LUISS Università Guido Carli

Corso di Laurea Magistrale a Ciclo unico in Giurisprudenza

Tesi di laurea in

Diritto Penale 2

LA FRODE INFORMATICA

Relatore
Ch. mo Prof.
ANTONIO GULLO

Candidata
GINEVRA GUGLIELMI
Matr. 152233

Anno Accademico

2021-2022

Introduzione

Il reato di frode informatica, disciplinato dal libro II, titolo XIII, ed in particolare dall'art. 640 ter c.p., è stato introdotto alla legge n. 547 del 1993, unitamente ad altre fattispecie delittuose avente come comune denominatore la criminalità informatica.

I reati informatici sono tutti quei reati caratterizzati dal ricorso alla tecnologia informatica, sia quale oggetto materiale del reato che quale strumento di realizzazione.

L'obiettivo dell'indagine è quello di ricostruire i reati informatici con particolare riguardo alla frode informatica. Il primo capitolo dell'indagine è dedicato proprio a tale ricostruzione, in quanto esamina il reato di frode informatica nell'ambito dei reati informatici. Il secondo capitolo, invece, si sofferma, in maniera dettagliata, sulla frode informatica, sull'oggetto di tutela, sulla condotta, sulle modalità di realizzazione, sull'elemento soggettivo, tutti elementi del reato analizzati con i contributi della dottrina e della giurisprudenza. Infine, si sofferma su una particolare tipologia di frode informatica, il *phishing*, una tecnica molto diffusa e pericolosa, che pone numerosi problemi di inquadramento e riconduzione sotto le fattispecie esistenti, non esistendo attualmente alcuna norma che lo reprima direttamente.

Il terzo e ultimo capitolo, infine, propone una disamina della responsabilità amministrativa degli enti da reato con particolare riguardo proprio alla frode informatica. Inizialmente il legislatore non aveva inserito la frode informatica tra i reati presupposto nel d.lgs. n. 231/2001, ma successivamente si è reso conto che era necessario responsabilizzare gli enti anche con riguardo ai reati informatici e, dunque, è stato introdotto nel catalogo, tra gli altri, anche il reato di frode informatica.

CAPITOLO I
IL CONTRASTO AL CYBERCRIME: I REATI INFORMATICI NELL'ORDINAMENTO GIURIDICO ITALIANO

Sommario: 1. La nozione di "crimini informatici", 2. Il fenomeno del cybercrime; 2.1. Analisi degli elementi caratterizzanti il reato informatico; 2.2. Le modalità di manifestazione del reato informatico 12 2.3. Analisi degli aspetti caratterizzanti il cybercriminale; 2.3.1. La figura dell'hacker; 3. La normativa sovranazionale, 3.1. La direttiva NIS 1; 3.2. La direttiva NIS 2; 4. La normativa italiana in materia di reati informatici; 4.1. I lavori preparatori della legge n. 547/1993; 4.2. Il contenuto della legge n. 547/1993; 5.1. Il ruolo dell'ENISA; 5.2. L'istituzione dell'Agenzia per la cybersicurezza nazionale; 6. I reati informatici: un allarme crescente; 6.1. Accesso abusivo a un sistema informatico o telematico (615 ter c.p.); 6.2. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quiquies c.p.); 6.3. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.); 6.4. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies c.p.); 7. La tutela dei minori al cospetto dei reati sessuali commessi online

1. La nozione di "crimini informatici"

Con l'avvento di Internet e delle nuove tecnologie il mondo che conoscevamo ha assunto una veste del tutto originale. Gli uomini hanno avuto accesso ad una nuova dimensione, connotata da una natura dematerializzata e virtuale i cui sistemi di funzionamento sono ignoti ai più.

I sistemi informatici e i dispositivi elettronici sono creati da persone altamente competenti e qualificate in materia e distribuite sul mercato in modo tale che gli utilizzatori possano liberamente fruirne anche pur non conoscendone l'intrinseco funzionamento.

Dare una definizione di reato informatico risulta, quindi, estremamente complesso in ragione del carattere innovativo delle piattaforme e dei mezzi utilizzati[1].

La difficoltà nella definizione sta proprio nel fatto che i modelli tradizionali della costruzione del reato e l'approccio delle scienze criminologiche non sono adatte e sufficienti alla spiegazione e alla categorizzazione di questo fenomeno, che si presenta come nuovo perché parte integrante del sistema informatico.

Prima di procedere, dunque, pare opportuno individuare l'oggetto della trattazione. In particolare, è opportuno distinguere tra crimine informatico e cybercrime. Il crimine informatico si serve di apparecchi e sistemi informatici, ma non presuppone, necessariamente, l'utilizzo della rete internet per la commissione del reato. Diversamente, invece, i cybercrimes presuppongono, per la loro esecuzione, l'utilizzo della rete internet. Sotto questo punto di vista, i cybercrimes rappresentano l'evoluzione del concetto di crimine informatico. Parte della dottrina, in proposito, ha osservato che «sul piano fenomenico si è assistito, dopo l'"esplosione" di Internet, al passaggio dalla dimensione "privata" o "individuale" del computer e delle delimitate reti di computer alla dimensione "pubblica" o "collettiva" dei sistemi, basati sull'interconnettività globale. Nell'attuale società dell'informazione il fenomeno "criminalità informatica" risulta essere dunque flessibile ed aperto a fatti criminosi che possono essere commessi attraverso la rete o nel cyberspace»[2].

Va segnalato che parte della dottrina[3] ha avanzato una distinzione tra reati informatici "in senso stretto" e reati cibernetici. I reati informatici in senso

---

[1] Cfr. G. D'Aiuto, L. Levita, *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, pag. 44.

[2] R. Flor, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *Diritto penale contemporaneo*, 2012, pag.1.

[3] Cfr. L. Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id. (a cura di), *Il diritto penale dell'informatica nell'era di Internet*, Padova, 2004, p. 21 ss.

stretto sono caratterizzati dalla previsione, all'interno della fattispecie legale, di specifici elementi di tipizzazione, che contengono un riferimento esplicito alle nuove tecnologie dell'informazione e della comunicazione, a prescindere che essi si riferiscano alla condotta o ai mezzi, alle modalità oppure agli effetti o ancora a qualunque altro elemento essenziale oppure di carattere circostanziale[4].

I reati informatici in senso stretto sono caratterizzati dalla presenza di alcuni elementi informatici: nuovi fatti (accesso abusivo: art. 615 ter c.p.), nuove modalità (frode informatica: art.640 ter c.p.), nuovi "oggetti" (danneggiamenti: art. 635 bis ss. c.p., falsità informatiche: art. 491-bis c.p., violazioni di esclusiva su programmi informatici, banche dati e opere digitali, legge dir. autore); i reati cibernetici, invece, sono caratterizzati dal fatto di presentare il cyberspace come ambiente di ogni crimine (tra i nuovi reati ci sono attacchi DoS, phishing, identity theft, spamming, childgrooming, revenge porn, cyberbulling, cyberstalking, tra i reati tradizionali, invece, ci sono diffamazione: art. 595, co.3, c.p., pedopornografia: art. 600 ter s. c.p., riciclaggio: art. 648 bis c.p., estorsione: art. 629 c.p.).

I reati cibernetici, dunque, sono reati di ogni altro tipo, i cui elementi costitutivi o circostanziali, in via interpretativa o alternativa, permettano in ogni caso di ricondurli nell'ambito delle rispettive fattispecie legali. In tal caso, dunque, non potrà parlarsi di reati informatici in senso ampio, bensì di reati cibernetici, che a loro volta possono essere divisi in reati cibernetici in senso stretto (ad esempio il cyberstalking) e in senso ampio, a seconda che la commissione del reato tramite Internet sia elemento espresso o solo interpretativamente compatibile con la fattispecie legale (si pensi ai casi di diffamazione on line, di diffusione di materiale pedopornografico, di

[4] Cfr. L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Torino, 2019, p. 111 ss.

istigazione alla discriminazione e all'odio razziale, di violazione dei diritti d'autore, ecc.)[5].

Un'ulteriore categorizzazione avviene in base all'essenzialità che il dispositivo assume nella condotta, si parla in tal senso di reati propriamente informatici e di reati eventualmente informatici. I primi sono reati che vengono ad esistenza solo ed in funzione dello strumento informatico o telematico, i secondi sono invece fattispecie di reato che possono sussistere anche al di fuori dello spazio virtuale, fra questi sono contenute le ipotesi di violazione dei sistemi informatici, attacchi al patrimonio, diffusione di contenuti illeciti online, attentato a beni personali, violazione dei diritti di proprietà intellettuale, cyberterrorismo e cyber warfare.

Sarebbe necessaria l'introduzione di nuove categorie affiancate da una più puntale normativa in materia, capace di modificarsi seguendo l'evoluzione, sempre più veloce, del mondo della tecnologia.

Il progresso del mondo informatico ha creato la c.d. *information technology*, categoria che racchiude la tecnologia usata dai computer per creare, memorizzare, servirsi delle informazioni nelle sue più disparate forme

La sempre maggiore influenza di questo insieme di tecnologie e metodi necessarie per l'utilizzo dei sistemi informatici è andata a complicare la già difficile definizione e categorizzazione dei reati informatici.

I *cybercrimes* risultano di difficile definizione anche a causa delle condotte illecite estremamente differenziate fra loro, che inglobano comportamenti di varia natura.

Il mondo cibernetico appare di una disarmante complessità, figlia della dematerializzazione e della cancellazione dello spazio fisico, laddove questa dimensione virtuale accoglie il mondo dei reati, dovrà necessariamente accogliere anche il mondo della sicurezza.

