UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO
DIPARTIMENTO DI DIRITTO PUBBLICO, INTERNAZIONALE E COMUNITARIO

CORSO DI LAUREA MAGISTRALE IN GIURISPRUDENZA
A. A. 2023/2024

TESI DI LAUREA

IL DELITTO DI ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO: PROBLEMI ATTUALI

RELATORE: CHIAR.MO PROF. ANGELO ZAMBUSI

LAUREANDA: DARIA DAL CIN
MATRICOLA N. 1198176

INDICE

INTRODUZIONE

L'avvento dell'era digitale ha portato a innegabili vantaggi e miglioramenti per la qualità della vita. Gli studiosi Erik Brynjolfsson e Andrew McAfee hanno coniato l'espressione "La nuova rivoluzione delle macchine"[1], dichiarando che i computer hanno ampliato le capacità cognitive umane analogamente a quanto il motore a vapore fece per la forza muscolare.

L'epoca nella quale viviamo è caratterizzata da un avanzamento tecnologico che pervade ogni aspetto della vita quotidiana, influenzando settori fra i quali trasporti, sanità e commercio, e diffondendo nuovi canali di comunicazione che vengono da tutti considerati come una vera e propria rivoluzione. La convergenza digitale sta portando a progressi rapidi e tendenzialmente duraturi sul nostro mondo, imponendoci la sfida di assimilare questa transizione epocale per poter capitalizzare le nuove opportunità che essa comporta, mediante un loro sfruttamento responsabile.

La società moderna ha visto il susseguirsi di numerosi cambiamenti a seguito dell'avvento delle tecnologie informatiche, che hanno fornito un apporto positivo alla collettività, ma hanno al contempo sollevato nuove sfide e problemi dal punto di vista legale, in particolare nel campo del diritto penale. Non si può non tenere in considerazione che ci sono infatti anche degli svantaggi nel progredire: dal potere dei *social media* di plasmare l'opinione pubblica o dalla potenziale perdita della privacy, a fenomeni più preoccupanti, quali il cyberbullismo o la diffusione di materiale pornografico sul web. Internet pertanto rappresenta uno strumento di conoscenza e connessione globale che offre informazioni e permette di comunicare con persone in tutto il mondo; tuttavia, parallelamente è diventato anche un veicolo per la commissione di una serie indefinita di illeciti. Si tratta di reati altrettanto pericolosi e difficili da contrastare, soprattutto a causa dell'ampio ed incontrollato utilizzo degli strumenti digitali.

---

[1] E. BRYNJOLFSSON – A. MCAFEE, *La nuova rivoluzione delle macchine: Lavoro e prosperità nell'era della tecnologia trionfante*, Feltrinelli, aprile 2015: «*Digital technologies are doing for human brainpower what the steam engine and related technologies did for human muscle power. They're allowing us to overcome many limitations rapidly and to open up new frontiers with unprecedented speed. It's a very big deal. But how exactly it will play out is uncertain*».

La criminalità informatica è un fenomeno globale senza confini e, come Internet stesso, continua ad espandersi in termini di portata e di impatto. La superficie di attacco continua a crescere man mano che la società diventa sempre più digitalizzata, con un numero sempre maggiore di cittadini, imprese, servizi pubblici e dispositivi che si connettono a Internet. Di conseguenza, sta aumentando in modo esponenziale il potenziale impatto che il singolo utente malintenzionato può avere su un maggior numero di vittime.

La popolazione è abituata all'informatica di tutti i giorni, principalmente vedendo e vivendo in prima persona gli sviluppi positivi e i numerosi vantaggi che questa offre alla società. Tuttavia, spesso ignora i retroscena negativi: molte persone, infatti, non sono a conoscenza, o hanno solo una conoscenza parziale, dei crimini che possono essere commessi attraverso dispositivi elettronici connessi a Internet.

Uno dei reati che possono essere perpetrati sfruttando l'accesso ad Internet è il delitto di accesso abusivo ad un sistema informatico o telematico, fattispecie che sarà oggetto dello studio che segue. La scelta è ricaduta su questo argomento per le interessanti riflessioni che la peculiare struttura di detta fattispecie ha fatto emergere sia in dottrina sia in giurisprudenza. Trattasi, infatti, di una tematica che ha sollevato varie questioni giuridiche, sorte dalla necessità di adeguare le normative esistenti ai contesti tecnologici emergenti.

Più nel dettaglio, nel primo capitolo la tesi fornisce una panoramica sull'evoluzione di Internet e sui conseguenti effetti che tale sviluppo ha avuto per la società, ponendo attenzione anche alla figura del cybercriminale. Si prosegue poi con uno sguardo generale sugli interventi normativi che si sono susseguiti in materia, interventi giustificati dalla necessità di reinterpretare ed integrare le tradizionali leggi penali per far fronte a questi nuovi tipi di reati. Il quadro normativo richiede infatti un costante aggiornamento che tenga conto delle trasformazioni sociali e tecnologiche, per poter risultare davvero adeguato a perseguire le nuove forme di criminalità che si stanno sviluppando.

Il secondo capitolo tratta in maniera analitica la fattispecie di *accesso abusivo ad un sistema informatico o telematico* di cui all'articolo 615-*ter* del codice penale, esaminandone la struttura e riportando le diverse posizioni dottrinali e giurisprudenziali emerse a riguardo. Si discutono le questioni più dibattute, focalizzandosi, da una parte, sulla determinazione dell'interesse tutelato dalla norma, evidenziando in particolare l'esigenza di individuare nuovi beni giuridici, non essendo sempre pertinente riferirsi a quelli tradizionali a causa dello sviluppo tecnologico; dall'altra parte, sul concetto di

abusività che deve permeare le condotte tipiche di introduzione e mantenimento nel sistema informatico. Infine, la trattazione del capitolo si conclude con un esame delle circostanze aggravanti previste dalla norma.

In ultima analisi, nel terzo ed ultimo capitolo si tratteggia una panoramica generale dell'implementazione dell'intelligenza artificiale nella società, sottolineando le problematiche che questo comporta dal punto di vista dell'attribuzione della responsabilità penale per fatto illecito. Si termina con il mostrare come, avendo la rivoluzione digitale ridefinito il modo in cui le comunità comunicano, ottengono e condividono informazioni, il cambiamento sociale abbia comportato l'evolversi del fenomeno della disinformazione e, di conseguenza, richieda un impegno soprattutto per tutelare i minori. Si tratta di questioni che necessitano di uno sforzo e di una collaborazione tra Stati e soggetti privati o pubblici, in particolare gli *Internet Service Provider*.

Obiettivo primario della tesi è dunque quello di evidenziare il rapporto intercorrente tra le tecnologie informatiche e il diritto penale, esplorando le sfide che queste innovazioni pongono per individuare soluzioni innovative idonee a garantire un adeguato bilanciamento tra la tutela della sicurezza informatica e i diritti fondamentali delle persone.

A detta di chi scrive, risulta fondamentale riconoscere, a fini istituzionali e personali-sociali, i risvolti che l'incremento delle tecnologie hanno per lo svolgimento delle occupazioni personali e lavorative, allo scopo di comprendere meglio questa nuova tipologia di reati informatici, che possono compromettere irrimediabilmente lo svolgersi della vita quotidiana di ciascuno. Risulta quindi più che opportuno prendere consapevolezza del fenomeno per meglio fronteggiarlo e, se possibile, prevenirlo.

Il progresso tecnologico, insieme alla crescente integrazione dell'intelligenza artificiale nella società, sottolinea l'urgenza di affrontare queste questioni attraverso un dialogo multidisciplinare, un aggiornamento delle normative e lo sviluppo di standard etici e professionali comuni.

CAPITOLO 1

-

IL RAPPORTO FRA LE TECNOLOGIE INFORMATICHE E IL DIRITTO PENALE

SOMMARIO: 1. Progresso tecnologico: gli effetti sulla criminalità informatica. – **1.1.** Il web interattivo. – **2.** Emersione di nuove tipologie di reato. – **2.1.** Il *locus commissi delicti* – **2.2.** Il ruolo degli utenti di Internet. – **3.** Profilo normativo. – **3.1.** La Legge n. 547 del 23.12.1993. – 3.1.1. Interventi successivi.

1. *Progresso tecnologico: gli effetti sulla criminalità informatica*

L'avvento delle nuove tecnologie ha cambiato drasticamente il quotidiano impattando in maniera significativa non solo sul modo di comunicare, condurre affari e apprendere, ma addirittura sta modificando la percezione stessa della realtà, facendo emergere nuove e diverse sfumature dell'identità personale. La tecnologia digitale evolve costantemente e, superando i suoi precedenti limiti, fornisce comodità che difficilmente potevano essere immaginate anche solo una generazione fa. Grazie a questa accelerazione senza precedenti nel flusso di informazioni, il mondo globale è più connesso che mai e questo permette di generare nuove opportunità di dialogo e collaborazione. Negli ultimi decenni ci sono stati molti sviluppi delle tecnologie che hanno notevolmente migliorato la disponibilità, la velocità, la portata e la sicurezza dei canali di comunicazione. Esemplificativamente, si pensi allo sviluppo della tecnologia *wireless* (come le reti Wi-Fi o il Bluetooth) che, sfruttando le onde radio, consente di trasmettere informazioni tra dispositivi senza l'uso di cavi e perciò a distanza. Parallelamente a questo, ci sono stati sviluppi anche nei dispositivi attraverso i quali questi canali funzionano, ad oggi sempre più sofisticati e in grado di operare ovunque. Ad esempio, il moderno telefono cellulare non è semplicemente un telefono, ma è un computer completo, funzionante e connesso a Internet che consente comunicazioni visive, orali e scritte istantanee praticamente a costo zero; chiunque abbia uno *smartphone* può utilizzare il GPS per evitare di perdersi in città

sconosciute; si possono fare acquisti *online*, guardare film in *streaming* e si può usufruire di servizi bancari *online*. L'obiettivo primario dello sviluppo della tecnologia è supportare le persone nello svolgimento delle attività quotidiane, sia lavorative che ludico-ricreative, per migliorarle, renderle più accessibili, veloci e possibilmente più economiche[2].

La rapida trasformazione dell'economia globale verso il digitale e la progressiva informatizzazione delle attività rende oramai indispensabile l'utilizzo di strumenti informatici e telematici: i sistemi digitali e le Tecnologie dell'Informazione e della Comunicazione (TIC)[3] sono fondamentali e onnipresenti in tutti i settori dell'attività economica in Europa e oltre. L'accesso a Internet e il conseguente flusso ininterrotto di informazioni sono ormai essenziali per l'innovazione economica, in quanto posti alla base di molte imprese e del funzionamento quotidiano delle società.

Questo cambiamento offre occasioni per miglioramenti, crescita e occupazione, ma richiede approcci politici complessi che potrebbero non essere pienamente soddisfatti dalle amministrazioni pubbliche locali, richiedendo per lo più una coordinazione a livello sovranazionale. Per far fronte a questa sfida, uno degli obiettivi di lungo periodo della politica europea è proprio il *Digital Single Market*, per il tramite del quale si cerca di supportare e sviluppare l'utilizzo di beni e servizi connessi alle nuove tecnologie: «*Il mercato unico digitale è un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui, quale che sia la loro cittadinanza o nazionalità o il luogo di residenza, persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali*»[4].

La tecnologia permea totalmente la nostra esistenza, contribuendo a costituire una società globalizzata e sempre più connessa. Ad oggi si può pacificamente discutere di

---

[2] Oggigiorno, soprattutto dopo la pandemia COVID-19, sentiamo spesso parlare ad esempio di *smartworking* quale pratica lavorativa a distanza, che grazie all'uso della tecnologia consente di lavorare con orari più flessibili. L'obiettivo è, cioè, migliorare la produttività e la creatività, garantendo un maggior equilibrio tra vita privata e lavoro e riducendo al contempo i costi d'ufficio e i tempi di spostamento.

[3] TIC (o ICT dall'acronimo inglese *Information and Communication Technology*) identifica la scienza che studia le tecniche per ricevere, trasformare e trasmettere le informazioni che circolano sul web: «indica la convergenza dell'informatica con le telecomunicazioni e identifica ogni settore legato allo scambio di informazioni e tutti i metodi e le tecnologie che servono a realizzarlo, compreso l'hardware, il *software* e i servizi connessi.» in https://www.treccani.it/enciclopedia/ict_(Lessico-del-XXI-Secolo)/.

[4] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "*Strategia per il mercato unico digitale in Europa*" {SWD (2015) 100 final}.

"rivoluzione" informatica poiché tale fenomeno, oltre a coinvolgere la collettività tutta – interessando ogni sfera della vita, privata e pubblica – ha provocato una transizione dall'era industriale ad una società dell'informazione[5].

Le informazioni circolano velocemente perché la digitalizzazione permette di convertire dati e documenti analogici in formato digitale[6]; cambiano quindi, e sono rese più facili ed istantanee, le modalità di accesso e di archiviazione a dati e informazioni. Nel mondo contemporaneo, gli uni sono costantemente collegati agli altri, ma non sempre si è pienamente informati. La dipendenza dalla tecnologia e dalla Rete offre innumerevoli possibilità di comunicazione e maggiore accessibilità all'informazione, permettendo una connessione istantanea con persone in tutto il mondo e la scoperta di idee innovative e diverse prospettive (pensiamo ad esempio alla circolazione delle informazioni mediche, alle maggiori opportunità educative o di lavoro). Questa costante connessione però rischia al tempo stesso di creare una sorta di "rumore informativo" poiché, sommersi da una quantità enorme di dati, diventa difficile distinguerne la veridicità o la provenienza[7]. È di importanza primaria dunque pervenire ad una consapevolezza critica e mantenere un impegno nell'educare sé e gli altri sull'uso responsabile delle tecnologie e delle informazioni che circolano nella Rete.

Questi progressi permettono alla società di raggiungere risultati vantaggiosi, in termini di qualità della vita e prospettive economiche, rendendo la società sempre più inclusiva ed interconnessa, ma, molto spesso, vengono anche utilizzati, abusati o sfruttati per scopi criminali.

In altre parole, l'innovazione tecnologica offre prospettive di crescita entusiasmanti per imprese e cittadini, grazie alla collaborazione e alla condivisione di idee a livello globale;

---

[5] L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme,* in *Cybercrime,* Milano, 2023, p. 34: «a quella che si deve definire "rivoluzione informatica" o, meglio, "cibernetica", si deve riconoscere un'importanza strutturale o, se si preferisce, strategica per l'evoluzione del diritto, non solo penale, in quanto rappresenta la frontiera più avanzata dell'innovazione e del cambiamento nell'odierna società globalizzata, avendo già determinato, e quotidianamente determinando un esteso e prolungato impatto sulle forme ed i modi di essere dei rapporti sociali, economici, politici, culturali, fino a quelli interpersonali e privati».

[6] Ad esempio, è possibile scansionare un documento cartaceo per convertirlo in formato PDF e memorizzarlo su un computer.

[7] Cfr. *Il contesto nei sistemi informativi: cos'è e perché è sempre più importante*, in https://www.agendadigitale.eu/cultura-digitale/il-contesto-nei-sistemi-informativi-cose-e-perche-e-sempre-piu-importante/.

tuttavia, crea anche nuovi vettori di attacco per i criminali: la maggiore connessione tra dispositivi, utilizzati per migliorare la vita quotidiana dei cittadini e il funzionamento delle imprese e dei servizi pubblici, crea anche nuove opportunità per i criminali informatici. Queste minacce cibernetiche si manifestano nello spazio virtuale ma poi hanno ricadute concrete nella realtà fisica. Oltretutto, Internet non solo ha dato origine a questa forma di criminalità completamente nuova ma può anche facilitarla o agevolarla in quasi tutte le altre aree criminali.

È evidente come il panorama della criminalità sia cambiato drasticamente negli ultimi anni, in gran parte a causa dei progressi tecnologici che hanno avuto un impatto profondo e negativo sulla società e sull'economia in generale. I criminali adottano e integrano rapidamente nuove tecnologie nei loro *modi operandi* o costruiscono attorno ad esse nuovi modelli di *business*. Bisogna confrontarsi con la realtà in continua evoluzione e prendere atto di come oggigiorno la tecnologia sia diventata una componente chiave per gran parte delle attività criminali.

L'elenco dei dispositivi vulnerabili cresce man mano che si espande la connessione. Gli sviluppi tecnologici hanno notevolmente influenzato l'ascesa della criminalità informatica, alimentati anche dal fatto che talvolta chi si collega *online* usa approcci iniziali e deboli alla sicurezza informatica, diventando perciò un facile obiettivo. Nonostante esistano ancora hacker solitari che rappresentano una minaccia reale per gli individui e le piccole imprese, nel contesto attuale, i criminali informatici, sfruttando il supporto che offre Internet, creano reti di comunicazione tra loro riuscendo a coordinarsi per pianificare attacchi di ampia portata contro grandi aziende o governi. Gli attacchi informatici su larga scala di successo tendono ad avere un effetto a catena, andando a colpire persone e imprese lungo le catene di approvvigionamento che possono estendersi in tutto il mondo[8]. Le conseguenze della criminalità informatica possono essere deleterie, potendo determinare, nel breve periodo, perdite finanziarie e danni all'immagine e, nel lungo periodo, compromettere la reputazione al punto da poter provocare la chiusura dell'impresa[9].

[8] Dai dati del Cybersecurity Readiness Index 2023 emerge che solo il 7% delle aziende italiane ritiene di essere in grado di difendersi da un attacco informatico, mentre a livello globale la percentuale sale del 15%.

[9] Alla fine dello scorso anno, la criminalità informatica ha causato danni per un totale di 6mila miliardi di dollari in tutto il mondo e si prevede che tale cifra salirà a 10,5mila miliardi di dollari entro il 2025. I costi della criminalità informatica comprendono il danneggiamento e la distruzione di dati, il furto di denaro, la

Gli incidenti di cybersicurezza, permettendo ai criminali informatici di raccogliere informazioni personali, possono compromettere gravemente i servizi essenziali e le attività economiche e sociali. I criminali utilizzano tutti i canali di comunicazione disponibili, non solo per i propri scopi di comunicazione interna, ma anche per contattare potenziali vittime[10], cosa che la tecnologia moderna consente di fare in numeri senza precedenti. Internet oggi è il portale più semplice per commettere un crimine informatico. Un mondo sempre più connesso auspica ad esaltare i suoi benefici, ma non può sottovalutare gli svantaggi che ad esso pur sempre si ricollegano.

1.1. *Il web interattivo*

Nonostante non sia inquadrabile un preciso evento che abbia portato a definire determinate forme di illeciti come crimini informatici, la maggior parte degli esperti concorda nel ritenere che questi abbiano effettivamente preso piede alla fine degli anni ’80, quando la posta elettronica è diventata una tecnologia comunemente utilizzata. Nel suddetto periodo, molti dei primi crimini informatici venivano commessi mediante l’utilizzo di e-mail, con le quali inviare virus o perpetrare truffe, una tendenza che continua ancora oggi ed è nota come *phishing*[11]. Con il termine *phishing* ci si riferisce ad un tipo di truffa perpetrata tramite Internet per "pescare" (dall’inglese *fishing*) dati sensibili -informazioni finanziarie e password- di un utente: in pratica, l’aggressore (*phisher*) inganna l’utente inviando un messaggio di posta elettronica, o anche un SMS, che appare essere quello di una istituzione nota al destinatario (per esempio la sua banca) e che tipicamente contiene avvisi di problemi verificatesi con il proprio conto corrente o

perdita di produttività, il furto di proprietà intellettuale, il furto di dati personali e finanziari, l'appropriazione indebita, la frode, l'interruzione del normale svolgimento delle attività post-attacco, le indagini forensi, il ripristino e l'eliminazione dei dati e sistemi hackerati e danni alla reputazione.

[10] Uno degli esempi più lampanti è quello del cyber-terrorismo: le organizzazioni terroristiche sfruttano la potenzialità degli strumenti digitali nel creare canali comunicativi *ad hoc* non solo per diffondere ampiamente la propria ideologia, destabilizzando le comunità e creando paura, ma anche per reclutare nuovi membri. Il reclutamento *online*, permettendo l’accesso a una vasta gamma di individui, agevola la possibilità di entrare in contatto e persuadere soggetti vulnerabili, per il tramite di video di addestramento o creazione di comunità virtuali.

[11] Enc. on. Treccani definisce il *phishing* come «una frode informatica finalizzata all'ottenimento di dati personali sensibili (password, numero di carta di credito ecc.) e perpetrata attraverso l'invio di un messaggio di posta elettronica a nome di istituti di credito, finanziarie, agenzie assicurative, in cui si invita l'utente, generalmente al fine di derubarlo, a comunicare tali informazioni riservate».

account; in questo modo si invita il destinatario della e-mail a seguire un link (per evitare un addebito e/o per regolarizzare la sua posizione con la società di cui il messaggio simula la grafica e l'impostazione), che, tuttavia, porta a una copia fittizia apparentemente simile al sito ufficiale, situata però sul server controllato dal *phisher*; i dati personali che il destinatario inserisce vengono quindi memorizzati nel server gestito dal *phisher* e utilizzati per autorizzare pagamenti, trasferire somme di denaro o conservati per ulteriori successivi attacchi.

A metà degli anni '90 del secondo scorso, l'apertura di Internet al pubblico ha determinato la nascita del c.d. *cyberspace*[12], ovverosia di uno spazio in cui gli utenti riescono a comunicare continuamente tra di loro grazie all'uso di sistemi interconnessi: «*l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi*»[13]. Con questo concetto ci si riferisce, cioè, a quell'ambiente virtuale in cui avvengono tutte le interazioni che sfruttano Internet, divenendo quindi un luogo che, nonostante la sua immaterialità, risulta estremamente influente nella vita quotidiana delle persone, sia a livello professionale sia personale. Questo ha consentito ai criminali informatici di indirizzare di nascosto le vittime verso pagine in cui rivelare involontariamente informazioni personali o scaricare virus, spesso tramite una tecnica chiamata *pharming*[14]. Come nel *phishing,* l'obiettivo è entrare in possesso di informazioni di identificazione personale e credenziali di accesso degli utenti, ma in questo caso la vittima entra immediatamente, attraverso una serie di reindirizzamenti automatici, in un sito web falso.

È stata però l'era dei *social media* nel nuovo millennio a creare un mondo completamente nuovo che i criminali informatici possono sfruttare maggiormente per i propri scopi

---

[12] «Tale concetto associa la cibernetica (termine derivato dal greco *kyber*, timoniere o pilota, scelto agli inizi del secolo scorso per indicare una nuova scienza, che intendeva studiare i meccanismi con cui uomini, animali e macchine comunicano con l'ambiente esterno e lo controllano) alla nozione pluridimensionale e dinamica, non meramente lineare, di "spazio" – impropriamente detto "virtuale" – che appare idonea a rappresentare l'estensione pervasiva del nuovo mondo, nel quale, singolarmente e collettivamente, siamo tutti realmente (non solo "virtualmente") immersi, in quanto ormai permanentemente connessi ed interagenti, se non anche dipendenti» in tal senso L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme,* cit., pp. 36-37.

[13] Art. 2, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale* adottata con d.p.c.m. 24 gennaio 2013, pubblicato nella Gazzetta Ufficiale 19 marzo 2013, n. 66.

[14] v. https://www.kaspersky.it/resource-center/definitions/pharming: «Il *pharming* è un tipo di attacco informatico basato su tecniche di social engineering in cui i criminali reindirizzano a un sito falso gli utenti di Internet che cercano di raggiungere un determinato sito Web».

illeciti. All'improvviso, persone in tutto il mondo hanno messo volontariamente le proprie informazioni personali *online* - notizie e foto della propria vita privata - e spesso le hanno rese visibili al pubblico. I *social network* (Facebook, Instagram, Twitter, etc.) sono molto affollati e popolari tra le persone, soprattutto di giovane età, in quanto ormai sono ritenuti indispensabili per l'interazione sociale, gli affari e l'istruzione, non configurandosi più quale mero mezzo di comunicazione. L'impatto positivo è che i suoi utenti possono accedere rapidamente ai dati e alle notizie, riuscendo così facilmente ad espandere le relazioni e compiere attività di *business*. Nel mondo degli affari, infatti, i s*ocial media* sono una delle strategie di *marketing* che i venditori adottano per far conoscere i loro prodotti e la loro merce in modo più rapido. Tuttavia, si devono prendere in considerazione anche, e soprattutto, gli effetti negativi, da rinvenire nel fatto che le informazioni ottenute tramite Internet possono essere utilizzate come strumento o intermediario per la conduzione di attività inerenti alla sfera della criminalità informatica: per riportare degli esempi, basti pensare a frodi, umiliazioni, crimini sessuali, gioco d'azzardo *online*. Questo ha oltretutto alimentato un vero e proprio esercito di ladri di identità, che sono riusciti a ottenere l'accesso a conti bancari, carte di credito e altro ancora, a fronte di sistemi scarsamente protetti.
La vita di ognuno è oggi trasferita in questa dimensione virtuale, in cui tutti sono interconnessi e dipendenti. Internet è fondamentalmente una fonte di informazioni e un ambiente in cui le comunità di individui possono incontrarsi e confrontarsi. Ne consegue che l'elenco delle informazioni che potrebbero essere utilizzate dai criminali è essenzialmente infinito, tenuto conto, in particolare, del fatto che i contenuti dei dati che vengono caricati rimangono poi memorizzati dai motori di ricerca e dai sistemi informatici.

Il mondo reale esterno e quello cibernetico sono oggigiorno inscindibilmente intrecciati. L'avvento della tecnologia e dell'innovazione ha fatto sì che gli aspetti digitali influiscano costantemente sulla vita quotidiana di ognuno. Consapevoli di questo, gli studiosi hanno individuato l'emergere di nuove fasi, che segnano il passaggio da una comunicazione statica e incentrata sulla sola consultazione di informazioni ad una comunicazione interattiva e incentrata primariamente sulla figura dell'utente. Ormai si è superata l'«*originaria architettura "unidirezionale" del web, in cui l'utente era il destinatario*

passivo di informazioni e comunicazioni, alle quali poteva accedere e che poteva leggere o acquisire, ma la cui produzione, circolazione e diffusione dipendeva dai gestori degli accessi e dei servizi in rete (ISP e, più in generale, c.d. webmaster). Da tempo (2000-2006) si è parlato di un web 2.0, caratterizzato invece dalla progressiva interazione attiva degli utenti, posti in grado di creare e condividere contenuti in blogs, forum, social network»[15].

Il concetto di web 2.0[16] è stato introdotto per la prima volta da Tim O'Reilly e Dale Dougherty, con riferimento alle nuove caratteristiche e funzionalità del web che andavano oltre la semplice pubblicazione e consultazione di informazioni. Il web 2.0 è considerato una nuova versione del World Wide Web[17] (comunemente indicato come WWW) e si basa su tecnologie che, sfruttando piattaforme *online*, consentono agli utenti di creare, condividere, modificare e interagire con altri contenuti *online*. A differenza dell'era precedente, quando era necessario avere conoscenze avanzate di programmazione per creare un sito web, ci si confronta qui con un web che viene definito partecipativo, perché basato su di una comunicazione bidirezionale. Il web 2.0 ha visto la nascita e l'espansione dei *social network,* piattaforme che consentono agli utenti di connettersi tra loro, interagire e creare comunità; qui gli utenti hanno la possibilità di partecipare attivamente, essendo coinvolti in prima persona nella produzione e modificazione dei contenuti *online* collaborando con altri utenti. «*Si moltiplicano poi le applicazioni che consentono la comunicazione interpersonale cd. one-to-one, in cui mittente e destinatario interagiscono istantaneamente senza alcuna mediazione: WhatsApp, Telegram, Snapchat, Tinder, etc. Il cuore della transizione verso il Web 2.0 è, in sostanza, la trasformazione dell'Internet da flusso di informazioni digitali a spazio per l'interazione sociale*»[18]. Il web 2.0 ha avuto

---

[15] V. L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme,* cit., pp. 57-58.

[16] Il termine, secondo questa accezione, è stato per la prima volta utilizzato dall'editore Tim O'Reilly nell'ottobre 2004, nel corso di una conferenza sul mondo digitale. Per una più approfondita analisi si rimanda a T. O'REILLY - J. BATTELLE, *Web Squared: Web 2.0 Five Years On*, O'Reilly Media Inc., 2009.

[17] Progettato da Tim Berners-Lee nel 1989 come strumento per consentire agli scienziati del CERN di Ginevra di conservare e condividere i loro esperimenti scientifici. La sigla WWW oggi si riferisce al principale servizio di recupero di informazioni di Internet.

[18] T. PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive*, in Sistema Penale, ottobre 2023, p. 8.

Si esprime in termini simili anche I. SALVADORI, *I reati contro la riservatezza informatica,* in *Cybercrime*, Milano, 2023, p. 698, che parlando delle nuove sfere virtuali emerse con lo sviluppo delle TIC, le descrive come «sfere di controllo, disponibilità e godimento esclusivo, (in cui) gli utenti possono non solo

un impatto significativo sulla società e sull'economia, aprendo nuove opportunità di comunicazione, collaborazione e partecipazione e offrendo altresì la possibilità di personalizzare la propria esperienza *online*. Il web 2.0 è un nuovo luogo in cui interagire, creare e mantenere relazioni, è uno strumento per raggiungere il pubblico. È un nuovo modello di comunicazione orizzontale, perché scompaiono le gerarchie, è un luogo in cui pubblico ed organizzazioni si trovano sullo stesso livello, e multidirezionale, perché il *feedback* può essere continuo.

Nel tempo l'approccio al web si è ulteriormente evoluto con l'avvento del web 3.0, il quale, basandosi anche sull'interconnessione di dati provenienti da diverse fonti, punta ad offrire un web ancora più personalizzato e intelligente, permettendo all'utente di impostare le proprie preferenze e inviandogli raccomandazioni filtrate in base ai suoi interessi. Il web 3.0 si concentra sulla capacità di comprendere il contesto e il significato dei contenuti per fornire risultati di ricerca più pertinenti. Questo grazie all'utilizzo di tecnologie avanzate come l'intelligenza artificiale[19] e il *machine learning*[20]. Gli utenti godono di una maggiore flessibilità nell'uso e nell'accesso ai contenuti *online*, avvantaggiati dalla possibilità di accedere ai contenuti da dispositivi diversi come smartphone, tablet, smart TV, e non solo dai tradizionali computer. In generale, il web 3.0 punta a migliorare ulteriormente l'esperienza dell'utente, offrendo materiali più accurati e rilevanti, consentendo la partecipazione attiva e rendendo l'accesso ai dati più semplice

raccogliere, organizzare, conservare, elaborare e scambiare informazioni e dati di natura riservata o segreta, nell'accezione tradizionale che tali concetti assumono nel diritto penale, ma anche contenuti informativi di per sé già noti e disponibili, che attraverso *software* e mezzi di trattamento automatizzato acquistano un valore ed una utilità del tutto nuovi. Tali spazi permettono inoltre agli utenti di comunicare o di interagire in tempo reale (mediante *webcam*, videoconferenze, messaggi video o audio, ecc.) e a costi assai ridotti».

[19] L'IA è un campo multidisciplinare della scienza che crea macchine in grado di eseguire attività che richiedono intelligenza umana. L'obiettivo principale dell'IA è quello di sviluppare sistemi che possono apprendere, ragionare e risolvere problemi in modo simile a quello degli esseri umani: si tratta di sistemi che riescono a comprendere e interpretare il linguaggio umano, riconoscere immagini, prendere decisioni e apprendere da esperienze passate per adattarsi a nuove situazioni. Per approfondire si veda Agenda Digitale, *Intelligenza Artificiale: Cosa si intende con Intelligenza Artificiale e quali sono le norme che la regolamentano.*

[20] T. MITCHELL, *Machine Learning*, 1997, New York: McGraw-Hill: «*Machine Learning is the study of computer algorithms that improve automatically through experience*». Con il termine *machine learning* (o apprendimento automatico) ci si riferisce a quell'area dell'intelligenza artificiale che si occupa dello sviluppo di algoritmi che consentono ai computer di imparare dai dati e dall'esperienza per migliorare le proprie capacità e prestazioni nel tempo, senza essere esplicitamente programmati per svolgere quel tipo di attività. La macchina diventa quindi in grado di scegliere tra più alternative e prendere decisioni da sola.

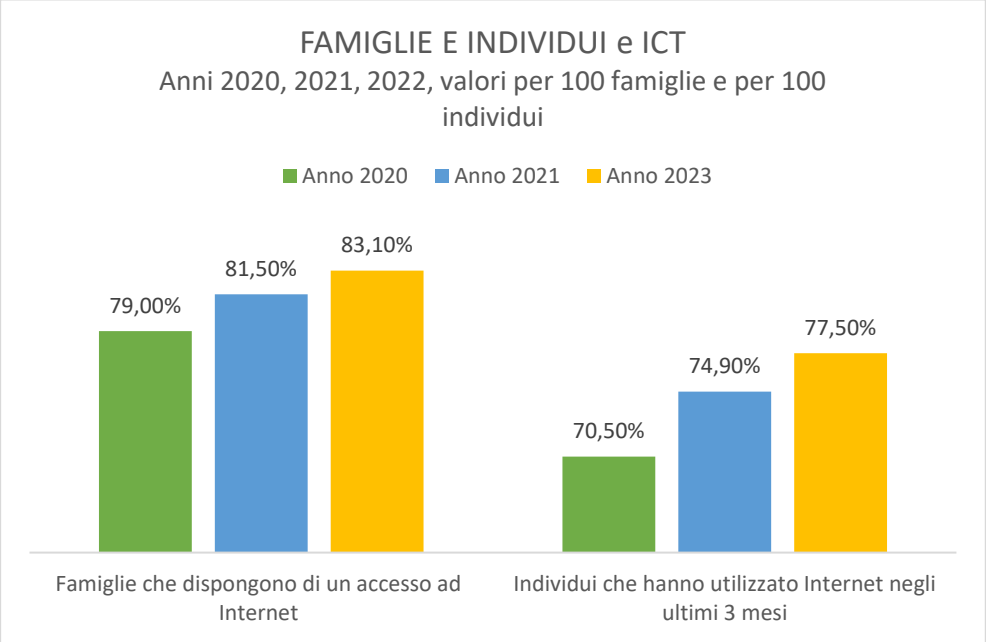
e integrato. Questa evoluzione del web ha aperto la strada a nuove opportunità e applicazioni, come ad esempio l'evoluzione grafica dal 2D al 3D.

Oggigiorno si parla di web 4.0, riferendosi alla futura evoluzione del web 3.0. Il web 4.0 si basa sull'idea di un web ancora più interconnesso e pervasivo, con una maggiore interazione tra il mondo virtuale e il mondo fisico, tale da consentire una maggiore automazione e scambio di informazioni tra i diversi dispositivi. In questo scenario, utenti, oggetti, dispositivi e ambienti digitali sono costantemente connessi per il tramite di Internet. Gli utenti in questo web 4.0 vivono un'esperienza altamente personalizzata e interattiva, grazie alla capacità delle macchine intelligenti di comprendere e assecondare le preferenze e i comportamenti degli utilizzatori. Pensiamo ad esempio alla domotica, che consente alle persone di controllare i dispositivi domestici tramite Internet, offrendo comfort, sicurezza ed efficienza energetica. Le macchine intelligenti, invece, sono già in grado di fornire suggerimenti e raccomandazioni ai consumatori in base alle loro preferenze e al loro storico di acquisti, influenzando quindi le decisioni di acquisto. Tuttavia, l'evoluzione del web 4.0 è ancora in fase di sviluppo e richiede certamente la creazione e l'implementazione di algoritmi sempre più complessi e sofisticati per l'elaborazione e l'interpretazione dei dati, che potrebbero comportare nuove sfide non solo tecniche ma anche etiche. Il concetto di alter-ego digitale solleva alcune preoccupazioni legate alla privacy e alla sicurezza dei dati che devono essere bilanciate con i vantaggi dell'automazione per garantire un'esperienza positiva e di fiducia[21]: la raccolta di informazioni personali attraverso algoritmi potrebbe essere considerata forse troppo invasiva? In sintesi, con il web 4.0 si sta avendo a che fare con un ambiente *online* in cui le macchine intelligenti e i Big Data rivestono un ruolo centrale nel comprendere e conseguentemente influenzare le decisioni degli utenti.

Addirittura, taluni stanno prefigurando la teorizzazione di un web simbiotico 5.0 in cui realizzare una comunicazione *online* ancora più evoluta, in grado di equiparare in *toto* quella che avviene nel mondo fisico. L'obiettivo è infatti quello di ottenere un web funzionale anche a comprendere la componente emozionale insita nelle interazioni che le persone hanno nella realtà. Questo permetterà di creare un ambiente digitale estremamente integrato, interattivo e intuitivo, in cui i sistemi di intelligenza artificiale

[21] Alcune annotazioni in C. CRESCIOLI, *La tutela penale dell'identità digitale*, in Sistema Penale, 5/2018, pp. 265 e ss.

riusciranno a collaborare con gli utenti per potenziare e personalizzare la loro esperienza *online*.



[22]

2. *Emersione di nuove tipologie di reato*

Lo sviluppo delle Tecnologie dell'Informazione e della Comunicazione rende la vita moderna di gran lunga più conveniente, come è già stato sottolineato. Tuttavia, poiché Internet è diventato un mezzo di comunicazione di massa grazie all'accesso alla Rete generalizzato, la digitalizzazione ha altresì aumentato il rischio di vulnerabilità dei sistemi informatici e dei dati in essi contenuti e queste nuove opportunità per gli utenti malintenzionati mettono oggi a rischio un numero sempre maggiore di potenziali vittime. L'aumento dei crimini informatici che sfruttano le tecnologie emerge come un grave problema sociale. Dall'inizio della pandemia COVID-19, sempre più utenti in tutto il mondo sono diventati dipendenti da Internet in tutti i settori, compresi l'istruzione, le

[22] Il rapporto Istat sull'uso della tecnologia da parte degli italiani del 17 marzo 2023 certifica che il 77,5% della popolazione (da 6 anni in su) ha usato internet negli ultimi tre mesi. Numeri che registrano un aumento del 7% tra il 2020 e il 2022.

transazioni finanziarie e il lavoro da casa, ed è emerso come i danni derivanti dai crimini informatici siano aumentati regolarmente, con una tendenza costante.
Dal momento che la vita delle persone trova espressione anche nel *cyberspace* attraverso le reti di informazione e comunicazione, altresì la perpetrazione dei crimini, che convenzionalmente hanno luogo *offline*, si è spostata *online*, talvolta peggiorando i casi e la gravità dei fatti. La manifestazione del crimine ora appare in varie forme o varianti che sono molto dannose per la vita delle persone o, addirittura, per gli interessi di uno Stato. I danni che causano i crimini informatici, anche se non immediatamente percepibili, sono pure maggiori rispetto a quelli causati dai crimini realizzati *offline* a causa del loro impatto – aggravato dalla facile, ma anche imperfetta, fuga di notizie attraverso i *social media* e – supportato dall'anonimato dell'ambiente *online*, in forza del quale gli aggressori riescono ad influenzare le proprie socialmente, psicologicamente e finanziariamente.
La criminalità informatica sta vivendo un rapido sviluppo i cui effetti non si limitano ad incidere sulle dinamiche del singolo Paese; infatti, il controllo dei dispositivi informatici da parte degli aggressori spesso coinvolge confini internazionali.

Quando si parla di criminalità informatica si fa riferimento ad una categoria ampia di fattispecie illecite che difficilmente può essere descritta con un'unica definizione, in quanto comprende una vasta gamma di comportamenti antigiuridici implicanti l'uso illecito dei computer e delle reti informatiche. Come ribadito nei paragrafi precedenti, essa è una minaccia sempre crescente e di conseguenza abbisogna di una consapevolezza diffusa per poterla contrastare, o quantomeno ridurre, anche attraverso un'efficace cooperazione a livello globale.
Lo sviluppo tecnologico ha contribuito al passaggio dai *computer crimes* ai *cybercrimes.* Ad oggi, infatti, possiamo distinguere due categorie di reati informatici: da una parte i reati informatici in senso stretto (*computer crimes*), che richiamano espressamente nella loro fattispecie legale le TIC, in quanto si tratta di fatti nuovi emersi solo dopo la diffusione delle nuove tecnologie; dell'altra parte, i reati informatici in senso ampio (*cybercrimes*), cioè quei reati diversi che riguardano forme di aggressione già tutelate dall'ordinamento ma che ora possono comunque essere commessi a danno o per il tramite di un sistema informatico[23].

[23] L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Tutela penale della persona e nuove tecnologie, CEDAM, Padova, 2013, p. 55: Distinguiamo fra reati informatici "in

Nella prima ipotesi il reato può essere commesso esclusivamente utilizzando computer, reti informatiche o altre forme di tecnologia, perché senza Internet non potrebbe dirsi commesso il reato e risulta perciò necessario coinvolgere lo strumento informatico.
Nella seconda categoria, quella dei reati informatici in senso ampio, invece, affinché la fattispecie di reato possa dirsi consumata, non è indispensabile l'accesso alla rete informatica, essendo questo un elemento solo alternativo alla possibilità di commettere il reato nelle forme tradizionali[24]. Questi ultimi sono solo agevolati dall'informatica, nel senso che lo strumento informatico diviene un mezzo di esecuzione privilegiata ma sono reati che possono essere commessi sia *online* che *offline*. Il ruolo svolto da Internet è quello di aumentare la portata geografica e la velocità di questi crimini, fornendo ai potenziali delinquenti un ambiente in cui possono operare con un maggiore livello di sicurezza e anonimato.

Chi si approccia per la prima volta a questa materia potrebbe allora ritenere che, considerando le Tecnologie dell'Informazione e della Comunicazione quale mero strumento di ausilio per la commissione del reato, ciò che conta ai fini della realizzazione della fattispecie delittuosa sia il verificarsi dell'evento giuridico, potendo questo aversi indifferentemente con l'utilizzo dei mezzi tradizionali piuttosto che con strumenti informatici. Tuttavia, questa visione neutrale delle moderne TIC nel contesto dei reati cibernetici [25] è stata messa in discussione da diversi studiosi. Ragionevolmente è

---

senso stretto", vale a dire «fattispecie legali che presentano, sul piano della definizione normativa, elementi di tipizzazione descrittivi di modalità, oggetti, attività, specificamente caratterizzati dalla o frutto della tecnologia informatica, vale a dire relativi o connessi a procedimenti di elaborazione automatizzata di dati secondo un programma, come sono per esempio l'accesso abusivo a un sistema informatico (art. 615-ter c.p.) o la frode informatica (art. 640-ter c.p.)», e reati informatici "in senso lato", ossia «tutte quelle fattispecie che pur non presentando elementi di tipicità del fatto così caratterizzati sul piano tecnico, tuttavia possono includere, nei casi concreti, le predette modalità, attività, oggetti, per l'ampiezza o elasticità dei requisiti costitutivi richiesti dal legislatore, suscettibili d'interpretazione e applicazione evolutiva».
Oppure R. BORRUSO, *La tutela dei documenti e dei dati,* in *Profili penali dell'informatica,* p. 1, distingue tra reati commessi sul computer (reati informatici in senso stretto) e reati commessi a mezzo del computer (reati informatici in senso lato): «I primi sono da considerarsi reati informatici propri perché l'evento non potrebbe mai verificarsi senza il computer; i secondi, invece, sono da qualificarsi reati informatici impropri perché l'evento avrebbe potuto, almeno in astratto, essere provocato anche senza ricorrere all'uso del computer che, pertanto, si configura soltanto come una delle possibili modalità della condotta criminosa».
[24] Il delitto di diffamazione può ad esempio essere commesso anche tramite Internet, ivi pubblicando contenuti offensivi; in ogni caso, il diritto penale sempre diffamazione la qualifica, sia che l'offesa reputazionale sia pubblicata sul giornale cartaceo sia che la si possa leggere sul *social network*.
[25] Per tali intendendosi i reati che «si realizzano o si possono realizzare, in tutto o in parte, nel *Cyberspace*, e che caratterizzano dunque la dimensione attuale della criminalità informatica, abbracciando entrambe le

opportuno considerare le TIC come parte integrante del contesto in cui si sviluppano i reati cibernetici, e questo perché si tratta di tecnologie che, per le caratteristiche che presentano, possono influenzare sia la commissione che la prevenzione dei crimini. Pensiamo solo al fatto che grazie alle TIC i criminali godono di vantaggi quali l'anonimato, la possibilità di agire a distanza e la possibilità di accedere ad un'inimmaginabile quantità di informazioni sensibili. Inoltre, sempre per merito delle TIC, i reati cibernetici sono più rapidi e diffusi rispetto ai tradizionali crimini fisici, proprio perché le informazioni riescono a circolare attraverso Internet in modo più veloce e ampio. In altre parole, grazie ad Internet si sono diffuse nuove modalità di attuazione delle condotte delittuose che già si conoscevano, ma che ora possono portare a risultati anche più tragici. Pertanto, le TIC non possono essere considerate solo strumenti alternativi o di supporto per la commissione del reato, ma svolgono propriamente un ruolo attivo nel favorire tali comportamenti illeciti. Le dinamiche e le modalità dei reati *online* sono diverse da quelle dei reati tradizionali (pensiamo semplicemente al fatto che i comportamenti tenuti *online* sono spesso caratterizzati dalla capacità di aggirare i confini geografici e temporali e che le modalità di commissione possono implicare alterazioni dell'identità digitale, creazione e diffusione di contenuti illegali, sfruttamento di vulnerabilità tecniche); inoltre, cambiando il tipo criminologico d'autore, gli elementi del fatto tipico e dell'evento giuridico, richiedono un approccio nuovo per una comprensione più adeguata del fenomeno[26]. Semplificare i reati informatici equiparandoli a forme tradizionali di reati non permetterebbe di tener conto delle peculiarità e della complessità della realtà digitale.

