego del *medium* digitale.

Le rapsodiche esemplificazioni riportate nel corso della trattazione dovrebbero aver (se non dimostrato, almeno) fatto sorgere il dubbio che l'aggiornamento in chiave tecnologica, da parte (non del legislatore, ma) della giurisprudenza, di fattispecie incriminatrici esistenti abbia aperto ampi margini di incertezza, di fatto impedendo in non pochi casi la corretta comprensione e prevedibilità dell'illiceità della condotta tenuta dall'agente.

Occorre, dunque, ribadire con forza come sia interdetto al giudice penale muovere dalla *ratio* incriminatrice per includere nella previsione legale fatti simili che esplicitamente non vi rientrano, anche qualora ciò sia necessario per colmare una (presunta) lacuna normativa ed anche là dove detta lacuna sia dovuta ad un mutamento sopravvenuto, come effetto, appunto, del progresso scientifico e tecnologico.

Viceversa, nell'ambito considerato, non di rado il "diritto vivente" tende a forzare le barriere di garanzia proprie dello *ius terribile*, rappresentate segnatamente dal principio di stretta legalità e dal correlato divieto di estensione analogica. Ma l'adeguamento del testo normativo al contesto da disciplinare che vada oltre i significati linguisticamente plausibili o che non rispetti lo specifico contenuto di disvalore che il legislatore ha espresso nella fattispecie legale non si concilia con il corretto esercizio dell'attività giurisdizionale[3].

Ed, infatti, «come le leggi impegnano legittimamente anche la società del futuro (che può modificarle attraverso il suo legislatore), così il vincolo di assoggettamento del giudice alla legge permane nonostante la vetustà della legge»[4]. In altre parole, è connaturata all'idea della legalità l'accettazione di una possibile frattura temporale tra l'emersione sociale di un fenomeno lesivo e il riconoscimento ordinamentale della sua rilevanza penalistica.

Sicché: un conto è cercare di adattare le categorie generali a realtà sociali e relazionali diverse da quelle cui facevano riferimento quegli istituti nella loro formulazione legislativa originaria: altro discorso, invece, deve essere fatto a

[3] F. Giunta, *Ghiribizzi penalistici per colpevoli. Legalità "malalegalità", dintorni,* cit., 112; F. C. Palazzo, *Legalità penale, interpretazione ed etica del giudice,* in *Riv. it. dir., proc. pen.,* 2020, 1262.

[4] F. Giunta, *Ghiribizzi penalistici per colpevoli. Legalità "malalegalità", dintorni,* cit., 111.

proposito delle norme incriminatrici di parte speciale, che hanno il compito di tracciare senza ambiguità il solido confine tra lecito e illecito. È, dunque, «soprattutto rispetto alla determinazione delle fattispecie incriminatrici che si pone forte l'esigenza che la legalità penale non vada smarrita»[5].

Del resto, non dovrebbe esserci bisogno di ricordare che la funzione garantista della legalità è destinata ad operare segnatamente sul "confine" della tipicità penale[6], in relazione cioè a quell'area grigia in cui la fattispecie concreta assomiglia (ma stenta ad essere ricondotta) a quella astratta.

La prassi allora non deve e non può prendere il sopravvento sulla scelte politico-criminali espresse dal legislatore. Il bisogno di giustizia non può tradursi nella disgregazione delle «ingabbiature semantico-concettuali elaborate dalla teoria nelle forme legali generali e astratte»[7]. Qualunque sia l'origine della lacuna, il solo potere legittimato a colmarla è il potere legislativo, il quale potrà o ripensare la scelta "selettiva" iniziale, ampliando lo spettro applicativo della norma, ovvero coniare nuove incriminazioni da modellare sui fenomeni emergenti[8].

Certo, si potrebbe obiettare che il quadro normativo è già molto articolato e complesso, basato peraltro su previsioni non di rado introdotte sulla spinta di emergenze (vere o presunte) o di *input* sovranazionali di tutela. A questo si aggiunga che non sempre dette previsioni appaiono coerenti tra di loro e facilmente distinguibili le une dalle altre quanto ad ambito di applicazione. Sicché, date queste premesse, verosimilmente non andrebbe incentivata un'ulteriore rincorsa del legislatore verso incriminazioni che si sforzino di fotografare in modo esasperatamente casistico ogni nuovo fatto che presenti un qualche disvalore, legato all'utilizzo delle nuove tecnologie, ritenuto meritevole di essere sanzionato. Come è ovvio, la necessaria frammentarietà dell'intervento penalistico va sempre preservata.

Vero tutto ciò, la prima complessa sfida potrebbe, dunque, consistere nel mettere ordine – se del caso apportando le opportune integrazioni – nel materiale normativo esistente. Il tempo e l'esperienza intercorsi tra i primi

[5] F. C. Palazzo, *Legalità penale vs creatività giudiziale*, in *Riv. it. dir. proc. pen.*, 2022, 991.

[6] Così, D. Micheletti, Jus contra lex. *Un campionario dell'incontenibile avversione del giudice penale per la legalità,* in *Criminalia* 2016, 164.

[7] F. C. Palazzo, *Sui rapporti tra teoria e prassi nel diritto penale: una panoramica*, in *Diritto penale tra teoria e prassi,* a cura di A. Bondi, G. Marra, R. Palavera, Urbino, 2024, 76.

[8] G. Marinucci, E. Dolcini, G. L. Gatta, *Manuale di diritto penale, Parte generale*, Milano, 2024, 78, 79.

interventi di adeguamento da parte del legislatore alla nuova dimensione digitale e il consolidarsi delle conoscenze in merito a determinate fenomenologie comportamentali e criminose, consentirebbero oggi alla scienza giuridica di affrontare con maggiore lucidità e consapevolezza le sfide aperte da questa importante transizione. L'occasione potrebbe, dunque, essere propizia per un ripensamento complessivo degli strumenti con i quali far fronte alle diverse forme di vulnerabilità aperte dall'irruzione delle nuove tecnologie.

Al contempo, tuttavia, si condivide l'idea che l'*horror vacui* dinanzi ad un'avvertita esigenza di tutela e l'eventuale presa d'atto dei limiti del diritto punitivo possa «forse essere fonte di frustrazione, ma induce ad una maggiore sobrietà nell'affrontare le questioni difficili, evitando di immaginare che vi siano soluzioni magiche, e che il diritto penale sia la bacchetta del mago»[9].

Del resto, il diritto penale non è il solo strumento di tutela al quale sia possibile fare ricorso, tanto più se la testarda convinzione che esso possa davvero esplicare in ogni situazione un'efficace azione preventiva e repressiva debba comportare costi eccessivi in termini di snaturamento della sua impalcatura garantista.

Il tema relativo alla responsabilità degli *ISP* ha, per esempio, mostrato quanto sia rischioso il tentativo di voler ricondurre a tutti i costi all'alveo penalistico, sulla scorta di ricostruzioni interpretative acrobatiche se non addirittura di ragionamenti presuntivi, i paradigmi di responsabilità degli intermediari.