[5] Cfr. L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., p. 112.

La sicurezza informatica, altresì chiamata *cybersecurity* viene definita dall'*International Telecommunication Union* (ITU) delle Nazioni come "l'insieme di strumenti, interventi, concetti, linee guida, impostazioni della gestione del rischio, azioni pratiche, procedute e tecnologie che possono essere utilizzate per proteggere lo spazio e la struttura cibernetica e i loro utilizzatori"[6].

La sicurezza informatica, dunque, si pone l'obiettivo di difendere lo spazio cibernetico dal pericolo della commissione dei reati informatici, tramite l'elaborazione di strategie preventive ed azioni di diverso genere.

2. Il fenomeno del cybercrime

2.1. Analisi degli elementi caratterizzanti il reato informatico

Dopo essere diventato parte integrante della vita quotidiana, Internet, allo stesso tempo, ha iniziato ad essere sempre più usato per commettere reati contro la persona, la proprietà privata e contro il sistema politico[7].

L'utilizzo sempre più diffuso nella vita quotidiana della tecnologia informatica e dei sistemi di telecomunicazione, nonché la creazione di reti informatiche globali hanno portato, come è stato analizzato precedentemente, alla creazione di un "cyberspazio" nel quale le attività illecite sono all'ordine del giorno ed in costante aumento.

La proliferazione dei reati informatici è agevolata dal fatto che questi attacchi possono essere compiuti anonimamente, in tempi brevissimi e a distanza. Queste caratteristiche vanno a costituire la c.d. asimmetria degli attacchi informatici.

Un secondo elemento che facilita la commissione di questi reati è costituito dalla potenziale semplicità del compimento della condotta illecita: nel

[6] UN ITU, *Overview of Cybersecurity. Recommendation* UTI-T X.1205, Ginevra, UN, 2008
[7] Cfr. V. Contraffatto, *Reati informatici*, Milano, 2007, pag. 19.

paragrafo precedente è stato messo in luce che la conoscenza di un sistema informatico non è scontata e che, anzi, sono necessarie competenze specifiche nel settore per arrivare a comprendere il funzionamento del dispositivo tecnologico; se da un lato questo dato potrebbe far pensare che la commissione del reato sia, quindi, limitata ad un numero estremamente ridotto di soggetti, ovverosia quelli dotati di alte competenze informatiche, dall'altro, in realtà, vista la fruizione su larga scala e la complessità del mondo della rete il reato è facilmente eseguibile anche ad opera di soggetti non dotati di particolari competenze tecniche, elemento che si lega anche all'esistenza di un rischio molto basso nell'essere individuati[8].

Come è stato analizzato nel paragrafo precedente, i reati informatici sono caratterizzati da una condotta illecita analoga a quella tradizionale, che tuttavia ha ad oggetto, o si serve, di componenti tecnologiche. Si è poi sottolineato, in particolare, che i cybercrimes, nell'ambito dei reati informatici, si servono della rete internet, che la categoria generale invece non presuppone come requisito fondante.

La maggiore difficoltà che si riscontra in relazione alla categoria dei reati informatici è legata alla corretta individuazione del bene giuridico da tutelare in riferimento a tali reati[9].

L'identificazione dei beni giuridici lesi dalle condotte illecite nella dimensione informatica rappresenta la maggiore difficoltà sul tema.

Come è possibile capire nel concreto i casi di illiceità e quindi di lesione del bene? Quali beni giuridici devono essere tutelati?

Con riferimento ai reati informatici c.d. propri o anche in senso stretto sussiste una vera e propria difficoltà di individuazione del bene giuridico, questo accade perché non esistono reati "tradizionali", motivo per cui il legislatore ha deciso di collocare tali reati in prossimità del reato tradizionale al quale

[8] Cfr. S. Amore, V. Stanca, S. Staro, *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Milano, 2006, pag. 44.
[9] Cfr. V. Contraffatto, *Reati informatici*, cit., pag. 38.

"assomigliano" (es. l'accesso abusivo con la violazione del domicilio, in questo caso tutelando l'interesse di ciascun individuo ad avere l'esclusività sul proprio spazio informatico al di fuori di illegittime interferenze da parte di terzi)[10].

Il legislatore, in questa maniera, ha voluto tutelare beni giuridici emergenti come il patrimonio, che si legano spesso a tutte quelle fattispecie di accesso non autorizzato ai sistemi informatici ai fini di danneggiare il patrimonio altrui, la privacy e riservatezza: in tal caso il legislatore si riferisce a tutti quei reati che violano, alterano e divulgano le informazioni private della persona attraverso la rete, l'integrità personale, cui si legano invece quei reati di pedopornografia, pornografia, comportamenti di incitazione all'odio, ed ancora la sicurezza informatica, che costituisce un nuovo ed importante bene giuridico oggetto di interesse e rilevanza penale.

A scopo esplicativo potrebbe essere utile una distinzione fra i reati di accesso abusivo e quelli di danneggiamento informatico, nelle loro versioni più ampie[11].

Ciò vale per i reati informatici c.d. propri, per i reati impropri invece è utile fare un discorso differente.

Essendo questi ultimi reati che possono essere eseguiti sia nel mondo reale che in quello virtuale, qui il legislatore ha tentato di unificare tutti i *cybercrime* sotto uno stesso unico bene giuridico, anche se questi reati informatici sottendono ad una serie di beni giuridici differenti da quelli dei reati tradizionali[12].

È stato per questo necessario inserire una serie di fattispecie penali informatiche specifiche.

---

[10] Cfr. S. Amore, V. Stanca, S. Staro, *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, cit., pag. 66.
[11] Cfr. V. Frosini, *La criminalità informatica*, in *Dir. Inf.*, 1997, pag. 48.
[12] Cfr. V. Contraffatto, *Reati informatici*, cit., pag. 41.

2.2. Le modalità di manifestazione del reato informatico

I reati informatici possono, poi, essere commessi secondo diverse modalità. Il metodo più semplice e più diffuso è costituito dal c.d. *data diddling*, ovverosia la manipolazione dei dati. Questa si estrinseca nella falsificazione di documenti e dei dati che sono poi inseriti nell'elaboratore.

La tecnica Salami prevede invece una modalità di commissione del reato con la quale vengono sottratte piccole somme provenienti da un grande numero di accrediti in modo tale da farle confluire nel conto di chi commette il reato.

Accanto a questi strumenti per commettere il reato, ha visto una notevole diffusione anche l'utilizzo del cd. *Malware*, crasi di *malicious software*, un software malvagio che ha lo scopo di cagionare danni interni ad un sistema informatico, impedendone il corretto funzionamento e causando malfunzionamenti anche alle reti.

I *malware* sono di diverso tipo, quello più conosciuto dagli utenti, nonché il più diffuso e utilizzato, è costituito dalla tipologia dei *virus*. Molti, proprio in ragione della sua diffusione, credono che il concetto di *virus* si sovrapponga esattamente a quello di *malware*, rendendo le categorie reciprocamente interscambiabili ma così non è[13].

Il *virus* consiste in un insieme di programmi nocivi contenuti all'interno di un programma che è apparentemente privo di conseguenze negative. Questi programmi, una volta avviati, possono attivare il *virus*, oppure questo può attivarsi autonomamente secondo una scansione temporale predefinita, quest'ultimo il caso delle cd. *Logic bomb*.

Fra i virus rientra il c.d. *Troyan horse*, il "Cavallo di Troia", che permette a colui che commette il reato di inserire nel computer di un programma diverso da quello che in principio deve eseguire, permettendo in tal modo al soggetto

[13] Cfr. L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici*, Torino, 2009, pag. 50.

di raggiungere i suoi scopi. Nella maggior parte dei casi con questo strumento vengono eseguite delle truffe[14].

Meno sofisticato del malware ma egualmente efficace è il c.d. *Ddos,* il "*distributed denial of service*".

Un attacco può colpire i software o direttamente l'hardware attraverso il software impossessandosi, così, del sistema informatico.

Questi strumenti vengono spesso utilizzati contro le imprese, i settori bancari ed assicurativi, che, come vittime degli attacchi, spesso decidono di non denunciare per evitare danni reputazionali o perdite economiche, accentuando la vulnerabilità del sistema e la difficoltà di punire i colpevoli.

La maggioranza dei reati informatici si sostanzia nella contraffazione dei prodotti, nella manipolazione dei dati, nel furto dei dati, nel riciclaggio di denaro e nell'attacco al sistema delle criptovalute.

A tal proposito, parte della dottrina suole suddividere i reati in base due categorie differenti, una prima della cd. *computer fraud* e una seconda della c.d. *computer abuse.* La *computer fraud* indicano tutti quelle condotte illecite di manipolazione dei dati a scopo fraudolento, le *computer abuse* comprendono, invece le condotte di utilizzo improprio delle tecnologie con il fine per il criminale di trarre un vantaggio per sé[15].

2.3. Analisi degli aspetti caratterizzanti il *cybercriminale*

Ciò che rileva particolarmente all'interno dei reati informatici sono le dinamiche psicologiche attinenti alla personalità del reo.

I "cybercriminali" possono essere classificati in base delle differenti motivazioni che li spingono a delinquere.

Possiamo distinguere i delinquenti occasionali che agiscono per pura curiosità o per motivi di natura emotiva o ancora per scopi ludici, i delinquenti politici

[14] Ivi, pag. 53.
[15] Cfr. V. Contraffatto, *Reati informatici*, cit., pag. 56.

che hanno un obiettivo determinato e una forte spinta ideologica e i delinquenti professionisti che agiscono abitualmente, soprattutto per ragioni economiche[16].

