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

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0254 • articolo sottoposto a peer review • pubblicato in anteprima il 15 dic. 2025

Gaetana Morgante

Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del law enforcement

L'impatto della transizione digitale sul diritto penale può essere apprezzato sul duplice versante del diritto sostanziale e del law enforcement. Pur a fronte di una tendenziale anelasticità del diritto penale agli effetti trasformativi di passaggi *disruptive,* l'evoluzione delle categorie sostanziali – dal soggetto attivo, alla condotta, dalla causalità alla colpevolezza – risulta inevitabile. La pervasività degli effetti della transizione digitale, infatti, si riverbera sui modelli di incriminazione e sui presupposti di imputazione di una responsabilità storicamente e strutturalmente legata alla prospettiva della persona fisica, dello spazio "analogico" e della fondazione antropomorfica delle categorie sostanziali. Come paradigmaticamente desumibile dai profili penali della cybersecurity, la trasformazione delle categorie sostanziali e dei presupposti della responsabilità si collega anche alla sperimentazione di nuovi percorsi di law enforcement, caratterizzati dall'enfasi sulle funzioni preventive e collaborative tra i diversi attori del mondo digitale.

Transizione digitale – Responsabilità penale – Cybercrime – Cybersecurity – Law enforcement

Digital transition and criminal law. From the evolution of substantive categories to the "new face" of the law enforcement

The impact of the digital transition on criminal law can be appreciated under two different perspectives: substantive law and law enforcement. Despite the tendency of criminal law to be inelastic to the transformative effects of changes that are disruptive, the evolution of substantive categories – from the author of the crime to the conduct, from causality to culpability – is unavoidable. The pervasiveness of the effects of the digital transition impacts on models of criminalization and on the prerequisites for attributing responsibility historically and structurally linked to the perspective of the natural person, the "analog" space, and the anthropomorphic foundation of substantive categories. As can be paradigmatically inferred from the analysis of the criminal issues of cybersecurity, the transformation of the substantive categories and elements of liability is also linked to new approaches to law enforcement, characterized by an emphasis on preventive and collaborative functions between the various actors of the digital world.

Digital transition – Criminal responsibility – Cybercrime – Cybersecurity – Law enforcement

L'Autrice è professoressa ordinaria di Diritto penale presso la Scuola Superiore Sant'Anna di Pisa

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

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement - Parte 1*, a cura di Gaetana Morgante e Gaia Fiorinelli

1. Transizione digitale ed effetti trasformativi sulle categorie penalistiche

La transizione digitale esprime in termini, per così dire, immaginifici il carattere pervasivo e totale dell'impatto della tecnologia in ambito sociale, economico, produttivo, pubblico e privato. Il riferimento alla "transizione" appare, ai fini che qui interessano, singolarmente pertinente all'analisi delle conseguenze sulle categorie giuridiche e, in particolare, penalistiche della digitalizzazione in quanto rimanda a quel "passaggio" da un mondo analogico ad un mondo *digital-based* che si riflette anche nell'evoluzione delle chiavi interpretative dei presupposti sostanziali della responsabilità penale e dei relativi percorsi di law enforcement. La categoria concettuale della "transizione" rimanda, infatti, ad un dualismo che può essere declinato sia nei termini diacronici del "prima" e del "dopo" sia in quelli sincronici del gemellaggio in linea con quel 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[1], come nei casi paradigmatici dei binomi sicurezza pubblica e cybersecurity oppure identità personale e digitale[2]. La prospettiva che viene prevalentemente in considerazione è quella di una sorta di diritto del metaverso[3] ove principi, regole, fattispecie e, ai fini che qui più interessano, modelli di incriminazione

1. Sul predetto "sdoppiamento" dei diritti v. T.E. Frosini 2020, p. 1. e V. Frosini 2000, p. 275, Iannuzzi 2024, p. 36 ss.
2. V. Iannuzzi–Laviola 2023, p. 9 ss.
3. Per un'analisi delle connessioni tra metaverso e trasformazioni del diritto v. Riccio 2023, p. 2 ss. ove si fa, per l'appunto, riferimento alla *Second Life* che, nella prospettiva estensiva sopra delineata, amplia le possibilità fisiche, per mezzo dell'affidamento allo strumento tecnologico. In argomento v. anche Sarzana di Sant'Ippolito–Pierro–Epicoco 2022, p. 50, Sciancalepore 2023, Incampo 2025, p. 59 ove si esaminano le conseguenze della necessaria spazializzazione del diritto e della dogmatica giuridica sulla a-spazializzazione indotta dalla transizione digitale. Sulle trasformazioni delle soggettività giuridiche v. Cheong 2022, p. 467 ss., Haber 2024, p. 843-891. Sulle intersezioni con i profili penali della cybersecuity con particolare riguardo all'individuazione dei responsabili dei reati, Razzante 2022, p. 216.

siano duplicati in una seconda e inedita vita dai contorni ampiamente derogatori e potenzialmente "sregolati" rispetto a quella "reale".

Se però la metafora del gemellaggio può risultare concettualmente e, soprattutto, assiologicamente compatibile con una prospettiva di estensione dei diritti di fronte alla crescente complessità indotta dalle trasformazioni, *rectius* transizioni, tecnologiche, la traslazione della nozione di *digital transition* all'universo penalistico risulta molto più ardua in ragione dell'incompatibilità di principio tra la portata "totalizzante"[4] della trasformazione tecnologica e la necessaria frammentarietà delle scelte di politica criminale. A fronte del carattere capillare degli effetti del *fenomeno* tecnologico, il diritto penale è innanzi tutto chiamato a punire singoli e concreti *fatti* (pur) commessi in ambiente digitale. Tale frammentarietà si declina altresì in una tendenziale, o quantomeno iniziale, anelasticità del diritto penale di fronte ai cambiamenti totali come ravvisabile nei settori diversi, se pur concettualmente limitrofi, dell'ambiente o del lavoro fortemente influenzati dal progresso scientifico e produttivo, i quali sono trasversalmente percorsi da quel progresso tecnologico che sfida la tenuta delle categorie generali del diritto penale sostanziale.

La menzionata tendenziale anelasticità del diritto penale di fronte alle trasformazioni totali può essere apprezzata tanto su un piano extrasistematico, ovvero di profili che investono elementi di contesto di rilievo non strettamente penalistico, quanto a livello intrasistematico con particolare riguardo a quelle categorie penalistiche sostanziali (soggetto attivo, condotta, colpevolezza) o processuali dalla natura storicamente umanizzata e antropomorfica e, come tali, resistenti alle forme di smaterializzazione indotte dalla transizione digitale.