Se ne deduce allora che l'incidenza della criminalità cibernetica non possa essere limitata ad un numero chiuso e definito di reati specifici, coinvolgendo all'opposto una vasta gamma di comportamenti che coinvolgono l'uso di mezzi informatici. Questa si evolve costantemente includendo una vasta gamma di crimini e modalità di violazione dei diritti e interessi di soggetti terzi. Alcuni di questi reati sono nuovi, derivati dallo sviluppo stesso

predette categorie dei reati informatici in senso stretto e in senso lato, sotto il comune requisito della commissione "in rete" di tutto o parte del fatto di reato, bastando che i relativi elementi costitutivi siano compatibili con detta realizzazione, almeno in parte, nel Cyberspace.» Così L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, cit., p.55.

[26] T. PIETRELLA, *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive*, cit., p. 32: «Ridurre la fenomenologia dei comportamenti devianti *online* a forme alternative di reati "tradizionali" equivale ad interpretare nuove realtà con schemi anacronistici».

della tecnologia, e vanno oltre i limiti dei reati tradizionali includendo attività come l'elaborazione, la comunicazione, la trasmissione e il trattamento di dati, informazioni e contenuti digitali su Internet.

La criminalità informatica, quindi, presenta una sfida continua per la legge e le autorità competenti, in quanto si adatta e si evolve insieme alla tecnologia stessa, comprendendo sempre nuove modalità operative lesive di interessi di altri. Queste nuove forme di aggressioni comportano la lesione di beni giuridici diversificati, tra cui il patrimonio, la fede pubblica, il domicilio, e al tempo stesso fanno emergere nuovi interessi meritevoli di protezione da parte dell'ordinamento (prima fra tutti la riservatezza informatica, quale spazio esclusivo e libero da intrusioni illegittime[27]). Ovviamente, all'espansione dei beni giuridici meritevoli di protezione penale consegue anche l'aumento delle potenziali vittime, titolari di questi nuovi beni.

Comprendere l'impatto delle tecnologie e di Internet sulla società e sull'individuo consente di valutare e regolare adeguatamente le azioni che si svolgono all'interno di questi contesti digitali. Le tecnologie in continua evoluzione e la struttura di Internet possono influenzare l'agire delle persone, determinando comportamenti non previsti o già affrontati dal sistema giuridico esistente. Allo stesso modo, le modalità di sviluppo delle tecnologie possono contribuire a creare situazioni in cui azioni o eventi possono verificarsi in modo difforme rispetto al passato (ad esempio, la diffusione di dispositivi mobili e l'accesso costante a Internet possono permettere di organizzare proteste o manifestazioni in modo più rapido ed efficace rispetto ai metodi tradizionali).

In generale, la pervasività delle TIC ha trasformato la nostra concezione di tempo e spazio: grazie ad Internet le informazioni sono accessibili in qualsiasi momento e da qualsiasi luogo, rendendo possibile una comunicazione istantanea e globale.

Tutto ciò richiede una riflessione sul modo in cui il sistema giuridico può affrontare queste sfide e regolare tali situazioni in modo adeguato, dovendo essere in grado di affrontare la velocità con cui si diffondono i reati digitali. Il legislatore può intervenire creando nuove leggi o adattando quelle esistenti al fine di tener conto dei cambiamenti sul piano tecnologico e sociale, e i giudici possono interpretare le leggi esistenti in modo progressista per affrontare le nuove sfide poste dalle tecnologie e da Internet e riuscire

[27] V. meglio cap. 2.

quindi ad integrare nel panorama giuridico le recenti forme di illeciti. Inoltre, l'adozione di sanzioni adeguate è fondamentale per garantire la protezione dei diritti e degli interessi delle persone coinvolte in queste situazioni, riferendosi sia al campo penale per quanto concerne la prevenzione e la repressione dei reati informatici, sia al settore civile in riferimento al risarcimento dei possibili danni causati da azioni *online*.

2.1. *Il locus commissi delicti*

Riuscire a collocare con precisione il reato nello spazio e nel tempo è operazione indispensabile al fine della determinazione della responsabilità penale del soggetto agente, questione che oltretutto presenta ripercussioni in tema di prescrizione del reato, successione delle leggi nel tempo ed individuazione del giudice territorialmente competente (tale è, in linea di principio, il giudice del luogo in cui il reato si è consumato). Tuttavia, determinare il luogo in cui viene commesso un reato informatico è un problema assai complesso, avendo in questo settore a che fare con condotte ed eventi che coinvolgono impulsi elettronici che si diffondono su piattaforme immateriali accessibili da chiunque e dovunque. L'idoneità dei dispositivi elettronici ad eseguire funzioni automatizzate è proprio il fattore che consente al fatto di reato di continuare a manifestare i suoi effetti nel tempo, garantendo una protratta circolazione dei dati che incide sul momento in cui poter ritenere il reato consumato: una volta avviato un processo automatizzato, gli effetti innescati per il tramite delle tecnologie possono continuare a ripercuotersi nel tempo senza bisogno di ulteriori azioni da parte del soggetto agente[28]. Tale fenomeno di prolungata persistenza degli effetti evidenzia la difficoltà per gli utenti di continuare a mantenere un effettivo controllo sulle proprie azioni *online*[29].

---

[28] R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applictive*, in *Cybercrime*, Milano, 2023, pp. 165-166: «Le stesse caratteristiche tecniche dell'automazione, infatti, investono anche la circolazione, messa a disposizione, nonché permanenza dei dati e dei contenuti nel *cyberspace*, e sembrano imporre la riconsiderazione delle condizioni alla cui stregua stabilire e circoscrivere il momento della consumazione del reato».

[29] L. PICOTTI, *Reati informatici, riservatezza e identità digitale*, report presentato al VII Convegno Nazionale dei Professori di Diritto Penale sul tema "Il diritto penale tra recenti modifiche e progetti di riforma", Torino, 2018: «è il fatto tipico che, nella parte in cui si realizza tramite i sistemi informatici, si deve ritenere che si protragga, espanda ed eventualmente "riproduca" in quei suoi elementi essenziali, che dipendono dall'esecuzione delle funzioni automatizzate (di memorizzazione, trasmissione, messa a

Lo spazio cibernetico si manifesta quale sistema dinamico, caratterizzato da una dimensione di dematerializzazione e atemporalità; con la conseguenza che questi attributi rendono maggiormente difficoltosa la gestione delle relazioni tra i soggetti che agiscono per il tramite di Internet. Queste caratteristiche sono infatti tali per cui creare un parallelismo tra le condotte che si tengono *online* e quelle che si esplicano *offline* non è così semplice. Difatti, essendo le condotte dei cybercriminali caratterizzate da ubiquità – avendo cioè, gli autori di reati informatici, la possibilità di agire collocandosi in più luoghi virtuali simultaneamente (non essendo più necessario un contatto diretto tra il soggetto agente e il computer) – le azioni che si svolgono nella realtà virtuale sono private della loro specificità spaziale e temporale.

L'azione penalmente rilevante si traduce nella realtà virtuale in impulsi elettronici: l'uomo, consapevolmente e volontariamente, invia un *input* al computer che poi procede automaticamente alle operazioni di codificazione, decodificazione, memorizzazione o trasmissione di informazioni. Tenere comportamenti illeciti *online* comporta un certo distanziamento dagli accadimenti fisici esterni, per cui risulta più difficile riuscire a delimitarli e circoscriverli geograficamente, a causa proprio della possibilità che offre Internet di agire da remoto.

In un ambiente come questo, privo di concreti e tangibili confini spaziali, emerge come un problema l'identificazione del *locus commissi delicti,* in applicazione del criterio di territorialità che richiede di determinare il luogo in cui viene realizzata la condotta[30].

---

disposizione, condivisione, circolazione, ricerca, ecc.), pur non sempre del tutto "dominabili" dai titolari, gestori e fruitori dei sistemi stessi».

[30] Cass. pen., Sez. Un., 26.03-24.04.2015, n. 17325: «nel *cyberspace* i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio). Pertanto non è sempre agevole individuare con certezza una sfera spaziale suscettibile di tutela in un sistema telematico, che opera e si connette ad altri terminali mediante reti e protocolli di comunicazione».

«Occorre porre a raffronto due elementari constatazioni: la prima è che Internet ignora i confini territoriali e, dunque, la territorialità degli ordinamenti giuridici; la seconda è che gli ordinamenti giuridici necessitano invece di uno spazio sul quale esercitare la propria sovranità esclusiva e ulteriormente tendono ad allargare i propri confini applicativi sulla base di valutazioni legate alla qualità del soggetto attivo o del soggetto passivo o alla natura del reato commesso». Così S. SEMINARA, *Locus commissi delicti, giurisdizione e competenza nel cyberspazio*, relazione al Convegno "Presi nella rete - Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012, p.1.

Il legislatore italiano per identificare quando il reato possa dirsi commesso nel territorio dello Stato adotta il principio di territorialità, sulla base del quale si applica la legge italiana sia che sul territorio dello Stato italiano sia avvenuta, in tutto o in parte, l'azione (o l'omissione), sia che in Italia si sia verificato l'evento[31]. Risulta allora sufficiente, perché trovi applicazione la legge italiana, che nel territorio dello Stato si sia realizzato anche un solo atto dell'*iter* criminoso.

Nel contesto della realtà cibernetica, il concetto di azione penalmente rilevante acquisisce nuove e diverse sfumature, poiché non si tratta più di azioni fisiche con effetti percepibili concretamente nell'ambiente in cui si realizzano, ma, anzi, la criminalità informatica concerne l'inserimento e la trasmissione di dati attraverso impulsi elettronici. Questo per l'appunto implica la detemporalizzazione delle attività e la deterritorializzazione dell'autore del reato, cioè la possibilità per il soggetto agente di programmare in anticipo le operazioni che si svolgeranno in modo automatizzato per il tramite del computer: gli effetti di un'azione criminosa possono dunque ripercuotersi in un luogo e momento diverso da quello in cui la condotta del reo è stata posta in essere. La situazione è inoltre aggravata anche dalla circostanza per cui ci sono soggetti professionisti in grado di mascherare il proprio indirizzo IP[32]. Gli utenti infatti non risiedono nel cyberspazio ma vi accedono ed escono a proprio piacimento, per cui, data la natura altamente dinamica del cyberspazio (come la possibilità di creare e pubblicare un sito web e successivamente rimuoverlo molto rapidamente), risulta molto complicata l'identificazione del luogo in cui vengono commessi i reati *online*. In questo senso possiamo dire che il cyberspazio offre ai criminali la possibilità di fuggire e superare le limitazioni geografiche e temporali convenzionali.

Per una corretta collocazione nello spazio dell'illecito compiuto *online*, è necessario tener conto delle descritte peculiarità della criminalità informatica, adottando criteri maggiormente flessibili che vadano ad integrare il principio di territorialità tradizionalmente inteso. I concetti di azione e di evento perdono infatti di concretezza

---

[31] Art. 6, co. 2 c.p.: «Il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione». Si v. G. FIANDACA – E. MUSCO, *Diritto penale. Parte generale*, Bologna, VIII edizione 2019, Zanichelli editore, pp. 145-146.

[32] L'indirizzo IP (*Internet Protocol*) è una serie di quattro numeri, ciascuno dei quali può andare da 0 a 255, assegnato matematicamente per identificare univocamente un dispositivo che si connette ad Internet ed ivi comunica con altri dispositivi.

quando si manifestano *online*, poiché l'utente realizza la condotta illecita mediante l'esecuzione automatica da parte del dispositivo di attività ulteriori, quale la trasmissione di dati che poi circolano in una Rete di comunicazione telematica e che sono contemporaneamente consultabili da più utenti situati in posti diversi. Potrebbero allora sopperire ai limiti che il principio di territorialità riscontra nel *cyberspace* il principio di personalità attiva e passiva: per individuare un qualche collegamento tangibile tra i soggetti partecipanti il reato e la dimensione immateriale in cui questo viene posto in essere, si potrebbe attribuire rilevanza rispettivamente alla nazionalità del reo (indipendentemente dal luogo in cui è commesso il reato) o agli interessi offesi (per cui la legge italiana troverebbe applicazione a fatti commessi da uno straniero all'estero ma a danno dello Stato italiano) [33].

In conclusione, lo sviluppo delle tecnologie informatiche ha cambiato le dinamiche sociali e relazionali e, di conseguenza, anche il modo di intendere le nozioni tradizionali di spazio e di tempo, le quali devono essere rilette alla luce del contesto attuale e conformemente al progresso scientifico e tecnologico, per riuscire ad inquadrare correttamente i confini dei reati commessi nel *cyberspace*. Tuttavia, finora la problematica è stata affrontata solo a livello casistico, fornendo – il legislatore e i giudici – soluzioni pratiche sul piano ermeneutico applicabili alle singole fattispecie analizzate, ma non estendibili alla teoria generale del reato[34]. La disciplina attinente al luogo di consumazione del reato pone dunque sfide complesse da affrontare, ma il cui studio, nella odierna società di Internet, oramai non può più essere rimandato.

2.2. *Il ruolo degli utenti di Internet*

È opportuno ribadire quanto i computer siano diventati parte integrante di ogni aspetto della quotidianità. Oggigiorno si fa affidamento sulle tecnologie per la maggior parte delle

[33] Tale soluzione è stata fatta propria dalla Francia, che, all'art. 113-2-1 del *Code pénal*, individua nel territorio francese il *locus commissi delicti* dei reati commessi per mezzo di una rete di comunicazione elettronica a danno di una persona fisica residente (o di una persona giuridica la cui sede sia situata) nel territorio della Repubblica: «*Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République*».

[34] Per il caso dell'accesso abusivo a sistemi informatici o telematici si veda cap. 2, par. 8.

attività e alla base del funzionamento della società vi sono le infrastrutture digitali. L'uso continuo di Internet, combinato con la ricchezza di informazioni personali che vengono messe *online*, ha generato un nuovo tipo di criminale. Gli studiosi pacificamente riconoscono come il cyberspazio sia un luogo di criminalità attiva, un luogo che ha cambiato la portata del delitto e della vittimizzazione. In questo mondo virtuale caratterizzato da un continuo scambio di notizie e da questa perenne connessione tra utenti, questi ultimi finiscono con l'essere nuove vittime e nuovi autori di reati. L'anonimato e la distanza fisica offerti dalla Rete possono facilitare la disumanizzazione degli altri e consentire comportamenti criminosi che devono essere ripensati a partire dalla natura stessa del crimine. L'anonimato, e quindi l'uso di pseudonimi o *account* falsi, permette alle persone di nascondere la propria identità *online*, rendendo più facile commettere atti criminali senza soccombere al senso di responsabilità che si potrebbe avere nella vita reale. Questo anonimato può, cioè, portare ad una deumanizzazione, fenomeno per mezzo del quale le persone si sentono distaccate dalle conseguenze delle loro azioni ed attuano condotte disumane o insensibili, non riconoscendo l'umanità propria del soggetto vittima[35]. Probabilmente il fenomeno della criminalità informatica è agevolato dal fatto che Internet priva le persone *online* della loro fisicità e sembra accentuare la distinzione del confine tra mondo virtuale e reale. Questo aspetto può consentire ai criminali di causare danni di maggiore portata e in tempi più brevi, sfruttando l'assenza della normale sensazione multisensoriale tipica degli incontri che si svolgono interfaccia nella realtà.

Risulta quindi opportuno, se non necessario, analizzare i comportamenti degli utenti *online* per comprendere in maniera esaustiva l'estensione che presenta la criminalità virtuale, considerando che, dopotutto, nonostante la comunicazione avvenga in un contesto smaterializzato, ci sono ancora esseri umani dietro gli schermi dei computer che prendono la decisione di perpetrare atti malevoli *online*.

La virtualizzazione delle relazioni sociali introduce infatti un nuovo ed inedito schema nelle dinamiche interpersonali: in questo paradigma, la socialità si sviluppa attraverso l'interazione tra gli esseri umani e i dispositivi tecnologici. Le tecnologie e le piattaforme digitali forniscono agli individui strumenti per comunicare, interagire e stabilire

[35] Si tratta di una tecnica di "disimpegno morale" volta a creare (false) giustificazioni per tenere comportamenti immorali che le persone, altrimenti, riconoscerebbero immediatamente come non etici ed ingiusti. Per una analisi più approfondita si veda C. VOLPATO, *Deumanizzazione. Come si legittima la violenza,* Roma-Bari, Editori Laterza, 2011.

connessioni con altre persone attraverso i loro dispositivi elettronici. Questo permette di superare le barriere spazio-temporali che limitano le interazioni nel mondo fisico, consentendo alle persone di connettersi con individui distanti geograficamente o di diverse culture e lingue. La comunicazione mediata dalla tecnologia è diventata una parte integrante della vita quotidiana. Le piattaforme dei s*ocial media* come Facebook, Instagram o Twitter creano spazi virtuali in cui le persone possono condividere pensieri, immagini, video e interagire con altre persone, e così facendo permettono ai loro utenti di creare una propria identità *online* e di costruire relazioni sociali attraverso i loro profili e le attività svolte *online*.

Di contro, alcuni sostengono che l'interazione *online* non riesca a fornire la stessa ricchezza di una comunicazione diretta "faccia a faccia", mancando segnali non verbali importanti come l'espressione facciale, i gesti o il tono della voce. Tali mancanze potrebbero portare a fraintendere o interpretare in modo errato le parole utilizzate e scambiate nel contesto digitale. Appare forse addirittura superfluo sottolineare come si risenta delle caratteristiche che contraddistinguono il mezzo di comunicazione: «*ipertestualità, ipermedialità, elevata velocità, sostanziale anonimato, giochi di identità, superamento dei normali vincoli spaziotemporali, parificazione dello status sociale, accesso a relazioni multiple, insorgenza di emozioni imprevedibili, anarchia e libertà di trasgressione*»[36]. La distanza emotiva emerge come elemento distintivo dell'agire *online*, dal momento che le interazioni in tale contesto tendono ad essere meno coinvolgenti rispetto a quelle *offline*, soprattutto in virtù dell'invisibilità di cui godono le persone. Questa caratteristica è ulteriormente accentuata dall'asincronicità delle conversazioni che si scambiano via *chat*, le quali non si conformano ai ritmi temporali della comunicazione diretta che si tiene nella realtà. A differenza dei dialoghi faccia a faccia, o delle chiamate

[36] T. CANTALEMI, San Paolo Edizioni, 2013, *Tecnoliquidità. La psicologia ai tempi di internet: la mente tecnoliquida*, p. 18: «Tutto viene consumato, "usato" e infine scartato: sia che si tratti di esperienze, di relazioni, amicizie, o di modi di essere e di presentarsi. ... Legami solidi, impegni o desideri di più ampio respiro, d'altronde, rischierebbero di rallentare i tempi di vita e potrebbero involontariamente condannare l'individuo a un destino di precoce inattualità, escludendolo dalle opportunità (lavorative e socio-affettive) che continuamente sembrano affacciarsi (per poi sparire velocemente all'aprirsi di una nuova offerta), chiedendo implicitamente di esser pronti a coglierle al volo e, dunque, sufficientemente svincolati e leggeri. Per meglio adattarsi al vivere è necessario essere sempre connessi e sempre equipaggiati, in modo da poter viaggiare in ogni direzione senza troppi rimpianti. Vi è poi un'ulteriore prova con cui deve confrontarsi l'abitante dello scenario tecnoliquido: la difficoltà di orientarsi nel flusso costante e magmatico delle informazioni, che gli si rendono man mano disponibili, prima ancora che questi le abbia cercate».

telefoniche, le *chat* permettono alle persone di inviare e ricevere messaggi in momenti diversi, facendo venir meno la necessità di una risposta immediata. La possibilità di riflettere sulle proprie parole e di ponderare il contenuto dei propri messaggi, accompagnata dalla facoltà di modificarli prima dell'invio, può portare ad una comunicazione sì più riflessiva e accurata, ma, a causa di questa mancanza di contestualità tra domanda e risposta, si perde la spontaneità e la fluidità delle interazioni, minando inevitabilmente la percezione di un legame emotivo.

Ecco che la fenomenologia che contraddistingue l'agire nell'ambiente *online* presenta connotati diversi dall'approccio che le persone hanno *offline*. L'interazione attraverso schermi e tastiere crea un'atmosfera di anonimato e distaccamento che può indurre le persone a manifestare comportamenti diversi rispetto a quelli adottati nella vita reale. La sfera digitale promuove una innegabile libertà di espressione, perché gli utenti possono sentirsi più liberi di dire ciò che pensano, esprimendosi con maggiore franchezza, senza la paura di essere giudicati o criticati direttamente. Questo condizione può portare, da un lato, a una maggiore apertura e sincerità, ma, dall'altro, a un aumento di comportamenti impulsivi e aggressivi. Le persone possono essere più propense ad esprimere opinioni forti o offensive senza subire le conseguenze reali delle loro azioni e, di conseguenza, adottando comportamenti negativi colorati di distorsioni e falsità. Il fatto di non percepire l'effetto concreto che le parole o le azioni *online* esercitano sugli altri può portare ad una insensibilità o mancanza di rispetto verso il prossimo.

Inoltre, l'interazione *online* può favorire la creazione di identità e personalità alternative, cioè i profili e le identità digitali possono essere diverse da quelle della vita reale. Questa opportunità di reinventarsi e di fuggire dalla realtà, favorendo magari la creazione di comunità di persone che condividono interessi o aspirazioni comuni, può incentivare comportamenti più audaci o esagerati. Gli individui, a fronte di questa separazione delle identità, non sperimentano inibizioni comportamentali nella stessa misura che si registra nei contesti *offline*, in parte anche a causa di un diminuito senso di vicinanza alla vittima che produce ridotti sensi di colpa e una minor paura di ritorsioni. Al fine di riuscire ad instaurare relazioni positive e significative, sia nel contesto *online* che in quello *offline*, è fondamentale comprendere e bilanciare l'uso delle piattaforme digitali nella vita sociale.

Le teorie criminologiche tradizionali si basano sulla confluenza di autori e vittime del reato nel tempo e nello spazio, ma nel cyberspazio il tempo e lo spazio non rilevano più come una volta. È possibile, infatti, pianificare un attacco che avvenga giorni o anni dopo, senza mai incontrare direttamente la vittima; non è nemmeno necessario essere nello stesso Paese, perché l'individuo può attaccare le vittime a distanza. I reati informatici presentano caratteristiche che divergono dalla criminalità tradizionale perché hanno scarsa aderenza alle restrizioni spazio-temporali. A causa della natura dinamica e non fisica dell'ambiente *online*, è difficile mappare i crimini informatici e prevedere quando e dove i trasgressori entreranno in contatto con obiettivi idonei.

Gli autori di crimini informatici sono quindi coloro che hanno elevate competenze in ambito informatico, capaci di conoscere e analizzare il funzionamento delle reti informatiche per poter individuare e sfruttare le vulnerabilità dei sistemi. Esaminare e capire il comportamento dei cybercriminali è fondamentale per sviluppare strategie di difesa efficaci per contrastare queste minacce crescenti. Dalle ricerche effettuate emerge che sono molteplici le motivazioni che possono spingere le persone a commettere crimini *online*, ed includono[37]:

a) Profilo economico: il desiderio di guadagno finanziario è uno dei principali fattori che incentiva i cybercriminali a commettere reati. Essi cercano di rubare password e informazioni personali, come dati di carte di credito o informazioni bancarie, per poterle vendere sul mercato nero e utilizzarle per commettere frodi finanziarie.
b) Vendetta o protesta politica: alcuni cybercriminali possono agire sulla base di motivi personali, politici o ideologici, prendendo di mira un'organizzazione o un governo.
c) Curiosità e sfida: alcuni individui potrebbero essere spinti dal desiderio di testare le proprie abilità e dimostrare di essere in grado di violare sistemi di sicurezza. Questa motivazione può essere alimentata dall'adrenalina e dalla ricerca di riconoscimento e notorietà; si tratta infatti spesso di delinquenti che tendono ad essere orgogliosi dei loro crimini e che, perciò, desiderano che gli altri sappiano che ne sono i responsabili.

[37] Vedi meglio M. ROTTIGNI, 2023, *Nella mente dei cyber criminali: le TTP che ogni professionista della sicurezza dovrebbe conoscere*: «Le TTP svolgono un ruolo essenziale per consentire ai difensori della sicurezza di contrastare efficacemente le minacce informatiche. Analizzando e comprendendo le TTP, i difensori ottengono informazioni preziose sui comportamenti e sulle metodologie utilizzate dagli avversari. Questo accelera il processo di identificazione dei potenziali attacchi, lo sviluppo di strategie di difesa proattive e l'implementazione di misure di sicurezza specifiche per i rischi aziendali e di settore».

d) Spionaggio industriale: i cybercriminali possono agire su commissione di aziende o governi interessati a rubare segreti commerciali o informazioni sensibili da competitori o avversari politici.
e) Terrorismo: i gruppi terroristici possono praticare attacchi informatici per danneggiare infrastrutture critiche, diffondere propaganda o ottenere informazioni strategiche. Di solito prendono di mira servizi statali e settori essenziali per massimizzare la distruzione e l'interruzione, destabilizzando un governo o un'organizzazione.

In questa prospettiva, risulta fondamentale soffermarsi sulla *Space Transition Theory of Cyber Crimes*[38], formulata da Jaishankar nel 2008. Essa presenta un approccio innovativo per comprendere i crimini informatici e fornisce una spiegazione su come la transizione dallo spazio fisico a quello virtuale abbia contribuito alla proliferazione dei crimini informatici, ampliando l'ambito di azione dei cybercriminali e permettendo loro di commettere atti illeciti su scala globale. L'autore di questa teoria sostiene che le persone si comportano diversamente quando si spostano da uno spazio all'altro (dallo spazio fisico al cyberspazio e viceversa). Coloro che, nello spazio fisico, reprimo tendenze criminali a causa del loro *status* e posizione sociale, nel cyberspazio mostrano una maggiore inclinazione a tenere comportamenti illeciti, che difficilmente mostrerebbero nello spazio fisico. In questa proposizione, Jaishankar prende in prestito i presupposti del modello di criminalità e *status* sociale di Arbak[39] e osserva che la tendenza degli individui ad inibire i propri comportamenti trova rilevanza solo nello spazio fisico. Apparentemente, infatti, uno dei fattori chiave che spinge la maggior parte dei membri della società a comportarsi in modo onesto e non violento è la paura di essere scoperti. Questa deterrenza, tuttavia, risulta attenuata nell'ambito digitale perché il cyberspazio consente agli aggressori di

[38] Cfr. K. JAISHANKAR, *Space Transition Theory of Cyber Crimes*, in F. SCHMALLEGER - M. PITTARO**,** *Crimes of the Internet*, Prentice Hall, 2008.
[39] Cfr. E. ARBAK, *Social Status and Crime*, 2005, mostra come gli individui provano diversi gradi di autorimprovero quando si impegnano in attività criminali perché a monte si preoccupano del loro *status* sociale, per cui, nel prendere le loro decisioni, valutano sia i rischi materiali che quelli sociali derivanti dall'essere un criminale piuttosto che un cittadino rispettoso della legge. In altre parole, nella vita reale il singolo tende generalmente ad anticipare le conseguenze negative, derivanti dal fatto di sostenere uno stile di vita criminale, e a valutare il loro impatto sul proprio *status* sociale; questo lo porta a percepire anticipatamente l'imbarazzo che ciò gli causerà, con la conseguenza di frenare i propri comportamenti devianti.

attaccare le loro vittime anche dalle località più remote, eliminando la necessità di una prossimità geografica. L'individuo è pertanto meno preoccupato del proprio *status* sociale perché si trova ad agire in un contesto in cui non può essere guardato e stigmatizzato direttamente. Ne discende che i criminali informatici percepiscono il rischio di essere scoperti dalle autorità come relativamente basso e le eventuali sanzioni meno intimidatorie. L'assenza di un'adeguata deterrenza, combinata ai fattori motivazionali, incoraggia gli individui a commettere crimini informatici. Non c'è più la paura di affrontare la vergogna sociale e l'umiliazione perché la vera identità rimane celata dietro la maschera del dispositivo informatico.

Una seria preoccupazione relativa al cyberspazio e legata al concetto di deindividuazione[40] è che non si può infatti mai sapere con certezza con chi si sta interagendo. Gli utenti possono adottare con facilità false identità (cc.dd. "falsi avatar") e continuare a chattare per giorni, persino mesi, prima che l'interlocutore scopra finalmente che la persona con cui sta comunicando non è chi afferma di essere. Le informazioni come lo *username*, la foto del profilo *social* e i dati personali forniti (come la data di nascita e il luogo di residenza) sono tutte indicazioni fornite direttamente dall'utilizzatore e difficilmente passibili di riscontri esterni da cui poter desumere la reale identità del soggetto con cui si interagisce. Nel cyberspazio non è possibile determinare con precisione l'identità e le informazioni fornite dalla persona al momento dell'accesso in Rete. L'identità digitale è allora dissociata dalla realtà perché non rispecchia l'identità della persona nella vita reale: l'identità digitale, in quanto rappresentazione virtualizzata che influenza la reputazione e le relazioni di una persona nel mondo reale, può essere manipolata, costruita e presentata in modo diverso rispetto all'identità reale di quella stessa persona[41].

Una teoria cui gli studiosi ancora si riferiscono, nonostante questo cambiamento di prospettiva nel mondo digitale, è la *Routine Activity Theory* (RAT), sviluppata da Lawrence Cohen e Marcus Felson nel 1979. Essi suggeriscono che la commissione di un

[40] La deindividuazione è un concetto della psicologia sociale e si riferisce ad un processo psicologico in cui alcuni fattori, riducendo l'identificabilità sociale e l'autoconsapevolezza dell'individuo all'interno di un gruppo, rendono possibili comportamenti che normalmente sono inibiti.

[41] Ad esempio, una persona potrebbe creare un profilo sui *social media* con un nome falso, utilizzare foto ritoccate o indicare informazioni fuorvianti di sé.

crimine dipenda da tre elementi: innanzitutto, la presenza di un delinquente motivato, ossia un individuo che vuole commettere un illecito o comunque arrecare danno; in secondo luogo, l'identificazione di un bersaglio adatto, nel senso che il potenziale autore del reato ha bisogno di una vittima e nell'ambiente *online* esistono ormai miliardi di possibili obiettivi, tutti accessibili senza doversi spostare fisicamente; terzo, l'assenza di controllo efficace, ovverosia la mancanza di fattori che potrebbero scoraggiare o prevenire il crimine, quindi qualcuno o qualcosa che possa impedire all'autore del reato di danneggiare la vittima (come un agente di polizia o un dispositivo di sicurezza). Secondo questa teoria, i criminali sono spinti a commettere reati in presenza di condizioni favorevoli, per cui la probabilità di commissione di un crimine aumenta quando le vittime sono vulnerabili e non riescono a proteggersi.

È possibile allora affermare che quanto maggiore è la presenza di un individuo su Internet e in un'ampia gamma di siti web, tanto aumentata è il rischio di vittimizzazione. La diffusione di Internet ha effettivamente aumentato la probabilità di divenire vittima di un reato *online*. Questo perché la presenza *online* comporta l'esposizione di informazioni personali, che per l'appunto possono essere utilizzate da malintenzionati per scopi illeciti[42]. Spesso i cybercriminali non scelgono una persona in particolare: la vittima viene selezionata perché ha risposto ad un annuncio o ad una e-mail; ha chattato con la persona sbagliata; visitato un sito e scaricato un malware. Gli utenti di Internet diventano cioè potenzialmente vulnerabili ad una molteplicità di attività criminali.

3. *Profilo normativo*

È emerso sotto diversi aspetti come la rivoluzione informatica abbia impattato profondamente sul diritto, richiedendo perciò un costante adeguamento delle norme e delle pratiche legali alle nuove sfide e opportunità emergenti nella società digitale.

[42] I ricercatori hanno dimostrato che la vittimizzazione delle molestie *online* dipende dalla quantità di tempo trascorso nelle *chat room* e impegnato nella messaggistica istantanea. Si veda sul punto l'articolo di T. J. HOLT e A. M. BOSSLER, *Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization.*

Fortemente avvertita è l'esigenza di armonizzare il sistema normativo per prevenire e reprimere i comportamenti illeciti tenuti nel *cyberspace*[43].

Il concetto di azione penalmente rilevante assume una nuova accezione, alla luce di questo mutato quadro socio-economico; di conseguenza, potrebbero non riuscire a trovare applicazione le regole tradizionali. Il legislatore penale si trova di fronte a sfide complesse, per fronteggiare le quali è necessaria l'elaborazione di norme adeguate a tutelare i cittadini dalle condotte criminali *online* e al contempo proteggere i sistemi informatici. Si tratta di emergenze collegate tra loro: per garantire la sicurezza dei cittadini e prevenire la commissione di reati *online* bisogna prima di tutto proteggere le infrastrutture digitali da attacchi esterni o da utilizzi impropri.

Innanzitutto, l'era digitale ha evidentemente portato alla necessità di regolare nuove questioni legali legate all'uso di Internet, come la protezione dei dati personali, la sicurezza informatica, la responsabilità degli intermediari *online* e la tutela della proprietà intellettuale. In generale, il lavoro del legislatore si è mosso su due direttrici strategiche: implementare nuove normative e revisionare le leggi esistenti per adattarle quanto più possibile alla realtà che cambia. In altre parole, da una parte si pone l'esigenza di individuare correttamente i nuovi reati informatici, creando norme specifiche per contrastare le condotte offensive; dall'altra parte si può raggiungere una tutela più completa andando altresì ad adattare i reati tradizionali al contesto digitale, ampliando il campo di applicazione delle norme esistenti per coprire anche queste nuove modalità di condotta.

In secondo luogo, come avuto modo già di dire, la rivoluzione informatica ha influenzato anche il modo in cui le persone vivono e interagiscono nella società, rendendo possibile lo sviluppo di nuove forme di comunicazione e di scambio di informazioni, come le piattaforme *social*, i servizi di messaggistica istantanea e le transazioni *online*. L'uso diffuso dei dispositivi mobili e dei *social network* ha portato a nuove dinamiche sociali e culturali che richiedono una riflessione giuridica, ad esempio riguardo all'intimidazione *online*, alla diffamazione digitale e all'etica nell'uso delle tecnologie. Lo sviluppo delle Tecnologie dell'Informazione e della Comunicazione ha infatti comportato un aumento

[43] L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme,* cit., p. 40: «ciò che è illecito *off line* non può essere lecito *on line,* o perché mediato o prodotto da sistemi di intelligenza artificiale, pur se si presenta in nuove ed inimmaginate modalità e forme».

della sorveglianza e della raccolta dei dati personali e, sotto questo profilo, sono sorte nuove sfide per il diritto in termini di diritti fondamentali, diritto alla privacy, libertà individuali, tutela dell'identità digitale e regolamentazione del commercio elettronico; parallelamente sono emersi nuovi diritti, come il diritto di accesso all'informazione, che mostra quanto sia importante avere accesso libero alle informazioni nell'ottica di una maggiore trasparenza e partecipazione democratica, e il diritto all'oblio digitale[44], che si riferisce alla possibilità di cancellare o rimuovere dati personali che non sono più rilevanti o che possono nuocere alla reputazione di un individuo. Si tratta di nuovi diritti che meritano e necessitano di protezione penale[45].

Un altro aspetto fondamentale è rappresentato dall'evoluzione delle tecnologie digitali nell'ambito della giustizia. La digitalizzazione dei procedimenti giudiziari ha permesso una maggiore efficienza e trasparenza del sistema legale, ma ha anche sollevato questioni relative all'accesso alla giustizia, alle garanzie processuali e alla sicurezza dei dati.

Insomma, soprattutto a seguito della rivoluzione tecnologica, che ha avuto riflessi decisivi sui rapporti sociali e giuridici, il diritto penale è cambiato negli ultimi cinquant'anni.

La criminalità informatica è un problema attuale e in peggioramento in tutto il mondo, ormai crimini che prima potevano compiersi localmente ora possono verificarsi a livello transfrontaliero e di conseguenza cambiano molte normative. Sono molti i reati informatici che si stanno diffondendo progressivamente e in maniera crescente, dalla pirateria informatica, al furto d'identità, a varie forme di frode finanziaria, ecc., grazie proprio, come suddetto, alla facilità con cui gli utenti hanno accesso alla Rete Internet.

La criminalità informatica rappresenta un problema di portata internazionale, che richiede sforzi legali per prevenire e fronteggiare questi comportamenti illeciti; si tratta, infatti, di attività illegali che costituiscono una minaccia per la società e risulta quindi fondamentale garantire ed accordare una protezione legale per tutelare i diritti delle persone coinvolte[46].

---

[44] Corte di Giustizia dell'Unione europea, sent. 13.05.2014 (C-131/12), caso *Google/Spain*.

[45] L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, cit., pp. 33-34: «Le nuove tecnologie» - viene ancora sottolineato - «determinano essenziali modificazioni e del tutto inedite possibilità d'intervento nella sfera dei diritti e interessi della persona, cambiando i modi di comportamento e i tipi di rapporto in cui essa viene coinvolta (…), per cui si delineano, da un lato, nuove e più specifiche esigenze di tutela e, dall'altro, originali ambiti di autonomia e di libertà della persona da salvaguardare rispetto all'intervento penale».

[46] Ad esempio, la diffusione di *fake news* può causare danni reputazionali a individui o organizzazioni, oltre a influenzare l'opinione pubblica in modo distorto. Pertanto, è necessario regolamentare la diffusione di informazioni false al fine di proteggere la reputazione e i diritti delle persone interessate.

È chiaro che qualsiasi sviluppo nell'uso della tecnologia da parte dei criminali deve essere coordinato e contrastato da una risposta del legislatore adeguata ed efficace: in questo contesto, la sfida non riguarda unicamente l'adattamento ai progressi tecnologici, ma anche il dovere di fronteggiare i nuovi reati emergenti e un panorama in continua evoluzione di minacce. Si richiede quindi al diritto una flessibilità e adattabilità tali da consentirgli di risultare adeguato allo sviluppo dei tempi, in modo da permettergli di continuare a svolgere la sua fondamentale funzione regolatrice[47].

Dal momento che i reati informatici che utilizzano le Tecnologie dell'Informazione e della Comunicazione sono dilaganti in misura preoccupante, ed essendo questi una seria minaccia per la sicurezza delle informazioni e per la privacy dei cittadini, sorge il problema di analizzare l'efficacia delle misure adottate dalla legislazione per prevenirli o affrontarli. L'interrogativo si giustifica poiché la criminalità informatica, in quanto ambito criminale relativamente nuovo, pone numerose sfide. Determinare chi c'è dietro un attacco e dove si trova a livello globale è particolarmente impegnativo, soprattutto perché molti aspetti della criminalità informatica si stanno sviluppando di recente e in breve tempo, richiedendo norme specifiche, conoscenze specialistiche e l'utilizzo di tecniche investigative all'avanguardia.

È fondamentale, dunque, che le misure adottate per prevenire e affrontare i reati informatici siano rafforzate e riviste costantemente. Le nuove tecnologie progressivamente introdotte comportano nuove sfide e metodi di attacco, per cui è imprescindibile che la legislazione si adatti ai cambiamenti tecnologici in corso. È pertanto necessario adottare un approccio innovativo e flessibile alla disciplina penale, riconoscendo che le attività illecite che si svolgono nel cyberspazio presentano caratteristiche uniche e complesse. Non è sufficiente estendere o adattare le norme vigenti e le categorie dogmatiche tradizionali, poiché queste potrebbero non essere adeguate a coprire i nuovi fenomeni emergenti essendo state concepite per contesti differenti. Il rischio, altrimenti, potrebbe essere quello di far emergere ambiguità ed incertezze legali che porterebbero a lacune legislative e a difficoltà nel perseguire i responsabili di tali crimini. Per garantire una tutela efficace dei diritti e degli interessi globali, è

[47] MENSI - FALLETTA, *Il diritto del Web*, II ed., Padova, 2018, p. 61: La disciplina giuridica della rete «si pone come una sorta di banco di prova per il diritto, che si confronta con l'ineludibile necessità di adottare istituti adeguati alle peculiarità di un fenomeno ormai non più nuovo, ma dalla sconvolgente portata eversiva».

indispensabile stabilire sistemi armonizzati di incriminazione dettagliandone già le relative sanzioni. Auspicabile sarebbe una cooperazione internazionale sempre più forte, che coinvolga non solo gli Stati, ma anche l'industria e le varie parti interessate, compresi gli enti e le associazioni che rappresentano gli interessi collettivi e diffusi. Come avremo modo di vedere meglio nei paragrafi che seguono, l'Unione Europea in questo senso ha avuto un ruolo importante nella promozione di una normativa comune per contrastare i reati informatici, incentivando la collaborazione tra i Paesi membri e armonizzando le legislazioni nazionali.

In conclusione, è necessario comprendere la complessità e l'importanza delle tecnologie stesse nel contesto di tali delitti, perché solo prendendo in considerazione il ruolo attivo delle TIC e sviluppando strategie di prevenzione adeguate, sarà possibile affrontare in modo efficace la sfida che i reati cibernetici pongono per la società odierna. Solo acquisire seria consapevolezza dell'impatto delle tecnologie e di Internet sugli individui e sulla società consentirà di contestualizzare adeguatamente i fatti storici e di adottare le misure giuridiche appropriate per affrontare le sfide e le opportunità che queste nuove realtà presentano.

La disciplina penale deve adattarsi alle sfide del cyberspazio e ai suoi rapporti complessi al fine di affrontare le minacce del mondo digitale in modo adeguato, superando un approccio conservatore che non tenga conto delle peculiarità e delle nuove dinamiche che si sviluppano *online*. In questo contesto smaterializzato diventa pertanto essenziale riconsiderare e aggiornare alcune categorie della giustizia penale, definendo in modo chiaro i nuovi reati digitali e stabilendo per essi le relative pene[48].

3.1. *La Legge n. 547 del 23.12.1993*

Prima di procedere all'analisi della normativa italiana vigente in materia di reati informatici, occorre considerare quello che era il contesto generale che ha portato all'intervento del nostro legislatore.

[48] «Le moderne tecnologie» hanno, in una certa misura, "messo in crisi" il diritto penale classico ponendolo di fronte alla «necessità di dare una risposta adeguata alle sfide della modernità.» V. PLANTAMURA, *Moderne tecnologie, riservatezza e sistema penale: quali equilibri?*, in *Il diritto dell'informazione e dell'informatica*, 2006, p. 417.