Un'ulteriore classificazione viene in essere se si analizzano le competenze informatiche dei criminali.

Alcuni di questi posseggono competenze informatiche estremamente elevate (crackers), altre competenze di medio livello (hackers), altri ancora competenze scarse (rodents).

Questa classificazione è importante perché l'identificazione del maggior numero e della maggiore diffusione di determinati reati commessi ad opera di criminali di una peculiare categoria potrebbe aiutare nella definizione di politiche di prevenzione e sicurezza che possano offrire una maggiore protezione dei sistemi informatici[17].

L'elemento psicologico assume una rilevanza ancor più peculiare se si pensi che questi agisce in uno spazio virtuale nel quale manca un qualsiasi contatto con la scena del crimine o con la vittima, creando una dimensione psicologica di estremo distacco rispetto alla condotta illecita.

La dematerializzazione dello spazio ha contribuito ad accorciare le distanze fisiche, rendendo il potenziale *cybercriminale* un pericolo non solo a livello interno statale ma anche a livello internazionale, potendo costituire un plausibile mezzo di spionaggio e una rete per il terrorismo transnazionale.

Per questa ragione il fenomeno necessita un'attenzione a livello internazionale ed europeo e di essere regolato al massimo anche dal punto di vista della prevenzione. È fondamentale che ci sia un coordinamento di politica penale fra i paesi proprio in virtù della facilità di espansione territoriale del criminale.

---

[16] Cfr. M. Mignone, *I cybercriminali: rischi e limiti dei profili criminologici*, in *Ciber. e dir*., 2001, pagg. 111 ss.

[17] Cfr. M. Mignone, *I cybercriminali: rischi e limiti dei profili criminologici*, cit., pag. 119.

Ulteriore elemento di interesse è costituito dalla circostanza per cui tipico agente è rappresentato dalla categoria dei cd. "colletti bianchi", soggetti che provengono da classi sociali agiate, hanno una vita rispettosa e mai ci si aspetterebbe che possano essere dei criminali.
Gli aspetti psicologici dei criminali informatici sono stati molto studiati sia in Germania che negli Stati Uniti d'America, offrendo nuove chiavi d'interpretazione alle situazioni. Questi studi hanno dimostrato che il profilo tipico del criminale è offerto nella maggior parte dei casi da soggetti che hanno un'età fra i 24 e 33 anni, istruiti, educati e molto spesso di sesso maschile.
Il fenomeno è stato, poi, analizzato anche da un altro punto di vista, con la teoria di Sutherland. Questa descrive il criminale informatico come totalmente inconsapevole del carattere illecito delle attività, ignorando la possibilità che la sua azione possa configurare una condotta criminosa.
Se si esamina il fenomeno dei reati informatici assume rilievo l'alta frequenza di concorso ed associazione nel reato.
Alcuni tipi di condotte risultano invece difficilmente inquadrabili in base alle categorie giuridiche, si pensi al cd. *self-harm*, caratterizzato da un comportamento di lesione che la vittima mette in atto contro se stesso sotto la spinta di una condotta altrui, diffusa, di solito, su pagine web che alimentano l'odio e inducono gli utenti di quelle pagine a comportamenti auto-lesionisti.
L'elemento soggettivo assume rilievo anche nelle categorie del *revenge porn* laddove il criminale agisce per odio, vendetta o risentimento personale diffondendo immagini personali o informazioni riservate sul web.

2.3.1. La figura dell'hacker

Il tipo di cybercriminale più diffuso è l'hacker.
Questi è un soggetto che agisce per finalità ludiche che portano all'acquisizione di dati personali e molto spesso all'utilizzo di questi dati.

L'autore dell'illecito, molto spesso, si procura le credenziali altrui per accedere ad un sistema informatico e compiere le più disparate attività[18].

Una delle tecniche utilizzate è la cd. *should surfing* che consiste nell'acquisizione furtiva dei codici di accesso mentre il titolare è intento nell'utilizzo. Questa tecnica è una delle più utilizzare nei casi di furto di carte di credito o conti bancari, essendo un metodo semplice ed efficace.

Una seconda tecnica è costituita dal cd. *social engineering*, o anche "ingegneria sociale", il nome potrebbe trarre in inganno: questa tecnica consiste nell'aggirare la vittima al fine di convincerla a dare le proprie chiavi di accesso al sistema.

L'hacker, di solito, utilizza strumenti ingannevoli, come una voce registrata, si fingerà una persona che non è, attaccherà soggetti psicologicamente più fragili, come anziani o persone in difficoltà economica[19].

Ulteriori tattiche utilizzate sono quelle legate a programmi che permettono di collegarsi al computer della vittima e trasferire tutti i dati al computer del criminale. Si parla in questo caso dei cd. Programmi *key-logging*.

Questi programmi sono utilizzati non solo dagli hacker ma anche dagli agenti di polizia per individuare i crimini informatici.

Un ulteriore strumento utilizzato dagli hacker consta nell'utilizzo dei c.d. *Decryptor*, dei software che decifrano le password degli utenti, illegalmente. Quest'ultimo strumento molto meno utilizzato perché prevede che l'hacker sostenga un costo non indifferente.

[18] Cfr. G. Fioriglio, *Sorveglianza e controllo nella società dell'informazione. Il possibile contributo dell'etica "Hacker"*. Relazione alla Conferenza "La filosofia del diritto tra storia delle idee e nuove tecnologie", Ravenna, 19 settembre 2014, in *Nomos*, 2, 2014, pag. 1 ss.

[19] Cfr. G. Ziccardi, *Il giurista hacker e il corretto approccio alle tecnologie informatiche*, in *Ciber. e dir*., 4, 2005, pag. 550.

3. La normativa sovranazionale

In un contesto in cui la tecnologia diviene di giorno in giorno sempre più incisiva sulla vita degli individui, questi finiscono per essere sempre vulnerabili rispetto ai rischi che si nascondono nel web.

I primi ragionamenti a livello internazionale ed europeo in tema di reati informatici sono avvenuti già a partire dagli anni Settanta; ci sono voluti più di trent'anni prima di arrivare alla definizione di un testo normativo.

La politica in materia di *cybersecurity* è stata segnata senza alcun dubbio da una data, l'11 settembre 2001, giorno in cui il non solo il mondo, ma anche il web è cambiato, a seguito degli attacchi terroristici subiti dagli Stati Uniti d'America.

Si è osservato, infatti, che «*Since the 1980s, deregulation and privatization have reduced the role of governments in economic affairs. After September 11, 2001, however, the United States government began to put in place new laws and regulations to strengthen homeland security. Security has become a central rationale for regulating commercial activities. However, one area continues to be relatively free from regulation*»[20].

Questa esigenza è stata avvertita non solo negli Stati Uniti, ma in tutto il mondo, a causa delle minacce terroristiche. Alla luce di queste considerazioni, ben si comprende il motivo per cui Umberto Eco ha definito i nuovi *media* come il maggior alleato del terrorismo internazionale: a suo avviso, infatti, proprio lo sviluppo dei nuovi media ha determinato il passaggio decisivo dal terrorismo al cyberterrorismo.

---

[20] J.A. Lewis, *Aux Armes, Citoyens: Cyber Security and Regulation in the United States*, in *Elsevier's Telecommunications Policy*, Fall 2005, pag. 1. «*The requirements of homeland security have seen an expansion of regulation for immigration and transportation, law enforcement, banking, and communications, but US cyber security policy still assigns government a minimal role. 2 This is even more peculiar given the vivid warnings of the potential for catastrophic attack, "where," according to a 1995 Time Magazine Cover story, "a tyrant with inexpensive technology could unplug NASDAQ or terrorist hackers could disrupt an airport tower". Why eschew regulation if the risk is apparently so great? To explain this, we need to look at the background from which homeland defense and cyber security emerged*».

Va segnalato, tuttavia, che bisogna fare attenzione ad utilizzare il termine "cyberterrorismo", perché esso è uno dei più utilizzati nell'epoca attuale, spesso in maniera distorta. Secondo un primo orientamento, il *cyberterrorismo* si concretizza in azioni terroristiche poste in essere attraverso il *web*, e motivate, dal punto di vista politico, con lo scopo di cagionare gravi conseguenze, sia dal punto di vista umano che economico: l'obiettivo, insomma, è quello di ingenerare terrore.

Secondo una diversa definizione, invece, il *cyberterrorismo* si concretizzerebbe in attacchi e minacce contro supporti informatici, al fine di costringere un determinato Stato o la sua popolazione ad assumere determinati comportamenti.

Altri ancora, invece, intendono il *cyberterrorismo* come lo strumento per paralizzare le grandi rete internet ed informatiche di uno Stato, ostacolandone pertanto tutte le funzioni.

Secondo una delle studiose che ha dedicato maggiore attenzione al tema, Dorothy Denning, il cyberterrorismo consisterebbe in una «convergenza tra terrorismo e *cyberspazio*»[21]. Il *cyberspazio*, secondo la studiosa, è da intendersi come il complesso di tutte le interconnessioni tra supporti che permettono il funzionamento di tutti i sistemi informatici.

Tutte queste definizioni sono allo stesso modo valide, ma solo la prima si avvicina a quello che è il senso proprio del cyberterrorismo,: il cyberterrorismo, infatti, deve essere considerato perfezionatosi nel momento in cui attacchi terroristici vengono posti in essere grazie all'utilizzo di internet e di tutte le sue potenzialità.

Il cyberterrorismo si inserisce perfettamente nell'ambito della *cyberwear*, ossia della guerra cibernetica che vede coinvolti non solo i terroristi, ma tutti gli Stati, i quali hanno ben compreso che sfruttando internet nelle sue infinite potenzialità è possibile "controllare il mondo".