Sul piano extrasistematico l'elemento che esprime in termini più significativi l'impatto della *digital transition* sul diritto (anche) penale è quello del *rischio* o, più correttamente, della generazione di nuovi profili di rischio connessi alla digitalizzazione di attività individuali, produttive e pubbliche[5]. Pur non trattandosi di un profilo extrasistematico di nuova emersione a seguito della transizione digitale, essendo, come ricordato, coessenziale ad altre forme di trasformazione, o rivoluzione, scientifica o produttivo-industriale, la proliferazione dei rischi connessi all'avvento della digitalizzazione ha assunto, ai fini dell'analisi del relativo impatto sul diritto penale, caratteri di ancora maggiore pervasività dal momento che la crescente complessità di processi e attività mediate dalla tecnologia e il *gap* di conoscenza dei presupposti di funzionamento ed operatività della stessa (o *digital divide*) ha dato luogo a forme di vulnerabilità del tutto inedite le quali, prevalentemente tematizzate sul versante – *lato sensu* fisiologico e positivo – dei diritti[6], risultano in una parallela dimensione – patologica e negativa – di prevenzione e contrasto delle nuove forme di offesa agli stessi, coessenziali a disvelare la necessità di nuovi spazi e modi di intervento del diritto penale.

Dal punto di vista della riflessione teorica, come ricordato, si tratta di uno scenario non del tutto sconosciuto in quanto più in generale riferibile all'analisi degli effetti delle trasformazioni indotte dal progresso scientifico-tecnologico, per l'appunto, sulla generazione di nuove forme di offesa agli interessi meritevoli di tutela penale e sulla necessità di concettualizzare nuove forme di "coesistenza" tra pericolo e utilità sociale di attività tecnologicamente avanzate[7]. Come ampiamente esaminato nel settore, che con quello ambientale condivide alcuni tratti comuni con il tema oggetto della

4. In questi termini v. Garapon–Lassegue 2021, p. 79. Per un'ulteriore analisi della trasformazione della funzione giurisdizionale a fronte della trasformazione tecnica v. Longo 2023, p. 47 ss. ove si esamina il tema dello sviluppo del processo digitalizzato "per comprenderne la sostenibilità, anzitutto in termini costituzionali".
5. Per una compiuta concettualizzazione dell'effetto *disruptive* e totalizzante del progresso tecnologico sulla generazione di nuovi profili di rischio v. Beck 2000.
6. In questa prospettiva di valutazione dei "rischi" di nuove ed inedite offese e limitazioni dei diritti umani v. Sartor 2017, p. 424 ss., che riconduce all'impiego delle tecnologie informatiche anche effetti (sociali e di potenziale rilevanza penale) negativi, tra i quali: disoccupazione, alienazione, disuguaglianze, sorveglianza (da parte di soggetti pubblici e privati), profilazione, condizionamenti, discriminazione, esclusione sociale, forme inedite di censura.
7. Per una riflessione sui nuovi profili di rischio penalmente rilevante nel settore del diritto ambientale v. Gargani 2019, p. 111 ss., ove si dà conto di come "la determinazione dell'oggetto e dei limiti di tutela" assuma

presente indagine, del diritto penale del lavoro la progressiva emersione della nozione di "rischio", non solo come ulteriore anticipazione della soglia dell'intervento ma come elemento coessenziale e, soprattutto, non eliminabile dalle potenziali fonti di offesa dei beni giuridici rilevanti, ha condotto ad una rapida trasformazione dei confini delle categorie del diritto penale generale[8] passando dalla tralatizia logica binaria e, per così dire, ultimativa del dovere di eliminazione del pericolo come condizione per la prosecuzione dell'attività a quella plurale dell'obbligo collettivo di gestione di un rischio impossibile da azzerare.

Sul versante della variazione degli elementi intrasistematici, la transizione digitale e la pervasività delle trasformazioni tecnologiche induce significativi variazioni nella definizione del *soggetto attivo*, in considerazione della sua frequente invisibilità, *rectius* anonimato, dovuta alla mancanza di un *locus commissi delicti* fisico[9] e all'attitudine dell'ambientamento digitale del reato a fare da schermo alla sua identità, della delimitazione delle *condotte* in forza della necessaria variazione dei modelli di incriminazione[10] e, in diretta connessione con il tema del tendenziale anonimato del soggetto attivo, dei confini e degli stessi margini di operatività dell'accertamento dell'*elemento soggettivo*, peraltro prevalentemente di tipo doloso e quindi storicamente connesso a profili psicologici di ardua traslazione alla sfera digitale.

Posto che, dunque, alla riflessione penalistica non sia estranea l'esperienza di modificazioni, o rivoluzioni, con effetti *disruptive* sulle categorie giuridiche di riferimento della parte generale e speciale[11], il dato che differenzia potentemente la transizione digitale da altre forme, in parte note, di "rivoluzioni" scientifico-produttive è il carattere di totale immaterialità della transizione digitale, come tale astrattamente incompatibile con un diritto, quale quello penale, fortemente legato alla materialità e all'"ambientamento fisico-analogico" del soggetto attivo, della condotta, della colpevolezza e di ogni altro segmento della filiera della politica criminale e del law enforcement. Non stupisce, dunque, che la primigenia reazione a questo cambiamento sia stata quella dell'angoscia[12], della sottomissione[13] o dello smantellamento[14] dell'esistente rispetto a trasformazioni che paiono mettere in crisi la stessa praticabilità del diritto penale nell'affrontare i rischi e le nuove vulnerabilità emergenti in ambiente digitale.

Pur a fronte delle indubbie variazioni trasformative imposte dalla transizione digitale, il diritto penale si trova, tuttavia, di fronte ad una straordinaria opportunità di essere rifondato a partire dalle sue categorie concettuali di riferimento proprio nel nome dei principi fondamentali che ne informano l'esistenza valorizzando il contenuto di garanzia dinamica, e non statica, dei diritti fondamentali rispetto a nuove forme di aggressione. La caratterizzazione antropomorfica dei modelli di incriminazione, infatti, parrebbe poter essere, per così dire, riferita più alle tecniche di costruzione delle fattispecie che ai principi e alle funzioni del

"un'intrinseca processualità e relatività", non potendo la eventuale rilevanza penale della condotta essere apprezzata a priori, in base a parametri naturalistici e senza essere mediata dall'operatività di elementi giuridici extrapenali volti a stabilire "soglie" e presupposti di legittimità delle attività rischiose. In questi termini, si argomenta la natura "convenzionale" e non più "assoluta" della tutela. Sul punto cfr. anche De Francesco 2004, p. 62 ss.

