DIRITTO PENALE DELL'INFORMATICA

Reati della rete e sulla rete

A cura di
Cesare Parodi
Valentina Sellaroli

Giuffrè Francis Lefebvre

ISBN 9788828824701

Stampato da Galli Edizioni S.r.l. - Varese

INDICE

Capitolo II

I REATI PATRIMONIALI

di Cesare Parodi

Capitolo III

I REATI FAMILIARI E RELAZIONALI

di Valentina Sellaroli

Capitolo IV

I REATI INFORMATICI IN AMBITO AZIENDALE

di Costantino De Robbio, Francesco Agnino

Capitolo V

PEDOPORNOGRAFIA E REATI IN AMBITO SESSUALE

di Valentina Sellaroli, Salvatore Lombardo, Lorenzo Ghirardi

Capitolo VI

LA FALSITÀ IN DOCUMENTO INFORMATICO

di Irene Scordamaglia

Capitolo VII

I REATI IN TEMA DI COMUNICAZIONI

di Claudio Orazio Onorati, Maria Sofia Cozza

Capitolo X

LA TUTELA DEL DIRITTO D'AUTORE IN AMBITO INFORMATICO/TELEMATICO

di Simona Lavagnini

Capitolo XI

I DANNEGGIAMENTI INFORMATICI

di Ivan Salvadori

Capitolo XII

INFORMATICA E TUTELA DELLA RISEVATEZZA

di Giuseppe Vaciago, Nicole Monte

Capitolo XIII

DATA RETENTION E GIUSTIZIA PENALE IN ITALIA

di Roberto Flor

Capitolo XIV

CYBERCRIME E DIRITTO PENALE

di Lorenzo Picotti

Capitolo XIV

CYBERCRIME E DIRITTO PENALE

di Lorenzo Picotti

1. RIVOLUZIONE CIBERNETICA E DIRITTO PENALE.

1 — L'impatto della rivoluzione informatica — o meglio, come si dirà, "cibernetica" — in tutti i settori dell'odierna società globalizzata, quale sua "frontiera mobile" avanzata, per le sempre più estese e sofisticate applicazioni, rappresentate oggi dall'intelligenza artificiale e dalla robotica, ha da tempo riguardato tutti gli ordinamenti giuridici ed, in particolare, anche il loro diritto penale, impegnando, oltre alla dottrina ed alla giurisprudenza, anche i legislatori, che per la spinta dei più autorevoli organismi internazionali e per l'urgenza di fronteggiare situazioni di incertezza e lacune normative, sono intervenuti ad "ondate" successive fino a creare un complesso sempre più esteso, ma non altrettanto organico e sistematico, di nuove disposizioni e regole, che si accompagnano a decisioni, prescrizioni, elaborazioni teoriche di grande e crescente importanza.

Oggi non si può più parlare soltanto di un settore speciale del diritto penale e processuale penale, denominato "diritto penale dell'informatica", quale si conosceva fino a pochi anni orsono ed è insegnato in corsi specialistici universitari, perché s'impone ormai una prospettiva più ampia e diversa: occorre riconsiderare l'intero ordinamento penale (oltre che giuridico in genere) alla luce delle nuove tecnologie e del loro impatto sulle forme e modalità dei rapporti sociali ed interpersonali, in ambito pubblico e privato, economico e culturale, nazionale e sopranazionale, dato che le applicazioni capillarmente estese, supportate da dispositivi mobili sempre più efficienti (dagli smartphone ai tablet, ai laptop), incidono sull'organizzazione e sul funzionamento complessivo del sistema economico, sociale, politico.

Ai fini dell'analisi giuridica vanno evidenziati due caratteri fondamentali di questa "rivoluzione cibernetica".

La prima è l'automazione sempre più spinta, che si è sviluppata dal "trattamento dei dati" inteso quale mera elaborazione "meccanica" fondata su calcoli matematici (1) all'impiego di programmi che grazie a processori ed elaboratori sempre più veloci e potenti, consentono l'applicazione e lo sviluppo di algoritmi via via più sofisticati ed evoluti, in grado di auto-apprendere e di correggersi, in funzione delle finalità per cui sono predisposti.

La seconda caratteristica, strettamente correlata, è la connettività, divenuta oggi "iperconnettività", perché grazie alla velocità di accumulo, elaborazione e scambio di dati di ogni genere, garantita dal parallelo sviluppo delle reti e delle strutture di trasmissione, ne è possibile una raccolta e condivisione crescenti, quotidianamente incrementate dagli stessi utenti, fino alla creazione di loro enormi insiemi, denominati big data (2). Se poco tempo fa si sono celebrati i 50 anni dalla prima rete di computer, embrione di Internet, reso accessibile al pubblico solo verso la metà degli anni '90, che ha gettato le basi non solo tecnologiche, ma anche sociali, dell'attuale Cyberspace, a ragione si parla ormai di una pervasiva "Infosfera" quale nuova dimensione in cui siamo tutti permanentemente immersi (3).

Il concetto di Cyberspace associa infatti alla "cibernetica" — che allude alla scienza che studia i modi e meccanismi con cui gli esseri viventi e le macchine comunicano fra loro e con l'ambiente esterno, e lo controllano (4) — l'idea di uno "spazio" davvero globale, che non può affatto definirsi "virtuale" in quanto è ormai una dimensione imprescindibile della realtà sociale, con un ruolo propulsore della complessa dinamicità del mondo contemporaneo.