[21] D. Denning, *Cyberterrorism*, in *http://palmer.wellesley.edu/*, 24 agosto 2004.

Ciò spiega anche perché le istituzioni internazionali abbiano dedicato grande attenzione alla necessità di regolamentare il fenomeno, al fine di monitorarlo. Non a caso è datata al 2001 la prima Convenzione europea sul cybercrime, entrata in vigore nel 2004 e ratificata dall'Italia solo nel 2008, con la legge n.48.

Il Consiglio Europeo ha dato alla luce quello che viene considerato come la prima fonte vincolante internazionale in materia di criminalità informatica.

La Convenzione sulla criminalità informatica di Budapest offre una risposta ai reali pericoli che caratterizzano la società virtuale odierna: essa costituisce uno strumento tecnico di assistenza fruibile in tutti i paesi che l'hanno ratificata e, potenzialmente, a tutti i paesi del mondo, costituendo anche uno strumento di cooperazione internazionale[22].

Le maggiori complessità riguardanti il fenomeno del cybercrime sono rappresentate dal fatto che il soggetto che mette in atto la condotta illecita agisce tramite un pc, inserendosi in un sistema informatico in cui la distanza fra i Paesi risultano azzerate, dando la possibilità all'agente di produrre effetti in luoghi diversi rispetto a quelli da cui opera.

Il Trattato prevede, dunque, la definizione di sanzioni penali per reati commessi attraverso il web ed altre reti informatiche, focalizzandosi specificatamente sulle violazioni dei diritti d'autore, le frodi informatiche, la pornografia infantile, e le violazioni della sicurezza della rete.

In aggiunta a queste disposizioni, il testo prevede delle procedure particolari rispetto alla materia, come la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati.

La necessità di introdurre disposizioni procedurali nasceva dalla complessità di ottenere prove informatiche in ambito giudiziario; essendo quest'ultime di

[22] Cfr. A. Gammarota, *Lo scambio transnazionale di notizie di reati informatici: questioni di legittimità e di effettività dei diritti di difesa dell'indagato-imputato*, in *Inf. dir.*, 1-2, 2015, pagg. 391 ss.

difficile acquisizione a causa della loro inaccessibilità e mutevolezza, dal momento che la loro produzione avviene nello spazio virtuale.
Il trattato risulta essere frutto di lunghe riflessioni circa gli illeciti compiuti attraverso dispositivi informatici, recependo una serie di nuovi concetti poco conosciuti precedentemente, quali falso informatico, danneggiamento del software e tutto ciò che era inerente a nuove forme di reati che si consumavano nelle dimensioni informatiche.
Il principale fine del Trattato fu costituito dalla necessità della creazione di una politica penale comune che potesse efficacemente proteggere le persone ed i beni dalla commissione degli illeciti perpetrati nel cyberspazio.
Ulteriore obiettivo del Trattato è stato quello di stabilire una base giuridica per la cooperazione internazionale tra gli Stati che hanno aderito; la principale volontà del Consiglio fu quella di favorire gli scambi di informazione, l'assistenza reciproca tra gli Stati e l'estradizione relativamente ai reati informatici previsti[23].
Come è stato precedentemente anticipato, la Convenzione ha fornito una vera e propria guida relativamente alle definizioni di crimine informatico e di piattaforme web.
Nel primo capitolo, difatti, la Convenzione parte proprio con la definizione del sistema informatico, descrivendolo come qualsiasi apparecchio che compie un'elaborazione automatica dei dati tramite un programma. La concettualizzazione unitaria delle nozioni terminologiche appare quanto mai utile in una dimensione nuova e frammentaria, nonchè non conosciuta come quella del mondo virtuale.
Appaiono rilevanti anche le definizioni che la Convenzione fornisce di dati informatici e di service provider, indicati, i primi come fatti utilizzati in un

[23] Cfr. L. Luparia, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, Milano, 2009, pag. 16.

sistema informatico, i secondi come un ente preposto a fornire servizi di comunicazione e processazione di dati ai propri utenti.

La Convenzione ha avuto un grande impatto dal punto di vista dei Paesi aderenti, e diverse conseguenze tra le quali l'elaborazione di linee guida in materia, strumenti per la formazione degli operatori giudiziari soprattutto in ambito di prove elettroniche; ricerche che hanno ad oggetto l'entità finanziaria di tali illeciti; misure volte ad intensificare la tutela dei minori contro le operazioni di adescamento online; sviluppo della cooperazione internazionale attraverso un miglioramento degli organi preposti; programmi e conferenze appositamente istituiti come punti di riferimento per gli Stati coinvolti.

La Convenzione è stata corredata da un protocollo sugli atti di natura razzista e xenofoba[24].

I lavori del Consiglio non si sono fermati a questa prima importante tappa nella legislazione in tema di criminalità informatica, proseguendo i lavori con l'adozione di una Convenzione sulla prevenzione del terrorismo nel 2005.

L'attenzione al terrorismo si sostanzia in una condizione per cui gli attacchi informatici hanno la potenzialità estremamente alta di rappresentare una minaccia per la pace e la sicurezza internazionale.

Questa Convenzione definisce il reato di reclutamento e addestramento di terroristi tramite internet.

Nel 2007 i ragionamenti si sono evoluti nella direzione della protezione in ambito di abuso di minori e sfruttamento sessuale con la Convenzione di Lanzarote.

Nel 2013, in particolare, l'Unione europea è pervenuta all'elaborazione della Strategia dell'Unione europea per la cybersicurezza. Nell'introduzione di tale documento si legge che «negli ultimi due decenni internet, e più in generale

[24] Cfr. L. Luparia, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, cit., pag. 19.

il ciberspazio, hanno avuto un impatto impressionante su tutti gli strati della società. La nostra vita quotidiana, i diritti fondamentali, le interazioni sociali e le economie dipendono dal funzionamento impeccabile delle tecnologie dell'informazione e della comunicazione. Un ciberspazio aperto e libero ha promosso l'inclusione politica e sociale in tutto il mondo, ha abbattuto le barriere tra paesi, comunità e cittadini rendendo possibili l'interazione e lo scambio di informazioni e di idee in tutto il pianeta, ha creato un forum di libertà di espressione e esercizio dei diritti fondamentali e ha conferito potere partecipativo ai cittadini nella loro ricerca di una società democratica e più giusta, come è avvenuto in modo clamoroso durante la cd. Primavera araba»[25].

Tra i principi più importanti indicati nella strategia, spicca anzitutto la resilienza, da intendersi come la capacità, di un sistema informatico, di resistere e di preservare i suoi dati in caso di attacco esterno. La seconda priorità, invece, consiste nella lotta senza quartiere al crimine informatico, che rappresenta una delle cause più importanti dei danni economici, soprattutto a svantaggio del settore privato.

Un'altra priorità individuata risiede nella necessità di condurre la battaglia sulla *cybersecurity* a livello globale, perché solo in tal modo è possibile una strategia integrata e compatta, in grado di incutere timore a tutti coloro che hanno intenzione di commettere un crimine informatico.

[25] Si legge ancora che «Perché il ciberspazio rimanga aperto e libero è necessario che nell'ambiente online si applichino le stesse norme, gli stessi principi e gli stessi valori che l'Unione europea difende offline. Occorre tutelare nel ciberspazio i diritti fondamentali, la democrazia e lo Stato di diritto. La nostra libertà e la nostra prosperità dipendono sempre più dalla solidità e dall'innovazione di internet, che continuerà a fiorire a patto che l'innovazione del settore privato e la società civile ne guidino la crescita. Ma la libertà online presuppone la sicurezza. È necessario che il ciberspazio sia protetto da incidenti, attività dolose e abusi: gli Stati hanno un ruolo decisivo nella garanzia della libertà e della sicurezza del ciberspazio. I loro compiti sono numerosi: salvaguardare l'apertura e l'accessibilità, rispettare e proteggere i diritti fondamentali online e preservare l'affidabilità e l'interoperabilità di internet. D'altro canto, il settore privato è proprietario e fa funzionare quote notevoli di ciberspazio, per cui la riuscita di qualsiasi iniziativa in questo settore presuppone il riconoscimento del suo ruolo motore».

A tale strategia ha fatto seguito, proprio di recente, il *Cybersecurity Act*, del 2019, un regolamento che, proposto dalla Commissione europea, è stato approvato dal Parlamento europeo con l'obiettivo di sviluppare ed aggiornare la normativa in materia di sicurezza cibernetica a livello europeo. Tale atto valorizza il ruolo dell'ENISA, ossia dell'Agenzia europea per la sicurezza informatica, e istituisce un quadro normativo più organico e coerente al fine di individuare la nozione di sicurezza informatica e dei rischi della sicurezza.
Tra gli Stati nazionali, quello più avanti sotto il profilo della regolamentazione della *cybersecurity* è sicuramente il Regno Uniti, anche a causa dell'influenza degli Stati Uniti[26]. A partire dall'inizio del secolo in corso, infatti, il Regno Unito è stato capace di predisporre un apparato di tutela dei sistemi informatici molto avanzato, capace di controllare e gestire in maniera adeguata la minaccia cibernetica[27].
Tra i Paesi virtuosi, poi, è da segnalare l'Estonia, che già dal 2008 si è dotato di una strategia finalizzata a reprimere sul nascere attacchi alla sicurezza informatica, anche perché lo Stato baltico è rimasto vittima di un attacco ai propri sistemi informatici nel 2007. Del resto, come è stato affermato, «il tema della *cyber warfare* sta gradualmente acquisendo una notevole importanza ai fini delle logiche di difesa nazionale, considerato che il concetto tradizionale di conflitto tra Stati è in continua evoluzione: infatti, oggi, esso ha maggiore probabilità di manifestarsi tramite il furto di informazioni riservate (*cyber* spionaggio) o la paralisi di infrastrutture critiche nazionali piuttosto che tramite mezzi militari convenzionali. La guerra tradizionale ha sempre meno occasione di verificarsi, in contesti di tensione tra stati avanzati, e le nuove frontiere delle minacce alla sicurezza nazionale attengono sempre più alla dimensione cibernetica»[28].