A livello internazionale, i primi interventi volti a contrastare gli usi illeciti dello strumento informatico si registrano a partire dagli anni '80 del secolo scorso. I primi a dotarsi di una legge penale sull'informatica sono gli Stati Uniti con il *Counterfeit Access Device and Computer Fraud and Abuse Act* del 1984, poi integrato e sostituito dal *Computer Fraud and Abuse Act* del 1986; segue poi la Danimarca, con la legge n. 229 del 6 giugno 1985; la Norvegia, con la legge n. 54 del 12 giugno 1987; l'Austria, con la legge n. 605 del 1987; la Francia, con la *Loi n. 18-19 relative à la fraude informatique*; la Grecia, con la legge n. 1805 del 30 agosto 1988; la Gran Bretagna, con il *Computer Misuse Act* del 1990.
In ambito europeo si è manifestata l'esigenza di stabilire un quadro normativo armonizzato cui far riferimento per regolare la crescente diffusione della criminalità informatica. L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) si è attivata in questo senso a partire dagli anni '80, interrogandosi sulla possibilità di applicare le leggi penali a livello internazionale e nel 1986 ha pubblicato la relazione "*Computer-Related Crime: Analysis of Legal Policy*", in cui esamina la normativa esistente e avanza proposte di riforma per contrastare l'emergente forma di criminalità.
In questo contesto il Consiglio d'Europa ha svolto un ruolo fondamentale, incentivando ripetutamente il perseguimento di una politica legislativa comune per garantire una migliore e più stretta collaborazione tra i diversi Paesi nella lotta alla criminalità informatica. La Raccomandazione del Comitato dei Ministri del Consiglio d'Europa n. R (89) 9 «*sur la criminalité en relation avec l'ordinateur*» del 13.09.1989[49] è stata un punto di riferimento in materia, anche per il legislatore italiano, in quanto riconosce immediatamente l'importanza di trovare una risposta rapida e adeguata alle nuove sfide che pone la criminalità informatica, considerando anche che questa spesso presenta carattere transfrontaliero[50]. La raccomandazione in questione – partendo dall'assunto che, a causa della natura immateriale con cui si manifestano queste nuove condotte, potrebbe

[49] La Raccomandazione e il seguente rapporto possono essere visionati su www.oas.org/juridico/english/89-9&final%20report.pdf. La prefazione è chiara nel sottolineare che «*The computer revolution hash had -and continues to have- a profound impact on the social, political and financial institutions of almost every nation in the world… But the computer revolution has also spawned new forms of abuses and crime… it is important that governments take the necessary steps to agree on a coherent attitude towards computer criminals. The Council of Europe report constitutes an essential contribution to that fight. It is warmly recommended for further study*».

[50] Le raccomandazioni sono atti non vincolanti e come tali consentono alle istituzioni europee di rendere note le loro posizioni suggerendo altresì linee di azione, ma non impongono obblighi giuridici a carico dei destinatari.

essere difficile individuare chiaramente il confine tra ciò che è meritevole di tutela legale e ciò che non la richiede – distingue le fattispecie di reato in due liste di comportamenti criminali al fine di fornire maggiore chiarezza.

La prima lista, c.d. lista minima (*minimum list*), ricomprende quei reati che, per le caratteristiche di pericolosità con cui si manifestano, devono essere perseguiti penalmente in tutti gli Stati membri, non configurandosi come sufficiente a reprimerli la sola sanzione civile o amministrativa. Troviamo qui la frode informatica[51], il falso in documenti informatici[52], il danneggiamento di dati o programmi[53], il sabotaggio informatico[54], l'accesso abusivo ad un sistema informatico o ad una rete informatica violando delle misure di sicurezza, l'intercettazione non autorizzata[55] e la riproduzione non autorizzata di programmi protetti (comprensiva anche della diffusione o comunicazione al pubblico di tale programma) e di topografie protette dalla legge.

Nella seconda lista, c.d. lista facoltativa (*optional list*), vengono elencate quelle condotte criminose per le quali la possibilità di prevedere la sanzione penale è rimessa alla discrezionalità degli Stati; presentando, cioè, questi illeciti una minor gravità, l'incriminazione della condotta è solo eventuale. Rientrano in questa lista l'alterazione non autorizzata di informazioni o programmi informatici (se non costituisce già danneggiamento), lo spionaggio informatico[56], l'utilizzo non autorizzato di un

[51] «Introduzione, alterazione, cancellazione o soppressione di dati o programmi informatici o in qualsiasi altra interferenza con un procedimento di elaborazione di dati che influisca sul risultato del trattamento dei dati, cagionando ad altri un pregiudizio economico o materiale, al fine di procurare a sé o ad altri un ingiusto profitto».

[52] «Introduzione, alterazione, cancellazione o soppressione di dati o programmi informatici o qualsiasi altra interferenza in un procedimento di elaborazione di dati, in maniera o in condizione tale che, in base al diritto nazionale, sarebbe stato integrato un reato di falso se fosse stato commesso rispetto ad un oggetto tradizionale».

[53] «Cancellazione, danneggiamento, deterioramento o soppressione di dati o programmi informatici senza diritto».

[54] «Introduzione, alterazione, cancellazione o soppressione di dati o programmi informatici, ovvero interferenza in un sistema informatico, con l'intento di ostacolare il funzionamento di un sistema informatico o di telecomunicazione».

[55] «L'intercettazione, effettuata senza diritto e con l'impiego di mezzi tecnici, di comunicazioni provenienti da e all'interno di un sistema o di una rete informatica».

[56] «L'acquisizione attraverso mezzi illeciti ovvero la divulgazione, il trasferimento o l'utilizzo di un segreto commerciale o industriale senza diritto e senza alcuna giustificazione legale, con l'intento di cagionare un pregiudizio economico al titolare del segreto o di ottenere per sé o per altri un ingiusto profitto».

elaboratore o di una rete di elaboratori[57] e l'utilizzo non autorizzato di un programma informatico protetto[58].
Le due liste sono state poi unificate nel 1990, in occasione del XV Congresso dell'Associazione Internazionale di Diritto Penale, alla luce della sorta esigenza di perseguire non esclusivamente i reati previsti dalla lista minima ma anche i comportamenti descritti nella lista facoltativa. Successivamente, nel settembre 1994, il Consiglio d'Europa ha integrato la sua precedente Raccomandazione, inserendo il commercio di codici di accesso ottenuti illegalmente e la diffusione di virus e *malware*.

Il 4 gennaio 1989 il Ministro di Grazia e Giustizia Giuliano Vassalli nomina una Commissione – composta da magistrati, professori universitari ed un esperto di informatica, presieduta dal Direttore generale degli Affari penali del Ministero (Pietro Callà) – cui viene affidato il compito di predisporre uno schema di disegno di legge per modificare le disposizioni del codice penale e del codice di procedura penale, al fine di estenderne la portata fino a coinvolgere i nuovi reati informatici. La Commissione, dopo aver svolto diverse audizioni con aziende pubbliche e private per accertare le modalità di commissione dei reati commessi a loro danno per il tramite di strumenti informatici, consegna la relazione conclusiva a fine dicembre 1990, e viene presentato il testo del disegno di legge al Senato il 26 marzo 1993. Questo iter culmina con l'emanazione della Legge n. 547 del 23.12.1993 recante "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*".

Prima di detta legge il legislatore era intervenuto solo sporadicamente sulla materia dei reati informatici e con interventi oltretutto settoriali. Con la legge n. 191 del 1978 (*Conversione in legge, con modificazioni, del decreto-legge 21 marzo 1978, n. 59, concernente norme penali e processuali per la prevenzione e la repressione di gravi reati*) era stato introdotto nel codice penale l'art. 420 che, nel sanzionare l'attentato ad impianti

[57] Rientra qui l'ipotesi in cui «viene effettuato accettando un rischio significativo di cagionare una perdita al legittimo utente del sistema o di danneggiare il sistema o il suo funzionamento; oppure effettuato con l'intenzione di cagionare un pregiudizio al legittimo utente del sistema o di danneggiare il sistema o il suo funzionamento; oppure cagioni di fatto un pregiudizio al legittimo utente del sistema o danneggi il sistema o il suo funzionamento».
[58] «L'utilizzo senza diritto di un programma informatico protetto abusivamente riprodotto, con l'intenzione di ottenere per sé o per altri un ingiusto profitto, o di cagionare un pregiudizio al titolare dei diritti sul programma».

di pubblica utilità, menzionava espressamente anche gli impianti di elaborazione di dati[59]. La legge n. 121 del 1981 (*Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*) ha istituito un Centro di elaborazione dati presso il Ministero dell'Interno, quale prima forma di tutela di dati archiviati in un sistema informatico. Nel 1991 l'art. 12 della legge n. 197 ha introdotto una disposizione che puniva l'utilizzo indebito di carte di credito o di pagamento e confluita poi nell'art. 55, co. 9, D.lgs. n. 231/2007[60].

L'esigenza di predisporre un testo normativo cui far riferimento non era dettata solo dalle spinte sovranazionali che, per l'appunto, suggerivano di recepire la Raccomandazione n. R (89) 9 per soddisfare un'esigenza di modernizzazione del sistema incriminatorio, ma anche, e soprattutto, per la preoccupazione di andare a violare il principio di tassatività[61]. In pratica, data l'assenza di disposizioni specifiche riguardanti i reati informatici, dottrina e giurisprudenza hanno cercato di ricondurre le nuove fattispecie criminose ai reati tradizionali. Il problema non riguardava tanto la parte fisica del sistema informatico (*hardware*) che più facilmente poteva trovare riconoscimento in ipotesi classiche, come il danneggiamento, il furto, ecc., quanto piuttosto il corretto inquadramento delle truffe commesse a mezzo computer[62] e la possibilità di predisporre una tutela del *software* e dei dati e delle informazioni contenute nel sistema informatico[63].

---

[59] Tale disposizione è stata poi integralmente sostituita dall'art. 2, L. n. 547/1993 e successivamente in parte abrogata dall'art. 6, L. n. 48/2008.

[60] La norma è stata abrogata dall'art. 7, D.lgs. n. 21/2018, il cui art. 4 ha introdotto l'art. 493-*ter* c.p. (*Indebito utilizzo e falsificazione di carte di credito e di pagamento,* rubrica modificata nel 2021 in *Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*) che riprende gli elementi costitutivi delle precedenti fattispecie.

[61] Il principio di tassatività (o sufficiente determinatezza) impone al legislatore di indicare con precisione i comportamenti che integrano forme di aggressione a beni giuridici perseguibili con la sanzione penale, in modo da permettere alla norma penale di fungere da guida per i cittadini.

[62] A partire dagli anni '80 si erano diffuse pratiche che consistevano nell'alterare il funzionamento dei sistemi di trasferimenti elettronici dei fondi per accreditare a sé stessi somme di denaro. Si trattava sicuramente di condotte gravi, tali da assumere rilevanza penale, che potevano essere assimilate alla truffa. Tuttavia, qui mancavano gli "artifizi o raggiri, per indurre taluno in errore": più che creare una falsa rappresentazione della realtà per indurre una persona a compiere un atto di disposizione patrimoniale, si incide sul funzionamento di una macchina. Ciononostante, la giurisprudenza di merito (Trib. Roma, 20 giugno 1984, *Testa ed altri*) ha applicato l'art. 640 c.p. in un caso riguardante l'immissione nell'elaboratore elettronico dell'I.N.P.S. di dati non veritieri relativi a contributi in realtà non versati, ritenendosi, peraltro, che in tal modo fossero ingannati i dipendenti preposti al controllo del versamento dei contributi e all'esazione degli stessi, e non il computer.

[63] Per il *software*, i dati e le informazioni custodite negli elaboratori, data l'assenza di fisicità, risultava difficile includerli tra i beni materiali già tutelati dall'art. 635 c.p., nei casi di danneggiamento, ovvero tra le "cose mobili" contemplate dall'art. 624 c.p., per i casi di furto (anche perché il "furto" veniva realizzato

Conseguentemente, si è reso indispensabile provvedere ad una regolamentazione specifica del fenomeno al fine di riuscire ad orientare i comportamenti a regole più chiare che tenessero conto dell'impatto delle nuove tecnologie informatiche sulla società contemporanea. L'obiettivo perseguito dalla Legge n. 547 del 1993 è stato proprio quello di individuare norme che permettessero a tutti – Stato, pubbliche amministrazioni, cittadini privati – di riuscire a difendersi da quei nuovi comportamenti altrettanto pregiudizievoli e dannosi. Nel '93 sono quindi state introdotte nuove figure delittuose nel codice penale, tra il titolo XII (Delitti contro la persona) e il titolo XIII (Delitti contro il patrimonio), e aggiornate alcune fattispecie già disciplinate per renderle adatte a comprendere al loro interno anche i nuovi comportamenti criminali.

È evidente fin da subito che il legislatore italiano considera i reati informatici come moderne forme di aggressione che, però, coinvolgono beni giuridici già tutelati dalle disposizioni normative presenti nel codice penale. Questo spiega perché, anziché creare un apposito titolo *ad hoc*, il legislatore segua la tecnica dell'integrazione evolutiva e collochi i reati informatici accanto alle già previste figure di reato con le quali vi sono maggiori somiglianze: affianca i reati informatici alle fattispecie con cui condividono maggiori affinità. Per quanto apprezzabile sia la scelta di evitare di ricorrere ad un'ulteriore legge speciale extracodice (sulla scia del fenomeno della decodificazione), il legislatore opera questa strategia di politica penale partendo dal presupposto che sussista un'analogia tra i comportamenti criminali tradizionali e quelli nuovi commessi a danno o per mezzo di strumenti informatici. Pertanto, taluni reati informatici presentano denominazioni e profili sanzionatori molto simili a quelli previsti per le figure classiche, proprio per non discostarsi eccessivamente dalle fattispecie legali già disciplinate; in altre ipotesi ancora, il legislatore nemmeno formula nuove fattispecie incriminatrici, limitandosi ad aggiungere oggetti passivi e mezzi nuovi o precisando le modalità di esecuzione della condotta, mantenendo però un linguaggio che mal si adatta alla realtà digitale[64]. Si legge infatti nella Relazione al disegno di legge n. 2773, tradottasi poi nella

attraverso la duplicazione del *software* o dei dati, senza cancellazione dell'originale, mancando quindi lo "spossessamento" fisico del bene). Tuttavia, una giurisprudenza isolata e parte della dottrina avevano ritenuto applicabili l'art. 635 c.p., l'art. 392 c.p. o anche l'art. 420 c.p.

[64] Come avremo modo di analizzare meglio nel capitolo 2, si pensi proprio all'accesso abusivo ad un sistema informatico o telematico, in cui ritroviamo il verbo "introdursi" che però, tecnicamente corretto per indicare l'accesso ad un luogo fisico, non appare adatto a definire l'accesso al sistema informatico.

L.547/1993, che «*nella convinzione che la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo; d'altra parte, il criterio seguito dal legislatore del 1930 nel prevedere i vari raggruppamenti di reati è ispirato all'unità dell'oggetto giuridico, inteso quanto meno come unico interesse di categoria, mentre le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice*».

Il legislatore al tempo stesso però si premura di chiarire e definire alcuni concetti propri dell'area dell'informatica, come quello di "violenza sulle cose", quale condotta che può turbare anche il funzionamento di un programma informatico o telematico (art. 1); di "documento informatico", intendendosi per tale *qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli* (art. 3); o di "corrispondenza", ricomprendendovi quella epistolare, telegrafica, telefonica e anche *informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza* (art. 5).

Dall'altro lato, invece, sono dottrina e giurisprudenza ad individuare altre definizioni tecniche su cui non si sofferma il legislatore, tra cui, ad esempio, "sistema informatico o telematico", "dati", "informazioni", o "programma"[65], in quanto trattasi di termini che

---

In tal senso I. SALVADORI, *I reati contro la riservatezza informatica*, cit., p. 696: così operando il legislatore ha «rinunciato a cogliere le specificità della criminalità informatica, che incide su beni giuridici, in tutto o in parte, nuovi, non avvedendosi delle significative ricadute che i reati informatici hanno sul piano dogmatico (in relazione al concetto di azione e di evento, al concorso di persone nel reato, al momento consumativo, al *locus commissi delicti*, ecc.)». L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme,* in *Cybercrime,* a cura di Cadoppi, Milano, 2019, p. 90: «la forte dipendenza della tecnica di formulazione delle nuove fattispecie rispetto a quelle preesistenti non sembra in ogni caso aver giovato alla loro chiarezza e precisione, data la difficoltà di far rientrare fatti, condotte od oggetti profondamente diversi in schemi concepiti per realtà differenti».

[65] Cass. pen., Sez. VI, 04.10.1999 - 14.12.1999, n. 3067: «Deve ritenersi "sistema informatico", secondo la ricorrente espressione utilizzata nella legge 23 dicembre 1993, n. 547, che ha introdotto nel codice penale i cosiddetti *computer's crime*, un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate -per mezzo di attività di "codificazione" e "decodificazione"- dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente».

abbisognano di maggiore chiarimento per comprendere la portata della norma, tenuto conto che nel diritto penale è sì ammessa l'interpretazione estensiva ma è vietato il ricorso all'analogia.

Forte dei principi di offensività e sussidiarietà, il legislatore ha individuato i comportamenti penalmente rilevanti in quattro settori, accumunati dall'uso delle tecnologie per la loro realizzazione (tralasciando qui però l'analisi dell'integrazione alle norme processuali penali in materia di intercettazione).

- Frode: viene inserito l'art. 640-*ter* c.p. (*Frode informatica*), modellato sulla truffa tradizionale[66] di cui all'art. 640 c.p., per punire l'alterazione del funzionamento o la manipolazione dei dati contenuti nel sistema informatico o telematico al fine di procurare a sé o ad altri *un ingiusto profitto con altrui danno*. Vengono inserite nel codice penale le fattispecie di cui agli artt. 617-*quater* (*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*) e 617-*quinquies* (*Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche*).
- Falsificazione: per assicurare l'equiparazione dei documenti informatici a quelli tradizionali viene introdotta una clausola generale all'art. 491-*bis* c.p. (*Documenti informatici*). È stato aggiunto l'art. 617-*sexies* c.p. (*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*).
- Danneggiamento: a fronte delle aggressioni alla integrità dei dati e dei sistemi informatici, viene inserito l'art. 635-*bis* c.p. (*Danneggiamento di sistemi informatici*

BUONOMO G., in *Profili penali dell'informatica,* cap. IV *Metodologia e disciplina delle indagini informatiche,* Giuffrè Editore, 1994: «Più sistemi informatici, tra loro collegati per lo scambio di informazioni e conoscenze, costituiscono un sistema telematico se le connessioni hanno carattere permanente (LAN o rete collegata via cavo) o stabile (collegamenti non occasionali attraverso i canali di comunicazione televisivi o telefonici) e se lo scambio di informazioni e il collegamento tra elaboratori elettronici distanti fra loro costituisce il mezzo necessario per conseguire alcuno dei fini operativi del sistema.»

G. PICA, *Diritto penale delle tecnologie informatiche: computer's crimes e reati telematici, Internet, banche-dati e privacy*, UTET, Torino, 1999, p. 25: «Il programma (o software) è costituito da una sequenza di istruzioni (costituite quindi da insiemi di "dati"), espresse in linguaggio comprensibile dalla macchina elaboratrice e progettate ed assemblate insieme per ottenere dalla macchina il compimento di operazioni prestabilite, semplici o complesse che siano.»

[66] Cass. pen., sez. II, 09.06.2016, n. 41435: «Il reato di frode informatica si distingue dal reato di truffa perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.»

e telematici) e la fattispecie di cui all'art. 615-*quinquies* c.p. (*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*).

- Intrusione illecita: alla categoria delle aggressioni alla riservatezza dei dati e delle comunicazioni informatiche vengono ricondotti gli artt. 615-*ter* c.p. (*Accesso abusivo ad un sistema informatico o telematico*) e 615-*quater* c.p. (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*).

In definitiva, attuando in questo modo la riforma, il legislatore priva di una loro autonomia i reati informatici, e, omettendo di evidenziare le specificità della criminalità informatica, non si sofferma compiutamente sui riflessi che queste fattispecie hanno sul piano dogmatico, tenuto anche conto che l'impianto normativo del codice penale appariva già inattuale e superato dalla realtà al momento di promulgazione della legge[67]. In aggiunta, con la legge in questione il legislatore intende regolare fenomeni nuovi che coinvolgono tecniche completamente innovative e, per ciò stesso, difficilmente inquadrabili all'interno delle logiche preesistenti nel quadro normativo.

Emerge come il legislatore italiano non si sia mosso con la prudenza e l'attenzione che la materia richiedeva, non essendosi soffermato sufficientemente sugli aspetti tecnici da regolare e sugli effetti della criminalizzazione di dette condotte: «*È una legge che utilizza la tecnica del 'taglia e incolla', cioè aggiunge gli aggettivi 'informatica e telematica' a fattispecie tipiche del codice penale, senza però addentrarsi in una specifica analisi di beni giuridici tutelati e di comportamenti criminosi reali. Sembra davvero essere stata concepita da persone all'oscuro della realtà pratica dell'informatica. Di fronte alle tematiche di Internet tale legge è assolutamente inadeguata. È stato adeguato il codice penale incollando qua e là la dizione 'informatica e telematica', riprendendo i reati di attentato, esercizio abusivo delle proprie ragioni, accesso illecito, intercettazione illecita, frode informatica. Le pene sono spropositatamente alte per comportamenti magari innocui sul piano pratico, ed estremamente basse quando, come nel caso di frodi internazionali o di danneggiamenti ai sistemi, i danni sono enormi. Infine, la legge non si pone per nulla problemi pratici di enorme rilevanza, come ad esempio chi debba essere*

[67] Tale scelta sistematica, più o meno criticabile, è comunque stata confermata dagli interventi legislativi che si sono susseguiti negli anni successivi, finalizzati ad attuare obblighi di incriminazione di fonte sovranazionale e a colmare le lacune emerse con la prassi applicativa.

il giudice competente» (G. Corasaniti, *La tutela penale dei sistemi informatici e telematici*).

3.1.1. *Interventi successivi*

In risposta alle crescenti sfide poste dalla criminalità informatica, il Consiglio d'Europa si è attivato nuovamente e il 24 aprile 1996 ha incaricato un gruppo di esperti di redigere una bozza di convenzione internazionale che affrontasse compiutamente la questione. Tale sforzo è stato intrapreso per fronteggiare le implicazioni derivanti dai rapidi sviluppi nel campo della tecnologia dell'informazione, che stavano impattando in modo sempre più significativo su tutti i settori della società moderna. In particolare, il Comitato di esperti sulla Criminalità nel Cyberspazio aveva il compito di analizzare i problemi emersi con lo sviluppo di Internet e di elaborare di conseguenza una disciplina comunitaria uniforme, che agevolasse la cooperazione internazionale nelle attività investigative dei *computer crimes*. Il comitato di esperti ha lavorato per quattro anni fino al 23 novembre 2001, anno in cui è stata emanata a Budapest la *Convention on Cybercrime*, realizzata anche grazie al contributo di Paesi extraeuropei (tra cui Stati Uniti, Canada, Giappone e Sud Africa)[68].

La Convenzione suddivide i reati informatici in quattro categorie ("titoli"):

I. Reati contro la riservatezza, l'integrità e la disponibilità dei dati e sistemi informatici: accesso abusivo a sistemi informatici (art.2), intercettazione abusiva (art. 3), attentato all'integrità dei dati (art. 4), attentato all'integrità del sistema (art. 5), e abuso di dispositivi (art. 6).
II. *Computer-related offences*: falsificazione informatica (art. 7) e frode informatica (art. 8).
III. *Content-related offences*: pedopornografia (art. 9).
IV. Reati relativi alle violazioni del diritto d'autore (art. 10).

[68] La Convenzione è stata poi integrata dal Protocollo addizionale del 28 gennaio 2003, riguardante l'incriminazione degli atti di razzismo e xenofobia commessi a mezzo di sistemi informatici. Il 12 maggio 2022 è stato firmato il secondo Protocollo addizionale, volto a rafforzare la cooperazione e la divulgazione delle prove elettroniche.

Allo scopo di armonizzare le legislazioni nazionali dei singoli Stati e garantire un quadro normativo uniforme, sono state introdotte definizioni di tipo tecnico per precisare alcuni dei termini più utilizzati nel linguaggio dei reati informatici – sistema informatico, dati informatici, *service provider* e trasmissione di dati[69] – e stabilite sanzioni[70] condivise per alcune specifiche condotte.

Tenendo poi conto dello sviluppo della prassi tecnologica, sono state inoltre implementate regole aggiornate per consentire alle forze dell'ordine e alla polizia giudiziaria di investigare e perseguire efficacemente i reati commessi per mezzo di strumenti informatici o che comportano la raccolta di prove in formato digitale.

Infine, sono stati predisposti modelli di cooperazione internazionale, sia di tipo verticale che orizzontale, partendo dalla constatazione per cui frequentemente i casi di criminalità informatica trascendono i confini nazionali. Si tratta, cioè, di modelli di collaborazione che mirano a facilitare lo scambio di informazioni tra le autorità competenti di diversi Stati.

Ad oggi, tale Convenzione rappresenta il principale strumento internazionale a cui far riferimento per la persecuzione dei reati informatici[71]. Essa prevede al suo interno sia norme di diritto sostanziale che di diritto processuale e trova applicazione per tutti i reati

---

[69] Art. 1, Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest 23.11.2001: «Ai fini della presente Convenzione:

a. "sistema informatico" indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati;
b. "dati informatici " indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione;
c. "*service provider*" (fornitore di servizi), indica:
    1. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico;
    2. qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;
d. "trasmissione di dati" indica qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio».

[70] L'art. 13 prevede che vengano stabilite sanzioni «effettive, proporzionate e dissuasive, che includano la privazione della libertà».

[71] Così R. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in *Cybercrime*, Milano, 2023, p. 113: «Ad oggi, la Convenzione *Cybercrime* costituisce il più importante trattato contro la criminalità informatica e un fondamentale punto di riferimento per l'armonizzazione delle normative penali sostanziali e processuali».

commessi tramite un sistema informatico e per quelli per i quali sia possibile fornire prove in forma elettronica, non essendo la sua portata limitata ai soli reati da essa definiti[72].

L'Italia ha ratificato la Convenzione sulla Criminalità Informatica con la Legge 18 marzo 2008, n. 48, che ha introdotto modifiche al codice penale[73] e al codice di procedura penale, estendendo anche ad alcune ipotesi di reati informatici la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (d.lgs. 231/2001).
In un momento successivo è intervenuta la L. 15.02.2012, n. 12 (*Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica*) che ha previsto un'importante modifica dell'art. 240 c.p. ed ha introdotto la confisca dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli artt. 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*, 640-*ter* e 640-*quinquies* c.p.
Il D.Lgs. 29.10.2016, n. 202, in attuazione della Direttiva europea 2014/42/UE del 03.04.2014, relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione Europea, novellando l'art. 240, co.1-*bis* c.p., dispone l'obbligatorietà della confisca – anche per equivalente – del profitto o del prodotto connessi ai reati di criminalità informatica indicati nella disposizione.

---

[72] Art. 14, co. 2: «Salvo diversa disposizione nell'articolo 21, ciascuna Parte applica i poteri e le procedure di cui al comma 1 del presente articolo a:
a) i reati penali stabiliti in conformità agli articoli 2-11 della presente Convenzione;
b) altri reati penali commessi tramite un sistema informatico; e
c) la raccolta di prove in forma elettronica di un reato penale».

[73] Viene modificato l'art.491-*bis* (*Documenti informatici*) e si aggiunge l'art.495-*bis* (*Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri*). Si sostituisce l'art. 615-*quinquies* (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*). È stato riscritto l'art. 635-*bis* (*Danneggiamento di informazioni, dati e programmi informatici*) e sono state poi introdotte tre ulteriori fattispecie agli artt. 635-*ter* (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*), 635-*quater* (*Danneggiamento di sistemi informatici o telematici*) e 635-*quinquies* (*Danneggiamento di sistemi informatici o telematici di pubblica utilità*). Viene aggiunto l'art. 640-*quinquies* (*Frode informatica del soggetto che presta servizi di certificazione di firma elettronica*). Sono stati abrogati i co. 2 e 3 dell'art. 420 c.p., che rischiavano di determinare problemi interpretativi con i nuovi artt. 635-*ter* e 635-*quinquies* c.p.

Un altro strumento fondamentale in termini di cooperazione comunitaria nel campo dei reati informatici all'interno dell'Unione Europea è rappresentato dalla Decisione Quadro 2005/222/GAI del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione[74]. Obiettivo perseguito con questo atto normativo è quello di raggiungere una migliore armonizzazione tra le diverse legislazioni nazionali per raggiungere un approccio comune nella lotta contro i reati informatici che, per loro natura, presentano spesso carattere transnazionale. Si promuove quindi la condivisione di informazioni e di strumenti investigativi tra autorità competenti, sia a livello nazionale che europeo, per garantire un'efficace persecuzione dei reati in questione.

Tale decisione quadro è poi stata sostituita dalla Direttiva 2013/40/UE del Parlamento europeo e del Consiglio del 12 agosto 2013. Trattasi di uno dei primi atti adottati dall'Unione Europea dopo il Trattato di Lisbona[75], a testimonianza del perseguimento di una politica criminale volta a rafforzare la *cybersecurity* in un'ottica di maggiore sviluppo del mercato ormai permeato e dipendente dalla tecnologia.

[74] «L'obiettivo della presente decisione quadro è quello di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione». Le decisioni quadro sono volte ad un ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri ed hanno efficacia vincolante quanto il risultato da ottenere, salva restando la competenza delle autorità nazionali in merito alla forma e ai mezzi.

[75] L'art. 83.1 TFUE prevede che il Parlamento europeo e il Consiglio possano «stabilire norme relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni» e in queste forme di criminalità più grave viene annoverata anche la criminalità informatica.

CAPITOLO 2

-

L'ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO

SOMMARIO: 1. Il problema. – **2.** La tecnica incriminatrice seguita dal legislatore italiano. – **2.1.** Bene giuridico tutelato: il domicilio informatico. – **2.1.1.** Critica. – **2.1.2.** Posizioni alternative. – **2.2.** Emersione di nuovi beni giuridici. – **3.** La struttura del reato. – **4.** I sistemi oggetto di tutela. – **5.** Le misure di sicurezza. – **5.1.** Critica. – **6.** Le condotte tipiche: introduzione e permanenza nel sistema informatico. – **6.1.** L'abusività della condotta. – **7.** L'elemento soggettivo. – **8.** La consumazione del reato. – **9.** Le circostanze aggravanti. – **9.1.** Circostanza aggravante determinata dal ruolo dell'attore. – **9.2.** Circostanza aggravante determinata dalla gravità della condotta. – **9.3.** Circostanza aggravante determinata dalle conseguenze della condotta. – **9.4.** Circostanza aggravante determinata dall'oggetto della condotta.

1. *Il problema*

Uno dei temi centrali più rilevanti nel contesto dei reati informatici è rappresentato dalla tutela da accordare ai sistemi informatici contro le intrusioni esterne, in quanto problematica emersa con l'avanzamento dello sviluppo tecnologico di cui si è discusso nel capitolo precedente. Nell'era attuale, la sicurezza informatica è una questione di primaria importanza, dal momento che la società odierna è profondamente digitalizzata e numerose attività quotidiane si svolgono *online*; pertanto, molti dati personali e sensibili vengono memorizzati e condivisi attraverso le reti informatiche.

La questione si impone sempre più insistentemente a causa del diffondersi del fenomeno dell'*hacking*, potenziatosi con la capillare espansione delle comunicazioni telematiche. Il termine *hacker* [76] designa ora quell'individuo che, essendo dotato di conoscenze

[76] *Hackers* si autodefinirono per la prima volta alla fine degli anni '50 degli studenti delle università americane capaci di scoprire le debolezze di un sistema informatico, i quali, mossi dall'idea *"information want to be free",* ambivano ad un progresso tecnologico. L'*hacking,* quindi, non nasce con intenti criminali ma per la voglia di dimostrare capacità tecnica e di innovazione; tuttavia, a metà degli anni '80 i media

informatiche specialistiche e avanzate, è in grado di superare le eventuali misure di sicurezza e di infiltrarsi nelle banche dati contenute nei sistemi informatici, causando danni elevati al titolare del sistema e compromettendo l'integrità del dispositivo informatico stesso.

L'evoluzione tecnologica è avanzata ad un livello tale da consentire l'interferenza nei sistemi informatici altrui, e addirittura il sabotaggio degli stessi, in numerosissimi ambiti della vita privata e pubblica, quali i trasporti, la sanità, l'ambiente, il settore industriale, ecc[77]. Tale fenomeno risulta oltretutto aggravato dalla circostanza per cui i responsabili di queste azioni sono spesso capaci di far disperdere o eliminare le proprie tracce *online*. Di fronte a tale scenario, si rende imprescindibile la predisposizione di strumenti che riescano a prevenire o quantomeno circoscrivere le possibili aggressioni informatiche, al fine di proteggere i sistemi informatici per garantire la riservatezza e l'integrità dei dati in essi contenuti. Il legislatore italiano, recependo la già citata Raccomandazione n. R (89) 9, introduce con l'art. 4[78] della legge n. 547, del 23 dicembre del 1993, l'art. 615-*ter* c.p., che espressamente sanziona l'accesso abusivo ad un sistema informatico o telematico. Tale Raccomandazione infatti sollecitava tutti gli Stati membri, essendo forte

---

hanno stigmatizzato tutti gli *hackers* in modo negativo come criminali informatici che agiscono per ottenere un guadagno finanziario, per protesta o per raccogliere informazioni - poi meglio individuati come *crackers*.

[77] Secondo il report Swascan nel secondo trimestre del 2023 gli attacchi *hacker* nel nostro Paese sono aumentati del 34,6% rispetto ai primi tre mesi e sono stati mirati al furto di dati e alla richiesta di riscatto in cambio del ripristino dei sistemi colpiti.

[78] «Dopo l'articolo 615-*bis* del codice penale sono inseriti i seguenti:

Art. 615-*ter*. - (Accesso abusivo a un sistema informatico o telematico). - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in essi contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio…»

il pericolo che aumentassero gli atti di pirateria informatica perpetrati dagli *hackers*, a rafforzare e migliorare le misure di sicurezza volte a prevenire tali pericoli e a criminalizzare le condotte di aggressione ai computer altrui.

È opportuno ricordare che, prima dell'entrata in vigore della Legge n. 547/1993, il codice penale italiano non prevedeva alcuna norma specifica atta a sanzionare l'accesso abusivo a sistemi informatici: non vi era infatti, in generale, nessuna disposizione normativa che si riferisse a questa tipologia di reati, nonostante, da almeno un decennio, fosse già avvertita l'esigenza di approntare una tutela giuridica adeguata a contrastare le emergenti forme di aggressione commesse per mezzo della tecnologia.
L'assenza di norme specifiche rendeva difficile perseguire e sanzionare le violazioni informatiche in modo efficace. Di fronte a questa lacuna legislativa, giurisprudenza e dottrina hanno allora compiuto dei tentativi per cercare di offrire quella tutela penale contro le intrusioni informatiche che ancora il legislatore mancava di dare, e questo è avvenuto attraverso l'applicazione in via estensiva di fattispecie di reato che già erano presenti nel codice penale, come il furto (art. 624), il danneggiamento (art. 635) e la truffa (art. 640). Tuttavia, al di là del fatto di essere stati orientamenti isolati, si è trattato di operazioni ermeneutiche basate su interpretazioni forzate ed eccessivamente elastiche, che hanno comportato un inammissibile ricorso all'analogia. Nella maggioranza dei casi la giurisprudenza ha perciò sollevato preoccupazioni in merito al rischio di andare a compromettere i principi di legalità e di tassatività. Anche la dottrina, dal canto suo, ha avvertito la necessità che il legislatore intervenisse quanto prima e che fornisse un quadro normativo specifico e chiaro per affrontare adeguatamente il problema[79].

[79] N. BUSSOLATI, *Accesso abusivo a un sistema informatico o telematico ex art. 615-ter c.p.: il nodo dell'abusività*, in *Studium iuris*, 2018, p. 429: «i tentativi di applicazione del tradizionale impianto normativo di parte speciale su condotte di accesso abusivo a sistema informatico - ad esempio, attraverso il ricorso al reato di violazione di domicilio, di sostituzione di persona e di intercettazione abusiva di comunicazioni telefoniche e telegrafiche - sono risultati per lo più inefficienti e potenzialmente lesivi del principio di stretta legalità, stante la diversa materialità del bene giuridico protetto e del mezzo di commissione del reato».

2. *La tecnica incriminatrice seguita dal legislatore italiano*

Con l'introduzione della Legge n. 547/1993, il legislatore italiano si è orientato nel senso di andare a tipizzare i reati informatici senza discostarsi troppo dai paradigmi delle fattispecie legali tradizionali, considerandoli semplicemente come nuove forme di aggressione a beni giuridici già oggetto di tutela[80].

In quest'ottica, l'accesso abusivo a un sistema informatico altrui viene considerato come una moderna forma di aggressione alla libertà individuale: «*La normativa trova la sua collocazione tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 c.p.*» (Relazione del disegno di legge n. 2773). Di conseguenza viene collocato dopo l'art. 614 c.p. che sanziona la violazione di domicilio, nella sezione IV "Dei delitti contro la inviolabilità del domicilio", del capo III "Dei delitti contro la libertà individuale", del titolo XII "Dei delitti contro la persona", del libro II del codice penale.

Emerge chiaramente il parallelismo stabilito dal legislatore tra gli articoli 614 e 615-*ter* del codice penale non solo e strettamente per quanto riguarda il bene giuridico tutelato (il domicilio, rispettivamente fisico e informatico)[81], ma anche per la struttura della fattispecie, modellata proprio secondo lo schema dell'art. 614 in base alla presunta analogia ravvisata. Innanzitutto, sia la tutela del domicilio fisico, tradizionalmente inteso, che la tutela del domicilio informatico trovano riferimento costituzionale all'art. 14 della Costituzione[82]; dopodiché entrambe le norme prevedono le due condotte alternative di

[80] Esemplificando si trova accanto alla truffa (art. 640) la frode informatica (art. 640-*ter*); fra i delitti di falsità in atti (artt. 476 e ss.) sono collocati quelli di falsità in documenti informatici (art. 491-*bis*); accanto al danneggiamento comune di cose (art. 635) è previsto il danneggiamento di dati e sistemi informatici (artt. 635-*bis* e 635-*quinquies*).

[81] V. meglio par. 2.1.

[82] Art. 14 Cost.: «1. Il domicilio è inviolabile. 2. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale. 3. Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali».

introduzione e mantenimento contro la volontà del titolare dello *ius excludendi*; oltre alla constatazione che i limiti edittali di pena erano gli stessi[83].

È qui opportuno analizzare l'impostazione sistematica seguita nel Codice Rocco per poi, nel proseguo, esaminare nello specifico il reato di cui all'art. 615-*ter*.
La logica che segue il legislatore penale nel garantire una tutela al domicilio, all'interno del più ampio titolo dedicato alla persona, è in linea con la tradizione costituzionale. L'art. 14 della Costituzione italiana stabilisce al comma primo il principio di inviolabilità del domicilio, analogamente alla previsione sulla libertà personale (di cui all'art. 13 Cost.). Pertanto, l'inviolabilità del domicilio è strettamente connessa alla tutela della persona e della sua sfera privata: valorizzare questo principio significa riconoscere la possibilità del singolo di autodeterminarsi all'interno del proprio spazio domestico, permettendogli di gestire liberamente e in autonomia le proprie attività e relazioni al riparo da possibili interferenze esterne indesiderate. La predisposizione di una tutela così forte per il domicilio emerge dalla constatazione che ogni individuo deve avere la possibilità di godere di una sfera di intimità e riservatezza all'interno della propria abitazione, al sicuro da visite ingiustificate e perquisizioni non autorizzate. Il diritto alla riservatezza costituisce un corollario, se non una specificazione, del diritto inviolabile della libertà individuale, tutelata dall'art. 2 Cost[84]. Il principio di inviolabilità del domicilio rappresenta quindi un importante pilastro dello stato di diritto, contribuendo a preservare e salvaguardare la dignità e la libertà delle persone e assicurando la facoltà di ammettere o escludere l'accesso ai terzi (*ius excludendi alios*)[85].
Riassumendo, concretizzandosi il domicilio nella proiezione spaziale della persona, la libertà domiciliare diviene un mezzo strumentale e funzionale a garantire la libertà

[83] Nella formulazione originale, infatti, anche l'art. 614 c.p. prevedeva, come ipotesi base, la reclusione fino a tre anni; la legge 26.04.2019, n. 36, all'art. 4, co.1, lett. a) ha previsto la reclusione da uno a quattro anni; dopo che l'art. 3, co. 24, legge 15.07.2009, n. 94, aveva sostituito la pena fino a tre anni con la pena da sei mesi a tre anni. La riformulazione delle disposizioni mostra come, nella prospettiva del legislatore, l'ipotesi di violazione del domicilio informatico sia meno grave rispetto al comune delitto di violazione di domicilio.
[84] Art. 2 Cost.: «La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale».
[85] BROCARDI, definizione: «L'espressione indica il carattere di esclusività tipico del diritto di proprietà. Esclusività significa che il proprietario, mediante azione negatoria, può far dichiarare inesistenti le pretese accampate da terzi; inoltre, per lo stesso principio, sulla stessa cosa non può esistere più di un diritto di proprietà. Materialmente, l'esclusività si manifesta nella facoltà di divieto d'accesso».

personale, poiché permette all'individuo di esprimere liberamente sé stesso in un determinato spazio fisico garantito[86].

2.1. *Bene giuridico tutelato: il domicilio informatico*

Il bene giuridico, inteso come il valore o l'interesse protetto dalla legge, riveste un ruolo fondamentale nell'indirizzare il legislatore nella configurazione delle fattispecie incriminatrici, permettendogli di collegare il diritto penale alla realtà empirica. Infatti, è analizzando il bene giuridico che si individuano le tipologie di comportamenti meritevoli di sanzione penale e si determina l'entità della pena da comminare in caso di trasgressione. In sintesi, le principali funzioni che vengono attribuite alla categoria del bene giuridico includono:

- La funzione politico-garantista, che limita le scelte di criminalizzazione del legislatore, imponendogli di ricorrere alla tutela penale esclusivamente a fronte di minacce a beni di rilevante interesse sociale;
- La funzione sistematica o classificatoria, che consente di raggruppare i reati in categorie che riflettono la protezione di specifici valori;
- La funzione interpretativa, che facilita l'applicazione della norma incriminatrice al caso concreto attraverso l'analisi dell'offensività sociale della condotta;
- La funzione dogmatica, che assicura la corretta applicazione di talune norme per evitare ambiguità ed incertezze interpretative.

La classificazione sistematica dell'art. 615-*ter* – oggetto di questo studio – ha sollevato l'interrogativo in merito a quale sia il bene giuridico tutelato dallo stesso. In particolare, la dottrina si è domandata se il bene giuridico tutelato coincida con quello comune alle norme che garantiscono la libertà domiciliare oppure se, nonostante la sua collocazione, sia possibile individuare un nuovo bene giuridico meritevole di protezione.
La molteplicità di teorie che si sono sviluppate a tal proposito rendono evidente la complessità e la controversia nell'individuare con precisione il bene giuridico protetto dalla norma.

[86] Cfr. TRECCANI, *Libertà e inviolabilità del domicilio,* in www.treccani.it.

Parte della dottrina, facendo leva proprio sull'argomento sistematico, ritiene che la norma, collocata tra i delitti contro l'inviolabilità del domicilio, tuteli il c.d. domicilio informatico, dovendosi intendere, con tale termine, un'estensione del domicilio fisico che si estrinseca nello spazio virtuale e che, in quanto parte integrante della sfera personale di un individuo, merita protezione. Il domicilio informatico, in quanto equivalente digitale del domicilio fisico, rappresenta il punto di accesso alla comunicazione elettronica: è, cioè, lo spazio in cui si esprime e si manifesta la persona nel mondo virtuale.