Il menzionato connotato dell'automazione quale carattere essenziale del concetto stesso di "sistema informatico" e — correlativamente — di "dati informatici" da esso trattabili, è riconosciuto da tempo in basilari definizioni giuridiche di rilievo penale, a partire dall'art. 1, lett. a) e b) della Convenzione Cybercrime del Consiglio d'Europa del 2001 fino all'art. 2, lett. a) e b) della Direttiva 2013/40/UE del Parlamento europeo e del Consiglio relativa agli attacchi contro

(1) Per cui si parlava originariamente di semplici "calcolatori elettronici", come è espresso dal termine inglese "computer", riconducibile alla c.d. macchina di Turing (cfr. A. TURING, On computable numbers, with an application to the Entscheidungsproblem (1936), che propose per primo un modello matematico capace di simulare il processo di calcolo umano, scomponendolo nei suoi passi ultimi, eseguibili così anche da una tecnica meccanica).

(2) Cfr. nella letteratura italiana G. DELLA MORTE., Big Data e protezione internazionale dei diritti umani. Regole e conflitti, Napoli, 2018.

(3) Per importanti sviluppi teorici si veda in specie L. FLORIDI, La quarta rivoluzione. Come l'infosfera sta trasformando il mondo (Oxford 2014), tr. it., Milano 2017.

(4) Il termine deriva dal greco kyber, che significa timoniere o pilota, ed è stato scelto agli inizi del secolo scorso da Norbert Wiener per indicare quella nuova scienza, che intende studiare i meccanismi con cui uomini, animali e macchine comunicano con l'ambiente esterno e lo controllano: N. WIENER, Cybernetics: Or Control and Communication in the Animal and the Machine (1. ed. 1948), 2. ed. Parigi, 1961.

i sistemi di informazione, che ha sostituito (peraltro senza modifiche sul punto) la decisione quadro del Consiglio 2005/222/GAI.

Il novum espresso dall'informatica, specie grazie al suo sviluppo nella cibernetica, penetra infatti alla radice dell'agire dell'uomo, assumendone sia le capacità cognitive, vale a dire di conoscere ed apprendere dall'esperienza del mondo "esterno", ricercando ed acquisendo informazioni e dati da elaborare e memorizzare, come si verifica nei c.d. sistemi esperti (5); sia le ancor più rilevanti e strettamente connesse capacità di auto-determinarsi di conseguenza, per giungere a "decisioni" e scelte operative che possono poi essere immediatamente attuate, fra possibili opzioni alternative (6).

Oggi può parlarsi di un equivalente della "volontà" umana espressa dai computer o, meglio, dai sistemi c.d. intelligenti (7), che trova paradigmatici riconoscimenti giuridici, di rilievo anche penale, concernenti ad es. la validità di atti, negozi, documenti, compresi i contratti, posti in essere e conclusi automaticamente (si pensi alle negoziazioni di borsa, in ambito privatistico, od ai provvedimenti amministrativi ed in taluni ordinamenti perfino giudiziari, in ambito pubblicistico), che le persone (fisiche o giuridiche), cui si imputano, non avrebbero potuto porre in essere negli stessi tempi, modi e contenuti (8).

(5) Altrettanto vale per tutto l'espansivo campo dell'"Internet delle cose" (Internet of Things) da cui siamo sempre più circondati: gli "oggetti" si connettono automaticamente in rete e comunicano tra loro o tramite ditte ed aziende competenti, che operano con adeguati algoritmi anche a nostra insaputa, per compiere in tempo reale le operazioni necessarie.

(6) La disponibilità ed accessibilità in tempi immediati delle informazioni acquisibili, in rete e dal mondo esterno, è presupposto essenziale di tale capacità d'azione. Esemplificando: una self driving car (ma lo stesso vale per un robot che operi in ambito medico o nell'esplorazione di ambienti sconosciuti) sarà tanto più affidabile, quante più informazioni potrà autonomamente e velocemente raccogliere dall'ambiente esterno, con sensori ottici, acustici, termici, ecc., ed attraverso connessioni a terminali e sistemi d'informazione presenti sulla rete stradale (cd. smart road).

(7) Si parla di "intelligenza artificiale" in molte accezioni, a partire dalle applicazioni dei motori di ricerca — capaci di indicizzare e personalizzare, sulla base di frequenze, preferenze e correlazioni acquisite dalle ricerche e dai dati lasciati dagli utenti stessi e dai dispositivi utilizzati (come i cookies di vario genere) le informazioni più utili da offrire, comprese le pubblicità più incisive in termini individualizzanti, od i gruppi sociali aventi interessi simili cui aderire, ecc. — fino a quelle più sofisticate applicate alla robotica, alla domotica, alla guida di veicoli. Nella Comunicazione della Commissione al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni del 7.12.2018 COM(2018) 795 final, recante il "Piano coordinato sull'intelligenza artificiale", si legge questa definizione: "Per "intelligenza artificiale" (IA) si intendono quei sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici". Più articolate definizioni sono state espresse *dall'High-Level Expert Group on Artificial Intellligence* istituito dalla Commission Europea e dall'*Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence* costituito presso il Consiglio d'Europa. Per riferimenti aggiornati sui relativi studi e documenti si veda il topic "Intelligenza Artificiale" al sito dell'"Osservatorio Cybercrime" (https://sites.les.univr.it/cybercrime/index.php/ia/).

(8) L'ordinamento giuridico, a livello europeo, limita, ma nel contempo riconosce, in ipotesi sempre più estese, l'efficacia giuridica di decisioni interamente automatizzate, che coinvolgano diritti ed interessi delle persone: cfr. già l'art. 15 Direttiva europea 95/46 ed ora l'art. 22 par. 1 Regolamento 2016/679 (GDPR) del 27.4.2016 relativo alla protezione e circolazione dei dati personali, secondo cui: "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Ma nel par. 2 è elencata una serie assai ampia di eccezioni e

È dunque in via di superamento l'idea che i sistemi cibernetici siano meri "strumenti" di cui dispongono i soggetti umani, data la loro sempre più evidente natura di agenti autonomi (si pensi ai robot, nelle loro più diverse applicazioni, alle self driving car, nell'ambito dei trasporti, ecc.) che sollevano nuovi problemi d'imputazione della responsabilità, non solo penale, nelle ipotesi non rare in cui determinino danni "ingiusti" o comunque la lesione di beni giuridici individuali o collettivi, se non anche diritti fondamentali di terzi, a partire dalla vita e integrità personale, fino alla libertà di opinione, di autodeterminazione, di disposizione patrimoniale.