[26] Sulla regolazione negli Stati Uniti si v. Z. Bohm, S.J. *Shackelford, Securing Critical North American Infrastructure: A Comparatice Case Study in Cybersecurity Regulation*, in *School of Law*, 40, 2006, pagg. 59 ss.
[27] Cfr., sul tema, C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, Roma, 2014, pagg. 13 ss.
[28] C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, cit., pag. 13.

Rispetto alla media europea l'Italia ha fatto registrare un ritardo in materia di cybersecurity.

Si ricorda che nel 2014 è stato istituito un ufficio per il programma sulla criminalità informatica (C-PROC) con sede a Bucarest, al fine di implementare il lavoro in materia di criminalità informatica, l'ufficio si occupa di creare progetti al fine di sostenere aziende, infrastrutture che utilizzano sistemi informatici.

Va segnalato, in conclusione, che l'Unione europea si è occupata di sicurezza cibernetica anche nell'ultimo Regolamento (UE) 2016/679, in materia di tutela dei dati personali. In particolare, il legislatore europeo pare aver individuato il punto di sintesi tra la tutela dell'identità personale e la protezione dei dati personali. Pur essendo un diritto fondamentale, il diritto alla tutela dei dati personali viene concepito non come diritto assoluto, ma come diritto che deve essere bilanciato con gli altri diritti fondamentali[29].

Per quanto concerne, in particolare, il profilo della sicurezza informatica, il GDPR ha il grande merito di aver superato un pregiudizio che ha da sempre caratterizzato la tematica in esame, ossia il fatto che la tutela e la salvaguardia dei dati informatici dovesse avere come obiettivo unicamente le minacce esterne, ossia gli attacchi di potenziali *hacker* interessati all'acquisizione dei dati per le finalità più disparate[30].

In realtà la situazione è assai diversa: in molti casi, infatti, la minaccia all'integrità dei dati informatici è frutto non di attacchi esterni, ma dell'adozione di comportamenti sbagliati da parte degli stessi dipendenti dell'azienda, i quali, a causa di una scarsa cultura informatica, adottano

[29] Cfr. ampiamente sul tema M.G. Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 4, 2016, pagg. 1249 ss.; G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuov. leg. civ. comm.*, 1, 2017, pagg. 1 ss.; M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti*, in *JusOnline*, 1, 2017, pagg. 218 s.

[30] Cfr., sul tema, N. Fabiano, *GDPR&Privacy. Consapevolezza e opportunità*, Milano, 2019, pagg. 65 ss.

modelli comportamentali idonei a porre in pericolo l'integrità dei dati informatici.

Assume rilevanza, in particolare, l'art. 32 del GDPR, rubricato "Sicurezza del trattamento"[31]. Tale disposizione, diversamente da quanto si verificava in passato, comprende la necessità di tutelare non solo la riservatezza dei dati, ma anche la loro integrità e sicurezza, nonché la loro disponibilità. A tal fine all'interno di ogni azienda è necessario adottare buone pratiche e formare tutti coloro che hanno accesso ai dati informatici circa i corretti comportamenti da tenere al fine di evitare che i dati possano essere persi o danneggiati.

Il regolamento GDPR consiglia il ricorso alla crittografia, come strumento in grado di proteggere i dati attraverso la loro cifratura. In secondo luogo, è prevista l'esigenza di formare tutti gli operatori dell'azienda ad un utilizzo corretto della posta elettronica, considerato che la maggior parte dei dati "viaggia" attraverso la posta elettronica.

Ancora, assume rilevanza la necessità di procedere ad una corretta gestione e ad un continuo *backup* dei dati, indispensabile per evitare che le informazioni contenute nei *files* possano andare disperse o possano essere corrotte.

[31] Il testo integrale dell'art. 32 del GDPR è il seguente: «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

Un altro profilo molto importante è quello dell'autenticazione, che si basa normalmente sulla coppia *username*/*password*. Si tratta normalmente del primo ostacolo che si frappone a chi abbia intenzione di intromettersi in un sistema informatico aziendale. L'obiettivo di ogni responsabile aziendale della sicurezza informatica deve essere quello di sensibilizzare tutti i dipendenti dell'azienda a non sottovalutare il profilo dell'autenticazione, prediligendo un'autenticazione forte, se possibile anche biometrica, in grado di ridurre in maniera significativa il rischio di accessi abusivi ai sistemi informatici.

Pare evidente, in definitiva, come il GDPR abbia avvertito il bisogno di tutelare la sicurezza informatica non tanto e non solo sotto il profilo della riservatezza dei dati quanto, piuttosto, su quello, spesso sottovalutato, della disponibilità/integrità degli stessi.

Durante il 2022 è stato siglato il secondo protocollo alla Convenzione di Budapest, con l'obiettivo di rafforzare la cooperazione internazionale.

I lavori in tema di cybercrime sono costantemente ripresi e il tema risulta estremamente attuale dal momento che i danni derivanti dai reati informatici sono quantificati in miliardi di euro l'anno. L'uso sempre maggiore di Internet e fenomeni come la pandemia hanno contribuito ad aumentare la commissione di truffe e attacchi informatici.

Durante il 2020 l'Unione Europea ha iniziato ad avviare una serie di riflessioni sulla necessità di rafforzare il sistema europeo in tema di protezione delle minacce informatiche[32].

Le intenzioni erano rappresentate dalla costruzione di un sistema più sicuro, dove la comunicazione potesse avvenire in modo trasparente e l'accesso ai dati per fini giudiziari fosse semplice. La Commissione europea e il Servizio europeo per l'azione esterna (SEAE) hanno presentato una nuova strategia

[32] Cfr. L. Luparia, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, cit., pag. 22.

con l'obiettivo di rafforzare il sistema di cybersecurity. La strategia contiene una serie di strumenti normativi che è necessario adottare nonchè l'invito ad adottare programmi di guida in campo digitale.

Con l'obiettivo di implementare le strategie dell'UE in materia, il Consiglio ha adottato conclusioni sul tema, nel marzo 2021.

Il Consiglio, nel 2020, ha, invece, adottato una risoluzione sulla crittografica, con lo scopo di aumentare il livello di sicurezza.

Accanto alle strategie, l'Unione Europea, consapevole della necessità di offrire un carattere vincolante alle indicazioni interna di reati informatici, ha iniziato a lavorare a diverse proposte legislative con lo scopo di proteggere la rete e i soggetti.

È stato, inoltre, istituito un Centro Europeo per la lotta alla criminalità informatica nella cornice dell'Europol.

Diverse norme sono state adottate dall'UE: una prima norma nel 2019 allo scopo di combattere le frodi commesse a mezzo di pagamento diverso dai contanti, attuazione prevista per gli Stati nel 2021.

Fra le proposte legislative la Commissione ha avanzato una normativa al fine di combattere l'abuso e lo sfruttamento di minori online, nonché norme sull'accesso transfrontaliero alle prove elettroniche.

Tutte queste attività sottolineano la grande rilevanza che l'Unione Europea conferisce al cyberspazio e alla necessità che questo sia un luogo sicuro e libero, dove tutti possono esprimersi senza alcun pericolo.

È per questo motivo che è stata implementata la cooperazione diplomatica. Il Consiglio, per la prima volta nel 2019, ha dato la possibilità all'UE di imporre sanzioni a cittadini o enti responsabili di reati informatici.

Questa azione consente all'UE di limitare la libertà di spostamento all'interno del perimetro europeo per la persona che compie il reato e di congelare i beni, sanzione applicabile anche agli enti[33].

La cooperazione è stata ulteriormente implementata con le attività dell'Agenzia Europea per la difesa (AED), che si coordina con l'Europol e l'Agenzia dell'Unione Europea per la cybersecurity.

Tutte queste azioni dimostrano quanto l'UE sia coinvolta e si impegni in materia di reati informatici.

3.1. La direttiva NIS 1

Molto importante, poi, è la Direttiva 2016/1148 (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, nota anche come direttiva NIS, Network and Information Security, nella quale si prende atto che «la portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. Tali sistemi possono inoltre diventare un bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi. Tali incidenti possono impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione»[34].

La direttiva NIS mette in atto una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, individuando, all'art. 7, i seguenti aspetti:

[33] Cfr. L. Luparia, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, cit., p. 25.