8. Fondamentali le riflessioni sul tema di Padovani 1996, p. 1161.
9. In argomento si rinvia alla riflessione di Incampo 2025, p. 59 ove si ripercorrono le radici filosofiche giuridiche del collegamento tra diritto e spazio "E il diritto? Cosa accade al diritto? Il nomos è sempre stato, per dirla con Carl Schmitt, 'nomos della terra' [*Nomos der Erde*]. Lo stesso concetto kelseniano di 'validità' [*Geltung*] indica l'"esistenza specifica' [*speziphische Existenz*] di un fatto o di una norma in un tempo e in uno spazio determinati".
10. V. *infra* sub 2.
11. Sulle origini perfino mitologiche della connessione tra crime e technology v. McGuire 2012, p. 7 ss.; Smith 2004, p. 105 ss.
12. Stortoni 2004, p. 75, rispetto alla "asserita non conoscenza né conoscibilità del pericolo", con le relative ricadute di tale impostazione sugli stessi istituti della condotta, della causalità e della colpevolezza.
13. Bodei 2019.
14. Hoffmann–Riem 2020, p. 143 ss.

diritto penale che si rivelano molto più elastici dei modelli consolidati in quanto chiamati ad adattarsi al mondo, anche e soprattutto quello criminale, che cambia in una logica di strumentalità rispetto alla protezione dei beni giuridici e dei rispettivi titolari che non può venir meno sol che cambi il contesto nell'ambito del quale nuove offese sono perpetrate. Si tratta, invero, anche rispetto alla distinzione tra piano dei principi e piano degli strumenti di incriminazione, di una riflessione nota anche se ancora una volta riferita ad una, solo apparentemente, più limitata analisi delle modalità[15] della condotta o, per l'appunto, dello *strumento*[16] dell'azione, la quale, ben lontana dal poter essere confinata entro la nicchia dei diversi modi in cui un interesse meritevole di tutela può essere offeso, pone, nella materia che ci occupa, la necessità che il diritto penale si adatti alle trasformazioni dei modelli di incriminazione acquisendo anche nel *cyberspace* una condizione di esistenza pur con forme completamente rinnovate[17].

2. I modelli di incriminazione dei reati commessi in ambiente digitale

La richiamata caratterizzazione anelastica del diritto penale sul piano dei diversi modelli di incriminazione è ravvisabile nella prima concettualizzazione[18] del c.d. *computer crime*. Nel quadro di una definizione saldamente "ancorata" ad un supporto "fisico", il *pattern* di riferimento era stato individuato nell'*abuso* ravvisato, nel più ampio scenario del valore dell'informazione generata e circolata grazie alle tecnologie informatiche, in "any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data". Invero, non stupisce che il modello di riferimento si sia attestato su una figura, quella dell'abuso, per un verso "fondazionale" della teoria generale del diritto e, per altro verso, facente leva su una sorta di modello "minimale" di diritto penale sanzionatorio *ex post* della violazione delle regole d'uso (definite *aliunde*) di sistemi che così prepotentemente si affermavano in conseguenza della rivoluzione delle tecnologie informatiche. In questa prima tranquillizzante definizione del reato commesso in ambiente digitale l'indicazione politico-criminale si attesta su solchi arati da millenni quali quelli dei *reati contro il patrimonio* nella duplice caratterizzazione delle *condotte di sottrazione* (l'immissione, l'alterazione, la cancellazione e/o la soppressione di dati informatici e/o programmi informatici eseguita volontariamente, con l'intento di commettere un trasferimento illegale di fondi o qualsiasi altro bene e la violazione del diritto esclusivo del titolare di un programma informatico protetto, con l'intento di sfruttare commercialmente il programma e immetterlo sul mercato) e *di intrusione/danneggiamento* (l'immissione, l'alterazione, la cancellazione e/o la soppressione di dati informatici e/o programmi informatici compiuta intenzionalmente, con l'intento di commettere un falso; l'immissione, l'alterazione, la cancellazione e/o la soppressione di dati informatici e/o programmi informatici, o altre interferenze con sistemi informatici, fatte intenzionalmente con l'intento di ostacolare il funzionamento di un sistema informatico e/o di telecomunicazione e l'accesso o l'intercettazione di un sistema informatico e/o telematico effettuato consapevolmente e senza l'autorizzazione del responsabile del sistema, violando le misure di sicurezza o con qualsiasi altro intento disonesto o dannoso).

A valle di un passaggio intermedio attraverso la nozione di *computer-related crimes* che cominciava a prendere timidamente le mosse dalla definizione "con ancoraggio fisico" dei reati commessi in ambiente digitale[19], la più coraggiosa concettualizzazione dei modelli di incriminazione del *cybercrime* può essere individuata in una tripartizione, frequentemente riferita al crimine organizzato ma generalizzabile anche a forme di reato non plurisoggettivo. Si tratta della fortunata triade *cyber-dependent, cyber-enabled* e *cyber-assisted*

15. Bricola 1978.
16. Delogu 1974, p. 19 ss.
17. Sulla natura "programmatica" della tutela penale a partire dai suoi principi fondamentali v. De Francesco 2004, p. 62 ss.
18. OECD 1986.
19. European Committee on Crime Problems 1990.

crimes elaborata dalla dottrina criminologica[20] ma di grande efficacia euristica anche ai fini dell'analisi delle trasformazioni indotte dalla transizione digitale nelle categorie concettuali del diritto penale e nei relativi modelli di incriminazione. In una sorta di progressione discendente in termini di connessione funzionale con l'ambientamento digitale si distinguono, infatti, (i) attività criminose che sono *create/rese possibili* dalle nuove tecnologie informatiche e che, per riprendere – pur in termini rovesciati – l'immagine del gemellaggio prima menzionata, non hanno un *analog twin* (come nel caso degli attacchi *ransomware* ad una infrastruttura critica), (ii) attività criminose che risultano variamente potenziate dal ricorso alle tecnologie informatiche (si tratta del caso, tra gli altri, dei reati a mezzo stampa commessi nell'ambito di social network) e che hanno una sorta di *analog twin* pur più debole e contenuto e (iii) reati che sono, per così dire, già conosciuti nel mondo fisico (si pensi al caso, ampiamente presente nella prassi giurisprudenziale, delle truffe *on line*) ma che, tra le diverse modalità di realizzazione, sono compatibili anche con quella *cyber* e ove l'immagine dell'*analog twin* dovrebbe essere la più pertinente, in quanto riferita, quantomeno nella logica della predetta concettualizzazione categoriale, allo *stesso* reato ma commesso *on line*.