Invero, anche la più recente disciplina introdotta dal *DSA* indica, invece, un percorso alternativo, basato *in primis* su obblighi di segnalazione, di rimozione, di collaborazione con le autorità, di valutazione dei rischi sistemici. Si tratta di interventi che, se correttamente attuati, parrebbero poter esplicare, soprattutto in relazione ai determinate tipologie offensive, un'efficacia ben superiore rispetto alla previsione di fattispecie incriminatrici delle quali, nel *cyberspace,* l'autore persona fisica spesso è destinato a rimanere ignoto.

Questo per dire che al diritto penale è possibile affiancare altri preziosi presidi più marcatamente forgiati tenendo conto di tutte le peculiari e originali insidie dello spazio digitale.

Non trascurabile appare infine il ruolo dell'educazione digitale, fonda-

[9] A. Bevere, V. Zeno-Zencovich, *La rete e il diritto sanzionatorio. Una visione d'insieme,* in *Diritto dell'informazione e dell'informatica,* 2011, n. 3, 380.

mentale, per mettere gli utenti del *web* nella condizione di riconoscere i pericoli nascosti nelle pieghe della Rete, aumentare la consapevolezza dei rischi specifici nel *cyberspace* ma anche dei possibili strumenti di difesa.

BIBLIOGRAFIA

–Accinni Giovanni Paolo, *Profili di responsabilità penale dell'hosting provider "attivo"*, Archivio penale web, n. 2 del 2017.

–Agustina Sanllehí José Ramón, *La arquitectura digital de Internet como factor criminogeno: Estrategias de prevencion frente a la delincuencia virtual,* in *International e–journal of criminal sciences*, 2009, 3, 1 ss.

–Agustina Sanllehí José Ramón, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?*. in *Estudios penales y criminológicos*, 2021, vol. 41, 705 ss.

–Albamonte Eugenio, *Il reato informatico nella prassi giudiziaria: le linee giuda internazionali per il contrasto ai nuovi fenomeni criminali*, in *Rivista elettronica di Diritto, Economia, Management*, 2013, n. 3, 146 ss.

–Alessandri Alberto, *Criminalità informatica,* in *Riv. trim. dir, pen. econ.,* 1990, 653 ss.

–Allegri Maria Romana, Ubi social, ibi ius*. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider,* Milano, 2018.

–Amato Mangiameli Agata C., Saraceni Guido, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, 2015.

–Amore Nicolò, *La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p.*, in *www.lalegislazionepenale.eu*, 20.1.2020.

–Anders Günther, *L'uomo è antiquato*, vol. II, *Sulla distruzione della vita nell'epoca della terza rivoluzione industriale*, Torino, 1992.

–Baccin Alice, *Responsabilità penale dell'Internet service provider e concorso degli algoritmi negli illeciti online: il caso Force v. Facebook*, in *www.sistemapenale.it*, 2020, n. 5, 75 ss.

–Barile Leonia, *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia il diritto penale è "cosa mobile"*, in *www.sistemapenale.it,* n. 3 del 19 marzo 2021, 139 ss.

–Bartoli Roberto, *L'accesso abusivo a un sistema informatico (art. 615-ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in *www.penalecontemporaneo.it*, *Riv. trim.,* n. 1 del 2012, 123 ss.

–Bartoli Roberto, *Brevi considerazioni sulla responsabilità penale dell'internet service provider*, in *Dir. pen. proc.*, 2013, 600 ss.

–Basile Fabio, *Intelligenza artificiale e diritto penale: quattro percorsi di indagine*, in *www.dirittopenaleuomo.org*, n. 10, 2019, 1 ss.

–Basile Fabio, *Art. 660,* in *Codice penale commentato,* fondato da E. Dolcini, G. Marinucci, diretto da E. Dolcini, G.L. Gatta, Tomo, III, Milano, 2025, 1258 ss.

–Bassini Marco, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Aracne Roma, 2019.

–Beguinot Giulia, *I reati contro la sfera sessuale della persona al tempo di internet, tra criticità tradizionali ed esigenze di prevenzione*, in *Riv. it. dir. proc. pen.*, 2023, 1001 ss.

–Bellacosa Maurizio, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *www.penalecontemporaneo.it*, 2015.

–Benevento Annalisa, *L'apposizione di filtri ai commenti degli utenti non esclude il concorso del blogger nella diffamazione,* in *Diritto di Internet,* 2019, 157 ss.

–Berghella Fulvio, Blaiotta Rocco, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, 2329 ss.

–Bevere Antonio, Zeno–Zencovich Vincenzo, *La rete e il diritto sanzionatorio. Una visione d'insieme,* in *Diritto dell'informazione e dell'informatica,* 2011, n. 3, 375 ss.

–Birritteri Emanuele, *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*, in *www.penalecontemporaneo.it, Riv. trim.,* n. 4 del 2017, 286 ss.

–Birritteri Emanuele, *Contrasto alla disinformazione, Digital Services Act e attività di private enforcement: fondamento, contenuti e limiti degli obblighi di compliance e dei poteri di autonormazione degli operatori*, in *MediaLaws*, n. 2, 2023, 52 ss.

–Bisori Luca, *I delitti contro l'onore,* in *Trattato di diritto penale. Parte speciale,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, vol. VIII*, I delitti contro l'onore e la libertà individuale,* Milano, 2010, 3 ss.

–Borgogno Roberto, *La prostituzione 'a distanza' in due recenti pronunce della giurisprudenza di legittimità*, in *Cass. pen.,* 2005, 3497 ss.

–Botto Matilde, *Le molestie sessuali nell'universo digitale. Riflessioni sulla dimensione "non fisica" della libertà sessuale,* in K. Summerer, M. L. Mattheudakis, G. M. Caletti, *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea,* Pisa, 2025, 185 ss.

–Braschi Sofia, Social media *e responsabilità penale dell'*Internet Service Provider, in *MediaLaws*, 2020, 3, 164 ss.

–Braschi Sofia, *La responsabilità penale dell'Internet Service Provider dopo il* Digitale Services Act, in K. Summerer, M. L. Mattheudakis, G. M. Caletti, *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea,* Pisa, 2025, 27 ss.

–Brighi Raffaella, *La vulnerabilità nel cyberspazio,* in *Ars interpretandi,* n. 1 del 2017, 81 ss.

–Brighi Raffaella, Chiara Pier Giorgio, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea,* in *www.federalismi.it,* n. 21, 8.9.2021.

–Buffa Francesco, *Responsabilità del gestore di sito internet. Nota a margine della sentenza di Cassazione n. 54946 del 27 dicembre 2016*, in *Questione Giustizia,* 9 gennaio 2017.

–Bussolati Nicolò, *L'associazione per delinquere "informatica",* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 249 ss.

–Cajani Francesco, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d. l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119),* in *Cass. pen.,* 2014, 1094 ss.

–Caletti Gian Marco, *Libertà e riservatezza sessuale all'epoca di Internet. L'art. 612–ter c.p. e l'incriminazione della pornografia non consensuale,* in *Riv. it. dir. proc. pen.*, 2019, 2045 ss.

–Camplani Francesco, Locus commissi delicti*, norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Archivio penale web, n. 2 del 2020*, 1 ss.

–Cantelmi Tonino, Talli Massimo*, Psicopatologia del Cyberspazio. Dislocazioni mentali, personalità avatar-mediate, derive autistiche e condotte fuori controllo*, in *Modelli per la mente*, 2008, vol. I, 29 ss.