[34] Considerando n. 2. Cfr. F. Scalia, *Energia sostenibile e cambiamento climatico*, Torino, 2008, p. 248 ss.

a) gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi;
b) un quadro di governance per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti;
c) l'individuazione delle misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;
d) un'indicazione di programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;
e) un'indicazione di piani di ricerca e sviluppo relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;
f) un piano di valutazione dei rischi per individuare i rischi;
g) un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi.
Nella direttiva si fa anche espressamente riferimento ai rischi che riguardano il settore energetico: il considerando n. 28, infatti, osserva che «in aggiunta ai fattori intersettoriali si dovrebbe tener conto anche di fattori settoriali al fine di stabilire se un incidente avrebbe effetti negativi rilevanti sulla fornitura di un servizio essenziale. Tali fattori potrebbero comprendere: per i fornitori di energia, il volume o la quota di energia nazionale prodotta; per i fornitori di petrolio, il volume su base giornaliera; per il trasporto aereo, inclusi aeroporti e vettori aerei, il trasporto ferroviario e i porti marittimi, la quota di volume di traffico nazionale e il numero di passeggeri o di operazioni di trasporto merci su base annua; per il settore bancario o le infrastrutture dei mercati finanziari, la loro importanza sistemica in base alle attività totali o al rapporto tra tali attività totali e il PIL; per il settore sanitario, il numero di pazienti assistiti dal fornitore su base annua; per la produzione, il trattamento e la fornitura di acqua, il volume e il numero e i tipi di utenti riforniti, inclusi, ad

esempio, ospedali, servizi pubblici, organizzazioni o persone fisiche, nonché l'esistenza di fonti idriche alternative per servire la stessa area geografica».

3.2. La direttiva NIS 2

Secondo la nuova direttiva NIS2, le reti e i sistemi informativi sono diventati un aspetto cruciale della vita quotidiana grazie alla velocità della trasformazione digitale, all'interconnessione della società e agli scambi transfrontalieri. Questa evoluzione ha causato anche un'espansione del panorama delle minacce informatiche con la conseguente comparsa di nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri.

A questo proposito, gli attacchi informatici massicci rappresentano una grave minaccia per la sicurezza dell'Unione, in quanto hanno la capacità di perturbare le attività economiche nel mercato interno, generare perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e alla società dell'Unione[35].

Le crescenti interdipendenze nell'UE sono il risultato di una rete di fornitura di servizi che utilizza infrastrutture critiche fondamentali in settori quali l'energia, i trasporti, le infrastrutture digitali, l'acqua potabile e le acque reflue, la sanità e alcuni aspetti della pubblica amministrazione.

L'obiettivo della direttiva NIS2 è quello di superare le differenze tra gli Stati membri, in particolare definendo standard minimi per il funzionamento di un quadro normativo coordinato. Inoltre, stabilisce anche i meccanismi che consentono alle autorità competenti di ciascuno Stato membro di cooperare efficacemente.

[35] Cfr. A. Valentini, *Dentro la NIS 2, più obblighi e regole per la cybersecurity europea*, in https://www.cybersecurity360.it/outlook/dentro-la-nis-2-piu-obblighi-e-regole-per-la-cybersecurity-europea/, 20 dicembre 2022.

La Direttiva NIS2 ha anche aggiornato l'elenco dei settori e delle attività soggette agli obblighi di cybersecurity e ha sviluppato misure di applicazione efficaci, essenziali per garantire la conformità.

L'obiettivo principale è quello di eliminare le differenze tra gli Stati membri per quanto riguarda i requisiti di sicurezza informatica e l'attuazione delle misure. A tal fine, vengono stabiliti standard minimi per un quadro normativo e meccanismi per una cooperazione efficace tra le autorità di ciascuno Stato membro. Verrà quindi istituita la rete dell'Organizzazione europea di collegamento per le crisi informatiche (EU-CYCLONe) per migliorare il coordinamento nella gestione di incidenti di cybersicurezza su larga scala.

Inoltre, l'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) avrà un ruolo più importante. Dovrà assistere la Commissione europea nel fornire orientamenti e modelli sull'obbligo degli Stati di presentare informazioni pertinenti[36].

La direttiva NIS2 si basa anche sull'idea che l'Unione europea debba essere incaricata di guidare il quadro giuridico per il mondo digitale, dopo il successo del Regolamento generale sulla protezione dei dati (GDPR) del 2016 e di altri nuovi strumenti per la regolamentazione della cybersicurezza.

In questo senso, la direttiva NIS2 segna un punto di svolta tra la regolamentazione europea e quella nazionale, argomento di tensione e di continuo dibattito. Con questa direttiva assistiamo a un aumento dell'importanza della regolamentazione europea e del processo decisionale regionale, cosa che si è vista molto più chiaramente dall'inizio della guerra in Ucraina e in altre normative sulla cybersecurity come la DORA.

In precedenza, le aziende dovevano attendere che l'UE le designasse per rientrare nell'ambito di applicazione, con un elenco eccessivamente lungo di criteri di valutazione. Con la Direttiva NIS2, il processo è ora diverso e ogni azienda dovrà autovalutare e definire se è un'azienda essenziale o importante.

[36] Cfr. A. Valentini, *Dentro la NIS 2, più obblighi e regole per la cybersecurity europea*, cit.

Questa divisione si basa principalmente sul settore di attività. In questo senso, le aziende più tradizionali, come quelle del settore energetico o bancario, sono considerate essenziali, mentre quelle dei nuovi settori, come quello logistico o farmaceutico, sono considerate importanti. A seconda della loro classificazione, avranno più o meno obblighi.

Inoltre, secondo la direttiva NIS2, sia le entità critiche che quelle importanti devono adottare un'ampia gamma di pratiche di igiene informatica di base. Queste includono gli aggiornamenti del software, la configurazione dei dispositivi, la segmentazione della rete e la gestione delle identità. Inoltre, includono anche la consapevolezza degli accessi o degli utenti, l'organizzazione di corsi di formazione per il personale e la sensibilizzazione sulle minacce informatiche.

Un'altra delle novità della Direttiva NIS2 è l'ampliamento dei settori che rientrano nel campo di applicazione della direttiva, indipendentemente dalle dimensioni dell'azienda. Inoltre, gli stessi Stati membri potranno decidere quali aziende possono rientrare nel suo campo di applicazione se le ritengono sufficientemente rilevanti, anche se non soddisfano alcuni o tutti i requisiti.

Ai sensi della Direttiva (UE) 2016/1148, gli Stati membri erano responsabili dell'identificazione delle entità che soddisfacevano i criteri per essere considerate operatori di servizi essenziali. Al fine di eliminare le ampie divergenze tra gli Stati membri a questo proposito, la Direttiva NIS2 stabilisce che deve essere stabilito un criterio uniforme per determinare quali entità rientrano nell'ambito di applicazione della direttiva[37].

Mentre nella precedente direttiva gli Stati membri erano responsabili di determinare quali entità soddisfacessero i criteri per essere considerate operatori di servizi essenziali, la nuova direttiva NIS2 stabilisce una regola sulle dimensioni massime. A questo proposito, il testo approvato include disposizioni aggiuntive per garantire la proporzionalità, un livello più elevato

[37] Cfr. A. Valentini, *Dentro la NIS 2, più obblighi e regole per la cybersecurity europea*, cit.

di gestione del rischio e criteri specifici per determinare quali enti rientrano nel campo di applicazione.

Il testo approvato specifica gli enti che non saranno coperti da questa direttiva. Saranno quindi esclusi dal campo di applicazione gli enti che svolgono attività in settori quali la difesa o la sicurezza nazionale, la pubblica sicurezza, la polizia, la magistratura o i parlamenti e le banche centrali. La direttiva NIS2 si applicherà anche alle pubbliche amministrazioni, data la loro crescente esposizione agli attacchi informatici.

Gli Stati membri possono anche stabilire quali piccole e microimprese - a condizione che soddisfino criteri specifici che ne evidenzino il ruolo chiave per la società, l'economia o per determinati settori o tipi di servizi - rientrano nell'ambito di applicazione della presente direttiva sulla sicurezza delle reti e dell'informazione.

Gli Stati membri, nelle loro strategie nazionali di cybersecurity, dovranno anche affrontare le esigenze specifiche di cybersecurity delle piccole e medie imprese. Secondo la direttiva NIS2, le piccole e medie imprese rappresentano, in tutta l'Unione, un'ampia percentuale del mercato industriale e commerciale. A questo proposito, si sottolinea che spesso faticano ad adattarsi alle nuove pratiche commerciali in un mondo più connesso e in un ambiente digitale, con lavoratori che lavorano da casa e attività sempre più svolte online.

Il fatto che un maggior numero di aziende rientri nell'ambito di applicazione della Direttiva NIS2 implica quindi un maggior numero di obblighi. Questi rientrano principalmente in tre grandi categorie. In primo luogo, a livello organizzativo, la Direttiva NIS2 obbliga le aziende a dotarsi di un documento di politica aziendale sulla sicurezza digitale. Sulla base di questo documento, devono essere redatti vari protocolli sui rischi tecnologici[38].

[38] Cfr. A. Valentini, *Dentro la NIS 2, più obblighi e regole per la cybersecurity europea*, cit.

In secondo luogo, vi è il livello tecnologico, relativo alle tecnologie critiche, e in terzo luogo il livello comportamentale, che deve essere basato sul quadro di sicurezza per la gestione del rischio di cybersecurity.
A partire dalla Direttiva NIS2, la responsabilità, la direzione e la leadership in materia di sicurezza digitale saranno assunte da due attori principali: il Consiglio di Amministrazione dell'azienda che rientra nel campo di applicazione e il Chief Information Security Officer (CISO) dell'azienda.
Pertanto, data l'importanza strategica dell'azienda, il consiglio di amministrazione deve essere formato in materia di sicurezza informatica. Secondo l'articolo 7 della direttiva NIS2, il consiglio di amministrazione deve anche approvare le misure, garantirne l'attuazione e ricevere una formazione adeguata per comprendere i rischi tecnologici. Il consiglio di amministrazione non può omettere o spostare la responsabilità della sicurezza digitale ad altre aree dell'azienda.