In verità, a ben vedere tale tripartizione tende a perpetuare l'anelasticità e l'antropomorfismo di un diritto penale refrattario ai cambiamenti indotti dalla tecnologia in quanto, pur nell'accezione negativa della ricordata mancanza di un corrispondente gemello analogico, tende a rappresentare il cybercrime come una sorta di anomalia del sistema penale a cui quest'ultimo deve faticosamente adattarsi opponendo al cambiamento, almeno fin dove possibile, un modello speculare tradizionale in tal modo istituendo anche una sorta di ideale, o forse, cripto-progressione ascendente dell'impatto della transizione digitale su principi e regole del diritto penale dal minimo della categoria (iii) al massimo della categoria (i).

Posto che, tuttavia, come ricordato il fondamento di garanzia dei principi cardine del sistema penale debba sfuggire tanto ad una logica antropomorfica quanto all'anelasticità rispetto ai cambiamenti indotti dalla transizione digitale, non parrebbe, invero, contestabile che i principi fondazionali del sistema (a partire da quello di legalità) debbano trovare ugualmente applicazione quale che sia la subcategoria di *cybercrime* e forse proprio *a fortiori* nelle ipotesi che si sono definite *cyber-dependent* nel nome di quella storicità[21] dei diritti – e delle relative garanzie – che ne costituisce contenuto essenziale e che, come tale, si oppone ad approcci conservativi ed anelastici come anche ad attenuazione delle garanzie a fronte di inedite forme di criminalità smaterializzata.

Spostandosi, invece, dal livello dei principi fondamentali a quello dei modelli di incriminazione, la tripartizione, pur di grande e perdurante valore euristico e classificatorio, sopra menzionata presenta, dal versante delle trasformazioni delle categorie di diritto penale sostanziale, taluni profili meritevoli di valutazione critica. Sembrerebbe, infatti di poterne inferire una diversa gradazione della *vexata quaestio* del dibattito[22] tra "eccezionalisti" e "non eccezionalisti" nell'analisi del rapporto tra diritto e transizione digitale e, per quello che attiene alla presente indagine, tra diritto penale tradizionale e cybercrime. Mentre, infatti, parrebbe prevalere una logica non eccezionalista ma di rapporto, per così dire, da *genus* a *species* rispetto alle categorie dei *cyber-enabled* e dei *cyber-assisted crimes* che in questa logica sarebbero diverse forme di manifestazione modali o strumentali di fattispecie incriminatrici già note, l'approccio alla categoria dei *cyber-dependent crime* sarebbe dominata da una prevalente logica eccezionalista di un orizzonte di incriminazione totalmente inedito e al limite dell'anomalia in un sistema fondato sulla (indimostrata, indimostrabile e storicamente smentita) necessità che il modello-standard di crimine sia solo quello commesso nel mondo fisico-analogico. Un tale ragionamento paralogistico in quanto basato sulla premessa erronea che i

20. Wall 2004-a, p. 20 ss.; Wall 2004-b, p. 309 ss., McGuire–Dowling 2013, Di Nicola 2022, Di Nicola 2021.

21. "Perché i diritti dell'uomo, per fondamentali che siano, sono diritti storici, cioè nati in certe circostanze, contrassegnate da lotte per la difesa di nuove libertà contro vecchi poteri, gradualmente, non tutti in una volta e non una volta per sempre", Bobbio 1990, p. 7.

22. Goldsmith 1999; Johnson–Post 1996.

modelli di incriminazione siano anelastici rispetto alle trasformazioni digitali e che, in mancanza di un *analog twin*, il modello di incriminazione del *cyber-dependent crime* abbia una portata eccezionale rispetto al sistema potrebbe porre le premesse per un'inaccettabile impostazione da doppio standard anche rispetto all'operatività dei principi fondamentali, rigidamente applicabili, in analogia ai modelli tradizionali di incriminazione, ai *cyber-enabled* e *cyber-assisted crimes*, e, invece, più sfumati con riguardo ai *cyber-dependent crime*.

Nella richiamata ottica di una specularità tra transizione digitale e transizione dei modelli giuridico-penali di riferimento per l'incriminazione dei reati commessi in ambiente digitale, parrebbe, piuttosto, doversi ritenere che tutti i *cybercrimes* siano, *by definition, cyber-dependent* necessitando di una rifondazione *ab imis* di programmi e modelli delle incriminazioni che, pur con diversi riferimenti categoriali, permettano di valorizzare le funzioni del diritto penale nel più ampio quadro della prevenzione e del contrasto al reato commesso in ambiente digitale.

3. Verso nuovi paradigmi di diritto penale sostanziale *by cyber-design*

Nella ricordata ottica della proposta di un nuovo volto del diritto penale di fronte alla transizione digitale in una prospettiva autonomistica e non analogica si pone la necessità di valorizzare i tratti comuni di tutte le forme di *cybercrime* andando oltre la tripartizione dei modelli di incriminazione. In particolare, si tratta di valutare la fattibilità di un'evoluzione della definizione del modello di incriminazione delle condotte poste in essere in contesto digitale oltre il *paradigma analogico* che sfrutta le fattispecie esistenti adattandole alla variante digitale e il *paradigma strumentale* che fa leva sul mezzo informatico per costruire fattispecie modellate tenendo conto degli effetti del ricorso allo strumento informatico. Si pensi al noto esempio del domicilio informatico per concettualizzare i modelli di incriminazione dell'accesso abusivo e che ha indotto a collocare nella sezione relativa ai *delitti contro l'inviolabilità del domicilio* le fattispecie di cui agli artt. 615-*ter* c.p. (*Accesso abusivo ad un sistema informatico o telematico*), 615-*quater* c.p. (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*), e 615-*quinquies* c.p. (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*), tutte trainate dalla fattispecie generale di "Violazione di domicilio" ma punite – almeno avuto riguardo alla pena-base – meno gravemente rispetto alle analoghe fattispecie relative al "domicilio fisico". Si ponga altresì mente al binomio dato/cosa mobile ai fini dell'applicazione dei delitti contro il patrimonio, dall'appropriazione indebita al furto, allo scopo di sussumere in un fatto tipico "noto" la condotta di chi, a seguito di un accesso abusivo, si appropri di informazioni presenti nel database violato[23] e rispetto alle quali si postuli un valore economico.