–Cantelmi Tonino, *La mente tecno-liquida ai tempi di internet: una nuova sfida per la comprensione umana*, in *www. https://www.psicologiacontemporanea.it/blog/la–mente–tecno–liquida–ai–tempi–di–internet/*

–Cappai Michele, *La qualificazione delle "violenze" prive di un contatto* corpore corpori *alla prova della recente giurisprudenza in tema di atti sessuali*, in *www.penalecontemporaneo.it., Riv. trim.,* n. 2 del 2017*,* 43 ss.

–Cappellini Alberto, Machina delinquere non potest? *Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia* 2018, 499 ss.

– Carani Miriam, *L'appropriazione indebita dei dati informatici: perché i files si possono considerare cose mobili,* in *Cass. pen*., 2020, 4159 ss.

–Carcaterra Gaetano, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla recente giurisprudenza. Opinioni a confronto*, in *Criminalia* 2010, 348 ss.

– Caroli Paolo, *Dei post e delle pene. Considerazioni su eguaglianza, social network e giustizia penale*, in *La giustizia penale tra ragione e prevaricazione. Dialogando con Gaetano Insolera*, Roma, 2021, 81 ss.

– Caroli Paolo, *Quando guardare è un reato. Accesso intenzionale a materiale pedopornografico e novità in materia di reati sessuali nei confronti di minori,* in *Dir. pen. proc.,* 2022, 973 ss.

–Carr Nicholas, *The shallows. What the Internet is doing to our brains*, trad. it. a cura di S. Garassini, *Internet ci rende stupidi? Come la Rete sta cambiano il nostro cervello*, Milano, 2011, *e–Book*.

–Carrillo Miranda Juan José, *Factor humano: la teoría de las Actividades Cotidianas en la Ciberseguridad,* in *https://www.academia.edu,* novembre 2020.

–Catullo Francesco Giuseppe, *Sullo sfruttamento della prostituzione online,* in *Cass. pen*., 2004, 3581 ss.

–Catullo Francesco Giuseppe, *Sulle molestie via e-mail,* in *Cass. pen.,* 2011, 1039 ss.

–Catullo Francesco Giuseppe, *La responsabilità penale del direttore del giornale telematico tra legislatore pigro e giudice intraprendente,* in *Diritto di Internet*, 2019, 173 ss.

–Checcacci Giulia, *Facebook come un luogo pubblico: un caso di "analogia digitale"* in malam partem*,* in *Criminalia* 2014, 503 ss.

–Cecchini Francesco, *La responsabilità del direttore di periodico telematico ex art. 57 c.p. tra divieto di analogia, "esigibilità" del controllo e prevedibilità dell'esito giudiziario*, in *Archivio penale web*, n. 2 del 2019.

–Cipolla Costantino, Canestrini Edi, (a cura di), *La dissoluzione della sessualità umana nell'era digitale*, Milano, 2018.

–Consulich Federico, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *Banca, borsa, titoli di credito*, 2018, 195 ss.

–Consulich Federico, Flash offenders. *Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. proc. pen*., 2022, 1015 ss.

–Consulich Federico, Maugeri Marco, Milia Carlo, Poli Tommaso Nicola, Trovatore Gianfranco, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?,* in *Quaderni giuridici Consob,* n. 29, maggio 2023, 7 ss.

–Corbetta Stefano, *Caso "Google": nessuna responsabilità dell'Host Provider per l'omesso impedimento di reati realizzati dagli utenti della rete*, in *Diritto penale e processo*, 2014, 277 ss.

–Corrias Lucente Giovanna, *Al direttore di un periodico on line non si applica il reato previsto dall'art. 57 c.p.,* in *Diritto dell'informazione e dell'informatica,* 2012, 82 ss.

–Corrias Lucente Giovanna, *La diffamazione a mezzo Facebook,* in *MediaLaws,* 25 febbraio 2013.

-Corrias Lucente Giovanna, *Le testate telematiche registrate sono sottratte al sequestro preventivo. Qualche dubbio sulla "giurisprudenza legislativa",* in *Diritto dell'informazione e dell'informatica,* 2015, 1041 ss.

–Corrias Lucente Giovanna, *Ma i* networks, *i* service providers *e gli* access providers *rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che loro gestiscono?,* in *Giur. Merito,* 2004, 252 ss.

–Costa Davide., *La responsabilità dell'Internet Service Provider per i reati in materia di diritto d'autore*, in *Giurisprudenza penale web,* n. 2 del 2022.

–Cristianini Nello, Machina sapiens. *L'algoritmo che ci ha rubato il segreto della conoscenza,* Bologna, 2024.

– Cuomo Luigi, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico,* in *Cass. pen.,* 2002, 1018 ss.

–Cupelli Cristiano, *Divieto di analogia* in malam partem *e limiti dell'interpretazione in materia penale: spunti dalla sentenza n. 98 del 2021*, in *Giur. cost.,* 2021, 1807 ss.

–D'Agostino Luca, *Disinformazione e responsabilità delle piattaforme. Obblighi di attivazione e misure di* compliance*,* in *www.penalecontemporaneo.it, Riv. trim.,* n. 4, 2021, 282 ss.

–D'Amico Laura, *La misura della (im)prevedibilità. Modelli d'imputazione della responsabilità al tempo dell'intelligenza artificiale*, Napoli, 2025.

–de la Mata Barranco Norberto Javier, *Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 197 bis CP). El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación,* en *Cudernos de politica criminal,* n. 118, Mayo 2016, 43 ss.

–Demuro Gian Paolo, *Dai big data all'intelligenza artificial*e. *Alla ricerca di principi,* in *Diritto @ Storia,* n. 19, 2022.

–Di Giovine Ombretta, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla recente giurisprudenza. Opinioni a confronto*, in *Criminalia* 2010, 355 ss.

–di Martino Alberto, *Una legalità per due? Riserva di legge, legalità CEDU e giudice–fonte,* in *Criminalia* 2014, 91 ss.

–Diotallevi Lorenzo, *Reato di molestia e Facebook tra divieto di analogia in materia penale, (presunta) interpretazione "evolutiva" dell'art. 17 Cost. e configurabilità di un diritto di accesso ad Internet*, in *Giur. cost.*, 2014, 4104 ss.

–Diotallevi Lorenzo, *La Corte di cassazione sancisce l'"equiparazione" tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di "scivolamento" dalla "nomofilachia" alla "nomopoiesi"?*, in *Giur. cost.,* 2015, 1062 ss.

–Donini Massimo, *Il diritto giurisprudenziale penale. Collisioni vere e apparenti con la legalità e sanzioni dell'illecito interpretativo,* in *www.penalecontemporaneo.it,* n. 3, 2016, 13 ss.

–Ellul Jacques, *Il sistema tecnico. La gabbia delle società contemporanee,* Milano, 2009.

–Federici Maria Antonietta, *In tema di molestie mediante posta elettronica,* in *Giur. it.,* 2013, 1169 ss.

–Fiandaca Giovanni, *Il giudice di fronte alle controversie tecnico–scientifiche. Il diritto e il processo penale,* in *Diritto & questioni pubbliche,* 2005, n. 5, 7 ss.

– Fiandaca Giovanni, Musco Enzo, *Diritto penale. Parte speciale. I delitti contro il patrimonio*, vol. II, tomo secondo, Torino, 2023.