Ne consegue che il bene giuridico oggetto di tutela non è un bene nuovo, bensì risulta essere una specificazione del domicilio tradizionale, che viene individuato a seguito della presa di coscienza di quelle che sono le peculiarità della realtà digitale. Il domicilio informatico è il risultato dell'interpretazione estensiva del concetto di domicilio fisico ai sensi degli articoli 14 Cost. e 614 c.p., adeguata alla nuova realtà e resasi necessaria per rendere compatibile tale nozione tradizionale alle innovazioni apportate dal potenziamento della tecnologia. Infatti, come già illustrato, il quadro criminologico è mutato con il progresso tecnologico e indubbiamente il rischio di pericoli di aggressione alla sfera privata è aumentato esponenzialmente. Il legislatore, con l'introduzione di tale disposizione, intende contrastare le minacce sempre più presenti alla riservatezza personale derivanti dall'evoluzione delle moderne tecnologie, che hanno permesso l'emersione di nuove forme di intrusione nella vita intima nemmeno immaginabili in epoca precedente, al fine di tutelare i diritti inviolabili sanciti dagli articoli 2 e 14 della Carta Costituzionale.

Lo stesso diritto di escludere gli altri – noto come *ius excludendi alios* – che viene riconosciuto al titolare del domicilio fisico, viene esteso anche al domicilio informatico. Di conseguenza, la tutela penale risulta particolarmente ampia, formale e onnicomprensiva, in quanto viene riconosciuta indipendentemente dal contenuto dei dati e dei programmi presenti nel sistema, i quali possono anche non avere carattere personale. Da questo parallelismo consegue che – così come si commette il reato di violazione di domicilio ai sensi dell'art. 614 c.p., ed il relativo bene è considerato leso, anche se l'abitazione non contiene mobili o arredi, essendo sufficiente che non si tratti di uno spazio abbandonato – anche la tutela del domicilio informatico non viene apprestata in base alla natura dei dati inseriti, o alla possibilità che questi possano essere danneggiati. Si tratta di una tutela che trova il suo limite, al di là degli specifici limiti imposti dalla

legge che autorizzano l'accesso in determinati casi, nella specifica volontà del titolare di negare l'accesso non autorizzato (*voluntas excludendi*)[87].
In questa prospettiva, viene tutelato il rapporto persona-ambiente, ossia l'esplicarsi della persona in una sfera spaziale (qui virtuale) che ne renda possibile la piena realizzazione. Pertanto, secondo tale orientamento, il domicilio trova tutela in quanto preordinato a permettere a ciascuno di svolgere liberamente qualsiasi attività lecita all'interno dello spazio informatico, quale «*sfera di manifestazione della personalità individuale o di autodeterminazione della propria vita privata*»[88].

È proprio la già citata Raccomandazione sulla criminalità informatica R (89) 9, grazie al cui recepimento il legislatore italiano introduce la fattispecie di cui all'art. 615-*ter* c.p., ad indicare come il principale bene giuridico tutelato dal reato di accesso abusivo sia l'inviolabilità del domicilio informatico (*computer domicile*). Tale bene viene individuato proprio attraverso il raffronto con l'irruzione non autorizzata in abitazioni o uffici, comunemente considerata una forma di violazione di domicilio (*house breaking*).
La previsione di una tutela in questo senso costruita permette altresì di salvaguardare, in una fase precoce e indiretta, dai pericoli di sabotaggio derivanti da forme di manipolazione informatica, di danneggiamento dei dati e di spionaggio informatico. In altre parole, istituire un divieto penale all'accesso non autorizzato – quale norma che tutela il domicilio informatico – contribuisce ad ostacolare il compimento di atti dannosi che potrebbero derivare dall'intrusione nei sistemi informatici.

Anche la giurisprudenza, d'altra parte, apprezza e valorizza la tesi del domicilio informatico. La Corte di Cassazione, in particolare, dichiara espressamente come l'art.

---

[87] In tal senso R. BORRUSO, *La tutela dei documenti e dei dati,* cit., p. 28, ritiene che il legislatore abbia collocato correttamente l'art. 615-*ter* c.p. accanto alle norme che puniscono la violazione del domicilio, riuscendo così a cogliere il valore che il computer ha acquisito per l'uomo: «una sorta di propaggine della propria mente e di tutte le conoscenze, i ricordi, i segreti che essa custodisce». L'autore ritiene perciò che il reato di accesso abusivo si perfezioni «anche se l'intromettitore non ha preso conoscenza di alcuna informazione, né ha turbato il funzionamento del sistema, così come commette violazione di domicilio chi voglia trovarvi una persona che ivi abita anche se poi non la trova».
[88] S. SEMINARA, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente,* in Rivista di diritto dei media, 2/2018, p. 7: «La stessa sistemazione del codice penale, ove i reati contro l'inviolabilità del domicilio precedono quelli contro l'inviolabilità dei segreti, conferma che la nozione di riservatezza va intesa come pacifico godimento della propria sfera privata, indipendentemente dal successivo utilizzo dei dati o dei fatti la cui conoscenza viene preclusa a quanti siano privi di una facoltà di accesso».

615-*ter* c.p. sia volto a tutelare il domicilio informatico, inteso come luogo in cui vengono memorizzati i dati di un individuo sia personali che professionali, inclusi quelli di natura economico-patrimoniale. Si tratta pur sempre di uno spazio che, in quanto manifestazione della sfera privata di ciascuno, abbisogna di una tutela costituzionale e legale[89].

L'art. 615-*ter* c.p. è collocato perfettamente nella sezione dedicata ai delitti contro l'inviolabilità del domicilio, in quanto volto ad «*assicurare una protezione all'ambiente informatico o telematico che contiene dati personali che devono rimanere riservati e conservati al riparo da ingerenze ed intrusioni altrui e rappresenta un luogo inviolabile, delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche*»[90]. La tutela che viene offerta va perciò oltre la semplice riservatezza della propria vita privata (*pax deorum*), riconosciuta come connaturale ai diritti di libertà, perché include anche il diritto del titolare del sistema a escludere l'accesso o l'interferenza da parte di terzi, a prescindere dalla tipologia dei dati ivi presenti.

Questa opzione ermeneutica sembra essere, secondo la Suprema Corte, la più conforme all'intenzione del legislatore e al testo della norma in questione, che infatti non distingue i sistemi a seconda dei contenuti, limitandosi a richiedere che siano protetti da misure di sicurezza; in caso contrario, si finirebbe irragionevolmente per non tutelare anche gli aspetti economico-patrimoniali, che invece richiedono comunque garanzie.

Concludendo, il domicilio informatico, inteso come spazio in cui si manifesta la personalità di ogni individuo, è concepito come quel luogo virtuale in cui sono contenuti dati di varia natura, protetti contro qualsiasi tipo di intrusione e indipendentemente dallo scopo perseguito dall'autore dell'abuso[91].

---

[89] Cass. pen., sez. VI, 04.10.1999, n. 3067: «l'art. 615-ter c.p. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "*ius excludendi alios*", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati sia che il titolare dello *jus excludendi* sia persona fisica, sia giuridica, privata o pubblica, o altro ente».

[90] Cass. pen., Sez. Un., 24.04.2015, n. 17325.

[91] Così anche Cass. pen., sez. V, 06.02.2007, n. 11689: «Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa».

Cass. pen., Sez. V, 08.05-26.10.2012, n. 42021: «Con la previsione dell'art. 615 ter cod. pen., introdotto a seguito della L. 23 dicembre 1993, n. 547, il legislatore ha assicurato la protezione del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza

2.1.1. *Critica*

Nel corso del tempo sono emersi però anche orientamenti divergenti rispetto all'impostazione sopra esposta che identifica nel domicilio informatico il bene giuridico tutelato dall'art. 615-*ter* c.p. La dottrina maggioritaria critica la tesi del domicilio informatico perché, configurandosi il sistema informatico o telematico come proiezione spaziale della persona e dunque protetto indipendentemente dal tipo di dati contenuti al suo interno, e finanche in assenza di dati, si finisce per ampliare forse eccessivamente l'ambito della tutela penale.

L'obiezione di fondo muove in realtà dall'impossibilità di trovare una definizione unitaria di domicilio che permetta di equiparare i sistemi informatici e quelli telematici di cui all'art. 615-*ter* c.p. ai luoghi tradizionali previsti dall'art. 614 c.p. (abitazione, luogo di privata dimora, o pertinenze di essi). Associare al concetto di domicilio tradizionale quello digitale ha quindi fatto emergere problematiche che mettono in discussione la funzionalità e l'efficacia di tale nuovo istituto: il primo viene inteso come luogo fisico e tangibile, mentre il secondo è caratterizzato da astrattezza e aleatorietà, in quanto legato ad elementi immateriali, quali comunicazioni, dati e informazioni che circolano nel mondo virtuale. Risulta di conseguenza quasi insensato adottare un approccio formale nella valutazione del concetto di domicilio con riferimento alla normativa sui reati informatici, poiché i sistemi informatici vengono assimilati con una certa difficoltà agli spazi fisici tradizionalmente intesi.

Emerge allora la richiesta della previsione di una nozione di domicilio più ampia e flessibile, che tenga conto delle peculiarità del mondo digitale. Il computer non presenta caratteristiche comuni con i luoghi fisici che rientrano nella nozione di domicilio, in cui si manifesta e trova estrinsecazione la persona, per cui ancorare la tutela penale predisposta dall'art.615-*ter* c.p. ad uno specifico ambito spaziale finisce per privare di significato la disposizione stessa.

---

della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto».

Da ultimo, Cass. pen., Sez. V, 22.02-27.06.2023, n. 27900: «Il bene giuridico tutelato dalla norma in commento viene individuato dalla giurisprudenza di legittimità, del pari con orientamento costante, nel domicilio informatico sotto il profilo dello *ius excludendi alios*, anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente abilitati».

Sembra davvero difficile riuscire a paragonare la rilevanza che ha lo spazio digitale per la società odierna con il valore che il singolo attribuisce al proprio domicilio fisico. Proteggere lo spazio digitale, caratterizzato appunto dall'assenza di fisicità, riferendosi al concetto di domicilio tradizionale vorrebbe dire ignorare le nuove tecnologie e le nuove forme di aggressione alla privacy che esse comportano. È necessario guardare al progresso tecnologico perché è proprio lo sviluppo delle Tecnologie dell'Informazione e della Comunicazione a ridefinire i confini della sfera privata di ogni individuo, non più legata esclusivamente ad una dimensione fisica e materiale. Gli ambiti virtuali di cui oggi possiamo usufruire non sono paragonabili *tout court* al domicilio tradizionale, quale luogo di espansione dell'area personale di un soggetto, perché «*si tratta piuttosto di nuove sfere "virtuali" di libera, esclusiva ed immediata disponibilità. Attribuendo ai titolari o ai soggetti legittimati, la possibilità di «trattare» con estrema facilità e rapidità un'enorme quantità di dati e di informazioni, suddette sfere o spazi "virtuali" permettono di estrinsecare liberamente la propria personalità o di svolgere al loro interno ogni genere di attività (professionale, economica, sociale, culturale, ecc.)*[92]».

Nella tesi contestata emergono oltretutto diverse incongruenze. Paradigmatico in questo senso è il fatto che la normativa attuale limiti la tutela ai soli sistemi protetti da misure di sicurezza, pur individuando il bene giuridico salvaguardato nella privacy informatica. Considerando che tale riservatezza dovrebbe essere garantita a tutti coloro che abbiano esplicitamente espresso il loro dissenso all'accesso da parte di terzi, volendo ostacolare le intrusioni esterne, dovrebbe allora essere data una tutela a tutti i titolari di sistemi informatici, indipendentemente dal fatto di aver predisposto misure di sicurezza. Pertanto, la tutela dei sistemi informatici, strutturata in questo modo, appare non solo incoerente ma addirittura insufficiente.

[92] I. SALVADORI, *I reati contro la riservatezza informatica,* cit., p. 698: «L'incessante sviluppo delle nuove tecnologie dell'informazione e della comunicazione ha reso possibile la creazione e la fruizione di nuovi spazi o ambiti virtuali dove si possono intrattenere relazioni interpersonali, svolgere attività di diversa natura, inviare, ricevere o archiviare una quantità pressoché illimitata di dati informatici, sui quali il titolare può esercitare un controllo ed un godimento esclusivo».

2.1.2. *Posizioni alternative*

Le incongruenze emerse dall'analisi della teoria del domicilio informatico hanno indotto parte della dottrina a sostenere di non poter assimilare i sistemi informatici ai luoghi privati che tradizionalmente vengono fatti rientrare nella nozione di domicilio di cui all'art. 614 c.p., poiché non sempre il sistema informatico include dati dal contenuto strettamente personale.

Emerge un orientamento che individua la tutela offerta dall'art. 615-*ter* c.p. nella fruizione indisturbata del sistema informatico, assimilandola alla tutela del pacifico godimento della proprietà fondiaria (art. 637 c.p.[93]). «*Come nel 1930, in una società contadina, il codificatore proteggeva da ogni possibile turbativa la proprietà fondiaria che allora costituiva bene di preminente rilievo… così nell'attuale società, dominata dall'informatica, viene protetto il bene informatico da quelle intrusioni che costituiscano un ostacolo alla esclusiva, indisturbata fruizione del sistema da parte del gestore*[94]». In questo modo si riesce ad includere nell'ambito della tutela contemplato dall'art. 615-*ter* c.p. anche i contenuti non strettamente personali, che come tali sono estranei al bene giuridico protetto dall'art. 614 c.p.
Tuttavia, si tratta di un'impostazione poco condivisibile sotto molteplici aspetti. Anzitutto, le norme tutelano interessi diversi: l'art. 615-*ter* c.p. è orientato alla tutela della privacy (non tutela solo la signoria sulla *res* informatica), mentre l'art. 637 c.p. offre tutela patrimoniale della proprietà fondiaria, ovverosia il diritto di uso e sfruttamento economico esclusivo del fondo. Volendo assecondare questa tesi, il rischio sarebbe allora quello di creare un parallelismo troppo forzato tra le norme, in quanto non sempre l'introduzione o il mantenimento abusivo in un sistema informatico arrecano un pregiudizio tale per il titolare del sistema da impedirgli di utilizzarlo. Oltretutto, seppur è vero che entrambe le disposizioni sanzionano condotte che possono ledere la libertà individuale di una persona, il mero turbamento della signoria sull'immobile appare

[93] Art. 637 c.p. – Ingresso abusivo nel fondo altrui: «Chiunque senza necessità entra nel fondo altrui recinto da fosso, da siepe viva o da un altro stabile riparo è punito, a querela della persona offesa, con la multa fino a euro 103».
[94] F. BERGHELLA - R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici,* in Rivista Cassazione Penale, 1995, p. 2330.

scarsamente lesivo rispetto alle condotte previste dalla norma in esame; difformità che si riflette anche sul piano della sanzione comminata, dato che l'art. 637 c.p. si limita a prevedere la pena pecuniaria della multa, tra l'altro neppure di rilevante entità.
Complessivamente, questo orientamento non è in grado di cogliere le specificità della norma in commento, che introduce concetti e problematiche nuove legate propriamente all'era digitale e che, in quanto tali, non si adattano facilmente ai concetti tradizionali di domicilio, possesso e proprietà.

Una impostazione alternativa, basata sul comma 2, n. 3 dell'art. 615-*ter* c.p., che prevede quale circostanza aggravante la distruzione di dati o programmi ovvero l'interruzione del sistema, suggerisce che la norma intenda proteggere l'integrità dello stesso, nonché dei dati e dei programmi in esso contenuti dal pericolo cui risulterebbero esposti in presenza di un accesso abusivo[95].
Anche questa opzione non appare condivisibile. In primo luogo, pare introdurre un ulteriore elemento per la commissione del reato dato dalla messa in pericolo dell'integrità del sistema e dei dati, requisito non previsto dalla norma incriminatrice. Se così fosse, si finirebbe per valorizzare quella che in realtà è solo una eventuale conseguenza del reato, in quanto l'obiettivo primario della norma non è evitare la causazione di un danno (volontario o accidentale che sia) al sistema o alle sue componenti, visto che il danneggiamento risulta avere un rilievo statisticamente episodico. In secondo luogo, attribuendo una tale funzione alla norma, si finirebbe per sovrapporre tale disposizione con le previsioni volte nello specifico a disciplinare il trattamento di dati personali (Codice in materia di protezione dei dati personali - Regolamento 2016/679 UE) e a tutelare l'integrità dei sistemi informatici (ad esempio il reato di danneggiamento di sistemi informatici o telematici ex art. 635-*bis* c.p.), finendo quindi per privare di un loro reale significato tali disposizioni. Infine, sotto questo profilo, risulterebbe ingiustificato limitare la tutela offerta dall'art. 615-*ter* c.p. ai soli sistemi informatici protetti da misure di sicurezza, poiché l'interesse all'integrità dei dati, e di conseguenza la loro corretta utilizzabilità, sussiste sempre.

[95] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in *Il diritto penale dell'informatica nell'epoca di Internet,* Padova, 2004, p. 70.

Un terzo orientamento ritiene che oggetto della tutela offerta dalla norma in esame sia da ravvisare nel contenuto dei dati, così da individuare il bene giuridico protetto nella riservatezza dei dati e dei programmi contenuti all'interno di un sistema informatico. Questo sul presupposto che, una volta superate le misure di sicurezza poste a protezione del sistema, risulta estremamente facile acquisire le informazioni ivi racchiuse.
Tuttavia va tenuto presente che, trattandosi di attività che si svolgono all'interno di una sfera privata, non è il tipo di contenuti a giustificare il diritto alla riservatezza, bensì proprio il fatto che si tratti di un'area privata che deve essere gestita esclusivamente da colui che ne è il titolare, unico soggetto legittimato a disporne, decidendo se e come divulgare le informazioni a terzi[96]. In caso contrario sorgerebbe un rilevante problema, ovverosia di non riuscire più ad incriminare l'accesso ad un sistema che, anche se protetto da misure di sicurezza, non contenga alcun dato o programma ovvero contenga dati o programmi di pubblico dominio, facilmente reperibili da chiunque; questo perché, sulla base del principio di offensività, il fatto risulterebbe assolutamente inoffensivo per il bene protetto. Sicuramente questa è una soluzione che riesce a giustificare la previsione dell'adozione delle misure di sicurezza, circoscrivendo la tutela penale ai soli sistemi che il titolare ha dato dimostrazione di voler proteggere, ma non si può non considerare che anche la violazione di un sistema "vuoto" può comportare danni notevoli, potendo comunque costituire il mezzo per perpetrare ulteriori e successivi abusi.

2.2. *Emersione di nuovi beni giuridici*

Per soddisfare l'esigenza di garantire una tutela penale specifica e maggiormente appropriata ai computer, considerate le loro funzioni cruciali sempre più importanti per la società moderna, la dottrina è giunta ad individuare un nuovo bene giuridico nella previsione di cui all'art. 615-*ter* c.p., proprio per cercare di superare le lacune e le obiezioni che le tutele apprestate ai beni giuridici tradizionali presentano con riferimento al fenomeno digitale. Le offese commesse attraverso l'uso dei computer possono avere un impatto significativo sulle persone e sulle istituzioni, coinvolgendo una dimensione immateriale il cui studio difficilmente può essere affrontato in maniera adeguata riferendosi ai beni giuridici convenzionali.

[96] Crf. G. PICA, *Diritto penale delle tecnologie informatiche,* Torino, 1999.

Il nuovo bene giuridico dell'intangibilità informatica fa riferimento al diritto esclusivo del titolare del sistema di escludere gli altri dall'utilizzo non autorizzato dei suoi dati o, in generale, del suo sistema, realizzando così un controllo pieno, esclusivo ed indisturbato su quest'ultimo.

Quello che meglio possiamo definire come riservatezza informatica, insomma, rappresenta un diritto fondamentale per gli individui che interagiscono *online*, poiché, proteggendo la privacy e i dati personali che circolano su Internet per il tramite delle comunicazioni digitali, garantisce la libertà di comunicare e di condividere informazioni sottraendosi alle interferenze di soggetti non autorizzati. «*La riservatezza informatica ha ad oggetto l'interesse all'esclusività dell'accesso a uno o più spazi informatici, a prescindere dalla natura dei dati e delle informazioni ivi archiviati, nonché alla loro disponibilità rispetto a illegittime interferenze da parte di terzi soggetti*»[97].

La privacy è un diritto fondamentale dell'individuo che gli consente di decidere quali informazioni e aspetti della propria vita rendere pubblici e quali, invece, mantenere al riparo da indiscrezioni e divulgazioni indesiderate. Come diritto che garantisce la libertà e l'autonomia personale di ognuno, consentendogli di stabilire i confini della propria sfera intima, la privacy deve trovare corretta protezione anche nel mondo virtuale perché nessuno può invadere lo spazio privato (anche se non tangibile fisicamente) di un'altra persona senza il suo consenso. È quindi importante che la riservatezza sia garantita in tutte le direzioni, soprattutto nella società moderna, in cui la tecnologia ha reso più facile la raccolta, la conservazione e la diffusione delle informazioni personali.

Si tratta di un principio che trova conferma nelle fonti sovranazionali, quali l'art. 10 della Convenzione europea per i diritti dell'uomo (*Libertà di espressione*) e l'art. 11 della Carta dei diritti fondamentali dell'Unione Europea (*Libertà di espressione e d'informazione*) [98]: sono disposizioni che devono trovare applicazione anche nell'ambito del digitale, essendo

[97] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* cit., p. 21. In tal senso anche I. SALVADORI, *I reati contro la riservatezza informatica,* cit., p. 701: «La riservatezza informatica, quale autonomo nuovo bene giuridico della persona, concerne l'interesse all'esclusività e sicurezza della fruizione e dell'accesso ad uno o più spazi virtuali, anche se questi sono "vuoti" o contengono soltanto dati, informazioni e programmi di pubblico dominio».

[98] Art. 10, co.1, CEDU e art. 11 Carta di Nizza: «Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera».

la componente della riservatezza informatica indispensabile per salvaguardare la libertà di comunicazione.

La riservatezza informatica emerge quindi come nuovo diritto fondamentale dell'uomo (espressamente riconosciuto anche a livello costituzionale all'art. 2 Cost.), riferendosi alla libertà e all'autodeterminazione delle persone. Questo nuovo bene giuridico permetterebbe dunque di tutelare non solo l'interesse del singolo, bensì quell'interesse di natura collettiva a che l'accesso a sistemi informatici avvenga per finalità lecite, tali da garantire la sicurezza degli utenti: non si tratta pertanto di tutelare, mediante la previsione dei reati contro la riservatezza informatica, il solo *ius excludendi alios* del titolare del sistema, ma indirettamente anche l'interesse collettivo al regolare funzionamento, all'integrità e alla disponibilità dei sistemi (c.d. sicurezza informatica)[99]. In altre parole, l'interesse a sanzionare penalmente gli accessi abusivi a sistemi informatici non è da ricondurre strettamente e solo alla sfera individuale, riflettendo piuttosto istanze di natura superindividuale, tra cui l'intangibilità informatica, l'utilizzo indisturbato, la disponibilità e la sicurezza dei sistemi. Questo nuovo bene giuridico concerne dunque quelle istanze che in generale soddisfano funzioni di garanzia preventiva, essendo finalizzata a contrastare possibili e molteplici profili di vulnerabilità informatica. Nella dimensione di Internet, caratterizzata da una interconnessione globale, proteggere la singola vulnerabilità implica garantire la sicurezza dell'intera Rete e di conseguenza salvaguardare la corretta fruizione dei dati sensibili di tutti gli utenti[100].

---

[99] Cfr. I. SALVADORI, *I reati contro la riservatezza informatica*, cit., pp. 698-699: «Non si tratta dunque di tutelare (necessariamente) il contenuto personale, riservato o segreto delle informazioni contenute in suddetti spazi ovvero dei messaggi e delle conversazioni trasmesse o ricevute da un sistema informatico. Tanto che il delitto di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p. si configura anche qualora al suo interno non siano memorizzati dati personali, riservati o segreti ovvero non vi sia alcun dato o *software*… Si tratta piuttosto di garantire, anche in questi casi, il libero, esclusivo e pacifico godimento dei nuovi ambiti, spazi o dispositivi informatici, in modo da permettere la piena estrinsecazione della persona, che dipende anche dalla facoltà di poter comunicare in modo sicuro senza interferenze altrui».

[100] Cass. pen., Sez V, 08.07-01.10.2008, n. 3722: «È necessario ricordare che la norma in esame tutela, secondo la più accreditata dottrina, molti beni giuridici ed interessi eterogenei, quali il diritto alla riservatezza, diritti di carattere patrimoniale, come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo, interessi pubblici rilevanti, come quelli di carattere militare, sanitario nonché quelli inerenti all'ordine pubblico ed alla sicurezza, che potrebbero essere compromessi da intrusioni o manomissioni non autorizzate. Tra i beni e gli interessi tutelati non vi è alcun dubbio che particolare rilievo assume la tutela del diritto alla riservatezza e, quindi, la protezione del domicilio informatico, visto quale estensione del domicilio materiale. Tanto si desume dalla lettera della norma che non si limita soltanto a tutelare i contenuti personalissimi dei dati raccolti nei sistemi informatici,

La riservatezza informatica si ricollega, e in una certa misura si sovrappone, alla sicurezza informatica: la prima è salvaguardata in quanto siano garantiti elevati livelli di sicurezza, integrità e accessibilità dei mezzi informatici contro comportamenti abusivi, che portino quindi a considerare affidabili e genuini i servizi che vengono forniti sul web.
Va comunque distinta da altre sfere contigue, quali la privacy *tout court* intesa, la segretezza e la riservatezza domiciliare, perché non ha ad oggetto esclusivamente il trattamento dei dati personali e si concentra specificamente sulla protezione delle informazioni digitali, espandendosi quindi oltre ai tradizionali concetti di ambiti privati.
Si tratta di un bene volto a garantire il proprio "spazio informatico" libero e sicuro, in cui possa trovare esplicazione la personalità del singolo attraverso relazioni che sono dislocate nella Rete, consentendo alle persone di decidere chi possa accedere alle proprie informazioni personali e come poterle utilizzare. È di primaria importanza garantire ad ognuno la capacità di mantenere le proprie informazioni personali al sicuro e protette da accessi ingiustificati in un contesto in cui sempre più attività vengono svolte *online* e le informazioni personali sono archiviate e memorizzate su servizi digitali. La riservatezza informatica permette a ciascuno di esprimersi liberamente, senza il timore che i dati privati possano essere compromessi o utilizzati in modo improprio. In sintesi, garantisce la sicurezza e l'esclusività dell'accesso, della gestione e della disponibilità dello spazio informatico, proteggendo i dati immessi da possibili accessi indebiti o danneggiamenti di qualsivoglia tipo, resi possibili dall'illimitata possibilità di accesso che offrono le reti globali di comunicazione.
Tuttavia, questa proposta non è ancora stata pienamente accettata perché è ancora in corso il dibattito sulla sua validità e attuabilità, essendo un diritto dai confini non agevolmente determinabili. Chi si scontra con questa idea più innovativa ritiene, infatti, che l'attuale sistema giuridico sia già di per sé in grado di affrontare adeguatamente le problematiche derivanti dalle violazioni informatiche tramite il rinvio ai beni giuridici tradizionali, senza la necessità di avvalersi di un nuovo modello. In ogni caso, la discussione su questa teoria potrebbe rappresentare un momento di riflessione importante su quelle che più in generale sono le sfide legali emerse a seguito del diffuso utilizzo dei computer nella nostra società

---

ma prevede uno *ius excludendi alios* quale che sia il contenuto dei dati, purché attinenti alla sfera di pensiero o alla attività lavorativa dell'utente; è, quindi, evidente che da tale norma vengono tutelati anche gli aspetti economici e patrimoniali».

e, di conseguenza, un momento di reale comprensione sulla necessità di adeguare la legislazione penale alle nuove realtà tecnologiche.

3. *La struttura del reato*

Le opinioni sopra elencate differiscono in gran misura le une dalle altre e prediligendone una piuttosto che un'altra cambia la prospettiva da seguire e di conseguenza si struttura diversamente la fattispecie di accesso abusivo.

Il primo orientamento, che riconosce nel reato di accesso abusivo a un sistema informatico o telematico una figura che tutela la violazione di domicilio – qui informatico – configura il reato come un reato di danno, nel senso che, per la punibilità dell'agente, si richiede un'effettiva lesione del bene giuridico protetto. Questo implica allora che qualsiasi intrusione nell'elaboratore altrui realizza già compiutamente la lesione al bene della privacy informatica, a prescindere dalla circostanza che il sistema contenga dati di natura personale, riservata, o addirittura che non vi siano contenuti di alcun tipo, e dalle motivazioni che giustificano l'agire criminale. In quest'ottica è dunque prospettabile anche una tutela anticipata dell'interesse protetto, prevedendo la punibilità della condotta anche nella sua forma tentata. Inoltre, proprio per il parallelismo che si viene a costruire tra la figura dell'accesso abusivo e la violazione di domicilio emerge un'ulteriore constatazione: considerando che tradizionalmente, perché intervenga la tutela penale, è sufficiente che si tratti di luoghi non abbandonati e destinati, anche in via solo occasionale, alla libera esplicazione della personalità umana, ne discende che – operando la tutela di cui all'art. 614 c.p. indipendentemente dall'aver predisposto sofisticati impianti antiintrusione nell'abitazione – per l'art. 615-*ter* c.p. risulta bastevole l'esistenza di semplici misure di sicurezza che siano idonee a dimostrare inequivocabilmente la volontà del titolare del sistema di escludere l'accesso non autorizzato.

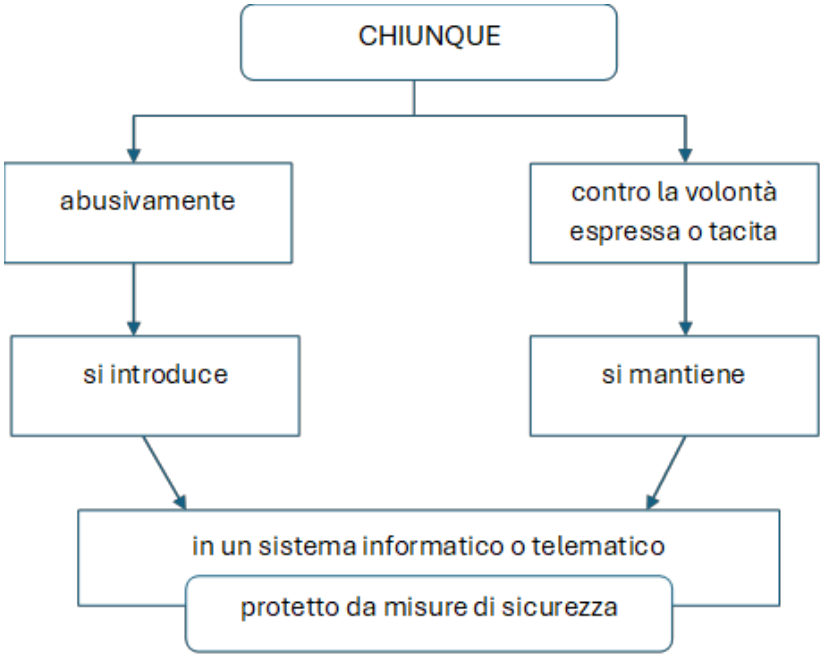
L'art. 615-*ter* c.p. si profilerebbe come reato di danno anche per coloro che costruiscono un parallelismo con l'art. 637 c.p.

Di contro, tanto per i sostenitori della tesi della tutela della riservatezza dei dati e dei programmi contenuti nel sistema, quanto per coloro che supportano la tesi della tutela dell'integrità dei dati e dei programmi, il reato in esame costituisce un reato di pericolo

astratto, ovvero un reato in cui il bene giuridico è solo minacciato perché solo potenzialmente potrebbe venire pregiudicato. In questo caso la soglia di punibilità è arretrata rispetto all'effettiva lesione di beni di natura personale o patrimoniale, proprio perché la riservatezza o l'integrità dei dati sono solo messe a rischio dalla condotta dell'agente, ma non è necessario che vengano davvero compromesse affinché la condotta di accesso abusivo venga sanzionata.

Infine, il reato di cui all'art. 615-*ter* c.p. si configura come delitto di pericolo astratto anche per coloro che ritengono di dover più correttamente individuare l'interesse giuridico protetto dalla norma nel nuovo bene della riservatezza informatica, con la conseguenza di far operare la previsione penale a prescindere dalla natura, e finanche della presenza, di dati contenuti nel sistema, dovendosi comunque garantire il pacifico godimento di questo ambito virtuale. In queste ipotesi, non è ammissibile configurare il tentativo, perché questo porterebbe ad un'eccessiva anticipazione della tutela penale, in violazione del principio di offensività[101].

102



[101] Contrariamente G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, p. 58, ritiene che si configuri un'ipotesi di tentativo qualora l'agente provi ad aggirare le misure di sicurezza poste a protezione del sistema informatico senza riuscirci.

[102] Figura presa da G. D'AIETTI, *La tutela dei programmi e dei sistemi informatici,* in *Teoria e pratica del diritto*, Milano, 1994, p. 66.

4. *I sistemi oggetto di tutela*

Il reato di cui trattasi si realizza accedendo abusivamente ad un sistema informatico o telematico.

Il concetto di sistema informatico[103] si riferisce ad un computer o un insieme di computer o di altri apparecchi elettronici (come il *router*) tra loro interconnessi in Rete ed in grado di elaborare automaticamente dati e informazioni in formato digitale. È un'espressione che comprende sia elementi *hardware* (dispositivi fisici, come computer, server, stampanti, scanner, ecc.) che *software* (programmi e applicazioni eseguiti sull'*hardware* per compiere diverse attività e processi). Si tratta quindi di un insieme di apparecchiature che, per il tramite anche di tecnologie informatiche, è in grado di compiere funzioni utili all'uomo, codificando/decodificando, registrando e memorizzando dati per mezzo di impulsi elettronici[104].

Il sistema telematico[105], invece, indica una forma di telecomunicazione tra sistemi informatici, per cui richiede la partecipazione di almeno due apparecchi che si trasmettono dati a distanza tra loro. Il sistema telematico è, cioè, quello che si avvale dell'uso dell'informatica per la gestione e la trasmissione delle comunicazioni; il supporto può cambiare, nel senso che la comunicazione può avvenire indifferentemente via cavo, onde elettromagnetiche o altri mezzi, ma l'elemento comune è dato dall'impiego delle tecnologie informatiche.

La dottrina prevalente fa rientrare nella nozione di sistema informatico o telematico di cui all'art. 615-*ter* c.p. anche i *personal computer,* sulla considerazione che questi ultimi

---

[103] L'art. 1 della Convenzione sulla criminalità informatica definisce il "sistema informatico" come «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati».

[104] Trib. Milano, Sez. III, 19.03.2007: «per sistema informatico deve intendersi una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche di guisa che non è un sistema informatico tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire, od elaborare dati in vista dello svolgimento di una funzione».

[105] V. PLANTAMURA, *Domicilio e diritto penale nella società post-industriale,* Pisa, 2017, p. 200: «Il sistema telematico è costituito da un apparato, diverso dai servizi telefonici e telegrafici convenzionali, per la comunicazione a distanza di dati tramite strumenti informatici e mezzi di telecomunicazione. La telematica vede, dunque, convergere la telecomunicazione, vale a dire la comunicazione a distanza, che elimina ostacoli di natura fisica, e l'informatica, cioè l'elaborazione elettronica dei dati. In definitiva, il sistema telematico è un sistema integrato, capace di gestire dati, voci, testi e immagini».

hanno raggiunto capacità elaborative potenzialmente enormi e che è sufficiente il loro grado di strutturazione e complessità per rientrare nella definizione di sistema. Di contro, si escludono dalla tutela penale i sistemi finalizzati alla gestione e al controllo esclusivo del funzionamento di apparecchi che erogano beni e servizi, poiché in queste ipotesi l'accesso abusivo è solo il mezzo che permette di avere la disponibilità di quei beni e servizi senza il relativo pagamento che altrimenti sarebbe dovuto; pertanto in casi simili la rilevanza penale discenderebbe dall'uso non autorizzato del sistema informatico o dall'ottenimento fraudolento delle sue prestazioni. Nel caso invece in cui il sistema informatico svolga una pluralità di funzioni, per cui oltre ad erogare una prestazione permetta altresì di consultare banche dati o ricevere informazioni riservate, sussiste sempre l'esigenza di tutelare la riservatezza dei dati accessibili contenuti nel sistema: ad esempio l'art. 615-*ter* c.p. troverebbe applicazione nel caso di distributori automatici di banconote che oltre ad erogare denaro contante forniscano anche informazioni quali il saldo del conto corrente, i movimenti bancari, ecc. (salva la possibilità di sanzionare anche reati più gravi), al fine di evitare che l'accesso non autorizzato possa poi compromettere la segretezza di informazioni riservate[106].

Più in generale, viene ricondotto al rango di sistema informatico o telematico qualunque dispositivo elettronico che, funzionando per il tramite di un *software*, possa interconnettersi con altri apparecchi e trattare una molteplicità di dati.

Per ampliare la portata della definizione, quindi, una giurisprudenza di legittimità tende a qualificare sistema informatico qualunque servizio – televisivo o telefonico – che si avvalga delle tecnologie informatiche, con la conseguenza di far rientrare anche i servizi telefonici nell'ambito della tutela offerta dall'articolo in esame[107].

---

[106] Rientrano nell'«ambito della tutela penale molti sistemi informatici e telematici privi di qualsivoglia contenuto personalistico e privatistico. Basti pensare, ad esempio, ai sistemi informatici industriali o commerciali o che gestiscono cataloghi bibliografici o informazioni per il pubblico (ad es. informazioni turistiche o sulla viabilità, appuntamenti culturali, ecc.) ed i cui dati vengono trattati solo per finalità di tipo scientifico, culturale ovvero per fornire determinati servizi agli utenti». Così I. SALVADORI, *I reati contro la riservatezza informatica*, cit., p. 727.

[107] Cass. pen., Sez. VI, 04.10.1999, n. 3067: «le linee telefoniche utilizzano, nell'epoca moderna, normalmente, tali tecnologie. La funzione di trasmissione delle comunicazioni si attua, invero, con la conversione (codificazione) dei segnali (nel caso fonici) in forma di flusso continuo di cifre (bit) e nel loro trasporto in tale forma all'altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato, dopo essere stato registrato in apposite memorie».

È opportuno comunque rilevare che delimitare la tutela offerta dall'art. 615-*ter* c.p. solo a determinati sistemi contraddice chi sostiene la tesi per cui il bene giuridico debba essere individuato nel domicilio informatico, il quale, per la definizione estensiva che lo contraddistingue, riconosce a tutti il diritto a vivere liberamente la propria intimità virtuale, senza subire intromissioni esterne, e non ammette di conseguenza che la tutela penale sia riconosciuta solo a chi sia titolare di sistemi caratterizzati da una certa qualità delle informazioni o dalla possibilità di svolgere funzioni particolarmente complesse. Il rischio sarebbe quello di creare un divario ed una disparità di trattamento tra soggetti che possono beneficiare appieno della protezione penale, avendo sistemi più avanzati e complessi, e soggetti che, invece, avendo sistemi meno sofisticati, non godono della tutela del domicilio informatico e rimangono perciò esposti a potenziali violazioni della loro privacy.

La disposizione di cui all'art. 615-*ter* c.p., riferendosi tuttora al sistema informatico e telematico, risulta obsoleta. Per evitare vuoti di tutela, sarebbe auspicabile una revisione della norma per andare ad ampliare la sfera di protezione offerta, tenendo conto dell'evoluzione nel panorama delle tecnologie che ha comportato un aumento esponenziale delle transazioni e delle comunicazioni *online*.
Includere nozioni più estese, che permettano di leggere e interpretare la norma alla luce della crescente interconnessione digitale tra dispositivi, riuscirebbe a garantire in modo più efficace la sicurezza nello scambio di informazioni in Rete e la privacy degli utenti. È una regolamentazione appropriata per il passato, ma ora appare indispensabile rivalutare la normativa in questione per adattarla alla realtà attuale, più interconnessa, aggiornandola alle nuove sfide digitali.

5. *Le misure di sicurezza*

L'accesso abusivo sanzionato dall'art. 615-*ter* c.p. può avvenire in qualsiasi modo, sia avendo un contatto diretto con il dispositivo elettronico (accesso da vicino o da tastiera), sia da remoto (tipicamente attraverso attività di *hacking*), purché però coinvolga un sistema informatico o telematico protetto da misure di sicurezza.

A questo punto, non avendo il legislatore provveduto a definire egli stesso la nozione di "misura di sicurezza", tale da giustificare il ricorso alla tutela penale, risulta necessario esaminare la controversa questione di cosa debba intendersi con tale concetto[108].

La Raccomandazione sulla criminalità informatica del 1989 (R (89) 9) indica come il reato di accesso abusivo sia finalizzato ad impedire l'accesso a sistemi o reti informatiche protette, però lascia alla discrezionalità dei singoli Stati membri il compito di individuare la tipologia dei mezzi protettivi da far rientrare nella definizione di misure di sicurezza e, in particolare, di definire il grado di complessità che questi devono presentare per potersi configurare il reato in esame.
La Raccomandazione, in realtà, prospetta la possibilità che si possa addirittura andare a sanzionare penalmente il mero accesso non autorizzato a tutti i sistemi informatici, cioè a prescindere del fatto che gli stessi siano o meno protetti da misure di sicurezza. Tuttavia, per il Consiglio d'Europa appare sensata la limitazione scelta, nel senso di richiedere uno standard minimo ed evitare così di favorire negligenze gestionali nella predisposizione di adeguati sistemi di tutela[109].

La dottrina prevalente (D'Aietti, Pazienza) sostiene che qualunque accorgimento tecnico in grado di impedire l'accesso al sistema a persone non autorizzate possa essere considerato una misura di sicurezza, indipendentemente dal grado di complessità ed efficacia. Ne discende che per giustificare l'intervento penale sia sufficiente qualsiasi misura di protezione, anche se facilmente aggirabile, purché manifesti in maniera chiara ed inequivoca la volontà dell'avente diritto di limitare l'accesso al sistema solo a persone

---

[108] Cfr. A. C. AMATO MANGIAMELI – G. SARACENI, *I reati informatici: elementi di teoria generale e principali figure criminose,* Torino, 2015, p. 54: «Considerando la questione dal punto di vista tecnico, notiamo come le misure di sicurezza possano essere divise in due grandi categorie: misure di sicurezza digitali e misure di sicurezza non-digitali. Le prime, possono a loro volta essere distinte in misure di sicurezza *software* – come, ad esempio, una *password* d'accesso o un *firewall* – e misure di sicurezza *hardware* – come, ad esempio un *badge* per la firma digitale o un sistema per il riconoscimento biometrico. Le seconde possono invece essere utilizzate per proteggere il sistema informatico o telematico inteso nella sua estrinseca materialità – pensiamo, ad esempio, ad una cassaforte».
[109] Recommendation R (89) 9 *on computer-related crime*, pp. 51-52, testo originale: «"*The access without right to a computer system or network by infringing security measures" … Consideration might even be given to criminal law prevention of the mere unauthorised access to all computer systems, in other words, not having regard to whether they are protected or whether security devices are overcome… In the controversy concerning this offence's eligibility for criminal punishment, the committee considers the chosen limitation to be sensible within the meaning of a minimum standard. It avoids the risk of favouring managerial negligence in the setting up of suitable protection systems*».

autorizzate o, in generale, di vietarlo a terzi. «*La esistenza del mezzo di protezione (anche se, in concreto, scarsamente efficace) ha la semplice funzione di rendere esplicito ed inequivoco che si è in presenza di un divieto di accesso al sistema informatico. Perché operi la norma penale basta che la protezione esista e sia percepibile da colui che si accinge ad "accedere" al sistema (il "domicilio informatico") senza esserne autorizzato*»[110]. Ad esempio, l'uso di una *password* semplice e non personalizzata, che potrebbe essere facilmente scoperta o ricostruita (che l'utente, per negligenza o imperizia non abbia mai sostituito), o l'utilizzo di un programma *antivirus* non adeguatamente aggiornato, possono essere considerati una valida manifestazione di divieto di accesso, potendo di conseguenza legittimare azioni penali di tutela.

Secondo invece un altro orientamento dottrinale (Ceccacci), rimasto però isolato, il fatto che il legislatore abbia parlato di misure di sicurezza al plurale induce a ritenere che l'uso di una semplice parola-chiave non soddisfi il requisito in esame. L'impiego del plurale è cioè indicativo della necessità di dover adottare protezioni più complesse di quella che può essere una semplice *password*, richiedendo, piuttosto, la predisposizione di misure di sicurezza più avanzate, tenendo anche conto che con l'evoluzione tecnologica le minacce alla sicurezza informatica sono sempre più sofisticate.