In questo scenario, anche la nostra privacy viene sacrificata, fino a ridursi ad un mito lontano, dovendo abbandonarsi la pretesa di "escludere terzi" o comunque di controllare effettivamente il trattamento delle proprie informazioni personali, per la necessità di bilanciamento con altri interessi e beni in gioco, in cui prevale l'esigenza di massima o miglior funzionalità possibile dei molteplici sistemi ed interventi automatizzati, a partire dal campo della sicurezza delle reti e della società che ne dipende, fino alla sanità, all'amministrazione, alla produzione, al commercio.

2. DAI COMPUTER CRIME AI CYBERCRIME: LA CRIMINALITÀ NEL CYBERSPACE.

Passando all'esame delle ricadute nel campo del diritto penale, lo sviluppo dell'informatica e della cibernetica ha segnato, a partire dalla menzionata svolta epocale dell'apertura di Internet al pubblico, il passaggio dalla categoria concettuale dei Computer crime (reati informatici strettamente intesi) a quella — non solo criminologica, ma anche giuridico-penale — dei Cybercrime (reati cibernetici) ([9]).

Ai primi si riferiva emblematicamente il Consiglio d'Europa con la Raccomandazione del 1989 sulla "criminalità informatica", o da computer, in cui era prevista una limitata elencazione di reati, dei quali era suggerita l'introduzione da parte dei legislatori nazionali ([10]).

---

condizioni, che sono ancor meno stringenti nella corrispondente previsione dell'art. 11 Direttiva UE 680/2016 del 27.04.2016 sul trattamento di dati per fini di indagini ed accertamento di reati.

([9]) L. PICOTTI, Presentazione, in: ID. (cur.), Il diritto penale dell'informatica nell'epoca di Internet, Padova 2004, p. VII.

([10]) Cfr. CONSEIL DE L'EUROPE, Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur, Strasburgo 1990, contenente una "lista minima" di otto incriminazioni ed una "lista facoltativa" di ulteriori quattro reati.

Ma per l'accelerato sviluppo determinato da Internet, lo stesso Consiglio d'Europa, dopo intensi lavori preparatori, ha varato pochi anni dopo la fondamentale Convenzione Cybercrime del 2001, già sopra citata, in cui è previsto un ben più articolato e soprattutto vincolante (per gli Stati parte) insieme sistematico di disposizioni, riguardanti sia il diritto penale sostanziale, sia quello processuale, sia la cooperazione internazionale, di cui è nel frattempo emersa l'assoluta necessità.

Limitandoci qui a richiamare i contenuti più significativi della parte di diritto penale sostanziale, va segnalato che i reati oggetto degli obblighi di incriminazione da parte degli ordinamenti nazionali sono andati oltre la basilare triade di beni giuridici costituita dalla "confidenzialità, integrità, disponibilità di dati e sistemi" (Confidentiality, Integrity, Avalaibility: c.d. CIA) di cui agli artt. da 2 a 6, nei quali al primo posto figura l'accesso abusivo, quindi l'intercettazione illegale ed, a seguire, l'alterazione di dati, l'alterazione di sistemi ed il nuovo reato preparatorio dell'abuso di dispositivi. Infatti, oltre ai due classici reati informatici del falso informatico (art. 7) e della frode informatica (art. 8), è prevista anche l'incriminazione di delitti che riguardano "contenuti" non necessariamente veicolati da dati o sistemi informatici, quali i delitti di pedopornografia (art. 9) e le violazioni gravi dei diritti d'autore e dei diritti connessi (art. 10).

Dunque, accanto a reati che si possono definire reati informatici in senso stretto, perché includono, fra i loro elementi costitutivi essenziali, la tipizzazione espressa di elementi tecnico-informatici (quali: "sistema informatico", "dato informatico", "trasmissione di dati informatici", "programma informatico", ecc.), senza cui non sarebbero neppure concepibili, è emersa un'altra categoria di reati — che si può considerare "aperta" — definibili informatici in senso ampio o, meglio, cibernetici, perché pur non presentando necessariamente le sopraddette caratteristiche tecnico-informatiche fra gli elementi costitutivi della fattispecie legale, meritano un particolare rilievo giuridico e processuale, anche sul piano della cooperazione internazionale, data la necessità di contrastarli con adeguate sanzioni penali e con specifici strumenti di indagine e di raccolta, nonché "circolazione" delle prove, se commessi in rete, non diversamente da quanto richiesto per contrastare e perseguire i reati informatici in senso stretto. La stessa Convenzione Cybercrime, nel delineare all'art. 14, in specie par. 2, il campo di applicazione della sua Sezione II, che riguarda le misure di diritto processuale, include alla lettera b) qualsiasi reato commesso tramite sistemi informatici — oltre a quelli previsti dalla Convenzione stessa, richiamati alla lettera a) —

mentre alla lettera c) include anche qualsiasi altro reato che lasci "tracce elettroniche", come poi sostanzialmente ripete nell'art. 23 che apre il Capitolo III, riguardante le misure relative agli obblighi di cooperazione internazionale.