– Fiandaca Giovanni, Musco Enzo, *Diritto penale. Parte generale,* Bologna, 2025.

–Fiorinelli Gaia, *L'attuale ruolo del provider nella società digitale: modelli di responsabilità penale,* in *www.lalegislazionepenale.eu,* 27.12.2022.

–Fiorinelli Gaia, Nomina nuda tenemus*? Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche,* in *disCrimen,* 3.1.2023.

–Fiorinelli Gaia, *La violenza mediata dalla tecnologia. Dogmatica, profili politico–criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Torino, 2024.

–Flick Caterina, *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona,* in *Diritto dell'informazione e dell'informatica,* 2008, 526 ss.

–Flor Roberto, Phishing, identity theft, e identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 899 ss.

–Flor Roberto, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung*,* in *Riv. trim. dir. pen. econ.,* 2009, 695 ss.

–Flor Roberto, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di* internet, in *www.dirittopenaleuomo.org*, 20.9.2012.

– Flor Roberto, V*erso 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 *www.penalecontemporaneo.it, Riv. trim.,* n. 2, 2012, 126 ss.

–Flor Roberto, *I limiti del principio di territorialità nel "*cyberspace*". Rilievi critici alla luce del recente orientamento delle sezioni unite,* in *Dir. pen. proc.,* 2015, 1296 ss.

–Flor Roberto, *Riservatezza informatica,* in *Enc. Giur. online,* 2017, 1 ss.

–Flor Roberto, *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere",* in *Dir. pen. proc.,* 2018, 506 ss.

–Flor Roberto, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 141 ss.

–Flor Roberto, Cyber-criminality*: le fonti internazionali ed europee,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 97 ss.

–Floridi Luciano, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, trad. it. a cura di M. Durante, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo,* Milano, 2017.

–Floridi Luciano, *La differenza fondamentale,* eBook, Milano 2025.

–Fondaroli Désirée, *La tutela penale dei «beni informatici»*, in *Diritto dell'informazione e dell'informatica*, 1996, n. 2, 291 ss.

–Forti Gabrio, *L'immane concretezza. Metamorfosi del crimine e controllo penale,* Milano, 2000.

–Fragasso Beatrice, Like *su* Facebook *ed* hate crimes*: note a margine di una recente sentenza della Cassazione*, in *www.sistema.penale.it,* n. 5, 2022, 63 ss.

–Fragasso Beatrice, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, Torino, 2025.

–Fragasso Beatrice, *Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura*, in *www.sistemapenale.it,* n. 10, 2025, 157 ss.

–Fulvi Francesca Romana, *L'unità virtuale del diritto penale dell'informatica,* in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali,* Torino, 2012, 167 ss.

–Fumo Maurizio, *La condotta nei reati informatici,* in *Arch. Pen.,* 2013, 771 ss.

–Galán Muñoz Alfonso, *Los ciberdelitos en el ordenamiento español*, Barcellona, 2019.

–Galimberti Umberto, *Psiche e techne. L'uomo nell'età della tecnica,* Milano, 1999.

–Galgano Francesco, *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto*, Bologna, 2010.

–Garapon Antoine, Lassègue Jean, *La giustizia digitale. Determinismo tecnologico e libertà,* trad. it. a cura di F. Morini, Bologna, 2021.

–Giunta Fausto, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla giurisprudenza,* in *Criminalia* 2010, 347 ss.

–Giunta Fausto, *Ghiribizzi penalistici per colpevoli. Legalità "malalegalità", dintorni,* Pisa, 2019.

–Giunta Fausto, *Il valore della dignità*, in *Sussidiario di diritto penale. Parte speciale*, a cura di F. Giunta, 2023, cap. XIV, § 9 (consultabile su *disCrimen*)

–GIUNTA Fausto, *Diritto penale. Un'introduzione*, Pisa, 2024.

–GIUNTA Fausto, *Il linguaggio del "penale" e il garantismo della norma,* in *Criminalia* 2024, 317 ss.

–GRABOSKY Peter N., *Virtual Criminality: Old Wine in New Bottles?,* in *Social & Legal Studies,* 2001,10, 243 ss.

–GRANDE Marcello, *Atti sessuali condivisi con minorenne mediante* videochat, in *Cass. pen.,* 2023, 3227 ss..

–GRANDI Matteo, Far Web. *Odio, bufale, bullismo. Il lato oscuro dei* social, Milano, 2017, *e–book*.

–GROSSO Carlo Federico, *Su di un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, in *Riv. it. dir. proc. pen.*, 2014, 1518 ss.

–GROTTO Marco, *Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell'art. 491 bis c.p.,* in *Il diritto dell'informazione e dell'informatica,* 2006, 589 ss.

–GUIDOBALDI Luca, You Tube *e la diffusione di opere protette dal diritto d'autore: ancora sulla responsabilità dei* providers*, tra* hoster *attivi, conoscenza dell'illecito e obbligo di sorveglianza*, in *Diritto dell'informazione e dell'informatica*, 2010, 278 ss.

–GULLO Antonio, *Delitti contro l'onore,* in *Trattato teorico pratico di diritto penale,* diretto da F. C. PALAZZO, C. E. PALIERO, M. PELISSERO, *Reati contro la persona,* a cura di F. VIGANÒ, Torino, 2022, 213 ss.

–GULLO Antonio, *Il* Digital Services Act *e il contrasto alla disinformazione: responsabilita dei* provider*, obblighi di* compliance *e modelli di* enforcement*,* in *MediaLaws*, n. 2, 2023, 13 ss.

–HAN Byung–Chul, *Nello sciame. Visioni del digitale,* Milano, 2023.

–INCAMPO Antonio, *Metaverso. Come del mondo (o del diritto o dell'economia) fin dalla sua origine*, in *Riv. fil. dir.*, 2025, n. 1, 57 ss.

–INGRASSIA Alex, *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine*?, in *www.penalecontemporaneo.it,* 2012.

–INGRASSIA Alex. *Responsabilità penale degli* internet service provider*: attualità e prospettive,* in *Dir. pen. e proc.*, 2017, 1621 ss.

–IRTI Natalino, SEVERINO Emanuele, *Dialogo su diritto e tecnica*, Roma–Bari, 2001.

–Kerr Orin S., *The Problem of Perspective in Internet Law,* in *Georgetown Law Journal,* vol. 91, 2003, 357 ss.

–King Thomas C., Aggarwal Nikita, Taddeo Mariarosaria, Floridi Luciano, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions,* in *Science and Engineering Ethics*, 2020, vol. 26, 89 ss.

–Lamanuzzi Marta, *Il "lato oscuro della rete": odio e pornografia non consensuale. Ruolo e responsabilità dei gestori delle piattaforme* social *oltre la* net neutrality, in *www.lalegislazionepenale.eu,* 25.5.2021.

–Lapidot-Lefler Noan, Barak Azy, *Effects of anonymity, invisibility, and lack of eye–contact on toxic online disinhibition*, in *Computers in Human Behavior*, 2012, n. 28, 434 ss.

–Larinni Claudia, *Garantismo europeista: un ossimoro? A proposito dell'accesso abusivo ad un sistema informatico o telematico (615–ter c.p.)*, in *Criminalia* 2019*,* 301 ss.