Di contro, la maggior parte degli studiosi argomenta che l'utilizzo del plurale rappresenti un mero collegamento grammaticale in parallelo con il vocabolo "sistemi" (più che riferirsi ad un requisito di complessità delle misure di sicurezza), cosicché anche la predisposizione di una misura mediocre permetterebbe di configurare il reato di accesso abusivo.

---

[110] G. D'AIETTI, *La tutela dei programmi e dei sistemi informatici,* cit., p. 72: l'autore prosegue ricostruendo un parallelismo con la tradizionale nozione di "domicilio" raffigurandosi l'immagine di una catena posta al confine di un fondo aperto con la scritta "vietato l'ingresso": «non vi è alcun dubbio che un tale sistema costituisca un mezzo inidoneo all'azione di malintenzionati che volessero penetrare nel fondo, ma è pur vero che esso, giuridicamente, è idoneo ad ingenerare nei terzi la nozione di "altruità" del fondo e nel fatto che scavalcando la catenella si attui una violazione di domicilio».

Così anche I. SALVADORI, *I reati contro la riservatezza informatica,* cit., p. 714: «La predisposizione di misure di sicurezza manifesta la *voluntas excludendi alios* del legittimo titolare del sistema informatico, che non necessariamente coincide con il proprietario del computer o con il soggetto cui si riferiscono i dati in esso memorizzati. Il richiamo alle misure di sicurezza facilita la verifica in sede processuale dell'abusività dell'accesso contro la volontà del titolare. Esso permette al contempo di garantire un condivisibile punto di equilibrio tra la tutela del bene giuridico della riservatezza informativa e l'altrimenti illimitata liberà di accesso ai dati e alle informazioni trattati da sistemi informatici».

In termini restrittivi si esprime inoltre chi (Pecorella) sostiene che le misure di sicurezza devono essere idonee a proteggere non solo l'*hardware* e il *software* del sistema informatico, ma anche la segretezza dei dati e dei programmi contenuti al suo interno. Si possono quindi utilizzare sia dispositivi tecnici di identificazione (strumenti di riconoscimento facciale o impronte digitali), sia misure di tipo logico (come l'utilizzo di codici numerici da digitare sulla tastiera), o di tipo fisico (come l'utilizzo di chiavi metalliche per l'accensione dell'elaboratore)[111]. È un orientamento che, nel valutare l'idoneità della misura di sicurezza a garantire un livello adeguato di protezione del sistema ai sensi dell'art. 615-*ter* c.p., esclude che si possa ragionevolmente far rientrare nella nozione in esame, tale da giustificare il ricorso alla sanzione penale, la sola misura di protezione del locale in cui è custodito il sistema informatico (porte blindate, personale di vigilanza). Quest'ultima, infatti, non rivestirebbe alcuna funzione deterrente, rivelandosi pressoché inefficace, nelle ipotesi di accesso abusivo compiuto a distanza per il tramite di mezzi elettronici connessi in Rete.

La giurisprudenza è dell'opinione di ritenere necessaria, perché operi la tutela penale, la presenza di un «*qualsiasi mezzo protettivo del sistema concretamente considerato, ancorché facilmente superabile da persona mediamente esperta, essendo sufficiente che questo mezzo renda palese la contraria volontà dell'avente diritto all'accesso e al trattenimento nel sistema*»[112].

---

[111] V. M. IASELLI, *Manuale di informatica giuridica,* Milano, 2012, p. 160: «Le misure di sicurezza possono articolarsi in più mezzi anche coesistenti sul medesimo sistema: mezzi fisici, ad esempio chiavi meccaniche o elettroniche; mezzi di accesso memorizzati dall'utente legittimo, ad esempio PIN, *password*; mezzi di accesso che confrontano caratteristiche fisiche dell'utente con quelle memorizzate nel sistema (i c.d. sistemi biometrici), ad esempio il riconoscimento tramite impronte digitali o tramite voce».
G. CECCACCI, *Computer crimes. La nuova disciplina sui reati informatici*, Milano, 1994, p. 19: «Sono tali quelle protezioni (che possono essere apposte sia a livello di apparecchiature (*hardware*) che di programmi (*software*) che integrano quei peculiari meccanismi operativi che impediscono un libero accesso al sistema e, quindi, la presa di cognizione di informazioni e dati ivi rinvenibili) a terzi estranei (ad esempio, codice alfanumerico di accesso, chiave di avviamento, eccetera)».

[112] V. Trib. Torino, Sez. IV, 07.02.1998: «E certamente non avrebbe pregio, per escludere la sussistenza del reato, rilevare che, a detta del testimone T., su quell'apparato non sarebbe mai stata inserita o resa operante una password specifica oltre a quella genericamente apposta all'elaboratore dalla casa fornitrice.»; Cass. pen., Sez. II, 21.02.2008, n. 36721: «È certamente necessario che il sistema non sia aperto a tutti, ma assume rilevanza qualsiasi meccanismo di selezione abilitati all'accesso. Ne consegue che anche l'adozione di una protezione semplice, costituita da una parola chiave (*password*) rappresenta pur sempre un'esplicitazione del divieto di accesso al sistema e legittima la tutela in sede penale».

In ogni caso, partendo dalla constatazione che l'art. 615-*ter* c.p. punisce sia l'introduzione abusiva nel sistema informatico che la permanenza non autorizzata nello stesso (v. meglio paragrafo 6), perché si possa configurare il reato in questione è sufficiente che siano state predisposte delle misure di sicurezza, ma non per forza che queste siano state aggirate: «*la violazione dei dispositivi di protezione del sistema informatico non assume rilevanza in sé, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone. Non si tratta perciò di un illecito caratterizzato appunto dall'effrazione dei sistemi protettivi, perché altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si mantenga contro la volontà del titolare. Ma si tratta di un illecito caratterizzato appunto dalla contravvenzione alle disposizioni del titolare*».

Conformemente a quanto detto, è irrilevante la circostanza che l'autore del reato abbia acquisito legittimamente le chiavi di accesso al sistema informatico protetto o che le stesse gli siano state comunicate in epoca precedente rispetto all'accesso abusivo, qualora si sia intrattenuto nel sistema adottando comportamenti sicuramente contrastanti ed esorbitanti con la volontà autorizzatoria del titolare dello *ius prohibendi*[113].

Il titolare, tra l'altro, può manifestare la volontà di escludere chiunque non sia autorizzato all'accesso o al mantenimento del sistema non solo con sistemi di protezione interna, ma anche con strumenti esterni destinati a regolare l'ingresso nei locali in cui gli impianti sono custoditi, cioè il meccanismo di selezione degli utenti deve essere un mezzo efficace ma non necessariamente tecnologico[114].

---

[113] Cass. pen., Sez. V, 22.01.2019, n. 2905: la Corte ha confermato la condanna di chi, avendo acceduto al profilo Facebook della ex moglie avvalendosi di credenziali note, ha letto conversazioni riservate e cambiato la *password* per impedirle di accedervi.

[114] V. Cass. pen., Sez. V, 07.11.2000, n. 12732, in cui prosegue riproponendo la distinzione tra «le banche dati offerte al pubblico a determinate condizioni e le banche dati destinate a un'utilizzazione privata esclusiva, come i dati contabili di un'azienda. In questo secondo caso è evidente, infatti, che, anche in mancanza di meccanismi di protezione informatica, commette il reato la persona estranea all'organizzazione che acceda ai dati senza titolo o autorizzazione, essendo implicita, ma intuibile, la volontà dell'avente diritto di escludere gli estranei». Della stessa opinione Cass. pen., Sez. V, 8.07-01.10.2008, n. 37322: «L'articolo 615 *ter* c.p. infatti punisce non solo chi si introduca abusivamente in un sistema informatico, ma anche chi nello stesso si trattenga contro la volontà dell'avente diritto. Ciò a prescindere dal fatto che nel caso di specie i sistemi di protezione dei *servers*, che erano quelli che custodivano i dati raccolti, esistevano, dal momento che essi non debbono consistere in strumenti tecnologici particolari, essendo sufficiente anche una semplice password, come era previsto nel caso di specie, che renda evidente la volontà dell'avente diritto di non fare accedere chiunque al sistema informatico… la protezione del sistema può essere adottata

Un altro aspetto da considerare è la possibilità che la misura di sicurezza sia temporaneamente disattivata, per esempio perché si sta aggiornando il *software*. In questo caso, secondo alcuni non potrebbe dirsi sussistere il reato di cui all'art. 615-*ter* c.p., poiché mancherebbe l'attualità e l'efficacia della protezione; per altri, di contro, si può comunque ravvisare un accesso abusivo anche durante la disattivazione temporanea della misura di sicurezza, non potendo escludersi a priori la sussistenza del reato, purché però l'agente sia a conoscenza della temporanea vulnerabilità del sistema e sempre che, essendo la previsione della misura di sicurezza finalizzata a qualificare i contenuti del sistema come riservati, i dati o i programmi contenuti non siano di dominio pubblico.

5.1. *Critica*

La scelta politico-criminale del legislatore di circoscrivere la tutela penale alla protezione di sistemi informatici dotati di misure di sicurezza è stata da taluni oggetto di dibattito.
In generale, i sostenitori della tesi del domicilio informatico sopra illustrata, ritenendo che questo bene altro non sia che un'estensione della mente e della personalità di ciascuno, considerano non giustificata la limitazione della tutela penale ai soli sistemi protetti da misure di sicurezza. Questo perché si presume che anche il gestore che non abbia adottato alcun dispositivo di protezione – magari per ragione di costi o di struttura del sistema – abbia interesse a beneficiare della tutela offerta dall'art. 615-*ter* c.p. In questa prospettiva, l'esistenza di misure di sicurezza non dovrebbe costituire un criterio sintomatico della violazione o meno della riservatezza informatica, quanto piuttosto avrebbe funzione probatoria circa la qualità dei sistemi da tutelare. Di conseguenza, appare erroneo e irragionevole restringere il campo di applicazione della norma in esame.
La considerazione iniziale che associa la dotazione di misure di sicurezza alla necessità di protezione del sistema è fallace, poiché l'assenza di tali misure non equivale e non implica il tacito consenso del titolare del sistema all'accesso altrui. Oltretutto, la presenza delle misure di sicurezza non rappresenta l'unico modo per manifestare la volontà di escludere l'accesso di terzi, perché tale intenzione potrebbe essere stata esplicitata anche attraverso altri mezzi.

---

anche con misure di carattere organizzativo che disciplinino le modalità di accesso ai locali ove il sistema è ubicato ed indichino le persone abilitate all'utilizzo dello stesso».

Tali obiezioni sono però superate sulla base della constatazione per cui l'adozione delle misure di sicurezza da parte del titolare del sistema dimostra chiaramente la sua volontà di proteggere l'accesso al sistema da parte di estranei non autorizzati, rendendo quindi superfluo richiedere un ulteriore consenso esplicito. Anche la giurisprudenza riconosce che la predisposizione di un mezzo di protezione renda «*penalmente apprezzabile una simile contraria volontà*» dell'avente diritto all'acceso[115]. Pertanto, risulta coerente e perfettamente giustificata la scelta del legislatore di circoscrivere la portata della tutela penale.

Più di recente, sulla base di una lettura in chiave vittimologica, è stato altresì dimostrato come il requisito in oggetto permetta di andare a responsabilizzare la potenziale vittima, contribuendo a rafforzare la sensibilizzazione dei singoli utenti sull'importanza della sicurezza informatica. Questi ultimi possono infatti confidare nella repressione penale solo nel caso in cui abbiano precedentemente provveduto a proteggere il proprio sistema informatico adottando una delle tante misure di sicurezza adeguate in base agli standard tecnologici vigenti ed idonee a prevenire accessi indesiderati.

6. *Le condotte tipiche: introduzione e permanenza nel sistema informatico*

L'art.615-*ter* c.p. punisce con la pena della reclusione fino a tre anni la condotta di chi si introduce abusivamente o si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo in un sistema informatico o telematico protetto da misure di sicurezza[116], a prescindere da un eventuale danneggiamento del sistema o dall'effettiva cognizione, alterazione o utilizzazione delle informazioni in esso contenute.

---

[115] Trib. Torino, Sez. IV, 07.02.1998. È una lettura conforme a quanto stabilisce la Relazione al disegno di legge n. 2773 contenente "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*": «dovendosi tutelare il diritto di uno specifico soggetto, è necessario che quest'ultimo abbia dimostrato, con la predisposizione di mezzi di protezione sia logica che fisica (materiale o personale) di voler espressamente riservare l'accesso e la permanenza nel sistema alle sole persone da lui autorizzate».

[116] Si aderisce dunque al paradigma del reato di violazione di domicilio ex art. 614 c.p.: «Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione da uno a quattro anni».

La prima delle condotte tipiche sanzionate penalmente è quella di introduzione nel sistema informatico, termine sicuramente adatto a delineare la condotta di chi oltrepassa fisicamente il confine di uno spazio materiale ma che è invece stato criticato in questo contesto dalla dottrina e dalla giurisprudenza. Forse, conformemente al linguaggio informatico, oltre che alla rubrica dell'articolo, sarebbe stato più corretto descrivere la condotta in termini di accesso ad un sistema piuttosto che impiegare il termine "introdursi".

È opportuno preliminarmente chiarire che la condotta di accesso al sistema informatico si articola in due fasi distinte: l'accesso fisico e l'accesso logico, riferendosi rispettivamente, con il primo concetto, alla materiale accensione del computer e, con il secondo, al momento in cui si inizia ad interagire con il *software*.

L'orientamento maggioritario in dottrina ritiene necessario – per potersi dire realizzata la condotta tipica penalmente rilevante di introduzione al sistema informatico – che sia stato eseguito l'accesso di tipo virtuale, nel senso che non potrebbe ritenersi sufficiente il semplice collegamento fisico, richiedendo piuttosto un'effettiva interazione con il sistema mediante l'inizio di un dialogo logico (o automatizzato) con il *software*[117]. Questo è dovuto al fatto che il collegamento fisico con il dispositivo – cioè la mera connessione elettronica – di per sé considerato, non implica necessariamente la possibilità di compiere attività illecite perché ancora non permette la presa di conoscenza dei dati memorizzati nel sistema.

---

[117] R. BORRUSO, *La tutela del documento e dei dati,* cit., pp. 31-32: «oggi molti computers sono collegati alla comune rete telefonica della SIP, sicché da qualsiasi parte del mondo è possibile chiamarli direttamente al telefono. Il computer risponde con un sibilo. Da quel momento in poi chiamante e computer sono in collegamento fisico (analogamente a quanto avviene quando, fatto il numero di un qualsiasi telefono, sentiamo alzare, dall'altra parte, il microfono). Poi, però, bisogna stabilire il collegamento logico: cioè bisogna cominciare a parlare. È a questo punto che, di solito, il computer chiede al chiamante di farsi riconoscere mediante uso di una chiave logica (o *password* che dir si voglia). Fornita la quale da parte del chiamante, non è raro che il computer gli prospetti una serie di alternative circa gli archivi informatici da consultare o vi sia, comunque, uno scambio di messaggi propedeutici, alla fine del quale, il chiamante, per penetrare nell'archivio che lo interessa, debba fornire un'ulteriore *password* (penetrazione finale del sistema).» L'autore ritiene che l'accesso abusivo possa dirsi avvenuto con riferimento all'ultimo di questi momenti, «quando, cioè, non ci sono più ostacoli da superare per arrivare a soddisfare lo scopo della intromissione abusiva.» G. D'AIETTI, *La tutela dei programmi e dei sistemi informatici, ibidem,* p. 68: «L'accesso è quindi un'attività che, pur non essendo completamente priva di "fisicità" (in quanto, nella fase dell'attuale tecnologia, produce, comunque, flussi guidati di correnti elettriche o luminose) non è, evidentemente, caratterizzata dagli elementi tipici della fattispecie della "violazione di domicilio"».

Pertanto, si ha introduzione in un sistema informatico o telematico protetto allorquando vengono superate le misure di sicurezza (sia fisiche che logiche) che presidiano l'accesso alla memoria interna del sistema, con l'effetto di poter consultare liberamente uno qualunque dei documenti ivi contenuti (e che risultano salvati sullo schermo) o, comunque, di navigare liberamente all'interno del sistema, avendo superato tutte le barriere di protezione progressive preposte a proteggere l'accesso al sistema. In questo modo l'agente è posto nella condizione di utilizzare, in tutto o in parte, le risorse del sistema altrui[118].

In ogni caso, come già rilevato, per potersi considerare perfezionato il reato di accesso abusivo, non è necessario che l'autore del fatto acquisisca effettiva conoscenza dei dati e dei programmi memorizzati e protetti nel dispositivo, essendo la soglia di punibilità anticipata ad uno stadio preliminare rispetto a quello della conoscenza di tali informazioni.

Solo un indirizzo minoritario in dottrina (Mantovani, Marini) sostiene che l'azione penalmente rilevante nell'ambito dell'accesso abusivo al sistema informatico sia solo quella che permetta al soggetto agente di usufruire delle informazioni contenute nella memoria del sistema informatico o trasmesse dal sistema telematico: essi opinano che il mero accesso non sia di per sé meritevole di criminalizzazione, poiché non ritengono che l'inviolabilità del sistema possa costituire un bene giuridico meritevole di tutela.

La condotta tipica della fattispecie in esame può, inoltre, essere integrata con la duplicazione dei dati conservati nel sistema e acquisiti in occasione dell'accesso abusivo[119].

---

[118] V. M. LAMANUZZI, *Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma,* in Archivio penale, 2/2022, pp. 8-9.

I. SALVADORI, *I reati contro la riservatezza informatica,* in *Cybercrime,* Milano, 2019, p. 669: «si deve trattare di una penetrazione di tipo elettronico, telematico o virtuale, e avviene tramite il superamento delle barriere che presidiano l'accesso alla memoria interna del sistema, sì che l'agente guadagna una libertà di movimento all'interno del sistema»; in *Cybercrime,* 2023, p. 705: «L'accesso si configura pertanto nel momento in cui il sistema informatico altrui esegue una data operazione, richiestagli dal soggetto agente mediante una serie di comandi, mettendolo nelle condizioni di poter operare e anche conoscere quanto in esso contenuto».

[119] Trib. Torino, Sez. IV, 07.02.1998: «la mera duplicazione dei dati acquisiti in occasione dell'accesso abusivo nel sistema è da ricomprendere nella condotta tipica del reato di cui all'art. 615 *ter* c.p., potendo l'intrusione informatica sostanziarsi sia in una semplice "lettura" dei dati che nella "copiatura" degli stessi… la sottrazione di dati altro non è che una "presa di conoscenza" di notizie». Riferimenti analoghi anche in Cass. pen., Sez. V, 8.07-01.10.2008, n. 37322.

Parallelamente e in via alternativa all'azione di introduzione, il legislatore sanziona la condotta di chi si mantiene in un sistema informatico o telematico protetto contro la volontà, espressa o tacita, del titolare del diritto di esclusione.

La distinzione tra queste due condotte è importante perché se da una parte la condotta di introduzione nel sistema è necessariamente prodromica rispetto a quella di permanenza (non essendo immaginabile permanere nel sistema se prima non vi si è acceduto), dall'altra parte l'introduzione nel sistema potrebbe essere stata inizialmente lecita e avere assunto carattere illecito solamente in un momento successivo, mediante la permanenza nel sistema in contrasto con gli accordi del titolare del sistema ovvero oltrepassando i limiti posti dalla sua autorizzazione. L'ipotesi considerata è dunque quella dell'accesso originariamente autorizzato, o accordato per determinate operazioni o per un certo periodo di tempo, ovvero casuale, che si tramuta in una permanenza nel sistema altrui non autorizzata, oltrepassando i limiti modali e/o temporali consentiti, ovvero contrariamente alla *voluntas domini*[120]. In altre parole, il primo comma dell'art. 615-*ter* c.p. sanziona anche la condotta di chi, violando le prescrizioni impartitegli, si mantiene nel sistema per compiere attività estranee alle proprie mansioni: il suo accesso, di per sé legittimo, a causa del suo protrarsi all'interno del sistema per fini estranei a quelli dell'istituto, diviene abusivo e perciò illecito.

Il dissenso all'accesso può essere generale, con la conseguenza che qualsiasi atto verrebbe ricondotto al delitto di accesso abusivo, oppure settoriale, cioè circoscritto a determinate modalità di accesso, per cui solamente la trasgressione degli specifici limiti posti dal titolare dello *ius excludendi* configurerebbe il reato in questione.

La mancanza di tale dissenso alla permanenza non permette di ritenere integrata la fattispecie oggettiva di reato, essendo questo un elemento costitutivo del fatto tipico: il dissenso dell'avente diritto deve essere manifestato chiaramente, sia in forma esplicita che implicita, ma in nessun caso potrebbe essere oggetto di sola presunzione.

Anche in questo caso, ciò che rileva è comunque la mera permanenza nel sistema – da intendersi sempre come mantenimento della connessione logica – e non anche le altre

[120] Si pensi al tecnico cui viene consegnato il computer per una riparazione nel funzionamento del sistema e, terminato questo lavoro, si mantenga ulteriormente nel sistema potendo compiere ulteriori attività rispetto a quelle assegnategli.
La permanenza nel sistema informatico che consegua ad una introduzione illegittima non costituisce un'ipotesi di concorso materiale, trattasi piuttosto di un semplice *post-factum.*

eventuali attività che possono essere compiute contestualmente, quale la presa di conoscenza effettiva di dati e informazioni.

6.1. *L'abusività della condotta*

Le sopraindicate condotte di introduzione e mantenimento nel sistema informatico o telematico, previste dall'art. 615-*ter* c.p., acquisiscono rilevanza penale in quanto realizzate "abusivamente" e "contro la volontà espressa o tacita di chi ha diritto di escluderlo".

Il legislatore ha inteso, tanto con l'uso dell'avverbio quanto con l'inciso, connotare entrambe le condotte tipiche con il requisito della mancanza di autorizzazione all'accesso [121] : il consenso, infatti, non deve sussistere solo nella fase iniziale di introduzione, ma è necessario che perduri per tutta la durata del mantenimento nel sistema. L'impiego della locuzione, in luogo del più sintetico "abusivamente", risponde cioè ad una scelta di stile, senza alcuna volontà da parte del legislatore di intendere attribuire alla condotta del mantenimento una diversa carica lesiva. Ne consegue allora che il sopraggiungere del dissenso renderebbe penalmente illecita una condotta inizialmente autorizzata.

L'abusività della condotta è qui elemento costitutivo del reato, nel senso che le mere azioni di accesso e di permanenza in sistemi informatici o telematici non presentano una intrinseca natura offensiva, ma appunto assumono rilievo penale in quanto poste in essere in mancanza di autorizzazione ovvero eccedendo i limiti della stessa.

La questione dell'utilizzo improprio (abusivo) dell'accesso autorizzato è stata oggetto di dibattito in giurisprudenza[122].

Inizialmente, un primo indirizzo giurisprudenziale attribuisce rilevanza penale non solo all'azione dell'*hacker* (o "pirata informatico") che – pur non avendone l'autorizzazione – riesca a violare le misure di sicurezza poste a difesa di un sistema informatico e ad

[121] L'avverbio in questione per alcuni autori è da intendere quale clausola di illiceità espressa, per altri invece assume rilievo come clausola di illiceità speciale: cfr. FIANDACA-MUSCO, *Diritto penale. Parte generale,* VIII ed., Torino, 2019, pp. 205 ss.

[122] Cfr. M. BELLINGERI, *Evoluzione giurisprudenziale del concetto di "abusività" nel caso di accesso ad un sistema informatico,* 12 maggio 2022, in ntplusdiritto.

accedervi, ma anche alle condotte dei soggetti che – pur essendo in possesso delle credenziali di accesso legittimamente ottenute (c.d. *insider*) – si mantengano nel sistema informatico contrariamente alla volontà del titolare, realizzando attività che eccedono i limiti posti alle mansioni per le quali l'accesso era stato originariamente autorizzato. L'uso del titolo di legittimazione all'accesso (come può essere ad esempio la *password* di servizio) per finalità diverse ed estranee a quelle consentite dimostra che il soggetto sta operando e si sta servendo del sistema oltre i limiti concordati; ne risulta allora che la permanenza nel sistema informatico o telematico stia avvenendo (tacitamente) contro la volontà del titolare del diritto di esclusione[123].

Diversamente, un secondo orientamento giurisprudenziale offre un'interpretazione difforme della disposizione legislativa contemplata all'art. 615-*ter* c.p. e, valorizzando la prima parte del comma 1, delinea in termini restrittivi il concetto di abusività, configurando il reato in questione esclusivamente nell'ipotesi di accesso effettuato da soggetto non abilitato e quindi del tutto privo di ogni tipo di autorizzazione[124]. In

---

[123] Cass. pen., Sez. V, 07.11.2000, n. 12732: «l'analogia con la fattispecie della violazione di domicilio deve indurre a concludere che integri la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa, e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'acceso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva».

Indirizzo ribadito con la Cass. pen., Sez. V, 8.07-01.10.2008, n. 37322: «Naturalmente l'accesso al sistema è consentito dal titolare per determinate finalità, ovvero il raggiungimento degli scopi aziendali, cosicché se il titolo di legittimazione all'accesso viene dall'agente utilizzato per finalità diverse da quelle consentite non vi è dubbio che si configuri il delitto in discussione, dovendosi ritenere che il permanere nel sistema per scopi diversi da quelli previsti avvenga contro la volontà, che può, per disposizione di legge, anche essere tacita, del titolare del diritto di esclusione.»; in dottrina v. S. DE FLAMMINEIS, *Art. 615-ter c.p.: accesso legittimo ma per finalità estranee ad un sistema informatico,* in Cass. pen., 2011, n. 6.

[124] Cass. pen., Sez. V, 20.12.2007-17.01.2008, n. 2534: «Non integra il reato di accesso abusivo ad un sistema informatico la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all'Arma dei Cararbinieri, si introducano nel sistema denominato S.D.I. (banca dati interforze degli organi di polizia), considerato che si tratta di soggetti autorizzati all'accesso e, in virtù del medesimo titolo, a prendere cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi a una agenzia investigativa, condotta quest'ultima ipoteticamente sanzionabile per altro e diverso titolo di reato».

Cass. pen., Sez. VI, 08.10-21.10.2008, n. 39290: «Il reato è integrato dall'accesso non autorizzato nel sistema informatico, ciò che di per sé mette a rischio la riservatezza del domicilio informatico, indipendentemente dallo scopo che si propone l'autore dell'accesso abusivo… Non può, pertanto, condividersi l' interpretazione della norma che individua l'abusività della condotta nel fatto del pubblico ufficiale o dell'incaricato di pubblico servizio che, abilitato ad accedere al sistema informatico, usi tale facoltà per finalità estranee all'ufficio e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Tale lettura della norma finisce con l'intrecciare le due condotte descritte dall'art. 615 *ter*, che sono differenti

quest'ottica risulta importante non confondere l'ipotesi di accesso non autorizzato da quella di uso improprio di un accesso legittimamente ottenuto, al fine di evitare un'inaccettabile espansione della portata del reato di accesso abusivo conformemente a quanto previsto nella lista minima della Raccomandazione R (89) 9 sulla criminalità informatica (che a tal riguardo parla propriamente di "*access without right*" nel senso di "accesso non autorizzato")[125].

Pur essendo entrambe le interpretazioni teleologiche perfettamente compatibili con il significato letterale del termine "abusivo", sono orientate a scopi diversi: la prima opzione ermeneutica illustrata, che amplia la portata del concetto di abusività, interpreta la fattispecie in esame come diretta a tutelare la riservatezza dei dati e dei programmi contenuti nel sistema, salvaguardando cioè l'interesse del titolare a limitarne la visione da parte di terzi; di contro, l'opzione che restringe il concetto di abusivo al solo ingresso in assenza di autorizzazione, interpreta l'art. 615-*ter* c.p. come volto a tutelare il domicilio informatico, con la conseguenza che non rileva penalmente l'ingresso del soggetto che, pur legittimato, ecceda i limiti che gli vengono impartiti perché non in grado di compromettere tale luogo[126].

---

e alternative, disgiuntamente considerate dal legislatore. Sarebbe stata pleonastica la descrizione della seconda condotta se la prima fosse integrata anche da chi usa la legittimazione all'accesso per fini diversi da quelli a cui è stato legittimato dal titolare del sistema».

Cass. pen., Sez. V, 25.06-14.10.2009, n. 40078: Nel caso di specie, la Corte esclude che possa considerarsi abusiva la condotta del soggetto agente che, originariamente abilitato a consultare i dati presenti nel sistema informatico, usi tale facoltà per finalità estranee al compito ricevuto, poiché non sarebbe immaginabile la contraria volontà del titolare dello *ius excludendi*. La Corte sostiene che la nozione di abusività debba essere «intesa in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza, apprestate dal titolare dello *ius excludendi*, al fine di impedire accessi indiscriminati. Non hanno quindi rilevanza la finalità che si propone l'autore e l'uso successivo dei dati che, se illeciti, integrano eventualmente un diverso titolo di reato… la sussistenza o meno della contraria volontà dell'avente diritto, necessaria alla configurabilità del reato, va verificata solo ed esclusivamente con riferimento al risultato immediato della condotta posta in essere dall'agente e non con riferimento a fatti successivi».

[125] Cass. pen., sez. V, 29.5.2008, n. 26797: «la formula "abusivamente si introduce" recata dalla disposizione in esame [art. 615-*ter* c.p.] appare la incerta traduzione di quella "accesso non autorizzato" (o accesso illegale) già utilizzata nella lista minima del Consiglio d'Europa che accompagnava la Raccomandazione (89) 9, cui s'è adeguato il legislatore nazionale con la legge n. 547 del 1993 e, quindi, della locuzione accesso "senza diritto" (*access… without right*) impiegata nell'art. 2 della Convenzione sul cybercrime».

[126] Per una disamina completa v. R. BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato,* in Diritto Penale Contemporaneo, n. 1/2012.

A fronte di questo contrasto giurisprudenziale, viene rimessa alle Sezioni Unite della Corte di Cassazione la seguente questione di diritto: «*se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato ma per scopi o finalità estranei a quelli per i quali la facoltà di accesso gli è stata attribuita*».

Le Sezioni Unite si pronunciano per la prima volta su questa questione con la sentenza Casani, con la quale stabiliscono di non dover valutare la questione prendendo in considerazione gli scopi perseguiti dal soggetto agente dovendo, invece, attribuire rilevanza penale soltanto al dato oggettivo dell'accesso e del trattenimento nel sistema. Questo approccio implica che la manifestazione di dissenso del titolare dello *ius excludendi* debba essere valutato esclusivamente in relazione all'azione immediatamente intrapresa, senza tener conto di eventuali azioni successive (ad esempio alterazione, danneggiamento di dati o rivelazione di segreti), le quali possono al più integrare fatti illeciti autonomi. In sintesi, il carattere dell'abusività è da riconnettere al solo fatto dell'introduzione o della permanenza nel sistema protetto: «*Il giudizio circa l'esistenza del dissenso del dominus loci deve assumere come parametro la sussistenza o meno di un'obiettiva violazione, da parte dell'agente, delle prescrizioni impartite dal dominus stesso circa l'uso del sistema e non può essere formulato unicamente in base alla direzione finalistica della condotta, soggettivamente intesa*»[127].

Correttamente, le Sezioni Unite sanciscono che ai fini dell'integrazione del delitto di accesso abusivo a un sistema informatico conta solo il momento in cui viene posta in essere la condotta che si connota per l'abusività, rimanendo irrilevanti le finalità, lecite o

[127] Cass. pen., Sez. Un., 27.10.2011-07.02.2012, n. 4694: «Rilevante deve ritenersi, perciò, il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi ed a permanervi sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (nozione specificata, da parte della dottrina, con riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro) sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito. In questi casi è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta. Il dissenso tacito del *dominus loci* non viene desunto dalla finalità (quale che sia) che anima la condotta dell'agente, bensì dall'oggettiva violazione delle disposizioni dei titolare in ordine all'uso del sistema. Irrilevanti devono considerarsi gli eventuali fatti successivi: questi, se seguiranno, saranno frutto di nuoti atti volitivi e pertanto, se illeciti, saranno sanzionati con riguardo ad altro titolo di reato».

illecite, perseguite. Quello che conta è che l'utente si relazioni con il sistema informatico altrui contrariamente alla volontà del soggetto che ha diritto di escludere l'*extraneus*. Diversamente si andrebbero a criminalizzare le condotte di introduzione e mantenimento in base ad un criterio difficilmente verificabile in sede giudiziaria[128]. Forte del valore della certezza giuridica, si determina il carattere abusivo della condotta sulla base di un parametro dai contorni più certi, guardando all'oggettiva violazione delle disposizioni dittatoriali, dei regolamenti, ovvero alla mancanza di un titolo legittimante.
Ne deriva che si configura il reato di cui all'art. 615-*ter* c.p. nel caso di:

- accesso non autorizzato;
- accesso da parte di soggetto abilitato ma posto in essere violando i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso;
- accesso autorizzato ma che comporti altresì il compimento di operazioni di natura ontologicamente diversa da quelle rispetto alle quali l'autore è stato incaricato ed in relazione alle quali l'accesso era a lui consentito, facendo dunque venire meno il titolo legittimante l'accesso e la permanenza nel sistema.

Le pronunce della giurisprudenza successiva hanno però finito per includere nelle ipotesi di abusività della condotta ai sensi dell'art. 615-*ter* c.p. anche forme di abuso meramente soggettivo.
Questo orientamento è stato confermato nella pronuncia a Sezioni Unite della Corte di Cassazione Savarese con cui, pur riferendosi esclusivamente all'ipotesi di cui al comma 2, n. 1 dell'art. 615-*ter* c.p. (vedi paragrafo 9), si afferma espressamente che integra il reato in esame qualunque condotta di accesso "ontologicamente incompatibile" con l'assolvimento delle funzioni pubbliche affidate e non conforme alle finalità istituzionali per cui sia stato conferito il relativo potere di accesso al sistema informatico. «*Integra il delitto previsto dall'art. 615-ter, secondo comma, n. 1, cod. pen. la condotta del pubblico*

[128] Cfr. I. SALVADORI, *I reati contro la riservatezza informatica,* cit., p. 712: «Una ricostruzione volta a ricavare l'abusività dell'accesso dallo scopo personale che persegue l'agente avrebbe inoltre l'effetto di dilatare eccessivamente l'ambito di applicazione della fattispecie, non fornendo un parametro normativo o comunque oggettivo sulla base del quale determinare l'abusività della condotta nel momento della sua commissione. La rilevanza penale del fatto di introdursi o mantenersi in un sistema informatico verrebbe a dipendere da un elemento labile e di non facile accertamento in sede processuale, vale a dire dalla finalità soggettiva che il soggetto attivo persegue con la sua condotta».

ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita»[129].

Più di qualcuno ha criticato tale impostazione che sostituisce il parametro oggettivo di valutazione dell'abusività (oggettiva violazione di prassi e norme) con uno soggettivo (accesso per ragioni personali e non d'ufficio). Viene infatti ritenuta un'interpretazione troppo forzata, dal momento che la Corte utilizza la circostanza aggravante di cui all'art. 615-*ter*, comma 2, n.1 c.p. come chiave di lettura dell'abuso di cui al primo comma[130].

Tuttavia, la più recente pronuncia n. 15629, depositata il 21 aprile 2022, ha accolto il principio di diritto sancito dalle Sezioni Unite Casani, ribadendo pertanto l'irrilevanza – ai fini della sussistenza del reato in questione – degli obiettivi perseguiti «*che abbiano soggettivamente motivato l'ingresso nel sistema*».

Sembrerebbe allora doversi intendere l'abusività diversamente a seconda che si faccia riferimento a soggetti privati, per i quali rileverebbe il solo dato oggettivo dell'accesso abusivo nel sistema informatico, e ai funzionari pubblici i quali, invece, risponderebbero di abuso anche a titolo soggettivo, per aver perseguito finalità non rispondenti all'esercizio dei loro poteri.

---

[129] Cass. pen., Sez. Un., 18.05-08.09.2017, n. 41210: La Corte considera abusivo l'accesso ai dati in questione, in quanto operazione posta in essere contrariamente alle facoltà di accesso che all'imputata erano state attribuite e, dunque, violando i canoni della correttezza e della lealtà.

[130] Cfr. S. SEMINARA, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente*, cit., p. 249: «Questa soluzione rappresenta però un'invenzione della giurisprudenza, che non trova nessun appiglio nel testo normativo – rivelandosi quindi incompatibile con il principio di legalità – e non appare dotata di un sufficiente fondamento politico-criminale, dovendosi dubitare della correttezza di un'equiparazione fra tutte le finalità private che abbiano ispirato l'accesso abusivo, addirittura prescindendo dal loro contenuto lecito o illecito. Neppure va trascurato che le condotte in esame potrebbero in parte trovare un'adeguata reazione in sede disciplinare, restando esclusa la loro rilevanza penale.»; V. anche F. FASANI, *Accesso abusivo a un sistema informatico: le Sezioni Unite cambiano di nuovo rotta (nota a Cass., Sez. un., 8 settembre 2017, ud. 18 maggio 2017, Savarese)*, in Le Società, 2017, pp. 1405-1406: «l'equivoco sta nel fatto che le Sezioni Unite si limitano a evidenziare come lo sviamento del potere da parte del pubblico ufficiale possa essere ricondotto alle specifiche modalità di condotta tipizzate dall'aggravante, senza tuttavia osservare alcunché in merito alla prima e fondamentale sussunzione che deve essere operata: quella della condotta all'interno del primo comma dell'art. 615-*ter* c.p.».

Concludendo, sicuramente la delimitazione dell'ambito di applicazione dell'art. 615-*ter* c.p. riflette l'interpretazione, in modo estensivo o restrittivo, dell'elemento dell'abusività. Conformemente a quanto previsto dal diritto europeo, la condotta di accesso si considera "senza diritto" quando posta in essere da persona «*che non è autorizzata da parte del proprietario o da un altro titolare di diritti sul sistema o su una parte, ovvero non consentiti a norma del diritto nazionale*»[131]. Per definire il concetto di accesso abusivo va quindi valutato caso per caso se siano state obiettivamente violate le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, il quale può sia escludere gli *outsider* sia delimitare il tipo di operazioni che possono compiere gli *insider*[132].

7. *L'elemento soggettivo*

Ai fini della configurabilità del reato di cui all'art. 615-*ter* c.p. è richiesto il dolo generico [133]. Risulta quindi necessario e sufficiente che il soggetto agente agisca consapevole dell'altruità del sistema e ciononostante voglia comunque introdursi abusivamente nel sistema informatico o telematico munito di misure di sicurezza, o ivi mantenervisi contro la volontà del titolare dello *ius excludendi alios*.
Il soggetto agente dovrebbe quindi rappresentarsi sempre anche l'esistenza delle misure di sicurezza ed il relativo aggiramento. Il rischio è di andare a delimitare eccessivamente l'area in cui trova applicazione il reato contemplato dall'art. 615-*ter* c.p., considerando che chi si introduce o si mantiene all'interno di un elaboratore elettronico non sempre è a

[131] Art. 2, lett. d), Dir. 2013/40/UE.
[132] Cass. pen., Sez. V, 26.10.2016, n. 14546: «Ai fini della configurabilità del delitto di cui all'art. 615 *ter* c.p., da parte colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto, violando le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, è necessario verificare se il soggetto, ove normalmente abilitato ad accedere nel sistema, vi si sia introdotto o mantenuto appunto rispettando o meno le prescrizioni costituenti il presupposto legittimante la sua attività, giacché il dominus può apprestare le regole che ritenga più opportune per disciplinare l'accesso e le conseguenti modalità operative, potendo rientrare tra tali regole, ad esempio, anche il divieto di mantenersi all'interno del sistema copiando un file o inviandolo a mezzo di posta elettronica, incombenza questa che non si esaurisce nella mera pressione di un tasto ma è piuttosto caratterizzata da una apprezzabile dimensione cronologica».
[133] In termini generali, consiste nella coscienza e volontà di realizzare gli estremi costitutivi del reato.

conoscenza della presenza di misure di sicurezza. Esemplificativamente, si può pensare al caso in cui venga disattivato momentaneamente un programma *antivirus* per aggiornarlo e un soggetto riesca perciò ad accedere fortuitamente nel sistema: in una simile situazione, la condotta del soggetto agente – pur meritevole di rimprovero penale – non potrebbe essere sussunta nella fattispecie di accesso abusivo, poiché mancherebbe la consapevolezza che il sistema sia protetto da misure di sicurezza.

Esclude l'integrazione del dolo il caso in cui l'agente ritenga erroneamente sussistente il consenso all'accesso da parte del titolare del sistema (ai sensi dell'art. 47 c.p.).

In ogni caso, non rilevano il movente e le finalità perseguite dal reo, non prevedendo la norma alcuna finalità speciale né lo scopo di trarre profitto, per sé o per altri, ovvero di cagionare ad altri un danno ingiusto[134].

8. *La consumazione del reato*

Il reato di accesso abusivo ad un sistema informatico o telematico può dirsi effettivamente realizzato nel momento in cui l'agente stabilisce il dialogo logico con la memoria del sistema, dopo aver oltrepassato tutte le barriere di protezione[135] (fisiche e/o logiche) preordinate a garantire l'accesso ai dati e ai programmi solo a chi sia autorizzato ad averne visione.

La questione relativa alla necessità che vi sia l'effettiva presa di conoscenza dei dati memorizzati nel sistema violato suscita ancora qualche dibattito; tuttavia, la dottrina

[134] Cass. pen., Sez. V, 25.03-02.05.2019, n. 18284; Cass. pen., Sez. V, 13.06-04.10.2022, n. 37459 : «Integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615 *ter* c.p., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, ovvero ponga in essere operazioni di natura ontologicamente diversa da quelle per le quali l'accesso è consentito. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema.»

[135] Parte della giurisprudenza ritiene necessario che l'agente abbia neutralizzato le misure di sicurezza poste a protezione del sistema: v. ad es. Cass. pen., Sez. V, 04.12.2006, n. 6459. Di contro, c'è chi sostiene che non sia necessario, ai fini della consumazione, l'aggiramento fraudolento delle misure di sicurezza, essendo il reato caratterizzato dalla contravvenzione alle disposizioni del titolare: v. Cass. pen., Sez. V, 07.11.2000, n. 12732.

maggioritaria ritiene che la configurazione del reato in esame possa prescindere da questo eventuale passaggio[136].

Nel caso della introduzione, il delitto si configura come un reato a consumazione istantanea per cui, esaurendosi la condotta in un solo momento, il momento consumativo coincide con l'ultimo atto dell'azione.

Nell'ipotesi del mantenimento, invece, dato che l'agente si trattiene all'interno del sistema per un certo periodo di tempo, si ha a che fare con un reato permanente, che si consuma allora nel momento in cui si interrompe l'accesso, venendo così meno la situazione antigiuridica. Il termine per uscire dal sistema (*log-out*) segna il momento a partire dal quale la condotta della permanenza è da considerarsi tipica, in quanto protratta oltre i limiti posti dal titolare dello *ius excludendi* ovvero dalle disposizioni organizzative o contrattuali che regolano le attività consentite al soggetto che opera sul sistema informatico.

Per quanto riguarda il luogo di commissione del delitto di cui all'art. 615-*ter* c.p., si è reso necessario rivisitare la tradizionale nozione di condotta illecita, posto che nell'ambiente informatico o telematico la condotta presenta caratteristiche che divergono significativamente da quelle che emergono nella realtà fisica, in cui le conseguenze dell'azione (o dell'omissione) sono immediatamente percepibili e verificabili. Pertanto, partendo dalla constatazione che la maggior parte dei casi vede il reato in questione realizzarsi a distanza mediante il collegamento telematico che si crea tra più sistemi informatici, la giurisprudenza di legittimità ha individuato il *locus commissi delicti* nel luogo in cui si trova il soggetto agente che effettua l'accesso abusivo, sia nell'ipotesi dell'introduzione sia in quella del mantenimento nel sistema informatico altrui.