L'assunto, logicamente connesso al binomio *cyber-enabled* e *cyber-assisted crime*s, secondo il quale si tratterebbe di *mere varianti* dell'analogo gemello tradizionale appare, tuttavia, revocabile in dubbio come direttamente dimostrato dagli equilibrismi interpretativi cui la giurisprudenza è frequentemente chiamata. Che l'accesso abusivo a sistema informatico presenti la stessa struttura dell'abuso di domicilio con l'unica variante del mezzo informatico appare fortemente criticabile. Radicalmente diversi risultano, infatti, il *soggetto attivo*, potenzialmente anche non corrispondente ad una persona fisica nei casi in cui tali forme di criminalità siano completamente automatizzate, il complesso degli *elementi normativi* referenti dei presupposti di legittimità dell'accesso, talvolta anche extragiuridici come, ad esempio, nel caso dell'utilizzo di strumenti crittografici, *modus* e *tempus commissi delicti* che, nella sfera dei *cybercrimes*, possono sensibilmente variare e contrarsi rispetto al mondo fisico-analogico rispetto alla persona offesa, che, anche nei reati a vittimizzazione individuale, risulta comunque connotata da una prospettiva, *lato sensu*, esponenziale in ragione della

23. In giurisprudenza *ex multis* v. Cass. Pen., sez. II, 18 febbraio 2016, n. 21596, in "Il penalista.it", 22 giugno 2016. Cfr. anche Cass. pen., sez. II, 7 novembre 2019, n.11959, in "dejure.it.", che sottolinea che si fa espressamente riferimento all'esigenza "di interpretare talune categorie giuridiche che, coniate in epoche in cui erano del tutto sconosciute le attuali tecnologie informatiche, devono necessariamente esser nuovamente considerate". Per una lettura critica v. Pisani 2020.

ripetibilità delle condotte e della loro scalabilità, mediata dalla tecnologia, verso numeri massivi di soggetti passivi. Si pensi, a tale ultimo proposito, agli effetti delle pratiche di *social engineering* sull'emersione di nuove vulnerabilità anche determinate dall'inattitudine della previa vittimizzazione da *cybercrime* ad aumentare la consapevolezza e la percezione del rischio[24]. In questi casi, la vittima, pur formalmente "singola" non è soltanto individuale, alla stregua del classico binomio individuale-collettivo del diritto penale tradizionale, ma è un target esposto a condotte penalmente rilevanti in quanto espressivo di caratteristiche riferibili ad un ampio gruppo che abilita soggetti, e spesso perfino gruppi criminali, alla commissione seriale di reati che, *mutatis mutandis*, possono comunque definirsi "a vittimizzazione collettiva non sincrona".

La profonda diversità dei *cybercrimes as such* rispetto al fondamento giustificativo dei modelli tradizionali di incriminazione, dunque, suggerisce di convergere su paradigmi autonomistici di *cybercrime by design* ove la fattispecie incriminatrice non costituisca la variante di un modello già conosciuto ma integri *ab initio* un illecito, non necessariamente penale, interamente calibrato sul contesto digitale del suo autore, della condotta e di tutti gli elementi costitutivi del reato. L'insidia da evitare nella costruzione di un modello di cybercrime che si è voluto definire *by design* è costituita dall'abuso della generalizzazione del modello, per rifarsi alla tripartizione sopra menzionata, del *cyber-dependent crime* e ove il piano del rispetto dei principi venga rarefatto a fronte di un modello di incriminazione altrettanto "smaterializzato" con la conseguenza che si possa, per così dire, tollerare, un affievolimento del vincolo alla tassatività e determinatezza della fattispecie in nome dell'efficienza dell'intervento penalistico, talvolta anche emergenziale e privo di una visione di sistema, a presidio degli interessi protetti.

Singolarmente paradigmatica di tale insidia è la fattispecie di pornografia virtuale di cui all'art. 600-*quater*.1 c.p. la quale estende l'applicazione delle disposizioni aventi ad oggetto la pornografia minorile (art. 600-*ter* c.p.) e la detenzione ed accesso a materiale pornografico (art.600-*quater* c.p.) anche ad immagini virtuali che potrebbero essere state realizzate con tecniche di elaborazione grafica non associate ad immagini reali ma la cui qualità di rappresentazione le faccia apparire come vere situazioni. Come ampiamente rilevato dalla dottrina[25], si tratta di forme di criminalizzazione ove l'esclusivo ambientamento virtuale può condurre ad una grave compromissione di principi fondamentali in quanto volta a stigmatizzare condotte espressive di un "tipo d'autore" e non di una condotta offensiva di beni giuridici meritevoli di tutela con scopi di moralizzazione che dovrebbero rimanere estranei ad un diritto penale laico. Sotto tale angolo visuale, la prospettiva autonomistica dei modelli di incriminazione del *cybercrime* e l'attribuzione allo stesso di una dignità autonoma dall'essere la variante di un corrispondente modello analogico può innanzi tutto contribuire, ribadita la necessità del rispetto dei principi fondamentali, a sottoporre le scelte di criminalizzazione ad un efficace e, in sede di *drafting* legislativo, preliminare *subsidiarity test* in ordine alla conformità con il principio di frammentarietà ed *extrema ratio* del diritto penale della stessa scelta dello strumento criminale per punire una condotta realizzata in ambiente digitale.

A tal riguardo il raffronto tra il reato di pornografia virtuale e la strategia legislativa a prevenzione e contrasto del *cyberbullismo* di cui alla legge 71/2017 può risultare, ai fini che qui interessano, particolarmente promettente in quanto espressivo di un ricorso simbolico e stigmatizzante del diritto penale non direttamente connesso ad adeguate azioni di efficace contrasto (la pornografia virtuale) e di un (più condivisibile) intervento che,

24. Albladi–Weir 2020, p. 4.

25. V. Delsignore 2023, p.388 ss. Sullo specifico punto della compatibilità con i principi fondamentali dell'uso del diritto penale per punire comportamenti posti in essere in modalità integralmente digitale v. anche Maugeri 2021, Maugeri 2020, p. 908 ss., con riferimento alle fattispecie di cui agli artt. 600-*quater* c.p. e 600-*quater*.1 c.p., rispettivamente considerate un esempio "paradigmatico" e un esempio "esasperato" del diritto penale "del nemico" *in subiecta materia*, con evidente anticipazione della soglia dell'intervento penale, a sanzionare comportamenti piuttosto sintomatici di un particolare "tipo di autore" che non direttamente lesivi del bene giuridico da tutelare. *Amplius* la compiuta analisi di Fiorinelli 2024, p. 110 ss.

al contrario, non viene affidato allo strumento criminale ma ad una diversa politica di prevenzione e contrasto basata sulla responsabilizzazione del gestore del sito Internet e la previsione di interventi immediati di blocco e rimozione dei contenuti on line, ferma restando la configurabilità di gravi reati, quali, ad esempio, quello di atti persecutori di cui all'art. 612-*bis* c.p., qualora ne ricorrano tutti gli elementi costitutivi. Come sostenuto dalla dottrina[26], si tratta di un approccio da valutare positivamente in ragione della sinergia tra strumenti penali e rimediali "attivabili anche al di fuori del (più impervio) percorso processual-penalistico di accertamento del fatto" facendo "ricorso a poteri coercitivi per l'eliminazione delle 'conseguenze' del reato, non più da intendersi quale adempimento posto programmaticamente a carico dell'autore dell'illecito" da parte dell'autorità di law enforcement "ma anzi quale obiettivo *primario* perseguito dal legislatore, nell'ambito di un paradigma di prevenzione *in concreto*".