–La Rosa Emanuele, *Offese in* videochat*. La Corte di Cassazione si pronuncia sui rapporti tra ingiuria e diffamazione*, in *Giur. it.,* 2020, 1750 ss.

–Lasalvia Francesco Paolo, *La diffamazione via* web *nell'epoca dei* social network, in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 331 ss.

–Leopizzi Alessandro, *La biblioteca (digitale) di Babele. Condotte umane nel cyberspazio e competenza territoriale per le violazioni del domicilio informatico*, in *La Giustizia penale,* 2015, III, 410 ss.

–Leucci Stefano, *Appunti sul difficile rapporto tra linguaggio, diritto penale e tecnologia,* in *Informatica e diritto,* 2013, n. 2, 151 ss.

–Lombardi Filippo, *La responsabilità del direttore del periodico telematico ex art. 57 c.p. tra interpretazione estensivo-evolutiva e analogia in* malam partem*,* in *www.giurisprudenzapenale.com,* 11 gennaio 2019.

–Lo Monte Elio, *Una riflessione su* spamming *e molestie: la problematica configurabilità della fattispecie incriminatrice di cui all'art. 660 c.p.,* in *Cass. pen.,* 2012, 2113 ss.

– Maestri Enrico, *Stupri digitali: una questione di* governance *del cyberspazio,* in *Annali online della Didattica e della Formazione Docente,* vol. 16, n. 27/2024, 27.

–Maestri Enrico, *Contro la riduzione bayesiana dell'intelligenza artificiale,* in https://www.pandorarivista.it/articoli/contro–la–riduzione–bayesiana–dell–intelligenza–artificiale/*,* 18 agosto 2025.

–Magro Beatrice, Robot*,* cyborg *e intelligenze artificiali,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 1179 ss.

–Malgieri Gianclaudio, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *www.penalecontemporaneo.it, Riv. trim.*, n. 2, 2015, 143 ss.

–Manes Vittorio, *Introduzione ai principi costituzionali in materia penale,* Torino, 2024.

–Mantovani Ferrando, Flora Giovanni, *Diritto penale. Parte speciale, II, Delitti contro il patrimonio,* Milano, 2024.

–Maraffino Marisa, *La sostituzione di persona mediante furto di identità digitale,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 307 ss.

–Marinucci Giorgio, *L'analogia e la "punibilità svincolata dalla conformità alla fattispecie penale"*, in *Riv. it. dir. e proc. pen.*, 2007, 1254 ss.

–Marinucci Giorgio, Dolcini Emilio, Gatta Gian Luigi, *Manuale di diritto penale, Parte generale*, Milano, 2024.

–Marotta Gemma, *Tecnologie dell'informazione e nuovi processi di vittimizzazione*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. VI, 2012, 93 ss.

–Martiello Gianfranco, *Il caso della molestia "telefonica" tra evoluzione tecnologica e primato della legalità,* in *La Giustizia penale,* 2011, II, 47 ss.

–Martiello Gianfranco, *Vincolo testuale» ed interpretazione nel diritto penale: la necessità di una riconciliazione,* in *Criminalia* 2022, 417 ss.

–Mattia Marco, "Revenge porn" *e suicidio della vittima: il problema della divergenza tra 'voluto' e 'realizzato' rispetto all'imputazione oggettiva degli eventi psichici*, in *www.lalegislazionepenale.eu*, 19 luglio 2019.

–Mazzacuva Nicola, *Tra analogia e interpretazione estensiva. A proposito di alcuni casi problematici tratti dalla recente giurisprudenza. Opinioni a confronto*, in *Criminalia* 2010, 367 ss.

–Mazzanti Edoardo, *Il delitto di diffamazione al tempo dei* social network*: punti fermi e spunti problematici*, in *Nodi virtuali, legami informali:* Internet *alla ricerca di regole,* a cura di P. Passaglia, D. Poletti, Pisa, 2016, 207 ss.

–Melzi d'Eril Carlo, Roma locuta: *la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line, in *Diritto dell'informazione e dell'informatica*, 2010, 904 ss.

–Melzi d'Eril Carlo, Vigevani Giulio Enea, *La responsabilità del direttore del periodico telematico, tra facili equiparazioni e specificità di* Internet, in *Diritto dell'informazione e dell'informatica*, 2010, 91 ss.

–Melzi d'Eril Carlo, *L'applicabilità della disciplina prevista per la stampa a* Internet: *l'ultima puntata di una lunga storia, tra legislatore assente e giurisprudenza (molto) creativa*, in *MediaLaws*, 5 novembre 2024.

–Mengoni Enrico, *Chattare con un* nickname *riconducibile ad altri (e comunicare il loro numero telefonico) integra il reato di sostituzione di persona*, in *Cass. pen.*, 2014, 148 ss.

–Merla Flaminia, *Diffusione abusiva di opere in* internet *e sequestro preventivo del sito* web*: il caso "*The Pirate Bay*"*, in *Diritto dell'informazione e dell'informatica*, 2010, 448 ss.

–Micheletti Dario, Jus contra lex. *Un campionario dell'incontenibile avversione del giudice penale per la legalità,* in *Criminalia* 2016, 161 ss.

–Micheletti Dario, *L'*interversio pubblicationis *quale elemento costitutivo della fattispecie di* revenge porn, in *disCrimen,* 7.1.2022.

–Miglio Mattia, *La responsabilità dell'amministratore di un gruppo* Facebook *per i commenti offensivi pubblicati da altri utenti: un travagliato percorso giurisprudenziale,* in *www.giurisprudenzapenale.com,* 9 settembre 2016.

–Miglio Mattia, *I gestori di un sito* internet *rispondono penalmente per i commenti offensivi pubblicati dagli utenti*, in *www.giurisprudenzapenale.com,* 3 gennaio 2017.

–Minicucci Gherardo, *Reati informatici e responsabilità degli enti: vecchi e nuovi scenari,* in *disCrimen,* 24.9.2022.

–Miró Llinares Fernando, *La oportunidad criminal en el ciberspacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen,* in *Revista Electrónica de Ciencia Penal y Criminología*, 13.7.2011.

– Miró Llinares Fernando*, La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio,* in *Revista Española de investigatión criminólogica,* n. 11, 2013, 1 ss.

–Mooney Zane RonaldA., Zhang Xihui, Crabtree John D., *Understanding cybercrime: A three–generation approach,* in *Issues in Information Systems*, 2022, vol. 23, n. 3, 25 ss.

–Morelli Alessandro, Pollicino Oreste, *Le metafore della rete. Linguaggio figurato,* judicial frame *e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Rivista AIC*, 2018, n. 1, 19 marzo 2018, 1 ss.

–Morgante Gaetana, *Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del* law enforcement, in *Riv. it. informatica e diritto,* 2025, 95 ss.

–Mucciarelli Francesco, *Commento alla legge 23 dicembre 1993, n. 547. Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica,* in *Leg. pen.,* 1996, 57 ss.

–Mucciarelli Francesco, *Intelligenza artificiale e condotte manipolative su strumenti finanziari: una nuova aggravante con effetto attenuante,* in *www.sistemapenale.it,* 17 ottobre 2025.

–Murro Ottavia, *Il ruolo delle piattaforme* online *nella prevenzione della violenza di genere: cosa cambia con il* Digital Service Act, in *www.penaledp.it*, 19 dicembre 2025.