Con l'evolversi e l'espandersi del Cyberspace, la categoria dei reati cibernetici (Cybercrime) ha dunque assunto un'importanza ed un'estensione via via maggiori, perché può abbracciare qualsiasi reato che possa commettersi nel Cyberspace. In essa ricadono quindi tutti quelli consistenti nella "comunicazione" e soprattutto "diffusione" (11) di contenuti penalmente illeciti in rete, come i delitti di diffamazione *on line* (12) o di pornografia minorile (13) che presentano un'estrema facilità di realizzazione e un effetto lesivo incommensurabilmente maggiore di quello che si avrebbe in caso di commissione con i tradizionali mezzi di comunicazione (quali la posta, la stampa, la radio, la televisione, le fotografie od i filmati su supporti fisici) (14).

Ma si manifestano oggi anche molte altre tipologie di reati, che offendono i più svariati beni giuridici e divengono ben più temibili, richiedendo adeguate risposte anche a livello normativo, oltre che investigativo, se commessi nel Cyberspace. Si pensi ai delitti via via introdotti per combattere il terrorismo che si manifesta (anche) nella rete, utilizzata sia come luogo di propaganda e proselitismo, sia come mezzo di "arruolamento", "addestramento", organizzazione anche di altre attività preparatorie, quali i viaggi all'estero in territori prescelti per attività terroristiche, nonché per il finanziamento anche tramite raccolte on line (15).

E si considerino le nuove fattispecie o le nuove circostanze aggravanti, via via introdotte negli ordinamenti giuridici, per colpire più severamente fenome-

(11) Sul punto sia consentito rinviare a L.PICOTTI, Profili penali delle comunicazioni illecite via Internet, in Il diritto dell'informazione e dell'informatica, 1999, Nr. 2, p. 283 s.

(12) In tal senso già L. PICOTTI, Profili penali, cit., p. 303 e per la successiva dottrina e giurisprudenza italiane v. F.P. LASALVIA, La diffamazione via web nell'epoca dei social network, in A. CADOPPI, S. CANESTRARI, A. MANNA e M. PAPA (cur.), Cybercrime, Milano 2019, p. 331 s..

(13) In argomento sia consentito rinviare a L. PICOTTI, I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l'offesa dei beni giuridici, in Scritti per Federico Stella, Napoli 2007, vol. II, p. 1267 s.; e da ultimo Id., 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. cfr. altresì S. DELSIGNORE., La tutela dei minori e la pedopornografia telematica: i reati dell'art. 600-ter c.p., in A. CADOPPI, S. CANESTRARI, A. MANNA e M. PAPA (cur.), Cybercrime, cit., p. 374 s.

(14) Altri significativi interventi di penalizzazione di reati cibernetici (in senso ampio) hanno riguardato la propaganda ed istigazione ad atti di odio e discriminazione razziale, oggetto in specie del Protocollo addizionale alla Convenzione Cybercrime adottato dal Consiglio d'Europa il 28 gennaio 2003 per contrastare il razzismo e la xenofobia in rete.

(15) Cfr. per un quadro di sintesi L. PICOTTI, Terrorismo e sistema penale: realtà, prospettive, limiti, in Riv. trim. Dir. Pen. Contemporaneo, 2017, p. 249 s.

ni, che pur si possono manifestare anche off line, quale il cyberstalking, il cyberbullismo, il revenge porn, fino alla cyberviolenza contro le donne, che la Corte europea dei diritti dell'uomo ha recentemente ricondotto alla categoria della "violenza domestica", per combattere la quale è previsto uno specifico "obbligo positivo di tutela" in capo agli Stati aderenti alla Convenzione di Istanbul (16).

Di fronte a questa nuova realtà, deve dunque cambiare di passo l'approccio alla criminalità informatica, perché ormai viene in rilievo tutta la criminalità che si realizza "nel" Cyberspace, non circoscrivibile ad un numero chiuso o limitato di reati e, quindi, di vittime potenziali, perché abbraccia una crescente molteplicità di illeciti e di modalità di offesa di interessi giuridici e di diritti anche fondamentali, che a loro volta si configurano come nuovi, quando siano frutto essi stessi del predetto sviluppo tecnologico.

Esemplificando: può costituire un crimine cibernetico (in senso ampio), se ed in quanto realizzata nel Cyberspace, l'estorsione (art. 629 c.p.) commessa con la criptazione illecita dei dati di un sistema informatico altrui, tramite un malware abusivamente installatovi da remoto (ransomware), con cui l'agente pone in essere una forma di minaccia o violenza (17) mediante l'intrusione informatica, in conseguenza della quale la vittima è costretta, per riacquistare la libera disponibilità dei propri dati, a corrispondere un prezzo ingiusto di riscatto (spesso esigito in bitcoin od altra valuta virtuale da corrispondere o trasferire nel c.d. dark web), non potendo altrimenti ottenere l'indispensabile chiave di decriptazione.

Un altro esempio di delitto comune, che presenta caratteri "nuovi" — anche di pericolosità e difficoltà di prevenzione e repressione — se commesso in rete, è il riciclaggio (art. 648-bis c.p.), che può essere realizzato con trasferimenti elettronici di fondi, investimenti od "altre operazioni" anche via web (o nel dark web), ad esempio movimentando e scambiando valute virtuali come bitcoin od ethereum, basate su sistemi di blockchain, mediante operazioni coperte dall'anonimato, idonee a sostituire il denaro o valori anche immateriali e così "ostacolando l'identificazione" della loro provenienza delittuosa (c.d. Cyberlaundering) (18).

(16) Cfr. Corte EDU, Sez. IV, 11 febbraio 2020, Ric. N. 56867/15, Buturuga v. Romania.

(17) È "violenza sulle cose" (ai sensi del comma 3 dell'art. 392 c.p. aggiunto dalla legge 23 dicembre 1993, n. 547) quella realizzata "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" (volendo, in argomento, cfr. L. PICOTTI, voce Reati informatici, in Enc. Giur. Treccani, vol. aggiorn. VIII, Roma 2000, p. 16 s.