A questo risultato sono giunte le Sezioni Unite[137], le quali, con ordinanza del 28 ottobre 2014, sono state chiamate a dirimere il potenziale contrasto giurisprudenziale che si stava

---

[136] Contrariamente si esprime F. PAZIENZA, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547,* in Rivista Italiana di Diritto e Procedura Penale, 1995, che ritiene che il reato si consumi nel momento in cui l'agente apprende i dati contenuti nel sistema.

[137] V. Cass, pen., Sez. Un., 26.03-24.04.2015, n. 17325, cui viene posto il seguente quesito: «Se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-*ter*, cod. pen., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il *server* che elabora e controlla le credenziali di autenticazione fornite dall'agente.» La Corte afferma il seguente principio di diritto: «Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-

venendo a creare in merito alla individuazione del giudice territorialmente competente. Due erano gli orientamenti emersi: il primo riteneva che il giudice territorialmente competente fosse quello del luogo in cui opera l'operatore remoto che connettendosi alla Rete effettua l'accesso abusivo; l'altro, invece, lo individuava nel tribunale del luogo di ubicazione del *server* violato. La Cassazione a Sezioni Unite ha ritenuto per l'appunto preferibile l'interpretazione di chi, privilegiando la natura dei sistemi informatici e telematici e il loro funzionamento delocalizzato all'interno della Rete, individua il luogo di commissione del reato nel posto in cui opera l'utente malintenzionato. Viene perciò enfatizzato il luogo da cui parte il dialogo elettronico tra sistemi interconnessi: «*L'accesso inizia con l'unica condotta umana di natura materiale, consistente nella digitalizzazione da remoto delle credenziali di autenticazione da parte dell'utente, mentre tutti gli eventi successivi assumono i connotati di comportamenti comunicativi tra il client e il server. L'ingresso o l'introduzione abusiva, allora, vengono ad essere integrati nel luogo in cui l'operatore materialmente digita la password di accesso o esegue la procedura di login, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca-dati*».

Già nel momento in cui l'operatore non autorizzato accede al computer remoto e instaura il dialogo logico con il sistema centrale, violando le misure di sicurezza fin dalla procedura di *login*, manifesta la sua volontà di introdursi abusivamente nel sistema altrui; nel caso poi in cui il *server* non dovesse validare le credenziali inserite, l'agente risponderà solo di delitto tentato. Nella diversa ipotesi del mantenimento nel sistema contro la volontà del titolare, dopo un accesso legittimo, è comunque irrilevante il luogo in cui è collocato il *server*, dovendo attribuire importanza alla postazione periferica dell'operatore remoto, da cui vengono trasferiti i dati.

Fare riferimento al luogo in cui opera il reo è, oltretutto, lettura coerente con il principio del giudice naturale precostituito (art. 25 Cost[138]), il quale, tipicamente, è il giudice del luogo in cui è più forte la richiesta di legalità e in cui si reperiscono maggiormente le prove del reato.

---

ter cod. pen., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente».

[138] Art. 25, co.1 Cost: «Nessuno può essere distolto dal giudice naturale precostituito per legge».

Tuttavia, questa è una tesi che non risulta convincente per una parte della dottrina[139], la quale critica una simile impostazione per il fatto di non aver tenuto adeguatamente conto di come si sia accentuata la dimensione tecnologica nel corso degli anni, dal momento che oggi la maggior parte dei criminali informatici è in grado di commettere un accesso abusivo attraverso *Internet Service Provider* collocati in luoghi diversi da quello in cui operano. Evidente è dunque la difficoltà nell'individuare il luogo in cui fisicamente si trova il terminale utilizzato per commettere un determinato accesso abusivo. Sotto questo punto di vista, risulta allora logicamente più corretto individuare il *locus commissi delicti* nel posto in cui si trova il *server* del sistema violato (dove, cioè, è materialmente situato l'elaboratore che controlla le credenziali di autenticazione del *client*), piuttosto che il luogo di inserimento dei dati o quello in cui si usano successivamente le informazioni eventualmente apprese. È una lettura coerente, anche perché la condotta sanzionata non è certo costituita dalle operazioni eseguite nell'elaboratore remoto (l'uso di credenziali o altra attività equipollente) e, per i reati di mera condotta – anche commessi *online* – è ben possibile che la volontà delittuosa dell'agente si formi e le attività preparatorie vengano realizzate in luogo diverso da quello in cui viene posta in essere la condotta giuridicamente rilevante che identifica il luogo di consumazione del reato[140].

Infine, in merito all'ammissibilità o meno del tentativo, si rimanda a quanto sopra già illustrato (paragrafo 3).

---

[139] Cfr. I. SALVADORI, *I reati contro la riservatezza informatica*, cit., pp. 716-717.

[140] Cass. pen., Sez I, 27.05.2013, n. 40303: «Il luogo in cui si consuma il reato, quindi, non è quello nel quale vengono inseriti i dati idonei a entrare nel sistema, bensì, quello in cui si entra nel sistema. Non possono prendersi in considerazione, pertanto, ai fini della determinazione del luogo di consumazione del reato, né le eventuali condotte successive di acquisizione ed uso dei dati, né il luogo in cui l'accesso al sistema è iniziato attraverso i terminali che costituiscono strumenti di accesso. La procedura di accesso deve ritenersi atto prodromico alla introduzione nel sistema che avviene solo nel momento in cui si entra effettivamente nel server… nel momento in cui l'utente dà l'invio all'esito alla digitazione delle credenziali non fa cessare la propria condotta, ma la fa strumentalmente proseguire, ancorché smaterializzata, sino alla verifica all'ingresso delle misure di sicurezza logiche presenti sul *server web*, essendo queste che manifestano lo *jus excludendi* del *dominus loci*».

9. *Le circostanze aggravanti*

All'ipotesi base disciplinata al primo comma, segue la previsione di quattro circostanze aggravanti ad effetto speciale, in presenza delle quali si registra un inasprimento della pena edittale, prevedendo la pena della reclusione da 1 a 5 anni (co. 2) ovvero, qualora la condotta ricada su sistemi informatici o telematici di interesse pubblico, aumentandola ulteriormente da 3 a 8 anni (co. 3).
Si tratta di ipotesi aggravate in cui la punibilità non è più a querela della persona offesa – come nell'ipotesi base in cui rileva prevalentemente la lesione della sfera privata della persona offesa – perché consentono che si proceda d'ufficio, in quanto atte ad arrecare danni maggiori e coinvolgenti interessi più generali[141].

9.1. *Circostanza aggravante determinata dal ruolo dell'attore*

Il delitto di accesso abusivo ad un sistema informatico o telematico è un reato comune, perché può essere compiuto da chiunque. Il legislatore prevede anche delle ipotesi in cui quella stessa azione viene posta in essere da soggetti qualificati dotati di competenze specifiche, cui fa seguire una risposta più grave sotto il profilo sanzionatorio. «*La pena è della reclusione da uno a cinque anni: se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema*».
La prima ipotesi contemplata è quella del funzionario pubblico che accede abusivamente ad un sistema informatico o telematico con "abuso dei poteri" o con "violazione dei doveri".
Giurisprudenza e dottrina hanno innanzitutto dibattuto se tale previsione costituisca una fattispecie autonoma di reato piuttosto che una circostanza aggravante ad effetto speciale[142].

---

[141] Art. 615-*ter*, co. 4 c.p.: «Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio».
[142] R. BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato,* cit., p. 126: «in una prospettiva di tutela del domicilio, dove l'accesso al di là dell'autorizzazione rappresenta un fatto lecito, la previsione di un'ipotesi che punisce l'ingresso abusivo

A sostegno della tesi che configura la disposizione quale ipotesi autonoma di reato sovviene la circostanza che gli elementi specializzanti di cui all'art. 615-*ter*, comma 2, n. 1 – ovverosia l'abusività della condotta e la violazione dei doveri inerenti alla funzione o servizio – integrano già la circostanza aggravante comune di cui all'art. 61, n. 9 c.p.[143]. La conseguenza è che, avendo il legislatore voluto espressamente dar rilievo a tali note modali, si ha a che fare con un'autonoma ipotesi di reato; diversamente, il legislatore avrebbe semplicemente taciuto le circostanze aggravanti, valendo il rinvio alla previsione di cui all'art. 61 c.p. In questa prospettiva, la fattispecie base contemplata al comma 1 si limiterebbe a punire le ipotesi di accesso abusivo poste in essere dal c.d. *outsider*, cioè da quel soggetto privo di qualsivoglia autorizzazione da parte del titolare dello *ius excludendi*; mentre il comma 2, n. 1 andrebbe riferito alle ipotesi di reato commesse dal c.d. *insider,* cioè il soggetto qualificato che abusi della formale abilitazione ad introdursi nel sistema informatico altrui, utilizzando quindi il sistema oltre i limiti consentiti[144]. Pertanto, si tratterebbe di una fattispecie caratterizzata dall'abuso delle prerogative derivanti dalla qualifica pubblicistica del soggetto agente, e non dal carattere abusivo della condotta nel senso di azione posta in essere contro la volontà del titolare del diritto di esclusione.

---

del pubblico ufficiale non può che rappresentare una fattispecie autonoma, in virtù del fatto che si prevedono modalità di condotta non contemplate nella fattispecie base, con la conseguenza che non esiste un vero e proprio rapporto di specialità tra la fattispecie base e quella aggravata, quanto piuttosto di interferenza. In una prospettiva di tutela della riservatezza dei dati, invece, la fattispecie aggravante deve essere qualificata come circostanza, essendo in rapporto di specialità per specificazione in ordine al soggetto attivo e alle modalità di condotta ed esprimendo un disvalore consentaneo rispetto alla fattispecie base».

[143] Art. 61, n. 9 c.p.: «Aggravano il reato, quando non ne sono elementi costitutivi o circostanze aggravanti speciali, le circostanze seguenti: 9) l'aver commesso il fatto con abuso dei poteri, o con violazione dei doveri inerenti a una pubblica funzione o a un pubblico servizio…»

[144] In questo senso Cass. pen., Sez. V, 30.09.2008, n. 1727: «L'accesso abusivo ad un sistema informatico (art. 615 *ter*, comma 1, c.p.) e l'accesso commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri o con abuso della qualità di operatore del sistema (art. 615 *ter*, comma 2 n. 1) configurano due distinte ipotesi di reato, l'applicabilità di una delle quali esclude l'altra secondo il principio di specialità; concernendo il comma 1 l'accesso abusivo ovvero l'intrusione da parte di colui che non sia in alcun modo abilitato, mentre il comma 2 – non costituisce una mera aggravante – ma concerne il caso in cui soggetti abilitati all'accesso abusino di detta abilitazione.»; Cass. pen., sez. V, 18.1.2011, n. 24583: «Il capoverso richiamato non costituisce una aggravante del fatto descritto nel comma 1, ma una ipotesi diversa di reato perché la disposizione si riferisce evidentemente a soggetti ordinariamente abilitati ad entrare nel sistema, il cui accesso sarebbe, pertanto, di regola legittimo, ma diviene penalmente rilevante quando i predetti abbiano fatto abuso di tale loro abilitazione».

Tuttavia, è una conclusione questa che non convince la giurisprudenza e la dottrina maggioritarie. Sono infatti molteplici gli elementi che inducono a riconoscere la natura circostanziale di questa ipotesi.

In primo luogo, dal punto di vista formale, già i lavori preparatori alla Legge n. 547/1993 qualificano tale ipotesi delittuosa come circostanza aggravante[145].

In secondo luogo, la condotta tipica della fattispecie in esame ricomprende tutti gli elementi costitutivi del reato-base, oltre a connotarsi per degli elementi ulteriori che giustificano la previsione di una pena più alta. Tra l'art. 615-*ter*, comma 1 e comma 2, n. 1, c.p. sussiste un rapporto di specialità unilaterale per aggiunta, dal momento che, per configurare l'ipotesi di cui al comma 2, n. 1, è necessario che il pubblico ufficiale o l'incaricato di pubblico servizio commetta il "fatto" di cui al comma 1. Gli elementi specializzanti che presuppongono l'individuazione di un'ipotesi circostanziata sono dati dalla qualifica pubblicistica del soggetto agente, il quale deve essere investito della funzione di pubblico ufficiale[146] o di incaricato di pubblico servizio[147], e dall'abusività della condotta sotto forma di abuso dei poteri o violazione dei doveri inerenti alle funzioni o al servizio.

Le disposizioni giuridiche, organizzative, contrattuali che delimitano le competenze del pubblico ufficio o che, più nello specifico, regolano i presupposti e stabiliscono i limiti per accedere ad un sistema informatico sono i criteri da guardare per determinare quando l'introduzione o il mantenimento in un sistema informatico da parte di un pubblico ufficiale o di un incaricato di pubblico servizio siano da considerare abusivi. Non si può dunque avere come riferimento esclusivamente i principi generali di trasparenza, buon andamento, fedeltà che conformano lo statuto della pubblica amministrazione. In altre parole, è abusivo l'accesso ad un sistema informatico da parte di questi soggetti qualificati,

---

[145] XI Legislatura, d.d.l. n. 2773, presentato alla Camera l'11.06.1993.

[146] Art. 357 c.p.: «1. Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. 2. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi, e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi».

[147] Art. 358 c.p.: «1. Agli effetti della legge penale, sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. 2. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale».

qualora questi si introducano o si mantengano nel sistema senza autorizzazione ovvero eccedendo i limiti che le disposizioni del titolare dello *ius excludendi*, la normativa di settore o le regole di condotta pongono all'esercizio delle loro funzioni e dei loro poteri[148]. Inoltre, integra il delitto di cui all'art. 615-*ter*, secondo comma, n. 1, c.p. anche l'ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio sia abilitato ad accedere al sistema informatico o telematico protetto e realizzi la condotta tipica per ragioni ontologicamente estranee a quelle d'ufficio, senza neppure violare le prescrizioni impartitegli dal titolare dello *ius excludendi,* ma perseguendo ragioni private e personali[149]. Si tratta dell'ipotesi di accesso formalmente autorizzato ma comunque abusivo, poiché viziato da uno sviamento di potere, il quale si manifesta allorquando il potere venga esercitato dal funzionario pubblico violando i doveri di fedeltà che dovrebbero indirizzare l'assolvimento dei compiti che gli vengono assegnati.

L'abuso dei poteri o la violazione dei doveri inerenti alla funzione o al servizio devono costituire il mezzo che permette o agevola l'esecuzione del reato, nel senso che deve sussistere una connessione funzionale tra l'accesso abusivo commesso dal funzionario pubblico e l'inappropriato esercizio dei poteri pubblici. Il pubblico ufficiale, o l'incaricato di un pubblico servizio, deve cioè servirsi strumentalmente ed abusivamente dei poteri di cui dispone per l'esercizio delle sue funzioni proprio al fine di accedere abusivamente nel sistema informatico[150].

La condotta tipica acquista qui un maggior disvalore a causa del rapporto fiduciario che lega il soggetto agente al sistema informatico violato, dal momento che il funzionario pubblico gode di poteri di cui può servirsi strumentalmente per accedere illecitamente

---

[148] Cfr. I. SALVADORI, *I reati contro la riservatezza informatica*, cit., pp. 720-721.

[149] V. Cass. pen., Sez. Un., 18.05-08.09.2017, n. 41210 ; Cass. pen., Sez. V, 07.11.2000, n. 12732: «D'altro canto, l'analogia con la fattispecie della violazione di domicilio deve indurre a concludere che integri la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa, e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'acceso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva».

[150] Cass. pen., Sez. V, 13.06-04.10.2022, n. 37459: «ai fini della configurabilità della circostanza aggravante di cui all'art. 615-*ter*, comma 2, n. 1, c.p., non è sufficiente la mera qualifica di pubblico ufficiale o di incaricato di pubblico servizio del soggetto attivo, ma è necessario che il fatto sia commesso con abuso dei poteri o violazione dei doveri inerenti alla funzione, di modo che la qualità soggettiva dell'agente abbia quanto meno agevolato la realizzazione del reato.»; Contrariamente Cass. pen., Sez. Un., 18.05-08.09.2017, n. 41210, ritiene che il reato commesso dai soggetti presi in considerazione dal comma 2, n. 1 è sempre aggravato, in quanto «la circostanza è inscindibilmente collegata a quella qualità soggettiva».

con più facilità. Il rapporto di agevolazione che lega la qualifica ricoperta dal soggetto agente alla commissione del fatto tipico giustifica, di conseguenza, l'aumento di pena e la procedibilità d'ufficio.
Il bene giuridico tutelato dalla ipotesi circostanziata acquista, dunque, una dimensione anche pubblicistica: non si tutela solo la riservatezza informatica, già offesa dalla condotta-base di introduzione o mantenimento abusivi, ma anche la pretesa a che la pubblica amministrazione tenga un comportamento corretto[151].

Per quanto riguarda l'accesso abusivo commesso da un investigatore privato che abbia esercitato abusivamente la professione, l'inasprimento della pena è giustificato per il fatto che qui l'agente è un soggetto che dispone, di regola, di mezzi specifici e conoscenze tecnico-informatiche più avanzate per violare la riservatezza del titolare del sistema. Ne risulta pertanto che la condotta di introduzione o mantenimento fraudolento nel sistema informatico altrui si caratterizza, potenzialmente, per una maggiore insidiosità.

Nel contesto della circostanza aggravante di cui al n. 1, comma 2, dell'art. 615-ter c.p., rientra anche l'ipotesi di accesso abusivo commesso dall'operatore del sistema, il quale, sfruttando la posizione ricoperta, abusi delle proprie funzioni.
In assenza di indicazioni specifiche, si interpreta la nozione di "operatore del sistema" in modo ampio, ricomprendendovi in generale tutti i soggetti che a vario titolo siano legittimati ad operare sul sistema informatico. Più coerente con il linguaggio informatico sarebbe stata la locuzione di "amministratore di sistema" (c.d. *system administrator*), con tale riferendosi a quei tecnici che riescono ad accedere più facilmente ai sistemi informatici, avendone il controllo sulle fasi del processo di elaborazione dei dati informatici (è colui cioè che dà avvio e arresto al sistema, che stabilisce le operazioni da far eseguire al *software,* eventualmente aggiornando gli algoritmi per compiere nuove e più specifiche funzioni, che può accedere e visionare tutti i settori della memoria del sistema). Rimangono fuori dalla nozione in esame il semplice operatore, cui vengono attribuite funzioni meramente esecutive, e figure professionali come il programmatore o

[151] Art. 97, co. 2 Cost.: «I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione».

l'analista, i quali dispongono di conoscenze limitate ad uno o comunque solo alcuni settori del sistema[152].

Anche in queste ipotesi, è il rapporto privilegiato con il sistema informatico conseguente alle mansioni tecniche svolte dall'operatore del sistema a giustificare il trattamento sanzionatorio più rigoroso. Il comportamento deviante qui risulta ancor più riprovevole in quanto è proprio il rapporto con il sistema ad agevolare l'abuso, andando al contempo a violare l'obbligo di buona fede nei confronti del soggetto che ha concesso quei privilegi.

9.2. *Circostanza aggravante determinata dalla gravità della condotta*

«*La pena è della reclusione da uno a cinque anni: se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato*».

Il concetto di "violenza sulle cose" comprende sia i casi in cui l'agente eserciti violenza fisica sulla componente *hardware* del sistema (ad esempio, sulle chiavi predisposte all'accensione del computer) ovvero sui mezzi di sicurezza (ad esempio, porte blindate poste a protezione del luogo in cui si trova l'elaboratore), sia i casi di violenza logica esercitata sulla componente *software* del sistema informatico (come l'elusione di programmi antivirus).

La legge 23 dicembre 1993, n. 547, integrando l'articolo 392 del codice penale con l'aggiunta di un terzo comma, ha ampliato le ipotesi di violenza sulle cose per includere specificamente le azioni perpetrare sul *software*. Questo si deve alla considerazione che i casi tradizionali di danneggiamento, trasformazione o mutamento di destinazione della cosa (previste al comma 2), potendo magari trovare applicazione alla violenza commessa a danno della parte *hardware*, mal si adattavano alla natura del danno inflitto sul *software*. Il legislatore allora, astraendosi dal contesto più propriamente materiale, ha stabilito che «*si ha altresì violenza sulle cose allorché un programma informatico viene alterato,*

[152] Cass. pen., Sez. V, 24.01-03.03.2022, n. 7775: «l'operatore del sistema di cui tratta il secondo comma dell'art. 615-ter non può pertanto identificarsi semplicemente con colui che è legittimato ad accedere al sistema, in quanto tale figura soggettiva è già considerata nel comma precedente tra i potenziali autori del reato base… L'operatore è, in definitiva, il soggetto che viene abilitato a modificare i contenuti o la struttura del sistema ovvero di una sua parte, con esclusione dunque di chi viene semplicemente autorizzato a fruire dei suddetti contenuti. Al contempo l'attribuzione della qualifica non necessariamente comporta anche quella della titolarità di poteri decisori sulla gestione di tali contenuti o sulla configurazione del sistema, potendo invece essergli riconosciuti anche compiti meramente esecutivi».

modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico»[153]. Da questa disposizione emerge che il legislatore, nel regolare tematiche che attengono al diritto penale dell'informatica, le forgia diversamente rispetto ai concetti tradizionali, prevedendo che già il mero temporaneo turbamento del sistema informatico possa costituire un danno per il funzionamento del sistema stesso. In un'ottica di modernità, si estende il concetto di violenza sulle cose anche al sistema informatico senza richiedere che la turbativa del programma sia permanente.

Per la configurabilità dell'aggravante in questione, è necessario che sussista una effettiva connessione funzionale[154] tra l'impiego della violenza sulle cose e l'accesso abusivo, nel senso che la violenza deve costituire il mezzo che renda possibile, o quantomeno faciliti, l'accesso abusivo (è, ad esempio, il caso di chi riesca a stabilire il collegamento logico con il computer altrui, avendo alterato il coretto funzionamento di un programma *firewall*).

Le altre ipotesi aggravanti previste sempre al n. 2, dell'art. 615-*ter*, comma 2, c.p., relative al caso del soggetto che per accedere abusivamente ad un sistema informatico o telematico usa "violenza sulle persone" ovvero che sia "palesemente armato", rivestono oggi un'incidenza alquanto marginale, in quanto riferite a situazioni in cui si esercita violenza sul personale di sorveglianza. Trattasi di circostanze che avevano una loro ragione nell'epoca in cui ancora era necessario un contatto fisico diretto con l'elaboratore per effettuare un attacco informatico; tuttavia, con il progressivo evolversi dell'interconnessione telematica, i criminali informatici riescono ad accedere da remoto sfruttando la Rete, rendendo meno centrale il ricorso alla violenza sulle persone.

Essendo un'ipotesi ormai priva di riscontri nella prassi, non si esclude che tale aggravante possa venire del tutto abrogata.

---

[153] Art. 392, co. 3 c.p.

[154] F. MANTOVANI, *Diritto penale. Parte Speciale. I delitti contro la persona*, I, Milano, 2016, p. 578, ritiene che debba sussistere un «rapporto teleologico strumentale».

9.3. *Circostanza aggravante determinata dalle conseguenze della condotta*

«*La pena è della reclusione da uno a cinque anni: se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti*».

L'art. 615-*ter*, comma 2, n. 3, c.p. prevede un'ipotesi di reato aggravato dall'evento, perché il reato base di mera condotta subisce un aggravio di pena per il verificarsi di un evento ulteriore (danni al sistema informatico o ai suoi contenuti) rispetto al fatto che già costituisce reato (introduzione o mantenimento abusivi).

Il danneggiamento dei beni informatici rileva quindi come mera conseguenza della condotta, perché nel caso in cui costituisse il mezzo necessario o agevolatore per realizzare l'accesso abusivo troverebbe applicazione la disposizione di cui al n. 2 del comma 2 relativa alla violenza sulle cose.

Il soggetto agente non deve aver voluto l'elemento qualificante della distruzione, del danneggiamento o dell'interruzione, in tutto o in parte, del funzionamento del sistema informatico ovvero la distruzione o il danneggiamento dei dati e dei programmi informatici ivi presenti. Diversamente, si configurerebbe la fattispecie di *danneggiamento di informazioni, dati e programmi informatici* [155] e di *danneggiamento di sistemi informatici o telematici*[156] in concorso con il reato di accesso abusivo ad un sistema informatico o telematico[157].

---

[155] Art. 635-*bis* c.p.: «1. Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. 2. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni».

[156] Art. 635-*quater* c.p.: «1. Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 *bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. 2. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata».

[157] Cass. pen., Sez. V, 25.03.2019, n. 18284: «In ipotesi di accesso abusivo ad una casella di posta elettronica protetta da *password,* il reato di cui all'art. 615-*ter* c.p. concorre con il delitto di violazione di corrispondenza in relazione alla acquisizione del contenuto delle *mail* custodite nell'archivio e con il reato di danneggiamento di dati informatici, di cui agli artt. 635-*bis* e ss. c.p., nel caso in cui, all'abusiva modificazione delle credenziali d'accesso, consegue l'inutilizzabilità della casella di posta da parte del titolare».

Un altro orientamento, invece, qualifica l'art. 615-*ter*, comma 2, n. 3, c.p. come ipotesi di reato circostanziato. Ne discenderebbe in questa prospettiva che il danneggiamento del sistema nel suo complesso o delle sue singole componenti, conseguenti alla condotta di introduzione o mantenimento, rileva come circostanza aggravante, con ricadute pratiche in termini di bilanciamento delle circostanze ai sensi dell'art. 69 c.p., valutazione inoperante nel caso di reato aggravato dall'evento.

La Corte di legittimità ha specificato dirsi sussistente il reato di accesso abusivo ad un sistema informatico, aggravato dal danneggiamento del sistema medesimo, nel caso «*in cui dall'accesso abusivo derivi un danno al sistema o alle sue componenti, logiche o fisiche, o anche l'interruzione totale o parziale del suo funzionamento e, così, rendendo il sistema parzialmente o totalmente inservibile per gli usi cui è destinato*»[158].

Infine, l'art. 491-*bis* c.p.[159] prevede che nel caso in cui il danneggiamento abbia ad oggetto un documento informatico pubblico avente efficacia probatoria trovino applicazione, in concorso con il delitto di accesso abusivo, le fattispecie più gravi di falsità per soppressione o distruzione[160].

9.4. *Circostanza aggravante determinata dall'oggetto della condotta*

«*Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o*

[158] Cass. pen., Sez. V, 15.11-05.12.2022, n. 46076, in cui la Corte ha ritenuto sussistente la circostanza aggravata prevista nel comma 2, n. 3, nel caso di modifica delle credenziali di accesso alla casella di posta elettronica altrui: «La password, in sé, rappresenta una serie di caratteri alfanumerici che regola l'accesso al sistema informatico ed è diretta a tutelare il sistema in sé e le informazioni in esso contenute. In quanto tale, quindi, rappresenta parte integrante del sistema, poiché permette al sistema stesso di svolgere le sue funzioni, impedendo l'accesso ad estranei. Ne consegue che l'alterazione della password e la sua modifica integra l'aggravante contestata in quanto condotta che altera una componente essenziale del sistema, rendendola inidonea all'uso al quale è destinata».

[159] «Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici».

[160] Art. 476 c.p.: «1. Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. 2. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.»; Art. 490 c.p.: «Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero, o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute».

alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni».

L'art. 615-*ter*, comma 3, c.p. prevede un inasprimento della pena, rispettivamente da uno a cinque anni e da tre a otto anni, qualora l'ipotesi base di accesso abusivo (comma 1) ovvero quelle circostanziate (comma 2) abbiano ad oggetto un particolare tipo di sistema informatico o telematico – di pubblica utilità.

La previsione di questo aggravio di pena è perfettamente giustificabile considerando l'importanza che il regolare funzionamento delle infrastrutture critiche dello Stato riveste per la comunità. Tali infrastrutture, che includono ad esempio la distribuzione dell'energia elettrica, le telecomunicazioni, i servizi sanitari e di trasporto, contengono dati e programmi la cui integrità è di importanza cruciale data la loro natura riservata, sicché l'accesso abusivo a questi sistemi si caratterizza senza dubbio per un maggior grado di pericolosità.

In dottrina, si critica che la disposizione pecchi di indeterminatezza per l'utilizzo della clausola di chiusura «*o comunque di interesse pubblico*», la quale – pur evitando di riportare una elencazione magari poco esaustiva che vada a restringere l'area dei sistemi pubblici meritevoli di tutela penale rafforzata – lascia incerti i criteri in base ai quali ritenere che la connotazione pubblicistica del sistema possa dar applicazione all'aggravante in esame[161]. L'impiego di espressioni vaghe porta inevitabilmente con sé il rischio di porre in essere delle disparità di trattamento.

La Suprema Corte ha adottato una concezione oggettiva dei criteri identificativi della natura pubblica di un servizio, pertanto, facendo leva sul tipo di interesse perseguito con l'attività svolta, riconduce alla nozione di sistema informatico o telematico di interesse pubblico solo quei sistemi destinati al servizio di una collettività indifferenziata e indeterminata di soggetti: «*il tenore della norma consente di fare rientrare in tale nozione, a prescindere dal soggetto che la espleta o al quale l'attività è collegata, ogni sistema che, per il carattere riservato dei dati che vi sono immagazzinati e per l'importanza che il loro funzionamento regolare e indisturbato può rivestire per l'intera collettività, soddisfa un interesse collettivo*»[162].

---

[161] Cfr. I. SALVADORI, *I reati contro la riservatezza informatica*, cit., p. 726.

[162] Cass. pen., Sez. V, 16.03-23.06.2021, n. 24576; Cass. pen., Sez. V, 13.12.2010-21.01.2011, n. 1934: «ai fini della configurabilità della circostanza aggravante dell'essere il sistema di interesse pubblico non è sufficiente la qualità di concessionario di pubblico servizio rivestita dal titolare del sistema, dovendosi

Nonostante l'intervento giurisprudenziale in funzione integratrice volto a chiarire la portata della norma, a fronte della mancanza di precise soluzioni normative si è giunti ad interpretazioni tra loro difformi, poiché il concetto rimane ancora vago e questo comporta una pluralità di incertezze nell'applicazione pratica del diritto[163]. Fintanto che non si arrivi ad emanare una normativa *ad hoc,* al giudice rimane una significativa discrezionalità nella determinazione del concetto di "interesse pubblico"[164].

accertare se il sistema informatico o telematico si riferisca ad attività direttamente rivolta al soddisfacimento di bisogni generali della collettività».

[163] Ad esempio, si nega la sussistenza dell'aggravante in questione in un caso di accesso abusivo al sito *web* fondatore di un movimento politico di rilievo nazionale (Cass. pen., Sez. V, 16.03-23.06.2021, n. 24576), ma si riconosce una tal tutela nel caso di accesso abusivo all'area riservata alla gestione della carta *Postepay* di un utente privato di Poste Italiane (Cass. pen., Sez. V, 13.01.2016, n. 6906); ancora, non viene considerata aggravata la lesione al circuito bancomat di un istituto di credito (Cass. pen., Sez. V, 18.12.2014, n. 10121), mentre si ritiene aggravato l'accesso abusivo agli archivi di posta elettronica degli studenti di una Università (Trib. de L'Aquila, 10.06.2005).

[164] Cass. pen., Sez. V, 30.01-27.04.2023, n. 17551: «Integra il delitto previsto dall'art. 615-*ter*, comma terzo, cod. pen. la condotta dell'ufficiale di polizia giudiziaria che acceda alla banca dati interforze in violazione delle procedure interne di carattere autorizzativo e per finalità meramente esplorative, onde acquisire informazioni su colleghi e personaggi pubblici in assenza anche solo di un qualificato sospetto idoneo a stimolare l'attività di iniziativa della polizia giudiziaria».

CAPITOLO 3

-

VERSO UNA CONSAPEVOLEZZA DEL DIGITALE

SOMMARIO: 1. L'evoluzione dell'intelligenza artificiale. – **1.1.** Le nuove frontiere della criminalità informatica. – **1.2.** L'etica dell'intelligenza artificiale. – **2.** Il ruolo dell'*Internet Service Provider*. – **3.** La disinformazione del digitale. – **3.1.** Il ruolo promotore dell'Unione Europea.

1. *L'evoluzione dell'intelligenza artificiale*

L'invenzione e la rapida diffusione dei *personal computer* hanno permesso all'informatica di divenire punto di interesse e riflessione anche tra i giuristi, i quali si interrogano su questioni di primaria importanza, tra cui la protezione da offrire ai dati informatici, la tutela dei programmi e del *software,* il diritto d'autore e la sicurezza nelle transazioni di *e-commerce*.

La rivoluzione digitale, creando una rete di connessioni su scala globale tra dispositivi elettronici e persone in tutto il mondo – facilitando così le interazioni sociali e promuovendo un flusso dinamico nella circolazione e condivisione delle informazioni – ha trasferito la vita lavorativa e sociale in una dimensione virtuale.

Questa trasformazione rapida e continua porta a parlare di rivoluzione dell'intelligenza artificiale: una indefinita categoria di attività, un tempo esclusivo appannaggio del lavoro dell'uomo, oggi può essere eseguita da macchine che col tempo sono state dotate di avanzate capacità di apprendimento e di ragionamento logico.

La manifestazione delle tecnologie nella realtà ha origine alla creazione dei *robot*, che oggi fanno parte della cultura scientifica ma la cui ideazione è frutto della narrativa fantascientifica di alcuni scrittori[165].

[165] Il termine *robot* deriva dal vocabolo ceco *robota* (accezione usata nel senso di "lavoro servile"), introdotto per la prima volta dallo scrittore Karel Capek nel suo dramma fantascientifico *R.U.R.* (*Rossum's Universal Robots*) del 1920, in cui descrive i *robot* come macchine antropomorfe progettate per alleviare le fatiche degli umani, che riescono a prendere il sopravvento e a dominare la società.

A partire dalla rappresentazione dei *robot* come sistemi meccatronici, imitativi e autonomi, si è sviluppata una consistente ricerca scientifica e tecnologica giunta a definire per la prima volta l'intelligenza artificiale negli anni '50 del secolo scorso, in occasione della conferenza tenutasi a Darthmouth: «ogni aspetto dell'intelligenza può essere descritto in termini tanto rigorosi da rendere possibile la programmazione di una macchina in grado di simularli»[166].

Ad oggi, parlando di intelligenza artificiale (IA) si fa riferimento a quel ramo della scienza e dell'ingegneria che studia come sviluppare sistemi e tecnologie che riescano ad imitare l'intelligenza umana. Quest'ultima viene intesa come la capacità di apprendere in modo rapido, risolvere problemi (*problem solving*) e adattarsi a nuove situazioni mediante ragionamenti di tipo creativo e logico (*decision making*).

Dall'analisi comparativa emerge che, così come l'intelligenza umana può essere sviluppata e consolidata attraverso l'educazione, l'esperienza e la pratica, anche l'IA – la quale è al momento confinata ai soli ambiti per i quali è stata progettata – possa essere ulteriormente potenziata. Sebbene i sistemi artificiali siano costruiti in modo più semplice rispetto al sistema nervoso umano, di per sé capace di interagire con i processi metabolici del corpo, essi hanno già dato prova di essere in grado di svolgere alcune operazioni più velocemente. Sono infatti sistemi dotati di ottima capacità logico-computazionale e capaci di includere l'analisi di una quantità elevata di dati, considerevolmente superiore rispetto alle informazioni che la mente umana saprebbe conservare.

Successivamente, altri autori iniziano a trattare del rapporto tra i *robot* (meccanismi androidi che svolgono in maniera autonoma un lavoro simile a quello dell'uomo) e gli uomini. In particolare, Isaac Asimov, nella raccolta di saggi *Io, robot* del 1950, introduce tre leggi sulla robotica volte a stabilire delle regole di convivenza:

1) Un *robot* non può recare danno ad un essere umano né permettere che, a causa del mancato proprio intervento, un essere umano subisca un danno.
2) Un *robot* deve obbedire agli ordini impartiti dagli essere umani, purché tali ordini non contravvengano alla prima legge.
3) Un *robot* deve proteggere la propria esistenza, purché tale difesa non contrasti con la prima o la seconda legge.

Asimov generalizza poi queste tre leggi in una Legge Zero: "un *robot* non può recar danno all'umanità o permettere che, a causa di un suo mancato intervento, l'umanità subisca un danno".

[166] J. MCCARTHY et al., *A Proposal for the Darthmouth Summer Research Project on Artificial Intelligence,* 1956, in https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html: «*every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it*».

Per ottimizzare questi sistemi, risulta perciò essenziale predisporre tecnologie *hardware* e s*oftware* appropriate. L'approccio iniziale all'IA come sistema simbolico-deduttivo, fondato, cioè, sull'utilizzo di simboli (testi, immagini o sequenze di dati) e regole per l'analisi e la soluzione di problemi di ragionamento[167], è stato progressivamente superato per lasciar spazio negli ultimi anni a tecniche più moderne e metodologie più avanzate che utilizzano metodi induttivi e probabilistici, come il *deep learning* o addirittura l'apprendimento automatico.

In particolare, l'autoapprendimento (o *machine learning*) è quel ramo dell'intelligenza artificiale che consente ai sistemi di apprendere e migliorare i servizi che offre a partire dall'esperienza pratica, senza cioè la necessità di dover essere esplicitamente programmati a priori per ogni specifica attività. Si tratta pertanto di un processo che può portare l'IA a compiere azioni e prendere decisioni non antecedentemente previste o comunque non poste sotto il controllo diretto degli sviluppatori o degli utenti, per adeguarsi ai nuovi stimoli che riceve dall'ambiente esterno. Il tipo di sorveglianza che l'uomo è in grado di esercitare sulla macchina diminuisce ancora di più qualora si faccia ricorso alle tecniche di *cloud computing*, mediante le quali il sistema di IA riesce a scambiare informazioni e ad apprendere dall'esperienza di un altro agente artificiale[168].

La macchina evolve oltre i confini dell'originaria programmazione, agendo in maniera autonoma e indeterminata, perché grazie alla flessibilità che caratterizza i moderni algoritmi "adattivi" riesce ad affrontare anche situazioni di incertezza o di non conoscenza[169].

Questa situazione solleva interrogativi di rilevante interesse, soprattutto per quanto concerne le potenziali implicazioni nel campo della responsabilità penale. Nel contesto

---

[167] I modelli di intelligenza simbolica erano in grado, ad esempio, di completare una partita di scacchi o risolvere problemi matematici e fisici applicando regole di tipo consequenziale, velocizzando le attività umana ma non riuscendo a gestire situazioni di incertezza.

[168] Si parla di *black box algorithms* per indicare funzionamento del sistema di IA di cui si conosce l'*input* iniziale (i dati inseriti) e l'*output* finale (comportamento tenuto), ma resta ignoto il processo seguito dalla macchina per giungere a quella decisione.

[169] M. B. MAGRO, *Il problema della responsabilità per l'uso di Intelligenze Artificiali*, in *Cybercrime*, UTET, 2023, p. 1233: «Dunque, il sistema di Auto Machine Learning aggiunge al sistema informatico un *quid pluris* rispetto la sua iniziale programmazione (c.d. *deep learning*): perciò questi sistemi sono in grado di reagire (cioè elaborare modelli decisionali) anche a quelle situazioni che non sono neppure previste dal programmatore, né interpretabili o spiegabili sulla base delle regole con cui l'essere umano ha costruito il modello originario di operatività».

giuridico, una delle sfide maggiori che attualmente si pone consiste nel determinare chi effettivamente possa essere considerato responsabile per le azioni intraprese da un sistema di intelligenza artificiale auto-apprendente. Tali sistemi infatti – per come vengono costruiti e dunque per la loro struttura intrinseca – sono capaci di sviluppare competenze o adottare comportamenti non facilmente anticipabili dai loro creatori: la complessità e l'opacità di molti algoritmi di IA, in particolare quelli che si basano su tecniche di apprendimento automatico, rendono difficile comprendere il processo decisionale alla base delle loro azioni. L'obiettivo primario è quindi quello di garantire un livello adeguato di controllo e supervisione su sistemi che sono progettati per funzionare con un certo grado di autonomia in contesti non pianificati, al fine di identificare e correggere possibili distorsioni, discriminazioni volontarie o comunque garantire agli individui la possibilità di contestare decisioni percepite come ingiuste o errate.

Al momento, tuttavia, la normativa relativa all'IA è ancora in fase di sviluppo. Un presupposto fondamentale per poter efficacemente integrare le IA nella società, nel pieno rispetto delle questioni etiche e legali, è la formulazione di leggi specifiche che vadano ad indirizzare le problematiche della responsabilità e del controllo degli agenti intelligenti. Inoltre, considerando che le questioni inerenti l'IA intersecano diverse aree, si auspica che l'elaborazione e la successiva adozione di nuove normative, volte a contemplare le sfide poste da queste nuove tecnologie, addotti un approccio multidisciplinare. L'obiettivo è quello di coinvolgere non soltanto i giuristi ma anche filosofi ed informatici, al fine di realizzare un quadro normativo equilibrato che permetta, da un lato, l'innovazione tecnologica, e, dall'altro, il rispetto e la protezione dei diritti fondamentali.

1.1. *Le nuove frontiere della criminalità informatica*

La ricerca e la regolamentazione dell'intelligenza artificiale, volte a massimizzare i benefici dell'innovazione digitale, hanno altresì determinato un riorientamento delle tecnologie rendendole strumenti suscettibili di essere impiegati anche per facilitare la perpetrazione di atti illeciti: la combinazione di autonomia operativa e la capacità di apprendimento delle intelligenze artificiali costituiscono il fondamento per applicazioni sia vantaggiose che dannose.

Il termine *AI-crime* viene adottato per identificare sia i reati tradizionali compiuti mediante l'ausilio di sistemi intelligenti sia le nuove forme di illeciti commesse dall'intelligenza artificiale. Si tratta di una categoria emergente di criminalità informatica, troppo nuova per trovare ancora una precisa tipizzazione normativa, la quale solleva ulteriori questioni bisognevoli di essere affrontate prontamente dall'ordinamento giuridico, data la crescente molteplicità di modalità attraverso cui possono essere lesi gli interessi altrui. In altre parole, i progressi dell'IA hanno portato con sé un ulteriore lato oscuro della tecnologia.

Dal momento che le macchine che funzionano grazie a sistemi di IA apprendono autonomamente dalla realtà circostante, autodeterminandosi nelle scelte da prendere, si pone il rischio che queste, anche se originariamente programmate per scopi leciti, si veicolino all'illecito adottando comportamenti pregiudizievoli per la dignità altrui. Se un reato è il risultato del processo di apprendimento automatico di un sistema di IA, si può considerare tale situazione sufficiente ad interrompere il nesso di causalità, tale per cui di quel fatto illecito non debba più risponderne l'operatore umano[170]?

È concepibile pensare che una macchina possa commettere un reato?

La tecnologia moderna è quindi giunta a delineare un nuovo soggetto (non umano) cui poter declinare il linguaggio giuridico dei diritti e delle responsabilità?

Comprendere il funzionamento delle macchine intelligenti e il modo che queste hanno di adattarsi alla realtà agendo in autonomia rappresenta il punto di partenza per discutere di una loro eventuale responsabilità giuridica nei confronti degli esseri umani.

I sostenitori dell'attribuzione di responsabilità giuridica alle IA adducono le stesse argomentazioni che hanno animato il dibattito culminato nel riconoscimento della

[170] Può davvero essere accusato un *robot* chirurgo che taglia i tessuti sani invece di quelli malati o un motore di ricerca che sovraespone un post diffamatorio in un social network? Cfr. L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme*, in *Cybercrime*, 2023, p. 83: «La c.d. impredittibilità delle decisioni e dei comportamenti posti in essere renderebbe impossibile la sicura determinazione del nesso causale fra il contributo riferibile ai diversi agenti umani che intervengono nella catena che sta a monte del loro operato e gli eventi offensivi concretamente realizzati». F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in Diritto Penale e Uomo, 2019, p. 27: «A prescindere dalla risposta che si vorrà fornire alla presente questione, sta di fatto che in tutti i casi in cui la condotta dell'uomo si intreccia e si interseca con l'attività di un sistema di IA, il percorso di attribuzione delle responsabilità indubbiamente si complica, giacché le scelte, le valutazioni, i bilanciamenti, sottesi alla commissione del fatto, non sono più opera esclusiva dell'uomo, ma sono quantomeno condivisi con (se non interamente delegati alla) macchina».

responsabilità a carico delle società per reati commessi da propri dipendenti[171]. Si potrebbe ipotizzare un regime di responsabilità delle IA andando a soggettivizzare queste ultime per il tramite dell'operato del loro programmatore o del loro utilizzatore. Sostanzialmente è la stessa logica seguita per affermare la responsabilità amministrativa da reato degli enti: le persone giuridiche, che neppure sono dotate di una loro corporeità fisica, sono ritenute responsabili per i reati commessi dalle persone fisiche in esse incardinate[172].