Laddove, invece, il *subsidiarity test* della meritevolezza di sanzione penale della condotta illecita posta in essere in contesto digitale venga superato e, nel rispetto del principio di frammentarietà, si proceda all'introduzione nel sistema di una fattispecie incriminatrice, l'approccio autonomistico potrebbe fondare tecniche di legislazione penale, per l'appunto, *by design* in quanto non volte ad appiattire il cybercrime sul "gemello analogico" ma a costruire reati calibrati sul peculiare modo d'essere della criminalità *on line*.

Pur con tutte le riserve legate alla prossimità temporale dell'intervento e alla necessità della formazione di una più consistente giurisprudenza di merito e di legittimità, un interessante modello di riferimento di forme autonome di cybercrime *by design* può essere tratto dall'ambito della *cybersecurity* dalle strategie nazionali ed internazionali al recente intervento di cui alla legge 28 giugno 2024, n. 90, la quale impone quel "riassestamento assiologico"[27] delle diverse forme di manifestazione di una criminalità che, in ragione della pervasività dei suoi effetti offensivi, sfugge ad una lettura riduzionistica ad una variante virtuale dei reati contro la sicurezza pubblica tradizionalmente intesa o, come ricordato, della criminalità contro il patrimonio per finalità di profitto. Dalle estorsioni informatiche alla coercizione digitale, dalle varie forme di attentato alle infrastrutture critiche alla progressiva emersione di nuove forme di criminalità organizzata digitale anche con accenti di *crime-as-a-service*, la criminalizzazione degli attacchi alla cybersicurezza si iscrive in un sistema ove la fattispecie incriminatrice non è più un elemento *standalone* ma si colloca all'interno di una più ampia strategia di prevenzione, contrasto e *rapid-reaction* che ruota intorno al volano della notifica degli incidenti al fine della realizzazione degli interventi immediati di reazione e contribuisce ulteriormente alla transizione verso un modello autonomistico ed integrato di intervento penale che, superato il *subsidiarity test*, possa assumere una marcata connotazione *multistakeholder* e collaborativa in una logica di partenariato esteso nella definizione delle politiche di contrasto alla cybercriminalità.

Alla medesima logica che si è voluta definire "autonomistica" può essere ricondotta anche la legge 23 settembre 2025, n. 132 avente ad oggetto *Disposizioni e deleghe al Governo in materia di intelligenza artificiale* la quale, al di là dell'apparente assonanza con modelli di incriminazione e circostanziali già conosciuti, affronta il tema dell'intersezione tra diffusione dell'intelligenza artificiale e criminalità in una prospettiva di sistema e non emergenziale e analogica. Alla predetta *ratio* politico-criminale sembrerebbero potersi, in particolare, ascrivere l'art. 612-*quater* c.p. (*Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*) che punisce con la reclusione da uno a cinque anni chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, o l'art. 294 (*Attentati contro i diritti politici del cittadino*) che punisce con la reclusione da due a sei anni l'inganno posto in essere mediante l'impiego di sistemi di intelligenza artificiale o, in termini ancora più generali l'art. 61 n. 11-*decies* c.p., ai sensi del quale viene introdotta una nuova aggravante comune consistente ne "l'avere commesso il fatto mediante l'impiego di sistemi

26. Fiorinelli 2024, p. 129.

27. *Ivi*, p. 146.

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 carattere sistematico dell'intervento coinvolge anche ipotesi di reati economici come l'aggiotaggio di cui all'articolo 2637 del codice civile che punisce con la reclusione da due a sette anni il fatto commesso mediante l'impiego di sistemi di intelligenza artificiale e il *market abuse* di cui all'articolo 185, comma 1, del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, analogamente punito con pene molto elevate qualora commesso mediante l'impiego di sistemi di intelligenza artificiale.

Nella prospettiva, antica ma autenticamente visionaria, della consapevolezza dell'effetto trasformativo del medium del reato sulle categorie della teoria generale del reato, la transizione digitale suggerisce, come lo "strumento" nella riflessione di Tullio Delogu, una transizione verso una nuova postura del diritto penale nel sistema di prevenzione e contrasto della criminalità in ambiente digitale che, in una prospettiva integrata, sia idealmente disposta, come nella *success story* del cyberbullismo, a rinunciare ad una funzione inutilmente simbolica a favore di un più efficace sistema di gestione del rischio e di contrasto dell'illecito. In questa prospettiva, e ben al di là del disegno del modello di incriminazione, una legislazione, anche penale, *by cyber-design* non può non fondarsi su un paradigma di responsabilizzazione condivisa ove ciascuno, a partire dalla vittima dell'illecito, si faccia "garante di prossimità" e cooperi, anche *praeter delictum*, alla prevenzione, alla repressione e alla riparazione delle conseguenze del *cybercrime*.

4. La trasformazione dei modelli di law enforcement dalla repressione *ex post* alla prevenzione cooperativa

La transizione verso nuove ed autonome forme di intervento del diritto penale di fronte alla criminalità in ambiente digitale porta con sé una trasformazione dei modelli di law enforcement il cui tratto, tra i molti, maggiormente distintivo è costituito dalla socializzazione o dalla solidarietà nella gestione del rischio-reato nel *cyberspace*. Nel solco della teorica dei reati omissivi impropri e della posizione di garanzia rispetto alla tutela di beni giuridici meritevoli di tutela (anche) penale, l'impatto della rivoluzione tecnologica sulla moltiplicazione dei predetti garanti ha un volto anch'esso "antico" in quanto riferibile all'ampio dibattito teorico, giurisprudenziale e regolatorio sullo statuto della responsabilità dei *digital service providers*. Pur non essendo questa la sede per trattare *funditus* il tema, la responsabilizzazione del provider rispetto agli illeciti commessi dagli utenti dei servizi messi a disposizione rimanda alla nozione sopra menzionata di "garante di prossimità". A fronte delle indubbie difficoltà di accertamento degli illeciti commessi on line, elevare il provider ad una posizione di controllo risulta senz'altro pertinente rispetto alle questioni problematiche del law enforcement nel *cyberspace*. Al di là dell'adesione al modello della caratterizzazione commissiva o omissiva della sua responsabilità, l'elemento di maggiore rilievo nell'ottica della transizione dei modelli di law enforcement è costituito dall'attitudine del provider a svolgere un *continous monitoring* idoneo ad andare oltre la prospettiva tradizionale, e puntuale-episodica, dell'obbligo giuridico di impedimento del singolo reato altrui.