4. La normativa italiana in materia di reati informatici

4.1. I lavori preparatori della legge n. 547/1993

Il problema della sicurezza informatica fu posto già a partire dagli anni Ottanta, quando iniziava ad espandersi l'uso della tecnologia ed iniziava ad avere una sempre maggiore rilevanza nella vita delle persone.
L'aumentare degli scambi e dello sviluppo economico ha reso più attraente il ricorrere all'utilizzo di mezzi illeciti al fine di trarne profitto, strumenti che si servivano di sistemi e programmi informatici.
La conseguenza di tutto ciò fu rappresentata da un arricchimento delle organizzazioni criminali, anche in termini internazionali.
Per questo motivo si ebbe la necessità di iniziare a lavorare su una legge che potesse avere ad oggetto i reati informatici.

La normativa italiana in materia di cybercrime ebbe un percorso travagliato e non fu di semplice formazione[39].

Sebbene l'esigenza di tutela dei beni informatici si fosse sviluppata precedentemente, i primi reali tentativi di lavorare sulla legge si ebbero nel 1989, quando il Ministro della Giustizia Vassalli nominò una Commissione che aveva il compito di modificare le disposizioni del codice penale al fine di contrastare la criminalità informatica.

Il primo incontro della Commissione avvenne nel maggio 1989. Durante questo incontro furono convocati anche i rappresentanti delle categorie maggiormente interessate dal fenomeno in questione, tra cui le associazioni del settore bancario ed industriale, i maggiori esponenti del settore professionale ed assicurativo e le più importanti associazioni di hardware e software.

I lavori della Commissione terminarono nel 1991, ma la proposta fu presto dimenticata.

I lavori furono poi ripresi dal successivo Ministro della Giustizia Conso, che sostenne l'importanza di elaborare una legislazione adeguata in materia di cybercrime e decise di riprendere il documento, trasmettendolo alle camere. Tuttavia, durante lo svolgimento dei lavori parlamentari emerse anche una loro incompleta conoscenza del fenomeno.

Durante l'elaborazione della legge la Commissione dovette affrontare numerose questioni attinenti all'esposizione della normativa e al metodo da utilizzare nei confronti del fenomeno.

Come primo obiettivo bisognava stabilire se l'introduzione di tale disciplina dovesse avvenire tramite una modifica del Codice penale o tramite l'inserimento di una nuova legge speciale. Dopo varie controversie si optò per la modifica del Codice penale, poiché si ritenne che la materia non fosse caratterizzata da una peculiarità tale da giustificare l'introduzione di un titolo

[39] Cfr. I. Salvadori, *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010. Profili di diritto comparato,* in *Ind. Pen.*, 2, 2011, pag. 767 ss.

specifico; inoltre bisognava fare riferimento al criterio scelto dal legislatore per catalogare le varie ipotesi di reato[40].

Si decise di utilizzare il criterio dell'unità dell'oggetto giuridico, introducendo ipotesi che riguardassero beni giuridici già tutelati dal codice, caratterizzate da elementi diversi in merito all'offesa.

Tale scelta risultò la sola percorribile, anche in virtù della previsione in cui si dovessero poi introdurre nuove figure contravvenzionali.

Tuttavia, successivamente si decise per l'esclusione dalla materia di fattispecie contravvenzionali, poiché le nuove ipotesi non potevano configurare né norme di carattere preventivo cautelare né norme di carattere amministrativo.

La Commissione si occupò anche di adattare le nuove disposizioni con quelle del nuovo codice di procedura penale soprattutto in materia di intercettazioni telefoniche, e lo fece introducendo il nuovo art 266bis, in tema di intercettazioni informatiche e telematiche e modificando l'art. 268 c.p.p. riguardante l'esecuzione delle operazioni.

La questione più complessa che la Commissione dovette affrontare fu quella di stabilire quali comportamenti rientranti nella materia fossero costituiti da rilevanza penale e quali invece potessero essere destinatari di sanzione amministrativa.

Per fare questa valutazione la Commissione dovette prendere in considerazione il giudizio di meritevolezza della sanzione penale e tutti i criteri introdotti precedentemente dal legislatore per l'utilizzo della stessa, quali il principio di proporzionalità e il principio di sussidiarietà.

Per ultima andava esaminata la questione attinente a quali nuove ipotesi fossero già punite dal Codice penale, laddove la condotta illecita realizzata si sovrapponesse a una già presente nel codice. Nel fare questo lavoro la Commissione esaminò anche le liste dei reati in materia di cybercrime

[40] Cfr. A. Palma, *In tema di reati informatici. Nota a Cass. sez. un. pen. 7 febbraio 2012, n. 4694,* in *Stud. Iur*., 6, 2012, pagg. 732 s.

introdotti dal Consiglio d'Europa, individuando così dei comportamenti che rientravano in norme penali già introdotte nel Codice penale. Tra questi vi erano le condotte di impossessamento avente ad oggetto cose materiali attinenti a sistemi informatici (hardware e software considerati nella loro materialità) infatti in tale caso poteva essere applicata la disciplina del furto, contenuta all'articolo 624 c.p.

Questa disciplina, però, secondo la Commissione, non trovava applicazione per quanto riguarda la "sottrazione" di dati, programmi e informazioni poiché l'art. 624 prevede, come oggetto della condotta, una "cosa mobile", concetto che difficilmente può essere applicato a tali elementi senza infrangere il divieto di analogia[41].

Per quanto riguarda poi il danneggiamento di sistemi informatici, la Commissione affermò che esso trovava tutela negli artt. 635 e 420 c.p., che però necessitavano di integrazione per essere adeguati alle peculiarità di tale nuova materia. Infatti, tali articoli non apparivano adeguati a fornire una tutela esemplare poiché non riuscivano a coprire le ipotesi in cui l'oggetto del danneggiamento fosse costituito dal software e dai dati.

La Commissione ha poi rilevato la dubbia applicazione dell'art. 640cp all'ipotesi della truffa in danno dei computer perché avrebbe costituito una forzatura dell'applicazione della norma, dal momento che l'art.640 faceva riferimento a "taluno", rendendosi così inapplicabile nell'ipotesi in cui non fosse indotta in errore una persona fisica ma un sistema informatico.

Un altro nodo critico fu rappresentata dal trovare una definizione di "bene informatico".

Venne allora adottata quella che caratterizzava l'opinione prevalente della dottrina, della giurisprudenza e anche della Commissione stessa, che stabiliva che i beni informatici, quindi dati programmi e informazioni, non sono

[41] Cfr. I. Salvadori, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. proc. pen*., 1, 2012, pag. 205.

assimilabili a cose materiali e ad energie, ciò poiché tali beni non possono essere sottratti e spossessati.

Questo significò non poter applicata a tali beni la disciplina che ha ad oggetto la tutela del patrimonio.

Quando si parla di possesso in tale ambito esso può riferirsi semplicemente alla "conoscenza" di dati, programmi ed informazioni informatiche, dunque ad un concetto meramente intellettuale e non materiale o fisico[42].

Questa tesi fu avvalorata anche dall'inapplicabilità, come è stato già sostenuto in precedenza, dell'ipotesi del furto che prevede alcuni elementi costitutivi (cosa mobile ed impossessamento) non conciliabili con le peculiarità degli oggetti informatici. Infatti, essi vengono tutelati attraverso altre norme, come quelle che tutelano la proprietà letteraria o artistica e quelle che proteggono i segreti industriali o da quelle inerenti la disciplina dei marchi e dei brevetti. Non viene, quindi, applicata la disciplina diretta a proteggere il patrimonio.

La soluzione che venne introdotta per punire l'illecita conoscenza di dati, programmi e informazioni informatiche fu la repressione dell'accesso non autorizzato a dati e sistemi informatici.

L'ultimo aspetto che si esaminerà è costituito dalla necessità, emersa durante l'elaborazione della normativa da parte della Commissione, di adeguare questa disciplina, emergente nel territorio nazionale, a quella contenuta nelle direttive emanate dagli organi europei.

Le direttive facevano riferimento alle liste dei reati informatici introdotte dal Consiglio d'Europa , una prima lista "minima" e necessaria, che riguardava l'introduzione dei reati di frode informatica, falso informatico, danneggiamento riguardante dati o programmi informatici, sabotaggio informatico, accesso non autorizzato, intercettazione non autorizzata, riproduzione non autorizzata di una topografia, e l'altra facoltativa, avente ad oggetto le fattispecie di alterazione dei dati o dei programmi informatici,

[42] Cfr. V. Contraffatto, *Reati informatici*, cit., pag. 39.

spionaggio informatico, utilizzazione non autorizzata di un elaboratore, utilizzazione non autorizzata di un programma informatico[43].

Il legislatore non si fermò all'introduzione dei reati della prima lista, ma introdusse anche molte figure presenti nella lista facoltativa, in modo da assicurare una più ampia tutela. Un'ulteriore tema emerso nei lavori della Commissione fu quello di lavorare ad una più efficace cooperazione internazionale attraverso l'introduzione di queste nuove figure di reato al fine di consentire non solo l'estradizione ma anche una più stringente collaborazione in materia penale. Difatti, molte ipotesi di reato, per il configurarsi di tale cooperazione è necessaria la c.d. doppia incriminazione.

In virtù di ciò molti paesi negli ultimi anni hanno provveduto a dotarsi di un'apposita normativa volta alla repressione dei crimini informatici; fra questi l'Austria, il Belgio, la Danimarca, la Finlandia, la Francia, la Grecia, l'Irlanda, il Lussemburgo, la Norvegia, il Portogallo, i Paesi Bassi.