Tuttavia, permangono differenze significative e di non poco conto che inducono a pensare con molta cautela prima di adottare un impianto sanzionatorio di questo tipo. Le persone che agiscono all'interno dell'ente giuridico rivestono infatti un ruolo fondamentale nel processo decisionale aziendale; ma una tale situazione non è riscontrabile per l'ente artificiale, per cui punirlo non avrebbe effetto dissuasivo sulle persone che rimangono estranee al processo decisionale robotico (c.d. *humans-behind-the-machine*)[173].

---

[171] Questo modello viene sviluppato per la prima volta da HALLEVY G., *Liability for Crimes Involving Artificial Intelligence Systems*, New York, 2015, il quale ritiene che le macchine possano essere rimproverate per i loro comportamenti dolosi o colposi così come si è riusciti a delineare una responsabilità penale degli enti. Cfr. anche L. SOLUM, *Legal Personhood for Artificial Intelligences*, in *North Carolina Law Review* 1992, p. 1248: «*The problem of punishment is not unique to artificial intelligences, however. Corporations are recognized as legal persons and are subject to criminal liability despite the fact that they are not human beings*». Un'analisi critica si rinviene in M. E. FLORIO, *Il dibattito sulla responsabilità penale diretta delle IA: "molto rumore per nulla"?*, in Sistema Penale, 2/2024.

[172] «Il tema quindi presenta forti analogie con quello dell'affermazione di un'etica aziendale e di una conseguente responsabilità da reato degli enti collettivi, sistema con cui potremmo confrontarci nell'ipotesi di danni arrecati dall'agire autonomo di IA. Le analogie sono evidenti: gli enti collettivi non hanno né corpo né anima, ma sono comunque "soggetti giuridici", cioè autori di reati (per il tramite delle persone fisiche incardinate in essi) per la legge penale; i robot invece hanno un "corpo" fisico che interagisce con l'ambiente tramite sensori, una materia su cui far ricadere la sanzione penale (ad esempio, la disattivazione o riprogrammazione della macchina o la sua distruzione) e sono dotati di autonomia decisionale. Ciò consente di ipotizzare un sistema di responsabilità dell'agente artificiale che, sulla falsariga della responsabilità amministrativa da reato degli enti, nel capovolgerne i presupposti, renderebbe responsabile l'agente artificiale soggettivizzato per il suo operare e per quello dell'uomo frontman, ovvero l'utilizzatore, il programmatore, il designer, il produttore, etc.» In questo senso MAGRO M. B., *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in Legislazione Penale, 2020, p. 8.

[173] «L'uomo si limita a crearle e programmarle. Dopo ciò, con il distacco dal proprio artefice, il loro centro decisionale si autonomizza.» Così A. CAPPELLINI, *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, in Criminalia, 2018, p. 18. Vedi anche C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in Riv. it. dir. proc. pen., 4/2020, pp. 1768 ss: «la *societas*, sia che la si interpreti in guisa di uno "schermo", sia alla stregua di un "organo", esiste nella realtà giuridica e sociale, ma è animata, naturalisticamente e spiritualmente, dagli uomini che le danno vita: i precetti che le vengono rivolti sono diretti ai soggetti che l'hanno creata e che la rappresentano, condizionandone il comportamento (specie in vista della dotazione di un'adeguata organizzazione

La previsione *de jure condendo* di una responsabilità diretta a carico dell'agente intelligente non avrebbe utilità pratica[174], in quanto l'eventuale misura sanzionatoria della disattivazione, della distruzione fisica o della riprogrammazione del *software* potrebbero semplicemente incentivare il programmatore a strutturare una macchina di cui sia maggiormente in grado di prevederne l'evoluzione, magari apponendo una serie di limitazioni all'apprendimento automatico. Di certo tutto questo non si tradurrebbe in termini di rimprovero sulla colpevolezza della macchina, nella quale manca il senso di intenzionalità delle proprie azioni (*mens rea*), considerando che, da un punto di vista ontologico, ancora non è in grado di porsi da sé obiettivi di comportamento. Insomma, l'applicazione della sanzione penale a un sistema di IA snaturerebbe le finalità di prevenzione speciale e generale intrinseche alla previsione della pena.

Allo stato, per quanto l'agente intelligente abbia la capacità di autodeterminarsi, è assente una consapevolezza della sua libertà di agire, il che impedisce di considerarlo un vero e proprio soggetto giuridico – centro di imputazione di diritti e doveri. Nonostante gli sviluppi impressionanti nel campo della robotica, è essenziale riconoscere che queste tecnologie derivano le loro capacità di apprendimento, interpretazione dei dati e decisione dagli algoritmi e dai principi di funzionamento che gli esseri umani hanno definito. Anche i sistemi di IA nelle forme più avanzate di *self-learning* costruiscono il loro apprendimento sulla base dei parametri forniti dall'uomo. Oltretutto, il ruolo dell'intelligenza umana non si esaurisce nella fase di programmazione iniziale, ma continua ad essere presente anche nel monitoraggio, valutazione e aggiornamento costante degli algoritmi. C'è un assioma di fondo la cui validità non sembra possa essere

---

preventiva dei reati)». GIANNINI A., *Responsabilità da reato degli enti e intelligenza artificiale*, in *Cybercrime*, 2023, pp. 1444-1445: «non è possibile rinvenire, ad oggi, una struttura sociale sottostante ai singoli sistemi di IA equiparabile a quello che è lo scheletro di una qualsivoglia persona giuridica… Le persone giuridiche, dunque, non sono solo intimamente legate agli "agenti umani", ma sono solo una finzione creata da quest'ultimi. Lo stesso non si potrebbe dire dei sistemi di IA che, invece, parrebbero vivere oltre a questo velo fittizio, in quanto possono, sempre più, agire senza il coinvolgimento degli esseri umani».

[174] Cfr. V. R. BHARGAVA - M. VELASQUEZ, *Is Corporate Responsibility Relevant to Artificial Intelligence Responsibility?*, in *Georgetown Journal of Law and Public Policy*, 2019, p. 851: «*appeals to corporate responsibility can provide no real insight into what moral responsibility might mean when attributed to AI agents*». Contrariamente F. BASILE, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, cit., pp. 31-32: «attraverso lo spegnimento definitivo o temporaneo della macchina, o attraverso la sottoposizione della macchina, dotata di congegni di autoapprendimento, ad un nuovo *training* "rieducativo", si potrebbero realizzare, rispettivamente, la funzione retributiva e la funzione special-preventiva della pena».

superata: *machina delinquere non potest*, nel senso che i soggetti artificiali non possono essere considerati direttamente responsabili per la commissione di un reato.

Al fine di evitare un vuoto di tutela, è fondamentale determinare a chi effettivamente possa imputarsi l'azione posta in essere da un sistema di intelligenza artificiale.
La questione verte più propriamente sulla responsabilità da attribuire alla persona che si avvale del *robot*, alla quale, in prima approssimazione, verrebbero imputati gli effetti degli atti illeciti commessi dai sistemi di IA. Si tratterebbe di sviluppare delle ipotesi di responsabilità vicaria: per i fatti commessi materialmente dalla macchina dovrebbe risponderne la persona fisica, in virtù del rapporto di creazione o di utilizzo che intercorre tra loro. Questo deriva dal fatto che la macchina, anche laddove sia dotata di autonomia decisionale, è pur sempre da considerare uno strumento al servizio dell'uomo.
Per quanto riguarda la previsione di una imputazione a titolo di dolo non emergono questioni particolari. La macchina agisce come una sorta di *longa manus* della persona umana poiché risponde alle sue volontà di programmazione. Di conseguenza, se l'operatore intenzionalmente sfrutta il sistema di IA per perseguire finalità illecite, o comunque accettando volontariamente il rischio che possano essere compiuti reati, dovrà lui risponderne penalmente[175].
L'ipotesi della responsabilità colposa è invece più complessa, in quanto attiene ai casi in cui l'agente intelligente arreca un danno all'insaputa e non voluto dallo sviluppatore o dall'utilizzatore. I sistemi di IA che sfruttano la capacità di *machine learning* rielaborano autonomamente gli stimoli che ricevono dall'esterno, indipendentemente da ulteriori *input* forniti dal programmatore; pertanto, la predeterminabilità dell'agire del *robot* risulta limata perché il costruttore può solo abbozzare genericamente ma non già tradurre in algoritmi tutti i possibili modelli di comportamento che l'entità può tenere dopo aver interpretato la realtà. «*Poiché non tutte le situazioni di vita possono essere*

[175] Tuttavia, c'è anche chi ritiene che «in assenza di prova di istruzioni illecite che precisamente identifichino, anche dal punto di vista spazio-temporale, oltre che del *modus*, il fatto criminoso commissionato all'agente artificiale e da questi poi realizzato, non vi sarebbe possibilità di condurre a processo il programmatore o l'utilizzatore del sistema di AI con un'accusa di dolo.» Così F. CONSULICH, *Flash Offenders. Le prospettive di Accountability penale nel contrasto alle intelligenze artificiali devianti*, in Riv. it. dir. proc. pen., 3/2022, p. 1031.

anticipate e tradotte in istruzioni da algoritmi, sussiste un'ineliminabile componente di imprevedibilità nel comportamento delle IA»[176].

Il diritto vivente configura la categoria della colpa eventuale, applicabile nel caso in cui il soggetto agente preveda l'eventualità che possa cagionarsi un evento dannoso, ma ciononostante agisca ugualmente nella convinzione di poterlo evitare. Questa forma di prevedibilità astratta richiede solamente di intuire la potenzialità di un rischio, senza che sia necessaria una rappresentazione dettagliata dello specifico evento dannoso. Di conseguenza, difficilmente si può pensare che il programmatore non abbia, quantomeno astrattamente, contemplato la possibilità che il sistema di IA dotato di capacità di autoapprendimento potesse tenere comportamenti divergenti dalla programmazione originaria.

Si pone allora la questione di stabilire in che misura il programmatore di un sistema di IA possa essere ritenuto responsabile delle possibili deviazioni illecite risultanti da uno sviluppo logico della macchina, essendo per natura un sistema strutturalmente pensato come evolutivo.

Dovrebbe incardinare l'ipotesi della responsabilità colposa, il programmatore che non pronostichi la possibile imprevedibilità nell'agire del *robot* e che, per negligenza o imprudenza, non abbia adottato le dovute precauzioni per evitare la possibilità di un malfunzionamento dell'agente intelligente.

Trasferendo nel piano del diritto penale la questione relativa alla produzione e distribuzione di prodotti potenzialmente pericolosi (alimentata dal diritto civile), risulterebbe indubbiamente responsabile il programmatore che non si sia attenuto al dovere di monitoraggio costante del suo prodotto, al fine di identificare i possibili effetti dannosi che dal suo utilizzo possono derivarne.

Ma, al di fuori di questa ipotesi, si tratta comunque di tematiche alquanto complesse che necessitano della ricerca di un punto di equilibrio tra l'imprescindibile esigenza di supervisionare il funzionamento degli agenti intelligenti in via precauzionale e la necessità di garantire il proseguo nella ricerca scientifica, che di fatto rischierebbe di paralizzarsi qualora si optasse per un atteggiamento eccessivamente cauto nell'impiego delle tecnologie più innovative. L'osservanza eccessiva del principio di precauzione

[176] M. B. MAGRO, *Il problema della responsabilità per l'uso di intelligenze artificiali*, cit., p. 1251.

rischierebbe, infatti, di limitare l'innovazione tecnologica e l'adozione di agenti intelligenti, precludendo anche i benefici che queste stesse tecnologie possono offrire.
La soluzione più adeguata consiste nello stabilire standard precauzionali differenziati in base all'uso specifico e alla tipologia di IA immessa nel mercato. In questo contesto diventa quindi rilevante definire la soglia del rischio consentito, cioè il rischio considerato socialmente accettabile in relazione all'attività svolta e il cui superamento giustificherebbe l'addebito di responsabilità penale [177]. Il Parlamento europeo muovendosi in questa direzione ha approvato il 13 marzo 2024 il testo dell'*AI Act*, con cui va a suddividere in diverse categorie le tecnologie di IA impiegate sulla base del criterio del rischio: in particolare distingue tra sistemi vietati, sistemi ad alto rischio e sistemi a basso rischio.
In assenza di previsioni in tal senso orientate, il rischio altrimenti è che rimanga impregiudicata l'area dei fatti illeciti commessi con l'ausilio di sistemi di IA – area destinata tra l'altro ad ampliarsi in corrispondenza della diffusione di tali tecnologie.

1.2. *L'etica dell'intelligenza artificiale*

La consapevolezza dell'origine umana delle capacità di un sistema di IA implica la necessità di riflettere sulle implicazioni etiche e sociali del loro utilizzo, prendendo in considerazione l'impatto che queste macchine hanno sulla società. L'IA non può simulare ogni aspetto della capacità umana, perché l'approccio computazionale su cui si basano questi algoritmi non permette di orientare le decisioni verso il senso comune. È quindi fondamentale, alla luce del quadro esposto, interrogarsi sull'opportunità di regolare e orientare le tecnologie IA affinché siano indirizzate verso l'obiettivo della giustizia, promuovendo il benessere degli individui e facilitando l'applicazione efficiente ed equa della legge. Piuttosto che scontrarsi con queste macchine intelligenti, è preferibile riflettere su come valorizzare e sfruttare la complementarità tra l'essere umano e la macchina: avvalendosi del supporto razionale fornito dalla tecnologia, è possibile integrare l'IA nelle esperienze di vita privata, sociale e professionale.

[177] Ad esempio, nel caso dei veicoli a guida autonoma (*self driving cars*) è necessario garantire l'osservanza delle regole che pone il codice della strada; o nel caso del *robot* che esegue attività medico-chirurgica, va garantito il rispetto delle linee guida da adeguare al caso concreto.

In un'era in cui sempre più decisioni vengono prese da algoritmi e sistemi automatizzati, risulta essenziale sviluppare meccanismi e linee guida che assicurino che tali sistemi agiscano in modo responsabile e rispettoso dei valori umani. Questo richiede un approccio olistico che tenga conto non solo delle implicazioni tecniche ma anche dei risvolti etici e sociali delle decisioni adottate dai sistemi intelligenti. Solo attraverso questa strategia sarà possibile garantire che l'IA contribuisca in modo positivo e costruttivo al benessere dell'umanità.

Una disciplina emergente, a cui dovrebbe essere riconosciuta maggiore rilevanza nel campo del diritto penale dell'informatica, è la roboetica, ossia quello studio interdisciplinare che si occupa delle questioni etiche legate all'uso e all'implementazione dei *robot*. La roboetica indaga i principi morali che dovrebbero guidare la progettazione, la costruzione e il trattamento dei *robot*, in quanto entità che interagiscono con l'uomo e che influenzano lo sviluppo della società umana. L'obiettivo principale di questo settore di studi è quello di analizzare le ripercussioni – positive e negative – derivanti dall'impiego di questo tipo di macchine intelligenti, al fine di ottimizzarne l'integrazione nella società in modo consapevole. Un elemento fondamentale dell'etica dell'IA consiste infatti nel garantire che i sistemi intelligenti riflettano i valori umani, aderendo alle normative giuridiche e ai principi morali che guidano l'agire umano. Soprattutto nelle ipotesi in cui la macchina agisce indipendentemente da qualsiasi preordine impostogli dal programmatore, è importante assicurare che l'autonomia di scelta non vada a pregiudizio della sicurezza e della privacy degli individui. La roboetica mira, pertanto, a disciplinare l'uso delle IA in modo che avvenga rispettando i diritti e le libertà fondamentali.

Un avanzamento in questa direzione è rappresentato dallo sviluppo della capacità nell'IA di *cognitive computing*. Al fine di riuscire a far emulare in toto l'intelligenza umana, si sta cercando di estendere le capacità delle macchine affinché queste riescano a relazionarsi con gli altri, sappiano ascoltare ed esprimere emozioni[178]. Dotare i *robot* di una coscienza artificiale ovviamente non significa che questi riescano a provare davvero dei sentimenti, bensì che possano proiettare le emozioni umane nelle scelte decisionali che assumono autonomamente.

[178] C. CORRIDORI, *L'intelligenza artificiale come vittima del reato*, in *Cybercrime*, Milano, 2023, p. 1396: «La capacità dei *robot* intelligenti di interagire anche a livello emotivo, non significa che gli stessi provino emozioni coscienti: i *robot* simulano le emozioni, senza provarle».

Pertanto, un problema che si pongono le nuove ricerche empiriche è rappresentato dal c.d. *value alignment*. Il processo di sviluppo responsabile dell'IA mira ad assicurare che le azioni, le decisioni e i comportamenti di un sistema di IA siano adottate in armonia con i valori e gli standard etici degli esseri umani. Operando in questa prospettiva di allineamento dei valori, si intendono sviluppare dei sistemi che tengano comportamenti conformi alle norme legali e sociali, prevenendo in questo modo danni e disapprovazione pubblica. Per riuscire ad implementare le regole etiche e giuridiche nell'agire degli agenti intelligenti si suggerisce di programmare il loro sistema decisionale sulla base di un sistema di valutazione alternativo *bonus*/*malus,* che la macchina deve sottoporre ad autovalutazione prima di prendere una determinata decisione, così da riconoscere l'eventuale ingiustizia della propria azione.

Si tratta di tecnologie emergenti che offrono numerosissime opportunità, tuttavia presentano anche dei rischi notevoli, dovuti principalmente all'incertezza nel loro sviluppo futuro e alla seguente applicazione che di esse verrà fatta. È lecito nel panorama attuale domandarsi se i sistemi intelligenti riusciranno in futuro (forse non lontano) esercitare un libero arbitrio. Ne discende, che solo l'adozione di queste tecnologie in modo etico e responsabile potrà preservare il valore primario della giustizia; in caso contrario, potrebbe sussistere il pericolo che queste finiscano per prevaricare e soppiantare l'attività umana con decisioni automatizzate, «*facendo del giurista stesso un servitore della macchina*»[179].

A fronte del rischio di andare a pregiudicare e violare le libertà e i diritti umani fondamentali, si prospetta l'opportunità per il legislatore di intervenire stabilendo dei limiti alla ricerca tecnologica che sfocia in sistemi autonomi che agiscono al di fuori della sfera di controllo dei loro programmatori. Pur riconoscendo l'importanza della libertà di ricerca scientifica, è necessario delineare una regolamentazione che implementi i valori etici, allo scopo di circoscrivere la creazione di entità capaci di arrecare danni imprevedibili alla società. L'impego di sistemi di IA *self-learning* in grado di apprendere dai precedenti e di assumere autonomamente decisioni basate sui *dataset* acquisiti, comporta il rischio infatti di perpetuare *bias* esistenti nei dati, giungendo ad adottare soluzioni potenzialmente discriminatorie o ingiuste. È quindi essenziale implementare

[179] V. *Prefazione* di G. SARTOR, in *L'intelligenza artificiale e il diritto*, Torino, 2022, p. XII.

meccanismi di controllo e verifica che assicurino l'imparzialità e l'equità dei sistemi decisionali basati sull'IA.

L'Unione Europea si sta impegnando attivamente per giungere all'elaborazione di un quadro normativo adeguato che sia in grado di affrontare le sfide poste dall'avanzamento della robotica, assicurando che il progresso tecnologico avvenga in maniera etica, sicura e responsabile[180]. L'idea da taluni avanzata – e da molti criticata[181] – è quella di dotare i sistemi di IA più sofisticati di personalità giuridica-elettronica (*electronic person*) e riconoscerla come un *tertium genus* da affiancare alle persone fisiche e giuridiche. La configurazione della personalità elettronica permetterebbe di trovare una più rapida soluzione ai problemi posti dall'individuazione del soggetto cui attribuire la responsabilità a fronte di danni causati da artefatti robotici.

Inoltre, nella consapevolezza che ormai il diritto penale non possa più ignorare le sfide poste dall'IA, sono in corso i lavori per il Congresso sull'intelligenza artificiale e il diritto

[180] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, al punto 56 precisa che «in linea di principio, una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere proporzionale all'effettivo livello di istruzioni impartite al robot e al grado di autonomia di quest'ultimo, di modo che quanto maggiore è la capacità di apprendimento o l'autonomia di un robot e quanto maggiore è la durata della formazione di un robot, tanto maggiore dovrebbe essere la responsabilità del suo formatore; osserva in particolare che, nella determinazione della responsabilità reale per il danno causato, le competenze derivanti dalla «formazione» di un robot non dovrebbero essere confuse con le competenze che dipendono strettamente dalle sue abilità di autoapprendimento; osserva che, almeno nella fase attuale, la responsabilità deve essere imputata a un essere umano e non a un robot».

[181] Dubbi in merito all'introduzione di una forma di personalità giuridica per le intelligenze artificiali sono stati espressi dal Comitato Economico e Sociale Europeo (CESE) nel parere su «L'intelligenza artificiale — Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società» (C-288) del 31 agosto 2017, dove nel punto 3.33. si legge: «Si discute molto sulla questione di chi debba essere ritenuto responsabile se un sistema di IA causa un danno. In particolare, nei casi in cui si tratti di sistemi che apprendono autonomamente e continuano ad apprendere anche dopo la loro messa in funzione. Il Parlamento europeo ha formulato delle raccomandazioni concernenti norme di diritto civile sulla robotica, proponendo di esaminare l'opportunità di introdurre il concetto di «personalità elettronica» per i robot, in modo tale che essi possano essere ritenuti civilmente responsabili degli eventuali danni causati. Il CESE è contrario all'introduzione di una forma di personalità giuridica per i robot o per l'IA (o i sistemi di IA), in quanto essa comporterebbe un rischio inaccettabile di azzardo morale. Dal diritto in materia di responsabilità civile deriva una funzione preventiva di correzione del comportamento, la quale potrebbe venir meno una volta che la responsabilità civile non ricade più sul costruttore perché è trasferita al robot (o al sistema di IA). Inoltre, vi è il rischio di un uso inappropriato e di abuso di uno status giuridico di questo tipo».

penale[182] che si terrà a Parigi dal 25 al 28 giugno 2024. Si tratterà di un'occasione in cui poter discutere in merito alle questioni giuridiche poste dall'IA.
La carenza di studi sugli *AI-crime* indebolisce la capacità di identificare tempestivamente le possibili soluzioni da seguire in questa nascente area di attività criminale. Si richiede pertanto uno sguardo vigile al rapporto tra diritto e intelligenza artificiale, per colmare le lacune legislative che caratterizzano questo settore.

2. *Il ruolo dell'Internet Service Provider*

Per creare un ambiente virtuale sicuro, in cui gli utenti sappiano gestire responsabilmente la propria presenza *online*, è importante che il legislatore collabori con i gestori delle piattaforme digitali nel definire politiche di tutela della privacy, regolamentare l'uso dei dati e implementare meccanismi efficaci volti alla prevenzione e alla gestione di comportamenti illeciti e dannosi. Nell'ambito del diritto penale dell'informatica, assume rilevanza fondamentale il contributo degli *Internet Service Providers* nel raggiungimento di quella auspicata certezza riguardo al comportamento da tenere *online*.
L'*Internet Service Provider* (*ISP*) è l'entità che fornisce l'accesso a Internet agli utenti e, in virtù della posizione strategica che ricopre, detiene perciò un ruolo centrale nella gestione e nella trasmissione dei dati *online*. Dell'*ISP* viene data un'accezione particolarmente ampia, ricomprendendovi pressoché ogni soggetto che metta a disposizione della collettività un servizio relativo ad un'infrastruttura informatica o telematica: «*1. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico; 2. qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio*»[183].
Dal punto di vista giuridico, l'*ISP* ha il dovere di proteggere la libertà di espressione e il diritto alla privacy degli utenti, ma al contempo deve anche attenersi a specifici obblighi legali che potrebbero imporgli di monitorare e, talvolta, bloccare o addirittura rimuovere

[182] XXI Congresso Internazionale di Diritto Penale (AIDP) sul tema "*Artificial Intelligence and Criminal Justice*".
[183] Art. 1, lett. c), Convenzione del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001.

i contenuti illeciti che transitano attraverso la Rete. È quindi il soggetto che, in vista di una maggiore responsabilizzazione delle Rete, deve fornire maggiori indicazioni agli utenti sul tipo di contenuti pubblicabili per contribuire a diffondere una maggiore consapevolezza su ciò che è consentito fare nel mondo virtuale, prevenendo così possibili comportamenti inappropriati o illegali. In questo modo, l'utente sarebbe messo nella posizione di conoscere i limiti da seguire nell'utilizzo di Internet, consapevole anche delle conseguenze delle sue azioni e dell'eventuale responsabilità legale che potrebbe conseguirne.

Nel contesto dei reati informatici, pensando proprio al delitto di accesso abusivo ad un sistema informatico o telematico, il ruolo degli *ISP* è particolarmente delicato e complesso, in quanto, da un lato, sono loro che permettono all'utente malintenzionato di commettere l'attacco informatico fornendogli il necessario accesso ad Internet, e, dall'altro lato, rivestono anche un ruolo attivo nella prevenzione e nella lotta contro tali reati, ad esempio segnalando alle autorità i sospetti che hanno in relazione a determinate attività che vengono compiute *online*.

Sommariamente, nell'ecosistema di Internet, il *provider* è la figura intermediaria che si interpone tra la rete Internet e l'utente finale: è l'*ISP* che assegna al computer dell'utente un indirizzo di *Internet Protocol* (IP) per reindirizzargli i pacchetti di informazioni. Qui bisogna considerare che, se è vero che storicamente sono stati pensati per consentire l'accesso alle reti di comunicazione e la diffusione passiva di contenuti, nel tempo gli *ISP* si sono attivati intromettendosi concretamente nei contenuti pubblicati, al fine di aumentarne la visibilità[184]. Si distingue quindi tra *Internet access provider* e *Internet content provider*: indicando rispettivamente, il primo, il soggetto che offre l'accesso ad una rete telematica e, il secondo, l'operatore che fornisce servizi ulteriori al mero accesso alla rete e che produce contenuti propri.

A fronte di questo quadro, è inevitabilmente sorto l'interrogativo di capire se dovesse essere delineato un loro obbligo di controllo rispetto alla natura e alla tipologia di contenuti pubblicati da terzi.

---

[184] ACCINI G. P., *Profili di responsabilità penale dell'hosting provider "attivo"*, in Archivio Penale, fascicolo 2, maggio-agosto 2017, pp. 8-9: «nell'esperienza tecnica e giuridica, è andata delineandosi una figura non più neutra, ma ibrida, di hosting provider, la cui caratteristica è cioè quella di essersi allontanato dal paradigma di provider passivo, mero ricettore di contenuti immessi in rete, per trasformarsi in una sorta di "manipolatore attivo" di contenuti».

Il problema è oltretutto complicato dal fatto che gli algoritmi di cui si servono oggigiorno i gestori di servizi sono piuttosto sofisticati e utilizzati per filtrare e promuovere automaticamente determinati contenuti, di cui facilitarne la diffusione. Questo vuol dire che il monitoraggio dei contenuti non è rimesso esclusivamente alla mente umana – cosa che oltretutto sarebbe ontologicamente impossibile dato il numero di utenti connessi alla rete contemporaneamente – in quanto residua uno spazio di operatività della macchina che sfrutta tecnologie capaci di ottimizzare da sé la piattaforma[185].

Gli studiosi sono andati dunque ad indagare se gli *ISP* possano essere considerati dei semplici intermediari neutri nella veicolazione di contenuti illeciti immessi da terzi, considerando quindi pressoché irrilevante il loro ruolo nell'esposizione dei contenuti, o se, piuttosto, nonostante l'autonomia che caratterizza le nuove tecnologie, sia da riconoscere loro un ruolo attivo nella realizzazione del reato. Quello che qui interessa è cioè – ferma la responsabilità dell'*uploader* che risponde direttamente per gli eventuali illeciti che commetta nel fornire i contenuti accessibili al pubblico (responsabilità per fatto proprio) – capire in che termini possa essere chiamato a rispondere l'*Internet Service Provider* del fatto illecito altrui posto in essere valendosi delle sue infrastrutture.

Bisogna preliminarmente osservare che non è semplice ricostruire un modello penale adeguato ad un soggetto non fisico, al cui interno individuare un destinatario delle norme penali, che agisce in un luogo virtuale.

La legislazione italiana, in armonia con le direttive adottate dall'Unione Europea, ha cercato di delineare i profili di responsabilità degli *ISP* per i reati commessi nel cyberspazio, bilanciando i diritti fondamentali con i sacrifici che possono essere richiesti agli *ISP*[186].

---

[185] Per la gestione delle piattaforme *online* si sfruttano tipicamente i cc.dd. algoritmi di associazione e di filtraggio, cioè tecnologie che creano collegamenti tra diversi contenuti e che sono in grado automaticamente di includere/escludere informazioni.

[186] L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale*, cit., p. 55: «Proprio questa dimensione sovraindividuale e di stretta interdipendenza, che assumono la sicurezza e la riservatezza, ma anche altri beni e diritti nel *Cyberspace*, dimostra altresì l'importanza crescente del ruolo degli *Internet Service Providers* (ISP), e, più in generale, dei gestori delle piattaforme *online*, nonché dei titolari dei servizi offerti in settori fondamentali per la società, basati su sistemi informatici e su tecniche d'intelligenza artificiale, che in relazione alle plurime attività che svolgono non possono non essere individuati anche quali centri d'imputazione di responsabilità - civili, penali ed amministrative – per gli effetti, gli eventi avversi e le offese che possano derivarne».

Con il Decreto Legislativo 9 aprile 2003, n. 70[187] il legislatore ha introdotto i primi importanti principi in materia di responsabilità dei titolari di piattaforme digitali, stabilendo che, non potendo essere imposto ai prestatori di servizio un obbligo generale di sorveglianza sulle informazioni trasmesse e memorizzate *online* e nemmeno di attivazione per ricercare i contenuti illeciti, non si possa configurare una responsabilità penale ai sensi dell'art. 40, secondo comma c.p.[188] per non aver impedito un reato commesso dagli utenti fruitori del servizio offerto. Inoltre, l'*ISP* non risponde neppure a titolo di concorso omissivo nel reato altrui (art. 110 c.p.), pur essendo ravvisabile, dal punto di vista causale, un suo indiretto contributo materiale, nell'aver messo a disposizione la piattaforma informatica: da un punto di vista strettamente tecnico, infatti, l'attività del *provider* si potrebbe qualificare come *condicio sine qua non* per la realizzazione dell'attività illecita del terzo.

Le aree di deresponsabilizzazione del *provider* riguardano nello specifico:

- l'attività di *mere conduit* (art. 14), che consiste nel fornire l'accesso alla Rete e nel trasmettere informazioni immesse dal destinatario del servizio;
- l'attività di *caching* (art. 15), ovverosia la memorizzazione temporanea o transitoria delle informazioni trasmesse e condivise tra gli utenti;
- l'attività di *hosting* (art. 16), che va dalla mera gestione del sito web alla conservazione duratura dei *files* del cliente.

Per dette attività è possibile riconoscere una responsabilità dell'*ISP*, subordinandola però all'ipotesi in cui quest'ultimo sia a conoscenza di attività illecite e non agisca prontamente per rimuovere tali contenuti adottando le misure necessarie a limitare le conseguenze del reato. Nello specifico, si richiede all'*ISP*, che venga a conoscenza di attività illecite compiute dai destinatari del servizio che offre, di informare immediatamente la polizia giudiziaria o le autorità di controllo anche amministrative (primo fra tutti il Garante della privacy) e qualora gli venga fatta richiesta di informazioni l'*ISP* è tenuto ad inoltrargli tutte quelle in suo possesso che permettano e facilitino l'identificazione del soggetto che

[187] D. Lgs. adottato in attuazione della Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.

[188] Art. 40, co. 2 c.p.: «Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo».

ha commesso l'illecito e che vadano ad inibire le condotte contrarie alla normativa[189]. Si potrebbe allora meglio parlare di "immunità condizionata".

Nella stessa prospettiva si pone la giurisprudenza di legittimità, la quale nel *leading case Google vs. Vividown*[190] ha escluso la sussistenza in capo al *provider* di una posizione di garanzia e di poteri impeditivi in mancanza di una specifica disposizione che fondi l'obbligo giuridico di impedire i reati commessi dagli utenti. La Corte ritiene cioè di non poter configurare alcun obbligo di controllo preventivo sui dati immessi dai terzi nel sito gestito dall'*Internet service provider*, in quanto si tratterebbe di un dovere inesigibile sia sul piano quantitativo – considerata l'enorme quantità di materiale immesso in Rete – sia sul piano qualitativo – per mancanza di un filtro che accerti la natura sensibile dei dati che vengono pubblicati e la presenza di un consenso del titolare dei dati. Concordemente al D. Lgs. n. 70/2003, si ritiene pertanto che il *provider* non sia responsabile per le informazioni memorizzate e caricate dagli *uploaders*, salvo che «*non sia effettivamente a conoscenza del fatto che il dato o l'informazione è illecita*» e che – fermo il suo obbligo di segnalazione alle autorità – non rimuova con prontezza i contenuti ritenuti illeciti.

---

[189] Art. 17, D. Lgs. 09.04.2003, n. 70: «1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto:

a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione;
b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente».

[190] Si v. per maggiori approfondimenti *Caso Google vs Vivi Down*, in particolare Cass. pen., sez. III, 17 dicembre 2013, n. 5107, in cui si definiscono i confini della responsabilità dell'*host provider* in relazione ai reati realizzabili dagli utenti della rete avvalendosi degli strumenti offerti dal provider stesso. Il fatto riguardava uno studente disabile ripreso mentre subiva bullismo dai compagni, i quali caricano poi il video in rete: «le limitazioni di responsabilità sono applicabili poiché il *provider* si è limitato a fornire ospitalità ai video inseriti dagli utenti, senza fornire alcun contributo alla determinazione del contenuto dei video stessi».

Progressivamente, ai fornitori di servizi di comunicazione elettronica sono stati imposti maggiori obblighi di cooperazione con la polizia giudiziaria e le autorità di controllo per permettere non solo la raccolta delle prove e l'identificazione degli utenti tramite obblighi di conservazione dei dati di traffico, ma anche agevolare la cessazione delle violazioni agli interessi meritevoli di protezione. Soprattutto la giurisprudenza europea[191] ha dato una forte spinta in questa direzione, nel senso di limitare il regime di *safe harbour* riconosciuto dalla Direttiva europea del 2000, a fronte della presa di consapevolezza della protezione da riconoscere ai rapporti che si andavano a svolgere nella realtà in continua espansione della Rete. Fermo pur sempre il principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali, esigenze di pubblica sicurezza e diritto degli utenti di pubblicare liberamente, la Corte Europea dei Diritti dell'Uomo e la Corte di Giustizia dell'Unione Europea stanno cercando di valorizzare sempre più la figura dell'*hosting* "attivo", andando a ridimensionare le originarie scelte di immunizzazione.

Per ora, tuttavia, si continua a considerare il *provider* prevalentemente quale semplice intermediario e fornitore digitale passivo al fine di evitare un accostamento dello stesso al soggetto terzo che pubblica contenuti illeciti nello spazio di rete concessogli. Soluzione questa che trova conferma anche laddove vengano utilizzati strumenti dotati di intelligenza artificiale che influiscano nelle interazioni tra gli utenti e sulla portata delle informazioni immesse, aumentandone le visualizzazioni e la diffusione, poiché non può essere equiparato il funzionamento dell'algoritmo con l'alterazione materiale dei contenuti da parte del *provider*.

Qualche dubbio da questo punto di vista permane. Avvalendosi consapevolmente di algoritmi di filtraggio che in qualche modo manipolano e gestiscono i contenuti presenti *online,* al fine di migliorare e ottimizzare la piattaforma, il *provider* riveste un ruolo attivo nella divulgazione dei contenuti. Tuttavia, non sarebbe ragionevole configurare una sorta di responsabilità oggettiva degli *ISP* che si avvalgano di strumenti automatizzati che vadano a performare la loro rete telematica, sì da immaginare un loro contributo causale nella commissione del reato[192]. Qualora sia l'algoritmo a commettere autonomamente

[191] Corte di giustizia UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger e a*.

[192] BACCIN A., *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso Force v. Facebook*, in Sistema Penale, 5/2020, p. 25: «il *provider* che si avvalga di un team editoriale specificamente orientato alla diffusione dei contenuti, sfrutti determinati processi

l'illecito (ad esempio, sovraesponendo, all'insaputa del programmatore stesso, un commento razzista o diffamatorio)[193], neppure si potrebbe pensare ad un modello di responsabilità penale colposa dell'utente, ritenendo che quest'ultimo, affidandosi all'innovazione tecnologica, assuma volontariamente il rischio di commissione degli illeciti, poiché mancherebbe in lui qualsiasi componente soggettiva in ordine alla realizzazione del reato.

La problematica relativa al tipo di responsabilità da riconoscere agli *ISP* nel contesto dei reati informatici non trova ancora adeguata soluzione. L'attualità di questo dibattito deve sollecitare giuristi e studiosi ad una riflessione sulle tradizionali categorie giuridiche per ripensarle e adattarle alla luce delle sfide poste dalla continua evoluzione tecnologica.

3. *La disinformazione del digitale*

Il panorama sociale attuale mostra come l'utilizzo e la pervasività delle tecnologie informatiche nella vita quotidiana abbia comportato l'evoluzione di una nuova generazione di individui. Il riferimento è ai cc.dd. *digital natives*[194], cioè quei giovani che sono nati e cresciuti in quello che è un ambiente già mediato dalla tecnologia. È una definizione che viene posta in contrapposizione alla figura dei *digital immigrants,* cioè quei soggetti nati in epoca precedente, in cui la tecnologia digitale era meno presente, o addirittura assente, e che hanno assistito al passaggio dall'analogico al digitale.

Queste definizioni permettono anche di delineare i differenti approcci che i soggetti hanno allo strumento digitale: per i *digital natives* la tecnologia digitale è parte del proprio percorso di crescita perché fin dalla nascita conoscono questo mezzo di comunicazione,

automatizzati e svolga attività di gestione, indicizzazione e organizzazione del materiale postato sarà automaticamente ritenuto *hosting provider* attivo e non potrà godere del regime speciale di esenzione, poiché la conoscenza effettiva del contenuto verrà presunta a fronte della rilevante manipolazione delle informazioni costantemente effettuata».

[193] CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale*, cit., p. 9: «Le macchine intelligenti, come prodotto soggettivizzato, possono tenere dei veri e propri comportamenti attivi assolutamente imprevedibili, derivanti dal lavorìo autoevolutivo del *machine learning*, tali che qualunque danno da essi derivante sfugga inesorabilmente alle capacità previsionali dei programmatori».

[194] Il termine viene utilizzato per la prima volta nel 2001 dallo scrittore statunitense Marc Prensky nel suo articolo *Digital Natives, Digital Immigrants*.

per cui sono abituati a utilizzare dispositivi come computer, *smartphone* e *tablet*; i *digital immigrants*, invece, utilizzano lo strumento informatico limitatamente allo svago o alla produttività individuale (utilizzo necessario), quindi possono incontrare maggiori difficoltà nell'adattarsi alle nuove tecnologie.

I nativi digitali, nascendo in un contesto già permeato dal digitale, sviluppano una familiarità naturale con la tecnologia e questo porta a presumere che conoscano meglio le potenzialità che il *web* offre all'utente, ma la facilità di utilizzo di questi mezzi può tradursi altresì in una difficoltà nel distinguere il confine tra *online* e *offline*. Si tratta appunto di individui che crescono in un'epoca dominata dalle tecnologie, di conseguenza il loro approccio alla comunicazione, all'apprendimento e alla socializzazione viene plasmato fin dalla nascita verso il contesto digitale. L'utilizzo così frequente della tecnologia comporta che il singolo si costruisca una propria identità *online*, adottando comportamenti che travalicano il confine del reale e si integrano col virtuale. Si registra nei giovani una costante connettività, la quale diviene il contesto in cui intraprendere nuove esperienze di vita, perché in questo mondo parallelo i giovani riescono ad esprimere la propria persona, manifestando appieno i propri interessi e molteplici aspetti della propria personalità. L'*alter-ego* digitale finisce per divenire un'estensione naturale del proprio modo di interagire col mondo, determinando perciò un'eccessiva immersione nel mondo virtuale.

Questa dipendenza da Internet può risultare estremamente pericolosa e portare a forme di psicopatologie quali depressione, ansia, disturbi del sonno o comunque può indurre a tenere comportamenti antisociali. Probabilmente un minore non ha proprio la capacità di comprendere determinati messaggi che vengono trasmessi *online*, accessibili ovunque e consultabili da chiunque, tra cui vengono inclusi siti che inducono a disturbi alimentari, o che promuovono comportamenti autolesionistici o suicidi, o ancora che incitano all'odio, alla discriminazione o alla violenza contro gruppi sociali o individui specifici.

Lo spostamento continuo tra questi due mondi, quello reale e quello virtuale, può essere fonte di grande pericolo, in quanto potrebbe mancare una piena comprensione del rischio di divenire vittime di aggressioni anche nel cyberspazio. L'effetto di disinibizione *online*, attribuibile alla dissociazione che si ha dal mondo reale, può infatti spingere gli utenti di Internet a rivelare più informazioni *online* di quanto farebbero *offline*. Questa tendenza alla condivisione eccessiva *online*, cumulata con l'uso di *password* banali e un'ignoranza

generale sui protocolli di sicurezza, fa sì che le informazioni personali diventino facilmente disponibili per potenziali criminali informatici, rendendo gli utenti vittime più facili da raggiungere.

Quello che emerge è che l'esposizione precoce durante la fase di sviluppo alle nuove tecnologie e l'innata dimestichezza nel loro utilizzo non implichi automaticamente che i nativi digitali siano degli esperti di informatica consci delle implicazioni etiche e legali legate all'uso di Internet[195]. Anzi, si registra che i fenomeni *online* che riguardano i minori abbiano oggi grande espansione, in gran parte dovuta all'abbassamento della soglia di età dei soggetti che navigano nel *web*[196].

Consci del fatto che la criminalità informatica rappresenta un fenomeno complesso, e che la proliferazione di dispositivi mobili, reti *Wi-Fi* e l'apertura di Internet hanno aumentato l'espansione degli attacchi informatici, con la conseguenza di far aumentare il fenomeno della vittimizzazione *online*, è importante iniziare ad adottare misure personali per proteggersi da queste forme di aggressione. Questo implica non solo l'adozione di misure tecniche, ma anche l'integrazione di queste ultime con una formazione professionale. L'acquisizione di competenze digitali assume un ruolo sempre più centrale nella società moderna e richiede un'attenzione particolare nell'impiego degli strumenti tecnologici, al fine di prevenire il rischio che l'utente divenga vittima di questo mondo parallelo che potrebbe non essere in grado di gestire adeguatamente.

I giovani, gli adolescenti in particolare, sono saturi di disinformazione in questa realtà di costante connessione *online* e il problema è che la maggior parte delle volte non verificano la veridicità dei contenuti che vengono pubblicati nelle diverse piattaforme *social*. Nei *mass media* circolano un'enorme quantità di informazioni incomplete o distorte, che ingannano lo spettatore e provocano un caos informativo. Nell'era della rivoluzione digitale, la maggioranza delle minacce alla sicurezza della società è proprio legata alla sicurezza delle informazioni, in quanto sempre più spesso vengono diffusi messaggi che intenzionalmente fuorviano i destinatari, al punto che i tempi attuali vengono anche definiti come l'era della disinformazione e delle false notizie: Internet e i

[195] V. A. R. LONGO, *Nativi e analfabeti digitali: il paradosso della "Generazione Google"*, Scientificast, 2017.

[196] Si registra che i giovani rappresentano 1/3 degli utenti Internet a livello mondiale e il 68% di loro ha un'età compresa tra i 9 e i 16 anni e possiede almeno un profilo sui *social network*.

social network permettono di manipolare e influenzare l'opinione pubblica su una scala senza precedenti[197].