–Pagallo Ugo, *Profili tecnico–informatici e filosofici,* in *Trattati giuridici.* Cybercrime. Diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 3 ss.

–Pagella Cecilia, *La Cassazione sulla responsabilità del* blogger *per contenuti diffamatori (commenti) pubblicati da terzi,* in *www.penalecontemporaneo.it,* 17 maggio 2019.

–Pagella Cecilia, *La Cassazione sulla riconducibilità dei* file *al concetto di "cosa mobile" oggetto di appropriazione indebita: un caso di analogia* in malam partem*?,* in *www.sistemapenal.it,* 4 marzo 2021.

–Palazzo Francesco Carlo, T*esto, contesto e sistema nell'interpretazione penalistica,* in *Studi in onore di Giorgio Marinucci,* a cura di E. Dolcini, C.E. Paliero, vol. I. *Teoria del diritto penale, criminologia e politica criminale*, Milano, 2006, 515 ss.

–Palazzo Francesco Carlo, *Legalità penale, interpretazione ed etica del giudice,* in *Riv. it. dir. proc. pen.,* 2020, 1249 ss.

–Palazzo Francesco Carlo, *Legalità penale vs creatività giudiziale*, in *Riv. it. dir. proc. pen.*, 2022, 975 ss.

–Palazzo Francesco Carlo, *Sui rapporti tra teoria e prassi nel diritto penale: una panoramica*, in *Diritto penale tra teoria e prassi*, a cura di A. Bondi, G. Marra, R. Palavera, Urbino, 2024, 73 ss.

–Palmisano Marta, *L'abuso di mercato nell'era delle nuove tecnologie.* Trading *algoritmico e principio di personalità dell'illecito penale*, in *www.penalecontemporaneo.it*, *Riv. trim.*, n. 2, 2019, 129 ss.

–Panattoni Beatrice, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel Cyberspace,* in *www.sistemapenale.it,* n. 5 del 2020, 303 ss.

–Panattoni Beatrice, *Violazioni "incorporee" della sfera sessuale. Possibili evoluzioni ed insidie nei reati sessualmente connotati*, in *Archivio penale web*, n. 3, 2022, 1 ss.

–Paoloni Lucia, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa:* ubi commoda, ibi et incommoda*?,* in *Cass. pen.,* 2015, 3437 ss.

–Paonessa Caterina, *Obbligo di impedire l'evento e fisiognomica del potere impeditivo,* in *Criminalia* 2012, 641 ss.

–Paonessa Caterina, *Ai confini del c.d.* Revenge porn. *Tessere di un mosaico normativo*, in *Criminalia* 2021, 283 ss.

– Paonessa Caterina, *La diffusione di contenuti illeciti* online. *Obblighi di incriminazione e contrasto del "*deepfake" *nella direttiva (UE) 2024/1385,* in *Criminalia* 2024, 229 ss.

– Parisi Francesco, *Violenza sessuale via* Whatsapp*? L'estensione della nozione di atto sessuale in una sentenza della Cassazione*, in *Il Foro Italiano*, 2021, II, 268 ss.

– Parodi Cesare, *I reati patrimoniali,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. Parodi, V. Sellaroli, Milano, 2020, 103 ss.

–Parodi Cesare, *Accesso abusivo a sistema informatico: può essere sufficiente lo "sviamento di potere"?*, in *www.ilpenalista.it,* 18 settembre 2017.

–Pascuzzi Giovanni, *Il diritto dell'era digitale,* Bologna Il Mulino, 2024.

– Pasquin Martina Elisabetta, *Atti sessuali in videochiamata su* Instagram *e "presenza" del minore: la linea di confine tra interpretazione estensiva e analogia in una recente sentenza della Cassazione in tema di corruzione di minorenne ex art. 609 quinquies, co 2 c.p.,* in *www.sistemapenale.it,* 2 maggio 2023.

–Pecorella Claudia, *L'attesa pronuncia delle sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo,* in *Cass. pen.,* 2012, 3692 ss.

–Pecorella Claudia, *Reati informatici,* in *Enc. Dir., Annali,* X, Milano, 2017, 707 ss.

–Petrini Davide, *Il direttore della testata telematica, tra* horror vacui *e prospettive di riforma; sperando che nulla cambi*, in *Riv. it. dir. proc. pen.*, 2012, 1611 ss.

–Petrini Davide, *Diffamazione* online: *offesa recata con "altro mezzo di pubblicità" o col mezzo della stampa?,* in *Dir. pen. proc.,* 2017, 1485 ss.

– Piccaluga Andrea, *L'art. 609–bis c.p. dai mille volti: il caso della violenza sessuale "a distanza e "in differita"*, in *Dir. pen. proc.*, 2025, 1041 ss.

–Piccardi Marco, *Il necessario coinvolgimento della corporeità sessuale della vittima nel reato di violenza sessuale*, in *Cass. pen.*, 2008, 3293 e ss.

–Picotti Lorenzo, *Reati informatici*, in *Enc. giur. Treccani*, XXIX, Roma, 1993.

– Picotti Lorenzo, *Profili penali delle comunicazioni illecite via* Internet, in *Diritto dell'informazione e dell'informatica,* 1999, 283 ss.

–Picotti Lorenzo*, La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale, in Dir. pen. proc.,* 2008, 700 ss.

–Picotti Lorenzo, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee,* in *Riv. trim. dir. pen. econ.,* 2011, 827 ss.

–Picotti Lorenzo, *Sicurezza informatica e diritto penale*, in *Sicurezza e diritto penale*, a cura di M. Donini, M. Pavarini, Bologna, 2011, 217 ss.

–Picotti Lorenzo, *La tutela penale della persona e le nuove tecnologie dell'informazione,* in *Tutela penale della persona e nuove tecnologie,* a cura di L. Picotti, Padova, 2013, 29 ss.

–Picotti Lorenzo, *Diritto penale e tecnologie informatiche: una visione d'insieme,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 33 ss.

–Picotti Lorenzo, *La pedopornografia nel* Cyberspace*: un opportuno adeguamento della giurisprudenza allo sviluppo tecnologico ed al suo impatto sociale riflessi nell'evoluzione normativa,* in *Diritto di Internet,* 2019, n. 1, 187 ss.

–Picotti Lorenzo, *La violenza sessuale via* Whatsapp, in *Diritto di Internet*, 2020, 685 ss.

–Picotti Lorenzo, Cybercrime *e diritto penale,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. Parodi, V. Sellaroli, Milano, 2020, 709 ss.

–Picotti Lorenzo, *Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palingenesi*?, in *www.sistemapenale.it*, 31 luglio 2024.

–Picotti Lorenzo, *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Dir. pen. proc.*, 2024, 293 ss.

–Picotti Lorenzo, *I contenuti penali della legge sull'intelligenza artificiale,* in *www.sistemapenale.it,* 2 dicembre 2025.

–Pierazzi Stefania, *I* social*; nuovi modi di comunicare o di esserci? I rischi e le condotte,* in *Nodi virtuali, legami informali:* Internet *alla ricerca di regole,* a cura di P. Passaglia, D. Poletti, Pisa, 2016, 221 ss.