(18) Il fenomeno è oggetto anche della Direttiva UE 2018/1673 del 23.10.2018, relativa alla lotta al riciclaggio mediante il sistema penale; in argomento cfr. R. M. VADALÀ, *La disciplina penale degli usi ed abusi delle valute virtuali*, in

Ma anche tutti i traffici illeciti — di droga, di armi, persino di persone ed organi, ecc. — come pure le più sofisticate frodi realizzate ad es. attraverso le tecniche di phishing, possono essere commessi nel Cyberspace, utilizzando altresì sistemi di intelligenza artificiale, che rendono più rapide, sicure, protette le azioni delittuose, scegliendo ed eseguendo quelle più utili o nei momenti più opportuni o nei confronti delle vittime più vulnerabili ([19]).

3. IL WEB INTERATTIVO ED IL DOPPIO RUOLO DEGLI UTENTI AUTORI E VITTIME DI REATI CIBERNETICI: NUOVI BENI GIURIDICI E DIRITTI FONDAMENTALI DA PROTEGGERE PENALMENTE.

Il superamento dell'originaria architettura "unidirezionale" del web, in cui il comune utente era il destinatario passivo di informazioni e comunicazioni, alle quali poteva accedere e che poteva leggere od acquisire, ma la cui produzione, circolazione e diffusione dipendeva da una cerchia relativamente ristretta di soggetti (c.d. content provider e, più in generale, i gestori dei servizi in rete od Internet Service Provider e webmaster) è emerso a partire dall'inizio degli anni 2000, quando si è sviluppato il c.d. web 2.0, caratterizzato dalla progressiva possibilità di interazione attiva fra gli utenti, posti in grado di creare e condividere propri contenuti in blogs, forum, social network, cui è seguita una dirompente estensione dell'uso di dispositivi mobili e terminali di qualsiasi tipo, resa possibile dall'ulteriore sviluppo delle capacità di memoria e di connessione, nonché della grafica, che permette l'utilizzabilità e lo scambio, in ogni luogo e momento, di contenuti multimediali disparati e complessi (quali audio, video, immagini, anche a tre dimensioni) immediatamente "prodotti" e messi in rete dagli stessi utenti che possono altresì connettersi in chat, streaming, videoconferenze in tempo reale (c.d. web 3.0). Oggi si parla addirittura di un web 4.0, dominato dall'intelligenza artificiale, in cui gli utenti sono non solo i sistematici creatori e diffusori di informazioni, contenuti, dati, ma anche la fonte inesauribile di quelli che vengono sistematicamente estrapolati (a loro insaputa o meno, con il loro consenso informato o meno) da tutte le loro attività, navigazioni,

Diritto di Internet, 2020, Nr. 3, p. 397 s. e più in generale L. PICOTTI, Profili penali del cyberlaundering: le nuove tecniche di riciclaggio, in Riv.trim.dir.pen.ec., 2018, Nr. 3-4, p. 590 s.

([19]) Significativa di tale evoluzione è anche la recente Direttiva (Ue) 2019/713 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. In argomento si veda R. M. VADALÀ, *La direttiva UE 2019/713 del 17 aprile 2019 e la tutela penale dell'uso legittimo dellevalute virtuali*, in "Osservatorio Cybercrime" (https://sites.les.univr.it/cybercrime/index.php/news-oc-2/)

utilizzazioni, grazie a configurazioni appositamente finalizzate degli spazi, dei servizi, delle app nel Cyberspace. Questo si trasforma così in un'enorme banca di dati, informazioni, materiali, nel quale è possibile la sistematica "profilazione" di chiunque vi operi, individuandone le preferenze, gli orientamenti anche culturali, ideologici, politici oltre che di consumo e di spesa, con correlato impressionante sviluppo di attività pubblicitarie, commerciali, imprenditoriali, produttive ed economiche, e financo di propaganda e condizionamento politico.

L'utente diviene dunque potenziale vittima e bersaglio, ma nel contempo è anche possibile autore di prevaricazioni ed offese di diritti ed interessi altrui, meritevoli di protezione penale ([20]), in parallelo con quanto si verifica nella vita reale, seppur con modalità e condizioni totalmente nuove, che determinano effetti qualitativamente molto più penetranti e lesivi ([21]).

Basti l'esempio dei minori, che accedono al ed utilizzano il web come parte integrante, talora patologicamente condizionante, della loro vita quotidiana di "nativi digitali": per cui — accanto allo straordinario potenziamento delle abilità e capacità di accesso e gestione delle informazioni, nonché di sviluppo dei rapporti sociali — emergono fenomeni molto allarmanti di sexting, cyberbullismo, revenge porn, prevaricazioni violente, con tutte le varianti di sfide anche mortali (Blue wahle ne è un esempio tragico), che possono pregiudicarne irreparabilmente lo sviluppo personale e l'inserimento proficuo nella vita reale ([22]).

L'espansione pervasiva del Cyberspace fa emergere allora una corrispondente e pressante esigenza di adeguamento della tutela penale, rispetto a beni giuridici identici (come nel caso dell'onore e della reputazione, o del patrimonio) ovvero caratterizzati da forti analogie (come nel caso dell'integrità dei dati e dei sistemi) o comunque da rango non inferiore (come nel caso della riservatezza informatica e della privacy) di quelli già protetti dal diritto penale rispetto ad analoghe offese commesse off line. Anzi: i nuovi connotati dei beni giuridici che possono essere offesi nel Cyberspace conferiscono loro un'importanza maggiore, e financo fondamentale, come nel caso della "riservatezza informatica" e della "sicurezza informatica".

([20]) Cfr. L. PICOTTI, I diritti fondamentali nell'uso ed abuso dei Social Network. Aspetti penali, in Giur. merito, 2012, Nr. 12, p. 2522 s..