Al giorno d'oggi, è evidente come manchi un'opportuna formazione digitale concernente l'uso corretto di Internet e questo genera inevitabilmente una serie di fattori che, nel corso del tempo, possono determinare l'insorgere di diverse problematiche. L'insufficiente informazione nell'ambito del digitale, analizzata in relazione ad Internet e ai vari motori di ricerca, ha ripercussioni tanto nel contesto *online* quanto in quello *offline* e, proprio partendo da questa constatazione, risulta imprescindibile e, anzi, necessitata, l'educazione delle giovani generazioni allo sviluppo di un pensiero critico.

Pertanto, da una parte, è importante che già a partire dalle scuole dell'infanzia si inizi a predicare una corretta alfabetizzazione ai *media* digitali, superando i tradizionali modelli didattici predisposti in un'epoca precedente in cui erano ancora assenti le novità introdotte con le nuove tecnologie. Sotto questo punto di vista, è indispensabile non solo insegnare competenze tecniche, ma anche formare gli studenti su tematiche quali la privacy *online*, la sicurezza informatica e l'etica digitale.

Dall'altra parte, anche gli Stati devono attivarsi per ridefinire il ruolo dei *media* al fine di condurre una lotta efficace contro la disinformazione; si tratta infatti di mezzi di comunicazione che dovrebbero fornire informazioni affidabili. In questa prospettiva, esemplificando l'UNICEF ha sollecitato i decisori politici ad elaborare una normativa finalizzata alla protezione dei bambini da informazioni inesatte o dannose, garantendo al contempo un accesso sicuro ai diversi contenuti[198]. O ancora, la Commissione europea ha avviato una serie di iniziative[199] volte a contrastare la diffusione della disinformazione *online,* allo scopo di ottenere un ambiente digitale più trasparente e affidabile e

---

[197] Cfr. Relazione introduttiva al d.d.l. n. 2688 del 2017: «Internet ha sì ampliato i confini della nostra libertà dandoci la possibilità di esprimersi su scala mondiale, ma la libertà di espressione non può trasformarsi semplicemente in un sinonimo di totale mancanza di controllo, laddove controllo, nell'ambito dell'informazione, vuol dire una notizia corretta a tutela degli utenti».

[198] Il Fondo delle Nazioni Unite per l'infanzia prende in considerazione il fatto che la digitalizzazione colpisca anche i bambini e gli adolescenti, i quali devono perciò essere protetti dai rischi che si annidano nell'ambiente virtuale, in https://www.unicef.org/globalinsight/stories/digital-misinformation-disinformation-and-children.

[199] V. *Affrontare la disinformazione online*, in https://digital-strategy.ec.europa.eu/it/policies/online-disinformation.

garantendo la protezione dei valori europei, tra cui ricopre una certa importanza il Codice rafforzato di buone pratiche sulla disinformazione[200].

L'esigenza di veder predisposta una regolamentazione adeguata emerge ancora più forte se si tiene presente che la linea di demarcazione tra comportamenti *online* leciti e illeciti è davvero sottile e questo può rendere difficile in determinate circostanze identificare e catalogare una certa condotta. Il raggiungimento di un equilibrio *online* che implichi trasparenza, responsabilità e salvaguardia dei diritti si configura come una sfida politica di notevole importanza. Internet è un ambiente virtuale in cui norme sociali e legali possono divergere rispetto a quelle vigenti nel mondo reale. A mero titolo esemplificativo, le leggi in materia di diffamazione possono essere diverse da un Paese all'altro e questo inevitabilmente complica l'individuazione dei casi in cui un commento *online* costituisca o meno diffamazione.

Ci si confronta con reati ancora troppo nuovi per comprenderne appieno il disvalore, reati per i quali potrebbe ancora mancare la percezione dell'antigiuridicità della condotta, accentuata dal fatto che all'azione perpetrata sul web è correlata una diminuzione del senso di riprovevolezza di ciò che si compie. La giurisprudenza si sta adattando a questa nuova realtà con un'attitudine propositiva ed un approccio costruttivo, cercando di interpretare e applicare le norme penali già esistenti in modo da includere i *cybercrimes*; tuttavia, questo processo di adattamento richiede tempo e può ancora lasciare spazio a diverse interpretazioni e, a volte, ad ambiguità.

Il potenziale autore di un reato informatico talvolta ignora l'illiceità della propria condotta, non essendo a conoscenza dei precetti che regolano il comportamento degli attori sociali, sicché si avverte sempre più l'importanza di conoscere le leggi che disciplinano la materia dell'uso delle nuove tecnologie, al fine di evitare, o almeno limitare, comportamenti illegali, anche involontari.

Attualmente, gli utenti sono tendenzialmente autodidatti nel processo di comprensione dell'utilizzo della Rete. È però cruciale ricordare che nonostante l'esperienza pratica ripetuta e maturata nel tempo porti ad avere una conoscenza superiore del funzionamento di specifiche applicazioni informatiche, non sempre quest'ultima viene utilizzata in modo corretto ed efficace: non sarebbe ragionevole ricollegare l'educazione sulle regole per un

[200] Firmato il 16 giugno 2022, si basa sul primo Codice di buone pratiche (2018) e tiene conto degli Orientamenti della Commissione del 2021 emersi dopo la crisi COVID-19 e la guerra in Ucraina.

utilizzo digitale veramente appropriato e sicuro esclusivamente al buon senso degli utenti. In altre parole, la semplice oculatezza nell'impiego dei dispositivi informatici non sarebbe certamente sufficiente o bastevole affinché gli utenti riescano da sé a identificare e prevenire le situazioni di rischio.

Come già evidenziato, pur manifestandosi nella sfera *online*, le azioni intraprese hanno comunque conseguenze *offline* e possono causare danni incidenti negativamente sulla sfera emotiva, psicologica e professionale degli individui. Dal momento allora che non sempre risulta facile o intuitivo adottare comportamenti responsabili e rispettosi degli altri, che rispecchino i confini tra lecito e illecito *online*, la regolamentazione delle dinamiche sociali nella Rete deve essere introdotta a monte affinché le regole della convivenza non siano dettate unicamente dalla prassi, ma piuttosto trovino un'armoniosa disciplina che possa giovare sia alle casistiche *online* che a quelle *offline*, soprattutto se riguardanti fenomeni di rilevante impatto sociale.

Nel contesto digitale emergono regole di comportamento autoctone, anche perché manca un'autorità centralizzata che indirizzi e educhi gli utenti ad una corretta interazione. All'interno di una determinata applicazione informatica, infatti, sono unicamente gli stessi utenti a generare le regole da seguire. Non essendoci restrizioni o norme sociali predefinite, questi modelli comportamentali possono discostarsi da quelli che normalmente si osservano nel mondo reale e il pericolo è che si finisca per normalizzare e accettare forme di interazione che in un contesto non virtuale sarebbero considerate inappropriate. Infatti, quando una determinata modalità di interazione *online* viene regolarmente ripetuta, questa viene conseguentemente accettata all'interno di una comunità e considerata come normale[201]. Pertanto, la sfida normativa consiste nel fornire gli strumenti per navigare consapevolmente nell'ecosistema digitale, promuovendo un'educazione all'uso responsabile delle tecnologie, che sia in grado di guidare gli utenti verso modelli comportamentali rispettosi ed etici.

[201] A titolo esemplificativo pensiamo al *cyber-flashing,* comunemente considerato come una forma di molestia *online* e pratica ritenuta tuttavia inevitabile, addirittura apprezzabile, se si utilizzano applicazioni informatiche come *Grindr* (qui viene normalizzata la condivisione di foto pornografiche).

3.1. *Il ruolo promotore dell'Unione Europea*

Nel panorama odierno, la rivoluzione informatica riveste un'importanza primaria, in quanto le piattaforme *online* rappresentano un settore fondamentale per lo sviluppo dell'economia e dei mercati digitali in ambito europeo. Di conseguenza, accanto all'educazione, promossa soprattutto dalle istituzioni scolastiche, riveste un ruolo complementare la regolamentazione giuridica. Gli Stati membri dell'Unione Europea devono collaborare attivamente con gli operatori del settore privato al fine di garantire un livello di sicurezza informatica e stabilità sufficiente e adeguato a prevenire/contrastare le minacce cibernetiche[202], le quali inevitabilmente minano la fiducia dei cittadini nello svolgimento delle attività *online*. La predisposizione di un quadro normativo chiaro ed esaustivo costituisce il presupposto indispensabile per poter efficacemente tutelare gli utenti (con particolare attenzione ai minori) dalle minacce del cyberspazio e, parallelamente, promuovere un ambiente digitale sicuro. Soprattutto, la preventiva identificazione delle vulnerabilità tecniche dei sistemi informatici permetterebbe di ridurre i costi successivi necessari per rimediare agli effetti derivanti dalle intrusioni informatiche.

A livello sovranazionale, l'Unione Europea si sta facendo promotrice di una serie importante di iniziative nel settore delle nuove tecnologie, assolvendo al suo ruolo di guida nel governo della digitalizzazione e offrendo stimoli critici per riflettere sulle implicazioni giuridiche che il processo di digitalizzazione sta comportando e comporterà. Il riconoscimento necessario di uno spazio digitale che possa essere definito da tutti come sicuro, moderno e impostato su regole chiare e comunemente condivise è la premessa da cui muovere per riflettere sulle soluzioni più adatte a definire queste tematiche. I servizi offerti in uno spazio digitale utopico dovrebbero infatti raggiungere un connubio equilibrato tra la tutela della sicurezza degli utenti *online* e la continua innovazione dei mercati digitali[203].

---

[202] L'art. 2, n. 8 del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio definisce la "minaccia informatica" come «qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone».

[203] L'atto che riporta le *Dichiarazioni comuni del Parlamento Europeo, del Consiglio e della Commissione Europea sui diritti e i principi digitali per il decennio digitale* (2023/C 23/01) del 23.01.2023 è finalizzato ad orientare in senso conforme ai valori europei comunemente accolti (rispetto della dignità umana, libertà,

Il quadro giuridico dell'Unione Europea relativo ai servizi digitali era rimasto sostanzialmente invariato dall'adozione della Direttiva sul commercio elettronico nel 2000[204] e aveva quindi urgente necessità di essere aggiornato. Tale esigenza di riforma era ulteriormente accentuata dall'evoluzione senza precedenti degli ulteriori cambiamenti che avevano caratterizzato le tecnologie digitali, i modelli di *business* e i vari servizi offerti nella Rete.

Alla fine del 2020 viene allora presentato alla Commissione Europea il *Digital Services Act package*, che si compone precisamente di due regolamenti: il *Digital Services Act*[205] e il *Digital Markets Act*[206]. Questo pacchetto legislativo viene adottato dal Consiglio e dal Parlamento europeo nel 2022 e diviene esecutivo nel 2023. Esso consente effettivamente un accesso a prodotti sicuri per gli utenti digitali, garantendo loro il riconoscimento dei diritti fondamentali e promuovendo una continua concorrenza libera ed equa nei settori digitali, al fine di stimolare l'innovazione e la crescita economica. A tal fine, infatti, non beneficiano delle nuove disposizioni unicamente i cittadini comuni fruitori delle piattaforme digitali, ma anche gli utenti aziendali e gli stessi fornitori dei servizi digitali, oltre alle società in generale. L'ambizione è quella di assecondare l'innovazione mediante la creazione di uno spazio digitale più sicuro in cui tutti gli operatori possano concorrere in condizioni di parità, tanto nell'ambito del mercato unico europeo quanto a livello globale.

Volendo delineare con più precisione una differenza nel contenuto dei due atti, il *Digital Services Act* (DSA), entrato in vigore il 16 novembre 2022, si propone di riformare la precedente direttiva sull'*e-commerce*, andando a contrastare la diffusione in Rete dei contenuti illegali o dannosi, nel pieno rispetto dei diritti fondamentali dei cittadini. In armonia con quanto previsto dalla Carta dei diritti fondamentali, analizza i rischi sociali correlati alla presenza *online* cercando di offrire soluzioni efficienti, tiene traccia dei

---

democrazia, uguaglianza) la trasformazione digitale nel periodo che arriva fino al 2030. La dichiarazione si propone di assicurare che la transizione digitale progredisca nel pieno rispetto dei diritti fondamentali, beneficiando a tutti i cittadini e promuovendo un'economia più inclusiva e al contempo sostenibile, andando a ridurre l'impatto ecologico delle tecnologie digitali.

[204] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

[205] Regolamento (UE) 2022/2065 relativo al mercato unico dei servizi digitali.

[206] Regolamento (UE) 2022/1925 sui mercati digitali.

commercianti nei mercati digitali per garantire loro una concorrenza equa, nonché impone nuove misure di trasparenza e responsabilità per le piattaforme *online* e assicura una supervisione sempre migliorata.

Il *Digital Markets Act* (DMA), invece, entrato in vigore poco prima, il 1° novembre 2022, si focalizza sulla creazione di condizioni di parità per le imprese all'interno dell'Unione Europea, regolamentando le grandi tecnologie. Con l'adozione di quest'atto si sono perseguiti scopi volti a delineare un settore digitale caratterizzato da competitività ed equità. Tra le misure introdotte figurano: il divieto di pratiche sleali delle piattaforme *online* che detengono la quota maggiore del mercato (denominate *gatekeepers*); la possibilità per gli utenti aziendali di offrire ai consumatori una varietà di scelte nei beni e servizi; la somministrazione di servizi migliorati e a prezzi più equi per i consumatori; l'imposizione di diritti e obblighi precisi alle grandi piattaforme *online*; la promozione dell'innovazione e di un ambiente digitale più equo per le start-up tecnologiche.

Gli Stati membri hanno quindi integrato le loro legislazioni nazionali per dare applicazione ai principi enunciati dal Regolamento, imponendo, in particolare, obblighi di diligenza per i fornitori di servizi di intermediazione[207] per quanto riguarda il modo in cui dovrebbero trattare i contenuti illegali, la disinformazione *online* o altri rischi sociali. Un comportamento responsabile e diligente da parte dei fornitori di servizi di intermediazione è essenziale per realizzare un ambiente virtuale sicuro, prevedibile e affidabile – spazio definito al considerando 3 del DSA con gli aggettivi "*safe, predictable and trustworthy online environment*" – e per consentire ai cittadini dell'Unione e ad altre persone di esercitare i loro diritti fondamentali, tra i quali emergono la libertà di espressione e di informazione, la libertà di condurre un'attività d'impresa, il diritto alla non discriminazione, con lo scopo di raggiungere un elevato livello di protezione dei consumatori.

Ai fini della corrente dissertazione, risulta rilevante quanto espresso al considerando 12[208] del *Digital Services Act*. In tale passaggio viene precisato il concetto secondo il quale il

---

[207] Per servizi di intermediazione *online* si intendono le piattaforme in Rete che consentono agli utenti commerciali di offrire beni e servizi, avendo quale obiettivo quello di facilitare l'avvio della transazione diretta con i consumatori; nello specifico ci riferiamo ai cc.dd. *marketplaces*, ai cc.dd. *app stores*, ai *social media* usati a scopi professionali, ecc.

[208] «*In order to achieve the objective of ensuring a safe, predictable and trustworthy online environment, for the purpose of this Regulation the concept of 'illegal content' should broadly reflect the existing rules in the offline environment. In particular, the concept of 'illegal content' should be defined broadly to cover*

materiale esposto *online*, in qualsivoglia forma, rientra nella dicitura di "contenuto illegale" – riferendosi a contenuti, prodotti, servizi e attività illegali, in una accezione molto ampia – laddove siano già presenti *offline* regole che ne disciplinano la medesima materia con fine sanzionatorio. La seconda parte del detto considerando 12 riporta poi a titolo esemplificativo quanto può essere motivo di rimozione nello spazio digitale a causa della natura illegale dell'oggetto in sé o dell'attività relativa. Viene palesato anche qui il continuo rispecchiarsi tra lo spazio *online* e quello *offline*, dove, sul piano normativo, il primo risulta molto spesso la fedele conseguenza del secondo.

Nonostante le positive novità introdotte dal Regolamento oggetto della corrente analisi, la possibilità che vengano perpetrati illeciti nell'ambiente digitale non è, oggi, azzerata. In questo contesto, entra in gioco la responsabilità degli operatori *online* nell'adempiere ai propri obblighi di trasparenza e corretta e completa informazione, oltre al dovere di ricorrere alle misure di rimozione e di controllo dei contenuti in maniera tempestiva. Si parla di *accountability* (responsabilizzazione), facendo riferimento alla condotta pro-attiva di chi, in relazione al ruolo o all'impatto che ha nell'ecosistema digitale, adotta le misure necessarie per rispettare i diritti e i doveri stabiliti dal Regolamento. Gli obblighi imposti da quest'ultimo sono proporzionati in relazione al tipo di servizio offerto e all'ampiezza di utenza che ne beneficia[209], fermo restando il vincolo imposto a tutti gli Stati membri circa: la fornitura di informazioni esplicite in relazione all'utilizzo dei contenuti e di indicazioni chiare sul servizio offerto, la trasparenza nei sistemi di suggerimento e pubblicità, il divieto di pratiche ingannevoli, l'obbligo di denuncia di reati o la segnalazione di illeciti, il controllo degli utenti e dei fornitori. Le piattaforme di

information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities».

[209] È lo stesso DSA a distinguere i servizi di intermediazione in relazione al servizio che essi offrono, così da poterne associare i relativi obblighi specifici. In particolare, essi sono suddivisi nelle seguenti categorie: gli *Intermediary Services*, quali i *mere conduit* (come i nomi di dominio, Wi-Fi hotspot ecc.), i *caching* (ad esempio le piattaforme *cloud* globali) e l'*hosting* (quali i motori di ricerca, *social network*, *marketplace,* ecc.); gli *Hosting Services Providers*, ossia i fornitori di servizi digitali che mettono a disposizione degli utenti i propri server e i propri spazi web; le *Online Platforms*, vale a dire piattaforme *online* che offrono un servizio di memorizzazione delle informazioni su richiesta; le *Very Large Online Platforms*, ossia le piattaforme che presentano più di 45 milioni di utenti attivi in tutta l'UE.

maggiori dimensioni devono poter ottemperare anche alle pratiche di prevenzione, sia di rischi singoli sia di rischi sistemici, e gestire le situazioni di crisi o di abuso del sistema. La legge si propone di incrementare la trasparenza delle regole per la moderazione dei contenuti *online*, fornendo al contempo un maggiore accesso ai dati per le autorità e i ricercatori, in modo tale da permettere loro anche la possibilità di comprendere meglio lo spazio digitale, il suo impatto sociale e i potenziali rischi ad esso correlati. Pertanto, risulta doveroso un adeguamento costante della legislazione in materia di reati informatici, privacy e protezione dei dati personali per riuscire a rispondere alle sfide poste dall'evoluzione tecnologica e, quindi, assicurare che tutti possano interagire in uno spazio virtuale rispettoso dei diritti di ogni individuo.

CONCLUSIONI

L'analisi svolta mira a fornire elementi per una riflessione critica su una tematica di indubbia attualità, quale appunto la criminalità informatica.

Negli ultimi anni siamo diventati testimoni di un'evoluzione senza precedenti che ha condotto la società a un punto di svolta. Le nuove tecnologie, pur offrendo possibilità e opportunità inimmaginabili fino a solo qualche decennio fa, al contempo sollevano interrogativi e introducono pericoli ai quali non eravamo precedentemente esposti: la digitalizzazione e l'interconnettività a livello globale hanno generato una nuova categoria di rischi legati ai reati informatici. Trattasi di un ambito che richiede una particolare attenzione e sensibilità giuridica, in quanto ricomprendente una vasta gamma di illeciti tecnologicamente insidiosi e raffinati, i quali, a causa della natura transnazionale che li caratterizza, pongono sfide significative in termini di giurisdizione, individuazione e perseguibilità. Gli esperti di diritto penale dell'informatica sono pertanto chiamati ad occuparsi di questioni emergenti e cruciali, nell'ottica di preservare il ruolo della tecnologia digitale quale strumento di integrazione positiva nella società.

La tesi focalizza in particolare la sua attenzione sul delitto di accesso abusivo ad un sistema informatico o telematico, in quanto fattispecie che in qualche modo potrebbe essere definita un po' come il punto cardine dei reati informatici dal momento che risulta prodromica alla realizzazione di ulteriori reati diretti contro l'integrità e la riservatezza dei dati e dei programmi contenuti all'interno del sistema (danneggiamento, falsificazione di documenti, violazione della corrispondenza, ecc.). La Raccomandazione sulla criminalità informatica R (89) 9, infatti, sollecitava gli Stati membri ad incriminare l'accesso abusivo per tutelare la sicurezza dei sistemi informatici – e dunque l'inviolabilità del domicilio – al fine di salvaguardare indirettamente i sistemi stessi dai rischi di manipolazioni informatiche successive. Questo perché l'accesso non autorizzato ad un sistema informatico, oltre a comportare pregiudizi economici rilevanti per chi lo subisce (pensiamo esemplificativamente ai costi delle verifiche e degli accertamenti dell'intrusione) appare sicuramente insidioso per la riservatezza e l'integrità dei programmi: una volta entrato nel sistema altrui, l'aggressore può acquisire i cc.dd. privilegi di *root* che gli consentirebbero di compiere operazioni sulla macchina come

fosse la propria, rendendo quindi passibili di lettura, modifica o cancellazione i dati e i programmi contenuti nel sistema.

Dall'analisi dei molteplici aspetti critici emersi nella disciplina oggetto di questo studio, risulta evidente la necessità di una riforma dell'art. 615-*ter* c.p. con l'obiettivo di adattare la normativa ormai obsoleta e superata dagli sviluppi tecnologici che si sono registrati dagli anni '90 ad oggi, nonché fornire una disposizione che sia più facilmente comprensibile non solo per gli operatori del diritto ma anche per i cittadini.

Innanzitutto, sarebbe auspicabile creare un autonomo titolo all'interno del codice penale dedicato esclusivamente ai reati informatici, per conferire loro quell'autonomia sistematica che già nel 1993 avrebbero dovuto vantare.

Avendo poi riguardo nello specifico al reato di accesso abusivo, alla luce delle considerazioni svolte sul bene giuridico tutelato e consapevoli dell'interconnessione che caratterizza oggi il cyberspazio, sembra opportuno rileggere la norma quale ipotesi posta a tutela della riservatezza informatica, piuttosto che del domicilio informatico. Rispetto a quello che può essere stato il primo approccio del legislatore alla realtà tecnologica, appare infatti di immediata comprensione l'esigenza di salvaguardare un diritto di più ampia accezione, in grado di ricomprendere sia la disponibilità dei dati e programmi presenti nel sistema di pertinenza della persona, sia la confidenzialità degli stessi.

Quanto al lessico utilizzato, va sicuramente posto rimedio all'impiego del verbo "introdursi", certamente inappropriato per il linguaggio informatico e non conforme alla rubrica dell'articolo, che invece correttamente parla di "accesso".

Inoltre, date le divergenze emerse in giurisprudenza, dovrebbe essere meglio specificato cosa debba intendersi per abusività della condotta. Sembrerebbe doversi accogliere più favorevolmente l'opzione ermeneutica che interpreta il carattere abusivo dell'accesso in senso oggettivo, non attribuendo pertanto rilevanza alle finalità personali perseguite dal soggetto agente e basandosi, invece, sulla violazione di regole specifiche inerenti alle mansioni assegnate.

Infine, da non condividere le critiche mosse in relazione alla previsione delle misure di sicurezza, che alcuni in dottrina propongono di eliminare. Trattasi infatti di una specificazione che conserva una sua utilità nel definire situazioni complesse e incerte in cui l'accesso ad un sistema informatico possa effettivamente dirsi aver integrato il reato di cui all'art. 615-*ter* c.p. poiché non autorizzato. Il rimando all'elemento delle misure di

sicurezza permette oltretutto di trovare un chiaro equilibrio con la libertà di accesso a informazioni e spazi virtuali, che pur sempre deve essere garantita.

In generale, l'avvento dell'era digitale ha radicalmente trasformato le modalità di comunicazione, informazione e partecipazione alla vita collettiva. Tuttavia, se da un lato le piattaforme digitali e i *social media* hanno amplificato le opportunità di espressione e di partecipazione, consentendo a ciascun utente di interagire con un pubblico vasto ed eterogeneo, dall'altro lato hanno anche dato origine a dinamiche preoccupanti che minacciano la qualità del dibattito democratico. Uno degli aspetti più critici di questo scenario è infatti rappresentato dalla formazione di quelle che vengono metaforicamente definite come "camere dell'eco": negli ambienti digitali gli individui e i gruppi tendono ad interagire esclusivamente con fonti di informazioni e con altri utenti con cui condividono le stesse vedute, precludendo quindi un dialogo costruttivo con opinioni diverse o contrapposte. Questo fenomeno è oggi amplificato e ulteriormente aggravato dagli algoritmi di personalizzazione che regolano la distribuzione dei contenuti sulle piattaforme *social* e che talvolta diffondono informazioni false o fuorvianti (*fake news*). Dal punto di vista giuridico, la sfida consiste nel trovare un punto di equilibrio tra la tutela della libertà di espressione – pilastro fondamentale delle società democratiche odierne – e la necessità di prevenire e contrastare i fenomeni che ne compromettono l'integrità e il funzionamento. Questo implica una riflessione approfondita sul ruolo che svolgono i prestatori dei servizi nelle piattaforme digitali e sulla loro responsabilità nel promuovere un ambiente *online* sano, inclusivo e veritiero. Il D. Lgs. n. 70/2003, recependo la direttiva europea sul commercio elettronico, fornisce alcune indicazioni sul regime di responsabilità di questi soggetti, ma è chiaro che il contesto attuale imponga un aggiornamento delle normative vigenti per adeguarle alle evoluzioni tecnologiche intervenute in tempi recenti.

L'introduzione e lo sviluppo delle tecnologie che sfruttano l'intelligenza artificiale, in particolare l'uso di algoritmi avanzati che operano sulla base di processi decisionali automatizzati, hanno portato ad una trasformazione significativa del tessuto socio-economico. Si tratta infatti di tecnologie che, non limitandosi a fornire dati e supporto informativo per le decisioni umane, in molti casi assumono veri e propri ruoli attivi nel processo decisionale, tenendo comportamenti che derivano dallo sviluppo auto-evolutivo e che, di conseguenza, sfuggono dalla sfera di prevedibilità iniziale del programmatore. I

sistemi di IA oggi sono in grado di analizzare grandi volumi di dati e identificare partner e tendenze, imparare dalle esperienze pregresse e adattare le loro future azioni in base ai risultati ottenuti e all'esperienza acquisita.

Tale evoluzione solleva questioni complesse dal punto di vista giuridico e etico, specialmente in relazione alla responsabilità per le azioni e le decisioni prese da sistemi automatizzati e, a monte, alla trasparenza e comprensibilità dei processi decisionali su cui si fondano. Questo richiede pertanto un'indagine approfondita sulle catene di causa-effetto e sull'effettiva capacità del sistema di IA di autodeterminarsi, per capire – fermo il principio del *machina delinquere non potest*– in che misura gli sviluppatori, i programmatori o gli utilizzatori possano essere ritenuti responsabili per le conseguenze delle decisioni automatizzate. Sebbene l'IA sembra poter raggiungere livelli di autonomia e capacità di apprendimento in grado di sfidare i limiti dell'innovazione tecnologica, l'intelligenza e l'etica umana rimangono centrali nel processo di sviluppo e implementazione dell'IA. Diventa allora imperativo interrogarsi su come regolamentare e gestire le implicazioni di queste tecnologie, soprattutto nei settori critici come la sanità, la sicurezza pubblica o la finanza, dove i comportamenti tenuti da macchine intelligenti hanno un impatto diretto sulla vita delle persone. È importante quindi riflettere sull'adeguatezza della normativa vigente e sulla possibilità di introdurre nuove disposizioni specifiche per l'IA, al fine di garantire che l'uso di queste tecnologie automatizzate sia conforme ai principi di giustizia, equità e trasparenza, promuovendo al contempo la ricerca scientifica e il progresso tecnologico.

Attualmente risulta imprescindibile, dal punto di vista normativo, l'elaborazione di un quadro regolatorio che riconosca le specificità e i rischi associati all'autonomia decisionale dell'IA. Questo implica definire precisi criteri di responsabilità e trasparenza per gli sviluppatori e gli utilizzatori di sistemi di IA, nonché stabilire protocolli per la sorveglianza e la revisione delle decisioni automatizzate. Inoltre, la questione dei confini dell'IA richiede l'introduzione di standard etici e buone pratiche nello sviluppo e nell'impiego di queste tecnologie, al fine di prevenire abusi e garantire un loro utilizzo responsabile e orientato al bene comune. In questo senso, diviene cruciale il dialogo interdisciplinare tra giuristi, informatici e filosofi per tracciare un futuro in cui tecnologie e umanità possano coesistere in armonia, favorendo così l'integrazione positiva degli agenti intelligenti nella società.

Nel panorama odierno dominato dalla rivoluzione tecnologica, potenziata dall'intelligenza artificiale, il diritto, in particolare il diritto penale, si trova di fronte a sfide che gli impongono una flessibilità, una fluidità e un aggiornamento costante per essere in grado di abbracciare anche i nuovi fenomeni e rispondere così alle mutate condizioni sociali e tecnologiche. È infatti impensabile concepire uno spazio virtuale libero dal diritto e, allo stato attuale, non si può più rinviare una riflessione critica che tenga conto di come implementare i sistemi di IA nel settore della giustizia penale, assicurando il rispetto dei diritti fondamentali che certamente abbisognano di riconoscimento e protezione anche nell'ambito del digitale. Si tratta di tematiche che impongono una rilettura delle nozioni giuridiche tradizionali di azione e colpevolezza per evitare che si vengano a creare aree di immunità, che in futuro rischiano di dilatarsi eccessivamente.

All'incessante sviluppo tecnologico si contrappone oggi una normativa giuridica spesso inadeguata. Le disposizioni vigenti offrono degli strumenti per il contrasto di alcuni di questi reati, ma è comunque necessario un continuo aggiornamento normativo che tenga conto delle innovative tecniche criminali rese disponibili dalla tecnologia. Una maggiore consapevolezza e una comprensione di questi rischi sono fondamentali non solo per gli operatori del diritto, ma per l'intera società. Le sfide da affrontare sono complesse e richiedono competenze tecnologiche avanzate. In questo scenario, non riuscendo il legislatore a tenere sempre il passo con l'evoluzione digitale, potrebbe essere utile orientarsi nel senso di andare ad incentivare, accanto agli strumenti repressivi, le misure di prevenzione. L'evoluzione delle Tecnologie dell'Informazione e della Comunicazione rende infatti la questione della sicurezza informatica una priorità da gestire tanto per gli Stati quanto per le organizzazioni pubbliche e private.

La giurisprudenza e la dottrina hanno, in questo contesto, il compito di interpretare le norme esistenti alla luce delle nuove realtà tecnologiche allo scopo di fornire una guida nella formulazione di nuove disposizioni che si dimostrino efficaci a contrastare i reati informatici, operando un bilanciamento che permetta di tutelare al tempo stesso i diritti fondamentali delle persone. È pertanto essenziale promuovere una cultura della sicurezza informatica, incentivare la ricerca e lo sviluppo di tecnologie sicure, adottando parallelamente un approccio legislativo proattivo e dinamico che possa adeguarsi tempestivamente alle nuove minacce.

GIURISPRUDENZA

Trib. Torino, Sez. IV, 07.02.1998

Cass. pen., Sez. VI, 04.10.1999 - 14.12.1999, n. 3067

Cass. pen., Sez. V, 07.11.2000, n. 12732

Trib. de L'Aquila, 10.06.2005

Cass. pen., Sez. V, o4.12.2006, n. 6459

Cass. pen., Sez. V, 06.02.2007, n. 11689

Trib. Milano, Sez. III, 19.03.2007

Cass. pen., Sez. V, 20.12.2007-17.01.2008, n. 2534

Cass. pen., Sez. II, 21.02.2008, n. 36721

Cass. pen., Sez. V, 29.05.2008, n. 26797

Cass. pen., Sez. V, 30.09.2008, n. 1727

Cass. pen., Sez. V, 01.10.2008, n. 37322

Cass. pen., Sez. VI, 08.10-21.10.2008, n. 39290

Cass. pen., Sez. V, 25.06-14.10.2009, n. 40078

Cass. pen., Sez. V, 13.12.2010-21.01.2011, n. 1934

Cass. pen., sez. V, 18.01.2011, n. 24583

Cass. pen., SS. UU., 27.10.2011-07.02.2012, n. 4694

Cass. pen., Sez. V, 08.05-26.10.2012, n. 42021

Cass. pen., Sez. I, 27.05.2013, n. 40303

Cass. pen., Sez. III, 17.12.2013, n. 5107

Cass. pen., SS. UU., 18.09.2014, n. 38343

Cass. pen., Sez. V, 18.12.2014, n. 10121

Cass. pen., SS. UU., 26.03-24.04.2015, n. 17325

Cass. pen., Sez. V, 21.07.2015, n. 31677

Cass. pen., Sez. V, 28.10.2015, n. 13057

Cass. pen., Sez. V, 13.01.2016, n. 6906

Cass. pen., Sez. V, 26.10.2016, n. 14546

Cass. pen., SS. UU., 18.05-08.09.2017, n. 41210

Cass. pen., Sez. V, 20.09-25.10.2018, n. 48895

Cass. pen., Sez. V, 29.11.2018-08.01.2019, n. 565

Cass. pen., Sez. V, 02.10.2018-22.01.2019, n. 2905

Cass. pen., Sez. V, 25.03-02.05.2019, n. 18284

Cass. pen., Sez. II, 28.03-15.04.2019, n. 16366

Cass. pen., Sez. V, 16.03-23.06.2021, n. 24576

Cass. pen., Sez. V, 30.04-06.07.2021, n. 25683

Cass. pen., Sez. V, 24.01-03.03.2022, n. 7775

Cass. pen., Sez. V, 13.06-04.10.2022, n. 37459

Cass. pen., Sez. V, 15.11-05.12.2022, n. 46076

Cass. pen., Sez. V, 30.01-27.04.2023, n. 17551

Cass. pen., Sez. V, 22.02-27.06.2023, n. 27900

BIBLIOGRAFIA

ACCINI G. P., *Profili di responsabilità penale dell'hosting provider "attivo"*, in Archivio Penale, fascicolo 2, maggio-agosto 2017

ACED C., *Web 2.0: the origin of the word that has changed the way we understand public relations,* 2013, in www.researchgate.net

AGGARWAL N. – L. FLORIDI – KING T. C. –M. TADDEO, *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, *Rochester, NY*, in *Social Science Research Network,* 2019

AMATO MANGIAMELI A. C. – SARACENI G., *I reati informatici: elementi di teoria generale e principali figure criminose,* Giappichelli Editore, Torino, 2015

BACCIN A., *Responsabilità penale dell'Internet Service Provider e concorso degli algoritmi negli illeciti online: il caso Force v. Facebook*, in Sistema Penale, 5/2020

BARTOLI R., *L'accesso abusivo a un sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato,* in Diritto Penale Contemporaneo, n. 1/2012

BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in Diritto Penale e Uomo, 2019

BELLACOSA M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in Diritto Penale Contemporaneo, 2015

BELLINGERI M., *Evoluzione giurisprudenziale del concetto di "abusività" nel caso di accesso ad un sistema informatico,* 12 maggio 2022, in

https://ntplusdiritto.ilsole24ore.com/art/evoluzione-giurisprudenziale-concetto-abusivita-caso-accesso-ad-sistema-informatico-AEGr8AYB

BERTOLESI R., *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere,* in Diritto Penale Contemporaneo, 03 ottobre 2017

BHARGAVA V. R. – VELASQUEZ M., *Is Corporate Responsibility Relevant to Artificial Intelligence Responsibility?*, in *Georgetown Journal of Law and Public Policy*, 2019

BORRUSO R., *La tutela del documento e dei dati,* in *Profili penali dell'informatica,* in Teoria e pratica del diritto, sezione III (diritto e procedura penale) n. 70, Giuffrè editore, Milano, 1994

CAMPLANI F., *Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato,* in Archivio penale, 2/2020, 1° settembre 2020

CAPPELLINI A., *Machina delinquere non potest*. *Brevi appunti su intelligenza artificiale e responsabilità penale*, in Criminalia, 2018

CORRIDORI C., *L'intelligenza artificiale come vittima del reato*, in *Cybercrime*, UTET Giuridica, Milano, giugno 2023

D'AIETTI G., *La tutela dei programmi e dei sistemi informatici,* in *Profili penali dell'informatica,* in Teoria e pratica del diritto, sezione III (diritto e procedura penale) n. 70, Giuffrè editore, Milano, 1994

DI GIORGI FEDERICO, *L'evoluzione di Internet: dal web 1.0. al web 4.0*, in linkedin.com

DOUTHWAITE A., *Cybercrime's Evolution Since the 80's: Historical Facts and Figures,* ottobre 2022, in https://virtualarmour.com/cybercrimes-evolution-since-the-80s/

FASANI F., *Accesso abusivo a un sistema informatico: le Sezioni Unite cambiano di nuovo rotta (nota a Cass., Sez. un., 8 settembre 2017, ud. 18 maggio 2017, Savarese)*, in Le Società, 2017

FIANDACA G. – MUSCO E., *Diritto penale. Parte generale*, Bologna, VIII edizione, Zanichelli editore, 2019

FINANCE & DEVELOPMENT, September 2016, Vol. 53, No. 3, *The Dark Side of Technology*

FLOR R., *Cyber-criminality: le fonti internazionali ed europee,* in *Cybercrime,* UTET Giuridica, Milano, giugno 2023

FLOR R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative,* in *Cybercrime,* UTET Giuridica, Milano, giugno 2023

FLOR R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet,* in Diritto Penale Contemporaneo, 20 settembre 2012

FLOR R., *Verso una rivalutazione dell'art. 615 ter c.p.?*, in Diritto Penale Contemporaneo, 2/2012

FLORIO M. E., *Il dibattito sulla responsabilità penale diretta delle IA: "molto rumore per nulla"?*, in Sistema Penale, 2/2024

FRAGASSO B., *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, in Sistema Penale, giugno 2023

GIANNINI A., *Responsabilità da reato degli enti e intelligenza artificiale*, in *Cybercrime*, UTET Giuridica, Milano, giugno 2023

GIUSTI P., *La responsabilità penale dell'intelligenza artificiale: i termini generali del problema, con particolare riguardo alle auto senza conducente*, in *Cybercrime*, UTET Giuridica, Milano, giugno 2023

HADZI A. – ROIO D., *Restorative Justice in Artificial Intelligence Crimes*, in *Journal for digital cultures*, novembre 2019, in www.spheres-journal.org

HALLEVY G., *Liability for Crimes Involving Artificial Intelligence Systems*, Springer, New York, 2015

IASELLI M., *Internet Service Provider. Guida all'ISP: cos'è, regime e tipologie di responsabilità*, in Altalex, 13 novembre 2019

INGRASSIA A., *Il ruolo dell'Isp nel ciberspazio: cittadino, controllore o tutore dell'ordine?*, in Diritto Penale Contemporaneo, 08 novembre 2012

INGRASSIA A., *La sentenza della Cassazione sul caso Google*, in Diritto Penale Contemporaneo, 06 febbraio 2014

JAISHANKAR K., *Space Transition Theory of Cyber Crimes*, in F. SCHMALLEGER – M. PITTARO**,** *Crimes of the Internet*, Prentice Hall, 2008

LAMANUZZI M., *Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma*, in Archivio penale, 2022 n. 2

LARINNI C., *Garantismo europeista: un ossimoro? A proposito dell'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)*, Criminalia in disCrimen dal 29.06.2020

LENA A., *Digital Single Market: la certificazione europea nel nuovo mandato permanente dell'Enisa.*, Torino, dicembre 2020, in www.analyticaintelligenceandsecurity.it

LOMBARDI F., *Alle Sezioni unite il rapporto tra accesso abusivo a sistema informatico e sviamento di potere,* in Giurisprudenza Penale Web, 4/2017

LOMBARDO S., *Spoofing: cos'è, tipologie di attacco e soluzioni di difesa,* dicembre 2022, in www.cybersecurity360.it

LONGO A. R., *Nativi e analfabeti digitali: il paradosso della "Generazione Google"*, novembre 2017, in https://www.scientificast.it/nativi-analfabeti-digitali-paradosso-della-generazione-google/

MAGRO M. B., *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in Legislazione Penale, 2020

MAGRO M. B., *Il problema della responsabilità per l'uso di intelligenze artificiali*, in *Cybercrime*, UTET Giuridica, Milano, 2023

MAZZEL M., *Attacchi informatici: la tutela penalistica. Le attuali previsioni normative forniscono un'adeguata risposta a fronte di tale fenomeno?,* in Altalex, 16 maggio 2022

MCCARTHY J. ET AL., *A Proposal for the Darthmouth Summer Research Project on Artificial Intelligence,* 1956, in https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

MENSI M. – FALLETTA P., *Il diritto del Web*, II ed., CEDEM, Padova, 2018

NORVING P. – STUART J. R., *Artificial Intelligence. A Modern Approach*, III ed., Prentice Hall, 2010

PICOTTI L., con il contributo di SALVADORI I. e FLOR R., *Reati informatici, riservatezza, identità digitale*, elaborato presentato durante il Convegno Nazionale dell'Associazione Italiana dei Professori di Diritto Penale, 2019

PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme,* in *Cybercrime,* UTET Giuridica, Milano, 2019

PICOTTI L., *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme,* in *Cybercrime,* UTET Giuridica, Milano, giugno 2023

PICOTTI L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Tutela penale della persona e nuove tecnologie, CEDAM, Padova, 2013

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in Il diritto penale dell'informatica nell'epoca di Internet*,* Padova, 2004

PIETRELLA T., *L'incidenza dello sviluppo tecnologico sulla tenuta di condotte offensive*, in Sistema penale, 10.2023

PLANTAMURA V., *Moderne tecnologie, riservatezza e sistema penale: quali equilibri?*, in Il diritto dell'informazione e dell'informatica, Giuffrè editore, Milano, 2006

RAVOTTO P., *Da "nativi digitali" a "consapevoli digitali", il ruolo della Scuola*, 16 novembre 2018, in www.agendadigitale.eu

REDAZIONE GIURISPREDENZA PENALE, *Accesso abusivo ad un sistema informatico: sul luogo di consumazione del reato*, in Giurisprudenza Penale, 8 novembre 2013

ROMANO A., *Sui reati informatici nella legalità costituzionale*, materiale didattico del corso di Informatica e Diritto, a.a. 2010-2011

ROMEO G., *Le Sezioni Unite sull'accesso abusivo a un sistema informatico o telematico,* in Diritto Penale Contemporaneo, 10 febbraio 2012

ROTTIGNI M., *Nella mente dei cyber criminali: le TTP che ogni professionista della sicurezza dovrebbe conoscere,* 2023, in www.securityopenlab.it

SALVADORI I., *I reati contro la riservatezza informatica,* in *Cybercrime,* UTET Giuridica, Milano, giugno 2023

SARTOR G., *L'intelligenza artificiale e il diritto*, Giappichelli Editore, Torino, 2022

SCHREIBER F. A. – TANCA L., *Il contesto nei sistemi informativi: cos'è e perché è sempre più importante,* Maggio 2018, in www.agendadigitale.eu

SEMINARA S., *Locus commissi delicti, giurisdizione e competenza nel cyberspazio*, relazione al Convegno "Presi nella rete - Analisi e contrasto della criminalità informatica", Pavia, 23 novembre 2012

SEMINARA S., *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)*, in *MediaLaws* – Rivista dir. media*,* 2018, n. 2

SHAW J., *How the internet made it easier for all of us to be criminals, or victims*, 2019, in www.wired.co.uk

SICIGNANO G. J. – DI MAIO A., *I nuovi reati informatici, disciplina sostanziale e profili processuali*, La Tribuna, 2022

T. O'REILLY – J. BATTELLE, *Web Squared: Web 2.0 Five Years On*, O'Reilly Media Inc., 2009

UBERTIS G., *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in Diritto Penale Contemporaneo, 4/2020