–Piergallini Carlo, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. proc. pen*., 2020, 1745 ss.

–Pietrella Tommaso, *Reati informatici e concorso di norme: l'evoluzione tecnologica informa il diritto penale,* in *disCrimen* 2.12.2021.

–Pietrella Tommaso, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive. Rilevanza giuridica della comunicazione degradante* online *nel reato di diffamazione*, in *www.sistemapenale.it,* 6 ottobre 2023, 5 ss.

–Pietropaoli Stefano, *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars interpretandi*, 2017, n. 1, 70 ss.

–Pisa Ilaria, *Profili di responsabilità penale del direttore di periodici telematici*, in *Dir. pen. proc.*, 2011, 455 ss.

–Pisani Nicola, *La nozione di "cosa mobile" agli effetti penali e i* files *informatici: il significato letterale come argine all'applicazione analogica delle norme penali,* in *Dir. pen. proc.,* 2020, 651 ss.

–Plantamura Vito, Internet*, sesso e minori tra rapporti virtuali e adescamento*, in *www.archivio.penale.it,* n. 1, 2015.

–Posada Maya Ricardo, *El cibercrimen y sus efectos en la teoria de la tipicidad: de una realidad fisica a una realidad virtual*, *Revista Nuevo Foro Penal*, vol. 13, n. 88, 2017, 72 ss.

–Razzano Giovanna, *Il primato dell'essere umano nell'era dell'intelligenza artificiale,* in *Bioetica, diritto e intelligenza artificiale,* a cura di A. Patroni Griffi, Milano–Udine, 2023, 103 ss.

–Resta Federica, *La responsabilità penale del* provider*: tra* laissez faire *ed obblighi di controllo*, in *Giur. merito,* 2004, 1715 ss.

–Riboldi Federico, *I criteri per la determinazione della competenza territoriale nella diffamazione telematica: l'accertamento dell'evento tra rigore tecnico e ricorso alle presunzioni,* in *MediaLaws,* n. 3, 2023, 204 ss.

–Risicato Lucia, *Argini e derive della tassatività. Una riflessione a margine della sentenza costituzionale n. 98/2021*, in *disCrimen*, 16.7.2021.

–Rodotà Stefano, *Persona, libertà, tecnologia. Note per una discussione*, in *Diritto & Questioni pubbliche*, 5/2005, 25 ss.

–Rodotà Stefano, *Una costituzione per* Internet*?,* in *Politica del diritto*, n. 3, settembre 2010, 337 ss.

–Rodotà Stefano, *Il mondo nella rete. Quali i diritti, quali i vincoli,* Bari, 2014.

–Romano Bartolomeo, *Delitti contro la sfera sessuale della persona,* Milano, 2022.

–Romeo Casabona Carlos Maria, *De los delitos informáticos al cibercrimen. Una aproximación conceptuale y político-criminal,* in *El cibercrimen: nuoevos retos jurídico-penales, nuevas respuestas político-criminales,* a cura di C. M. Romeo Casabona, Granada, 2006, 1 ss.

–Rossi Chiara, *Non ricorre l'aggravante dell'uso di un mezzo di pubblicità nel caso di diffusione di un messaggio offensivo in una "*chat*" attraverso "*WhatsApp*"*, in *Cass. pen.,* 2024, 1006 ss.

–Ruggiero Francescopaolo, *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002, 254 ss.

–Ruta Gaetano, *I.A. nei reati economici e finanziari*, in *Intelligenza artificiale e giurisdizione penale*, *Atti del* workshop *organizzato dalla Fondazione Occorsio* il 19 novembre 2021, in *www.sistemapenale.it*, 13 giugno 2022, 58 ss.

–Sabella Pietro Maria, *Il fenomeno del* cybercrime *nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di* Internet *per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali*, in *Informatica e diritto,* 2017, 139 ss.

–Salvadori Ivan, *Il trattamento senza consenso di dati personali altrui reperibili su* Internet *costituisce reato?,* in *Dir. pen. proc.,* 2006, 467 ss.

–Salvadori Ivan, *La normativa penale sulla stampa non si applica,* de jure condito*, ai giornali telematici*, in *Cass. pen.*, 2011, 2982 ss.

–Salvadori Ivan, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615–ter c.p.*, in *Riv. trim. dir. pen. econ.*, 2012, 369 ss.

–Salvadori Ivan, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in *Tutela penale della persona e nuove tecnologie*, a cura di L. Picotti, Padova, 2013, 125 ss.

–Salvadori Ivan, *Il diritto penale dei* software *"a duplice uso",* in *Quaderni della Facoltà di Giurisprudenza di Trento,* 2017, 361 ss.

– Salvadori Ivan, *I reati contro la sicurezza informatica,* in *Trattati giuridici.* Cybercrime*,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano, 2019, 655 ss.

–Salvadori Ivan, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen*., 2021, 83 ss.

–Salvadori Ivan, Dal cybercrime all'artificial intelligence crime. *Brevi cenni sui profili penali*, in *Criminalità informatica e intelligenza artificiale. Quaderno della Rivista trimestrale della Scuola di perfezionamento per le Forze di Polizia,* Roma, 2022, 57 ss.

–Sarzana di Sant'Ippolito Carlo, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa, in Dir. pen. proc.,* 2008, 1562 ss.

–Savona Ernesto U., Mignone Marco, *The fox and the hunters: how IC Technologies change the crime race,* in *European Journal on Criminal Policy and Research,* 10, 2024, 3 ss.

–Scagliarini Simone, *I diritti costituzionali nell'era di* Internet*: cittadinanza digitale, accesso alla rete e* net neutrality, in *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali,* a cura di T. Casadei, S. Pietropaoli, Milano, 2021, 3 ss.

–Scarcella Alessio, *Dato informatico, nozione penale di cosa mobile ed appropriazione indebita*, in *Cass. pen.*, 2021, 556 ss.

–Sciuba Maurizia Lina, *Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico,* in *Cass. pen.,* 2015, 3507 ss.

–Scollo Luigi, *L'intelligenza artificiale entra nel Codice penale*, in *Dir. pen. proc.*, 2025, 693 ss.

–Scopinaro Lucia, Internet *e delitti contro l'onore*, in *Riv. it. dir. proc. pen.*, 2000, 617 ss.

–Scopinaro Lucia, *Diffamazione via* Internet*: applicabilità della circostanza aggravante relativa all'uso del mezzo di pubblicità,* in *Riv. it. dir. proc. pen.,* 2001, 1410 ss.

–Scopinaro Lucia, Internet *e reati contro il patrimonio,* Torino, 2007.

–Scordamaglia Irene, *La falsità in documento informatico,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. Parodi, V. Sellaroli, Milano, 2020, 323 ss.

–Scotti Gerardo, *Dall'*habeas corpus *all'*habeas data: *il diritto all'oblio e il diritto all'anonimato nella loro dimensione costituzionale*, in *Diritto.it*, 7 settembre 2015, 1 ss.

–Scotti Lucio, Deepfake *sessuale e legalità penale: il costo costituzionale della tipizzazione dell'offesa artificiale*, in *Questione Giustizia*, 16 giugno 2026.

–Seminara Sergio, *La pirateria su* Internet *e il diritto penale,* in *Riv. trim. dir. pen. econ.*, 1997, 71 ss.