([21]) Applicando la definizione della Direttiva UE 2012/29 del 25.10.2012, in materia di protezione delle vittime di reato, poiché quello cibernetico è strutturalmente un reato transnazionale, le sue vittime (oltre a quelle specificamente protette, come i minori od i soggetti esposti a discriminazioni), possono spesso considerarsi "vulnerabili", in quanto persone "non aventi cittadinanza" negli Stati membri in cui esso è commesso.

([22]) Cfr. i dati forniti dai principali organismi internazionali e nazionali che si occupano della tutela dei minori in rete: riferimenti in SALVADORI I., Sexting, minori e diritto penale, in A. CADOPPI, S. CANESTRARI, A. MANNA e M. PAPA (cur.), Cybercrime, cit., p. 567 s.

La prima assurge alla nuova dimensione di diritto fondamentale della persona ad uno spazio informatico esclusivo, a prescindere dai contenuti che vi siano presenti o trattati, che deve essere lasciato come tale libero da intrusioni e manomissioni di terzi, in quanto strumento essenziale per l'odierna vita individuale e sociale, che neppure l'autorità pubblica può violare o comprimere, se non nei casi e modi previsti tassativamente dalla legge e con le garanzie del controllo giudiziario ([23]).

Ed essa ha un'autonoma portata rispetto al distinto e parimenti fondamentale diritto alla tutela dei propri "dati personali", ovunque siano localizzati o trattati, anche a prescindere dalla tecnologia informatica, essendo ormai superata l'originaria concezione della privacy quale mera barriera protettiva della vita privata (il diritto ad essere "lasciati soli") da intrusioni ingiustificate dei nuovi mass media, all'epoca rappresentati dalla stampa ([24]).

Oggi, nella dimensione pervasiva del Cyberspace, questo nuovo diritto fondamentale, che ha avuto specifico riconoscimento fin dalla Convenzione del Consiglio d'Europa n. 108 del 1981 "sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale", ha trovato nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea una peculiare configurazione, che nel riconoscerlo lo bilancia con la concomitante esigenza della loro "circolazione" e, dunque, possibile disponibilità anche in capo a terzi, in quanto sia condizione per la prestazione di servizi ed attività, a favore dell'interessato stesso e non solo (si pensi alle prestazioni sanitarie ed assistenziali, all'adempimento di ogni genere di obbligazioni contrattuali, fino alla personalizzazione della pubblicità o di altri servizi, che si fondano sulla c.d. "profilazione" dell'utente) ([25]).

Strettamente collegata a questi "nuovi" beni giuridici è anche la sicurezza informatica, meglio denominata oggi cibernetica (c.d. Cybersecurity), che non è più soltanto un onere dell'interessato, strumentale ad ottenere protezione —

([23]) Diritto ricondotto dalla giurisprudenza della CEDU all'art. 8 della Convenzione e dalla Corte di Giustizia dell'Unione europea all'ambito dell'art. 7 della Carta dei diritti fondamentali dell'Unione, mentre la Corte costituzionale tedesca, con la fondamentale sentenza sulle c.d. perquisizioni in rete (online-Durchsuchung), ne ha delineato il contenuto ed i limiti (Bundesverfassungsgericht, 27.02.2008, 379/2007-595/2007, su cui si veda il commento di R. FLOR., Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online-Durchsuchung, in Riv. trim. dir. pen. ec., 2009, p. 695 s.).

([24]) Così lo storico contributo di S. WARREN, L.D. BRANDEIS, The Right to Privacy, in Harvard Law Review, 1890, Nr. 5, 193 s..

([25]) Per il riconoscimento della nascita di tale "nuovo" diritto, come diritto al controllo sui propri dati e la loro circolazione, cfr. nella dottrina italiana i fondamentali contributi di S. RODOTÀ, a partire dalla storica monografia Elaboratori elettronici e controllo sociale, Bologna 1973, fino all'ultima Il mondo nella rete. Quali diritti quali vincoli, Roma-Bari, 2014.

anche giuridico-penale — dei "propri" diritti ed interessi, e dunque "disponibile" (come emerge dalla condizione prevista per l'incriminazione dell'accesso abusivo ad un sistema informatico dall'art. 3 Direttiva UE 2013/40, oltre che dall'art. 615-ter c.p. italiano). La sicurezza è diventata anche oggetto di obblighi, la cui violazione può essere sanzionata penalmente in molti ambiti, come era ad esempio stabilito dall'art. 169 Codice privacy italiano nella formulazione del 2003, nei confronti dei titolari di trattamenti di dati personali che non rispettassero le "misure minime" di sicurezza stabilite ed aggiornate con appositi decreti ministeriali ([26]). Oggi — nella nuova prospettiva dinamica del Regolamento UE 2016/679, c.d. GDPR — sono stabiliti diversi e più penetranti obblighi di valutazione e prevenzione dei rischi, nonché di risposta adeguata agli eventi avversi, facenti capo non solo ai titolari dei trattamenti, ma anche ai responsabili della privacy, ai programmatori, installatori ecc. fin dalla fase della progettazione e configurazione dei sistemi (by disegn).

Ma per la stretta e globale interdipendenza, che hanno ormai tutti i servizi e le attività nel Cyberspace, le più recenti disposizioni nazionali ed europee dimostrano che la "sicurezza delle reti e dei sistemi informatici" assurge addirittura ad una generale dimensione pubblica, di garanzia "preventiva" per i servizi, le funzioni, i rapporti che vi si svolgono e gli stessi interessi e diritti che vi si esercitano, divenendo rispetto ad essi un bene indisponibile di interesse collettivo, la cui concreta gestione è stabilita e controllata dalle autorità governative, dotate di speciali poteri al riguardo ([27]).