Invero, il dibattito sullo statuto giuridico della responsabilità del provider e sull'ampiezza della sua posizione di garanzia è stato prevalentemente dominato dall'inquietante spettro della criminalizzazione del mancato controllo o del mancato impedimento. Pur a fronte della limpida teorica[28] della simmetria tra poteri di intervento e obblighi di monitorare, di attivarsi per denunciare/segnalare o di impedire, la giurisprudenza ha progressivamente condotto il predetto statuto della responsabilità del provider dal minimale dovere di attivarsi in presenza della conoscenza di fatti illeciti al dovere generalizzato di impedimento del reato commesso in rete dal suo utente sulla scorta, per l'appunto, della *prossimità* del provider ad una fonte di rischio e ad illeciti difficili da accertare da parte della autorità pubblica di law enforcement.

Alla base della predetta estensione dei doveri impeditivi del *digital service provider* parrebbe, tuttavia, prevalere, per un verso, una logica monopolistica in capo all'autorità pubblica del

28. Fondamentale in argomento la riflessione di Leoncini 1999, p. 55 ss.

law enforcement che si traduce poi in una cripto-delega al garante prossimo per il tramite della panpenalizzazione della violazione dei suoi doveri di intervento (ed impedimento) *post factum*. Parrebbe, tuttavia, ancora una volta trattarsi di una soluzione "analogica" della questione problematica del law enforcement nel *cyberspace* operata attraverso il ricorso a categorie tradizionali, quali, per l'appunto, gli (estesi) obblighi di impedimento e le (dilaganti) diverse forme di responsabilità penale omissiva propria ed impropria.

In linea con l'approccio autonomistico alla trasformazione dei modelli di incriminazione indotti dalla transizione digitale, parrebbe invece opportuno valutare di postulare nell'ampia categoria che si è voluta definire dei "garanti prossimi" lo sviluppo di forme di *cooperative compliance praeter delictum* ove i doveri di collaborazione prescindono dal temuto paradigma del concorso per omissione del titolare della posizione di garanzia ma si collocano nel solco di un diverso costrutto dialogico tra "garanti (privati) di prossimità" e autorità (pubbliche) di law enforcement[29]. Dal binomio classico potere/responsabilità penale potrebbe, dunque, ipotizzarsi una più promettente scissione concettuale ove il potere (di monitoraggio ed intervento) sia finalizzato ad evitare l'imputazione di responsabilità (anche penali) valorizzando il volto difensivo e non ascrittivo del potere. Tale paradigma estensivo dei doveri di controllo sull'integrità del contesto digitale gestito dal provider costituisce, invero, la premessa concettuale per un cambio di paradigma anche nella prospettiva vittimologica. Attraverso un processo assimilabile, pur *mutatis mutandis*, a quello ravvisabile nel diritto penale del lavoro, l'impossibilità di limitare il monitoraggio al singolo fatto illecito commesso in rete porta con sé la "discesa" della responsabilizzazione fino agli *end users, rectius* gli utenti e, agli effetti della legge penale, dei titolari dei beni giuridici protetti che, analogamente ad altri ambiti del diritto penale dell'economia, si allontanano sempre più dal modello del creditore passivo, e a tratti inconsapevole, di protezione per divenire sempre più vicini alla nozione di co-obbligati alla (auto) tutela con tutto il corredo di *awareness, resilience* e *solidarity* che costituiscono la più moderna e internazionalmente condivisa declinazione di *cybersecurity*.

5. Prolegomeni del nuovo volto del diritto penale del *cyberspace*

In conclusione dell'analisi dell'impatto della transizione digitale sui modelli di incriminazione ed i percorsi di law enforcement, è proprio nel passaggio dal modello analogico e, a tratti, insidiosamente metaforico di soluzioni mutuate da ambiti tradizionali a quello che si è voluto definire autonomistico che parrebbe potersi individuare il nuovo volto del diritto penale del *cyberspace*. Al di là di logiche emergenziali che spesso collassano in forme di panpenalizzazione e incriminazione simbolica di illeciti che suscitano particolare allarme sociale, un rigoroso filtro di frammentarietà impone di riservare, anche e soprattutto nella dimensione digitale, al diritto penale il contrasto dei più gravi illeciti che offendano diritti fondamentali in una prospettiva ove il diritto penale non sia la *prima ratio* ma un elemento di un sistema integrato composto anche da misure preventive, rimediali, civili o amministrative e ove tra modelli di incriminazione e paradigmi di law enforcement vi sia una sinergia concettuale ed assiologica[30].

La necessità di approcci autonomistici alla definizione dei modelli di incriminazione nel *cyberspace* consente di rivalutare criticamente le classiche tripartizioni dei *cybercrimes* sulla base del crescente livello di analogia con fattispecie incriminatrici tradizionali come anche di rivedere la distinzione tra reati a vittimizzazione individuale e collettiva. Pur conservando anche questo binomio una sua validità classificatoria e politico-criminale, la pervasività del contesto digitale in diritto penale attribuisce alla vittima individuale un significato "esponenziale" e "scalabile" che trascende dalla nozione "fisico-analogica" della vittimizzazione singola potendo, peraltro, innescare

29. Pur trattandosi di una categoria sviluppata prevalentemente negli studi economico-manageriali e, in ambito giuridico, nel settore del diritto tributario (Björklund Larsen–Oats 2019, p. 165 e Troiano 2017/2024, p.10), la categoria della *cooperative compliance* può risultare molto pertinente, combinata alle più recenti evoluzioni della nozione di cyber resilienza, all'evoluzione dei modelli di law enforcement pubblico-privato nel *cyberspace*.

30. In argomento McGuire 2017, p. 35 ss.

processi di vittimizzazione a catena che presentano una nuova dimensione della collettività rispetto alle tradizionali definizione della sicurezza pubblica o collettiva.

Una concettualizzazione autonomistica dei modelli di incriminazione e di law enforcement presenta altresì il vantaggio di suggerire approcci "scalabili" anche in altri ambiti che con quello della transizione digitale condividano la stessa necessità di elasticità in presenza di cambiamenti "totalizzanti" quali, tra gli altri, quelli indotti dal cambiamento climatico, o dai rischi CBRN o dal sempre crescente impiego delle tecnologie robotiche nella produzione, nel lavoro, nella sanità.

Ribadito il principio di *extrema ratio*, il nuovo volto del diritto penale può disvelare le sue potenzialità preventive e cooperative non tanto e non solo in funzione di imputazione della responsabilità *post delictum* ma di prevenzione e organizzazione nella gestione del rischio *ante* e *praeter delictum* in una più moderna declinazione della prevenzione generale positiva che faccia prevalere su quello simbolico il profilo più solidaristico e collaborativo del contrasto (anche penale) alla cybercriminalità.