–Seminara Sergio, *La responsabilità penale degli operatori su* Internet*,* in *Diritto dell'informazione e dell'informatica,* 1998, 745 ss.

–Seminara Sergio, Internet *(diritto penale)*, in *Enciclopedia del Diritto, Annali*, VII, Milano, 2014, 567 ss.

–Seminara Sergio, *Delitti contro la persona,* in R. Bartoli, M. Pelissero, S. Seminara, *Diritto penale. Lineamenti di parte speciale*, Torino, 2021, 3 ss.

–Silvestre Pasqualino, *La sempreverde tentazione di sostituirsi al legislatore*, in *Giur. mer.*, 2013, 1577 ss.

–Simmler Monika, Frischknecht Ruth, *A taxonomy of human–machine collaboration: capturing automation and technical autonomy,* in *AI & Society,* 36, 2021, 239 ss.

–Simoncini Andrea, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal, Rivista di BioDiritto,* n. 1/2019, 62 ss.

–Spagnolo Andrea, *Bilanciamento tra diritto d'autore, libertà d'impresa e libertà fondamentali nella giurisprudenza recente della Corte di Giustizia*, in *Giur. merito*, 2013, 125 ss.

–Spena Alessandro, *La parola(–)odio. Sovraesposizione, criminalizzazione e interpretazione dello* hate speech*,* in *Criminalia* 2016, 577 ss.

–Spitzer Manfred, *Connessi e isolati,* trad. di C. Tatasciore, e–*Book*, 2018.

–Spitzer Manfred, *Digitale demenz. Wie wir uns und unsere Kinder um den Verstand bringen,* trad. it. a cura di A. Petrelli, *Demenza digitale*, Milano, 2019, *e–Book.*

–Stea Gaetano, *La diffamazione a mezzo* Internet*,* in *Riv. pen.,* 2008, 1247 ss.

–Suler John, *The Online Disinhibition Effect*, in *Cyberpsychology & Behavior*, 2004, vol. VII, n. 3, 321 ss.

–Taddei Elmi Giancarlo, Ortu Rosanna, Cifaldi Pierfrancesco, *La Raccomandazione del Consiglio d'Europa del 9 settembre 1989 n. R (89)–9 e la Legge 23 dicembre 1993 n. 547 in materia di* computer crimes*: una analisi comparativa,* in *Informatica e diritto,* 1996, n. 1, 113 ss.

–Tonellotto Maurizio, *Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. XVI, 2022, 6 ss.

–Torre Valeria, *Sulla responsabilità penale del* service provider *e la definizione del comportamento esigibile alla luce delle norme contro la pedopornografia,* in *Tutela penale della persona e nuove tecnologie*, a cura di L. Picotti, Padova, 2013, 163 ss.

–Tripodi Andrea Francesco, *Abusi di mercato e* trading *algoritmico*, in Il *diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, a cura di R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto, Milano, 2022, 745 ss.

–Tripodi Andrea Francesco, *Uomo,* societas*,* machina, in *www.lalegislazionepenale.eu*, 10 maggio 2023.

–Turing Alan Mathison, *Computing Machinery and Intelligence*, in *Mind,* 1950, 49, 433 ss.

–Tuzet Giovanni, *Luoghi, siti, bacheche. Un caso di interpretazione estensiva,* in *Criminalia* 2014, 513 ss.

–Ubiali Maria Chiara, *Molestie via* Facebook*: tra divieto di analogia ed esigenze di adeguamento alle nuove tecnologie,* in *www.penalecontemporaneo.it,* 5.3.2015.

–Valenti Alessandro, Cardarelli Maria Cecilia, Colaiacovo Guido, Cuocci Valentina Vincenza, Fontana Giorgio, Nocerino Wanda, Procaccino Angela, Viterbo Francesco Giacomo, Curtotti Donatella, *Sistemi di monitoraggio algoritmico delle comunicazioni e tutela dei diritti fondamentali: "*cyber social security*"* research project*,* in *www.sistemapenale.it*, n. 4 del 2026, 5 ss.

–Veneziani Paolo*, I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali,* in *Ind. pen.,* 2000, 139 ss.

–Vicinanza Anna, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso* Telegram *al* Digital Services Act, in *Quaderni AISDUE*, 1/2025, 1 ss.

–Vigevani Giulio Enea, *La "sentenza figlia" sul direttore del giornale telematico: il caso* Hamaui*,* in *Diritto dell'informazione e dell'informatica*, 2011, 795 ss.

–Vigneri Fabio, *Brevi considerazioni sulla natura e sulle caratteristiche dello spazio cibernetico*, in *SalvisJuribus*, 10.10.2019.

–Vimercati Silvia, Revirement *dei giudici di merito: il direttore della testata telematica non risponde del reato di omesso controllo. Verso due nozioni di "stampa"?,* in *MediaLaws,* n. 2, 2023, 382 ss.

– Violante Luciano, *Diritto e potere nell'era digitale.* Cybersociety*,* cybercommunity*,* cyberstate*,* cyberspace*: tredici tesi,* in *Rivista di BioDiritto,* 2022, 145 ss.

–Visconti Arianna, *La repressione delle offese* online *alla reputazione: tra anomia di contesto e anomia normativa,* in K. Summerer, M. L. Mattheudakis, G. M. Caletti, *La nozione di contenuto illecito online. Fattispecie e responsabilità penale nella prospettiva europea,* Pisa, 2025, 203 ss.

–Vitarelli Francesca, *Il disvalore penale tra testo e contesto,* Torino, 2025.

–Vormbaum Thomas, *Il diritto penale frammentario nella storia e nella dogmatica*, trad. it. di M. Donini, in *www.penalecontemporaneo.it*, *Riv. trim.*, n. 1, 2015, 51 ss.

–Wall David S., *Cybercrime. The Transformation of Crime in the Information Age,* Cambridge, 2024.

–Weulen Kranenbarg Marleen, van Gelder Jean–Louis, Barends Ard J., de Vries Reinout E., *Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets,* in *Computers in Human Behavior,* 140, 2023.

–Zampetti Roberto, *Sicurezza nazionale e spazio cibernetico. Una minaccia "invisibile" nell'era digitale,* in *Istituto di Ricerche Internazionali Archivio Disarmo,* n. 1/2015, gennaio 2015, 3 ss.

–Zannotti Roberto., *Accesso abusivo ad un sistema telematico: quale il locus commissi delicti?*, in *Diritto dell'informazione e dell'informatica,* 2014, 948 ss.

–Zapatero Luis Arroyo, *La armonizacíon internacional del derecho penal,* in *Piratas, mercenarios, soldados, jueces y policías: nuevos desafios del derecho penal europeo y internacional,* a cura di L. A. Zapatero, A. N. Martin, Castilla–La Mancha, 2010, 29 ss.

–Zeno Zencovich Vincenzo, *La pretesa estensione alla telematica del regime della stampa. Note critiche,* in *Diritto dell'informazione e dell'informatica,* 1998, 15 ss.

–Zuboff Shoshana, *Il capitalismo della sorveglianza*, 2019.

Edizioni ETS
Palazzo Roncioni - Lungarno Mediceo, 16, I-56127 Pisa
info@edizioniets.com - www.edizioniets.com
Finito di stampare nel mese di settembre 2026