4. OSSERVAZIONI CONCLUSIVE: NECESSITÀ DI ADEGUAMENTO DELLE CATEGORIE DEL DIRITTO PENALE E DI POTENZIAMENTO DELLE POSIZIONI DI GARANZIA NEL CYBERSPACE.

La complessa realtà, in perenne evoluzione ed espansione del Cyberspace, stimola ed anzi impone il costante adeguamento del diritto penale, che deve mantenere la propria funzione regolatrice e di tutela, attraverso l'interpretazione evolutiva, l'applicazione analogica, peraltro vietata in malam partem, quindi

([26]) Sul tema volendo L. PICOTTI, Sicurezza, informatica e diritto penale, in M. DONINI, M. PAVARINI (cur.), Sicurezza e diritto penale, Bologna 2011, p. 217 s..

([27]) In argomento, cfr. la Direttiva 2016/1148/UE ed il Regolamento 2019/881/UE; per un commento sulla recente normativa italiana introdotta dal D.L.21 settembre 2019, n. 105, conv. dalla L. 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di "perimetro di sicurezza nazionale cibernetica", cfr. L. PICOTTI, Cybersecurity: quid novi? in Diritto di Internet, 2020, Nr. 1, p.11 s.

soprattutto la modifica o creazione legislativa di nuove norme, in ogni caso l'elaborazione di appropriate categorie concettuali e dogmatiche.

Come ogni realtà strutturale che condiziona la sovrastruttura, la rivoluzione cibernetica sembra in effetti riconfigurare il rapporto stesso fra tecnologia e diritto, di cui tocca le condizioni operative e persino le funzioni, ponendosi in concorrenza con quella primaria di norma regolatrice: il "codice tecnico" — universale per sua natura — si presenta con la pretesa di essere anche il nuovo codice giuridico del mondo globalizzato ("Code is Law", per citare il famoso libro di Lawrence Lessig) ([28]). In effetti l'autotutela tecnologica e l'autoregolazione che si danno soprattutto i grandi signori del web (Facebook, Google, Amazon, ecc.), tende a divenire "diritto", se non a sostituirlo, perché in grado di munire in tempo reale di efficaci sanzioni i "precetti" che crea, compresa la drastica esclusione da servizi o dall'accesso alla rete, così condizionando i comportamenti di utenti, concorrenti, terzi, fino a limitare l'esercizio di diritti anche fondamentali.

Non solo è però palese l'infondatezza dell'utopistica o romantica idea di una "rete" quale spazio libero dal diritto ([29]), ipotetico porto franco di anarchia o totale libertà non limitabile dai poteri degli Stati ancorati alla materialità dei loro territori e dei loro confini geografici, entro cui soltanto potrebbero esercitare la sovranità: proprio l'analisi svolta dimostra la permanente necessità di un'efficace protezione giuridica, anche mediante sanzioni, investigazioni, processi penali, degli interessi e beni giuridici, spesso primari, compresi i diritti fondamentali delle persone, che vengono offesi con sempre nuove forme e modalità nel Cyberspace ([30]).

Il criterio basilare deve essere che quanto è illecito off line non può essere lecito on line, anche se si presenta in nuove ed inimmaginate modalità e forme.

Di qui la necessità di sviluppare un quadro sistematico generale, in cui collocare rinnovati criteri e regole d'imputazione della responsabilità, che tenga conto delle peculiari caratteristiche dei comportamenti e dei "fatti" penalmente rilevanti, che si commettono o manifestano nel Cyberspace.

([28]) L. LESSIG, Code and Other Laws of Cyberspace (1. ed. 1999), 2. ed., New York 2006.

([29]) Nella letteratura italiana basti il rinvio a G. ZICCARDI., Hacker — Il richiamo della libertà, Milano 2011, con ampi richiami anche all'esperienza americana.

([30]) Tanto che è stato autorevolmente promosso, elaborato e condiviso il progetto di un Internet Bill of Rights, di una "Costituzione per Internet" al fine di riconoscere e garantire, su scala globale, i diritti fondamentali nel Cyberspace, nei confronti di chiunque, partendo da quelli contenuti nelle Carte e Convenzioni internazionali. Cfr. — a partire dalla "Internet Magna Carta" di Tim Berners Lee — in Italia la "Dichiarazione dei diritti in Internet" elaborata da una Commissione parlamentare presieduta da Stefano Rodotà e reperibile al sito https://www.ca mera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_in ternet_pubblicata.pdf.

Se la parte essenziale dell'azione costitutiva del reato è ormai dominata dalla tecnologia informatica e dunque dall'automazione, questa incide anche sulla categoria della causalità, quale nesso di imputazione di un evento che non può essere più visto quale sua mera "conseguenza" naturalistica, anche quando può prodursi all'esterno della rete, come nel caso di morte, lesioni, danni fisici o patrimoniali, cagionati da robot, da self driving car, da azioni di cyberterrorismo o da una cyberextorsion. L'evento stesso, consumativo del reato, oltre a poter essere anche di natura psichica od immateriale (come quello cagionato dal cyberbullismo o dal cyberstalking), può presentarsi altresì di natura esclusivamente tecnologica, come nel caso di interferenze e danneggiamenti informatici, pur solo funzionali, che riguardino sistemi, programmi o dati. Il momento consumativo può quindi essere anche completamente "interno" al Cyberspace, ed il concetto basilare di fatto tipico non può dunque prescindere da una "porzione" sempre più rilevante realizzata in rete tramite o addirittura dai sistemi informatici, o da agenti autonomi, in esecuzione di programmi basati su algoritmi, che possono essere anche molto sofisticati e complessi, perfino capaci di autoapprendere ed evolversi di conseguenza, pur se in origine concepiti, attivati o controllati da soggetti umani che ne siano produttori, manutentori, titolari, fruitori, ecc. A questi ultimi non è dunque sempre agevole imputare giuridicamente la commissione delle conseguenze od effetti ed ancor meno la corrispondente volontà consapevole, richiesta per integrare il dolo del fatto, e, comunque, la rimproverabilità soggettiva, necessaria alla "colpevolezza *per* il fatto".