Riferimenti bibliografici

S.M. Albladi, G.R.S. Weir (2020), *Predicting individuals' vulnerability to social engineering in social networks*, in "Cybersecurity", vol. 3, 2020, n. 1

U. Beck (2000), *La società del rischio. Verso una seconda modernità,* trad. it., Carocci, 2000

L. Björklund Larsen, L. Oats (2019), *Taxing Large Businesses: Cooperative Compliance in Action*, in "Inter economics", vol. 54, 2019, n. 3

N. Bobbio (1990), *L'età dei diritti*, Einaudi, 1990

R. Bodei (2019), *Dominio e sottomissione. Schiavi, animali, macchine, intelligenza artificiale*, Il Mulino, 2019

F. Bricola (1978), *Responsabilità penale per il tipo e per il modo di produzione*, in Aa.Vv., "La responsabilità dell'impresa per i danni all'ambiente e ai consumatori", Giuffrè, 1978

B.C. Cheong (2022), *Avatars in the Metaverse: Potential Legal Issues and Remedies*, in "International Cybersecurity Law Review", vol. 3, 2022

G.A. De Francesco (2004), *Programmi di tutela e ruolo dell'intervento penale*, Giappichelli, 2004

T. Delogu (1974), *Lo "strumento" nella teoria generale del reato*, in "Rivista italiana di diritto e procedura penale", 1974

V. S. Delsignore (2023), *La tutela dei minori e la pedopornografia telematica: i reati dell'art. 600-ter c.p.*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), "Trattato di diritto penale – Cybercrime", Utet giuridica, 2023

A. Di Nicola (2022), *Towards digital organised crime and digital sociology of organised crime*, in "Trends in organised crime", 2022

A. Di Nicola (2021), *Criminalità e criminologia nella società digitale*, FrancoAngeli, 2021

European Committee on Crime Problems (1990), *Computer-related crime*, Council of Europe Publishing and Documentation Services, 1990

G. Fiorinelli (2024), *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, 2024

T.E. Frosini (2020), *Il Costituzionalismo nella Società tecnologica*, in Aa.Vv., "Liber amicorum per Pasquale Costanzo", in Consulta Online, 2020

V. Frosini (2000), *L'orizzonte giuridico dell'Internet*, in "Il Diritto dell'informazione e dell'informatica", 2000, n. 2

A. Garapon, J. Lassegue (2021), *La giustizia digitale. Determinismo tecnologico e libertà*, trad. it, Il Mulino, 2021

A. Gargani (2019), *Jus in latenti. Profili di incertezza del diritto penale dell'ambiente*, in "Criminalia. Annuario di scienze penalistiche", 2019

J.L. Goldsmith (1999), *Against Cyberanarchy*, University of Chicago Law Occasional Paper, n. 40, 1999

E. Haber (2024), *The Criminal Metaverse*, in "Indiana Law Journal", 2024, n. 99

W. Hoffmann-Riem (2020), *Digitale Disruption und Transformation. Herausforderungen für Recht und Rechtswissenschaft*, in M. Eifert (Hrsg.), "Digitale Disruption und Recht", Nomos, 2020

A. Iannuzzi (2024), *Metaverso, Ditigal Twins e diritti fondamentali*, in "Rivista italiana di informatica e diritto", 2024

A. Iannuzzi, F. Laviola (2023), *I diritti fondamentali nella transizione digitale tra libertà e uguaglianza*, in "Diritto costituzionale", 2023, n. 1

A. Incampo (2025), *Come del mondo (o del diritto o dell'economia) fin dalla sua origine*, in "Rivista di Filosofia del diritto", 2025, n. 1

R. Johnson, D. Post (1996), *Law and Borders – The Rise of Law in Cyberspace*, in "Stanford Law Review", 1996

I. Leoncini (1999), *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Giappichelli, 1999

E. Longo (2023), *Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, FrancoAngeli, 2023

A.M. Maugeri (2021), *I reati sessualmente connotati e diritto penale del nemico*, Pisa University Press, 2021

A.M. Maugeri (2020), *I reati sessualmente connotati e diritto penale del nemico*, in "Rivista italiana di diritto e procedura penale", 2020

M.R. McGuire (2017), *Technology crime and technology control*, in M.R. McGuire, T.J. Holt (eds.), "The Routledge Handbook of Technology, Crime and Justice", Routledge, 2017

M.R. McGuire (2012), *Technology, Crime and Justice. The question concerning technomia*, Routledge, 2012

M.R. McGuire, S. Dowling (2013), *Cybercrime: a review of the evidence*, Home Office Research report 75, October 2013

OECD (1986), *Computer related crime: analysis of legal policy*, OECD Publishing, 1986

T. Padovani (1996), *Il nuovo volto del diritto penale del lavoro*, in "Rivista trimestrale di diritto penale dell'economia", 1996

N. Pisani (2020), *La nozione di "cosa mobile" agli effetti penali e i file informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, in "Diritto penale e processo", 2020

R. Razzante (2022), *L'attribuzione degli attacchi informatici*, in "European Journal of Pricacy Law and Technologies", 2022

G.M. Riccio (2023), *Metaverso, logiche proprietarie e poteri privati*, in G. Cassano, G. Scorza, "Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT", Pacini Giuridica, 2023

G. Sartor (2017), *Human Rights and Information Technologies*, in R. Brownsword, E. Scotford, K. Yeung (Eds.), "The Oxford Handbook of Law, Regulation and Technology", OUP, 2017

F. Sarzana di Sant'Ippolito, M.G. Pierro, I.O. Epicoco (2022), *Il diritto del metaverso. NFT, DeFi, GameFi e privacy*, Giappichelli, 2022

G. Sciancalepore (2023), *Intelligenza artificiale, metaverso e diritto*, in "Iura & Legal systems", 2023

C.J. Smith (2004), *Research on crime and technology*, in E.U. Savona (ed.) "Crime and Technology", Springer, 2004

L. Stortoni (2004), *Angoscia tecnologica ed esorcismo penale*, in "Rivista italiana di diritto e procedura penale", 2004

U. Troiano (2017/2024), *Intergovernmental Cooperation and Tax Enforcement*, National Bureau of Economic Research Working Paper 2017 (revised December 2024)

D.S. Wall (2004-a), *What are Cybercrimes?*, in "Criminal Justice Matters", vol. 58, 2004, n. 1

D.S. Wall (2004-b), *Digital realism and the governance of spam as cybercrime*, in "European Journal on Criminal Policy and Research", 2004