Inoltre, il "reato cibernetico" può presentare una sorta di perpetuazione dei suoi effetti, che non sembrano riconducibili alla nozione di un post factum non punibile, perché il prolungamento dell'azione e/o dell'evento tipici non è separabile dagli elementi "tecnici" che li costituiscono, quale parte essenziale tramite cui l'autore li realizza.

Per un corretto inquadramento penalistico, un'importante indicazione metodologica potrebbe provenire dalla distinzione dogmatica fra momento di "perfezione formale" del reato, che si ha quando ne sono realizzati gli elementi costitutivi essenziali nel loro contenuto minimo, e momento di "esaurimento" (o consumazione sostanziale), che si ha quando esso ha definitivamente "esaurito" il proprio specifico contenuto e potenziale di offesa, avendo raggiunto il massimo grado di lesione del bene giuridico protetto ([31]).

([31]) Tale distinzione, accolta nella teoria generale del reato già da F. CARRARA, Momento consumativo del furto, in Lineamenti di pratica legislativa penale, Torino 1874, 229 s., è recepita nella manualistica italiana e straniera: cfr. F. MANTOVANI, Diritto penale — Parte generale, 10 ed., Padova 2017, 425 s.; H. JESCHECK, T. WEIGEND T., Lehrbuch

Fenomeno non riconducibile al paradigma del reato permanente propriamente inteso (come è ad es. un sequestro di persona), che presuppone la costante dipendenza della protrazione dell'offesa al bene giuridico (nell'esempio: la libertà personale della vittima) dalla diretta e contemporanea condotta volontaria del reo, il quale potrebbe in ogni momento farla cessare ([32]).

L'automazione e iperconnettività che determinano la specifica diffusione e permanenza dell'offesa nel Cyberspace escludono un diretto e costante controllo del reo, che pur vi abbia fatto ricorso.

Si pensi alla semplice diffamazione *on line*, che dopo la sua consumazione formale, da individuare nel momento della prima "comunicazione" a più persone (anche mediante messa a disposizione in un sito o in un social network) del contenuto lesivo della reputazione altrui, determina una protrazione ed anzi aggravamento ed estensione dell'offesa nel tempo e nello spazio, non più dominabili dall'agente, ma certo prevedibili e accettati fin dal momento della condotta. E lo stesso vale per la diffusione di pornografia minorile, per il reato di revenge porn, per la diffusione di discorsi d'odio nel Cyberspace, ecc.

Sembra allora emergere una peculiare accezione di evento, diversa dalla tradizionale nozione naturalistica, di cui ha caratteristiche equivalenti sul piano dei contenuti lesivi per la vittima e per gli interessi o diritti protetti, ma i cui requisiti e limiti di imputazione oggettiva, nonché di rimproverabilità soggettiva all'autore (a titolo di dolo o di colpa), vanno determinati alla luce delle tecnologie attivate e del sottostante rapporto conflittuale con i portatori degli interessi o diritti offesi, instauratosi e perdurante nel Cyberspace.

Ne derivano importanti conseguenze, per determinare la legge penale applicabile nel tempo e nello spazio, e la configurabilità, fino all'avvenuto "esaurimento", della partecipazione penalmente rilevante ex art. 110 c.p., in forma sia attiva sia omissiva (ad es. di utenti di social network che approvino e facciano a loro volta circolare il messaggio o contenuto lesivo, oltre che degli Internet Service Provider, che non adempiano ad obblighi di blocco o rimozione) ([33]).

In ogni caso, la complessità della rete rende necessario stabilire e regolare

---

des Strafrechts — Allgemeiner Teil, 5. ed., Berlino 1996, § 49, III, 517. Volendo, con riferimento ai reati a dolo specifico, L. PICOTTI, Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali, Milano, 1993, 565 s., 568.

([32]) Sulle caratteristiche del reato permanente cfr. per tutti, nella dottrina italiana, M. ROMANO, Commentario sistematico del codice penale, 3 ed., Milano 2004, Pre-Art. 39, §§ 118 s., 344 s.; sul postfactum si rinvia alla monografia di S. PROSDOCIMI, Profili penali del postfatto, Milano, 1982.

([33]) In tal senso Cass., 27.12.2016, n. 54946, T., che ha confermato la condanna penale per concorso in diffamazione di un blogger, che aveva "mantenuto" un testo con espressioni offensive sul proprio sito, nonostante ne fosse stato reso edotto. Per un'aggiornata analisi in materia cfr. B. PANATTONI, I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace, in www.sistemapenale.it, 22.5.2020.

normativamente molteplici "posizioni di garanzia" in capo ai diversi soggetti (enti, imprese, amministrazioni, ecc.) che nelle loro attività nel Cyberspace, potenzialmente pericolose per i diritti ed interessi giuridici degli utenti e di terzi, devono previamente riconoscere, valutare, circoscrivere i rischi e "dominare" le fonti da cui derivano, valorizzando le potenzialità proprio dei sistemi esperti e di intelligenza artificiale, che possono operare nel nuovo contesto tecnologico anche in funzione di prevenzione dei reati e riduzione dei rischi.

Si tratta di campi ancora in gran parte da esplorare, che richiedono rinnovate riflessioni ed elaborazioni anche dogmatiche, da parte del penalista, il quale, per non venire meno al proprio compito di giurista, deve saper adeguare gli strumenti conoscitivi e sistematici delle proprie categorie concettuali alla nuova realtà, per meglio riaffermare e rendere efficace la protezione penale e nel contempo preservare i principi e le garanzie fondamentali propri di un ordinamento democratico.