4.2. Il contenuto della legge n. 547/1993

La diffusione dell'informatica, soprattutto dopo l'apertura al pubblico dell'accesso ed utilizzo di Internet, collocabile a metà degli anni novanta del secolo scorso, ha determinato la comparsa e lo sviluppo crescente di "nuovi" reati, che si manifestano sia come reati informatici "in senso stretto" (vale a dire che già a livello normativo, a seguito della loro specifica incriminazione da parte del legislatore, richiedono necessariamente fra gli elementi costitutivi l'utilizzo delle tecnologie e dei prodotti informatici, o la produzione di effetti tipici su di essi: si pensi alle frodi informatiche, ai falsi ed ai danneggiamenti informatici, agli accessi abusivi a sistemi informatici ecc.), sia come reati informatici "in senso ampio" ed, in specie, come reati "cibernetici"[44].

[43] Cfr. V. Contraffatto, *Reati informatici*, cit., pag. 40.

[44] Così L. Picotti, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. mer.*, 12, 2012, pag. 2552. L'A. osserva che «la tumultuosa diffusione dei social network, che costituisce uno dei più recenti ed eclatanti effetti dell'impatto di Internet sulle

Questi ultimi, «pur essendo concepibili o tipizzati anche a prescindere dal riferimento alla tecnologia informatica e ad Internet, trovano in detti strumenti ed, in generale, nel *Cyberspace* una peculiare possibilità e modalità di realizzazione, che li rende solitamente più temibili o dannosi: tanto da richiedere una più specifica e spesso più severa risposta penale (si pensi alla pedopornografia ed alle violazioni dei diritti d'autore, ma anche alla diffamazione e ad altri reati di "manifestazione del pensiero" *on line:* ponendo nel contempo peculiari problemi di natura processuale, in particolare per quanto riguarda le modalità e le condizioni di raccolta, conservazione ed utilizzazione delle c.d. prove elettroniche»[45].

I reati informatici, dunque, sono i reati posti in essere attraverso o nei confronti di un sistema informatico. L'illecito, a tal proposito, può concretizzarsi nella sottrazione o distruzione delle informazioni contenute nella memoria di un computer; diversamente, il PC può anche rappresentare lo strumento utilizzato per commettere il reato, come ad esempio si verifica nell'ipotesi delle frodi informatiche.

La disciplina normativa in materia di reati informatici è stata introdotta per la prima volta in Italia con la legge n. 23 dicembre 1993, n. 547, recante "Modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica".

La *ratio* della legge risiede nella necessità di porre un argine ad un fenomeno sempre più diffuso, quale appunto quello della criminalità informatica.

---

relazioni interpersonali fra soggetti di ogni età, professione, estrazione sociale, ma in particolar modo fra i giovani — oltre che fra e con enti di qualsiasi natura — dimostra la grande rilevanza non solo dell'evoluzione tecnologica, ma ancor più della sua capillare penetrazione nella società contemporanea, in cui determina rilevanti cambiamenti dei modi della comunicazione e diffusione delle idee e delle informazioni, dei tempi e contenuti del confronto sociale, del costume stesso, condizionando o modellando lo svolgersi di comportamenti collettivi ed individuali anche nel mondo «reale», come dimostrano emblematicamente gli incontri, i dibattiti, le manifestazioni, i movimenti politici che si organizzano in brevissimo tempo in rete ovvero i fatti eclatanti e addirittura i tragici epiloghi posti in essere da singole persone per effetto di quanto accaduto o preannunciato in un social network».

[45] Ivi, pag. 2553.

Internet, del resto, si è rivelato terreno fertile per la diffusione dei reati informati. Internet, infatti, offre l'opportunità di interagire e di comunicare con grande semplicità, abbattendo le barriere fisiche e dando l'illusione dell'anonimato[46].

La diffusione dei supporti informatici, dunque, ha prodotto, oltre che effetti positivi, anche delle conseguenze estremamente negative, in quanto il circuito criminale ha progressivamente compreso le straordinarie potenzialità offerte dalla rete, avvalendosi degli strumenti informatici per realizzare fini illeciti.

Del resto, la percezione che si ha, di solito, dei criminali informatici non è la stessa dei criminali "di strada": è infatti piuttosto diffusa l'idea che i criminali informatici commettano reati connotati da un disvalore minore rispetto a quelli di strada. Tutto questo a causa della presenza di barriere virtuali, quali sono appunto i confini di internet, che lasciano presumere una certa impunità all'autore del reato.

Questa è una delle motivazioni per cui il legislatore italiano solo con la legge n. 547/1993 è intervenuto in materia di criminalità informatica. Precedentemente, sia la dottrina che la giurisprudenza avevano ricondotto i crimini informatici nell'ambito delle fattispecie di reato tradizionali, le quali, tuttavia, si erano rivelate del tutto inadeguate a cogliere le peculiarità della criminalità informatica.

Da queste riflessioni nacque la legge n. 547/1993, successivamente fu adottata la legge 18 marzo 2008, n.48, che ratifica ed implementa nel nostro ordinamento la Convenzione di Budapest sul Cybercrime del Consiglio d'Europa. Quest'ultima, entrata in vigore nel 2004, costituisce il primo trattato internazionale sulle infrazioni penali commesse via Internet e su altre reti informatiche e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia riguardante minori e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure

[46] Cfr. V. Contraffatto, *Reati informatici*, cit., pag. 44.

appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale è perseguire una politica comune in ambito europeo per la protezione dei consociati contro la cybercriminalità, adottando legislazioni appropriate e promuovendo la cooperazione internazionale[47].

Questa legge si è rivelata indispensabile nella lotta ai crimini informatici, crimini che vengono commessi con estrema facilità.

Molto spesso questi sono perpetrati attraverso le piattaforme di social network, dove per lo più vengono realizzate condotte diffamatorie, di incitazione all'odio e di discriminazione[48].

A livello nazionale, con il dlgs 231/2001, viene estesa la responsabilità per reati informatici anche nei confronti degli enti, di questo tema si tratterà in maniera approfondita nei successivi capitoli.

I reati informatici sono contenuti nel libro secondo del codice penale e costituiscono principalmente delitti contro la persona, dal momento che la maggior parte dei reati informatici lede diritti personali.

L'elaborazione della normativa non ha potuto racchiudere in un'unica categoria il bene protetto ma ha individuato i beni da proteggere in alcune fattispecie già esistenti come la riservatezza dei dati personali, la protezione dei sistemi informatici, il patrimonio, la persona, i diritti di proprietà individuale e anche l'incolumità pubblica.

Prima di analizzare le diverse fattispecie, pare opportuno sinteticamente analizzare un ultimo aspetto, quello della territorialità. Una parte della dottrina evidenzia che il criterio della «territorialità caratterizza per definizione tutti gli ordinamenti giuridici, il criterio della personalità attiva costituisce una variabile diversamente regolata nei vari Stati dell'Unione europea, che spazia da un massimo riconoscimento (ad esempio all'interno

[47] Cfr. V. Contraffatto, *Reati informatici*, cit., pag. 45.
[48] Cfr. A.C. Amato Mangiameli, G. Saraceni, *I reati informatici: elementi di teoria generale e principali figure criminose*, Milano, 2015, pag. 39.

del codice penale tedesco) fino a un riconoscimento assai modesto (ad esempio nel codice penale italiano). Dal confronto tra le diverse disposizioni, si può osservare che la Convenzione si avvale del criterio della territorialità e, nel caso in cui il reato sia punibile nel luogo in cui risulta essere stato commesso ovvero non rientri nella competenza territoriale di nessuno Stato, il principio della personalità attiva»[49].

Osservando l'ordinamento giuridico italiano il criterio utilizzato per l'individuazione del *locus commissi delicti* risulta essere il luogo in cui si la fattispecie criminosa si è consumata. Nonostante tale riferimento, non sempre individuare il luogo di commissione del reato è agevole: il caso dei crimini informatici ne è un esempio plastico. Il cyberspazio, infatti, rende possibile permette l'accesso alla rete, anche in modalità simultanea, in più luoghi virtuali: la peculiarità del cyberspazio, infatti, risiede proprio nell'assenza di perimetri spaziali, anche pin virtù del fatto che risulta facile ricorrere ad operazioni automatizzate, consentite anche in assenza di un collegamento tra il soggetto e il sistema informatico. Quanto descritto rendendo piuttosto complessa l'individuazione del punto esatto in cui il reato risulta essere stato commesso.

Alcuni atti sovranazionali evidenziano l'urgenza del problema individuando la necessità di definire i criteri per stabilire la giurisdizione al fine di evitare aree di impunità: tra essi, la Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, avente ad oggetto la lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che prevede che gli Stati membri siano tenuti ad adottare tutte le misure idonee a stabilire la propria giurisdizione nelle ipotesi di reato commesso tramite il ricorso a tecnologie informatiche a cui il presunto responsabile abbia avuto accesso dal loro territorio.

[49] Cfr. V. De Rosa, *La formazione di regole giuridiche per il "cyberspazio"*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2003, pagg. 361 ss.

In via tendenziale, oggi, l'individuazione del locus commissi delicti considera la concreta possibilità di individuare il luogo in cui ha agito l'agente, adottando piuttosto il criterio che individua il luogo di commissione del delitto nel luogo in cui è situato il server del provider che permette di accedere alla Rete, valorizzando, in tal senso, il principio di ubiquità, per effetto del quale si tende ad attribuire rilevanza, allo stesso modo, sia al luogo in cui l'agente ha agito che quello in cui è situato fisicamente il server. Per tale ragione, si ritiene che la rigida applicazione del principio di territorialità dovrebbe essere limitata e resa assai più flessibile, adattandola al contesto dematerializzato della rete[50].

Le previsioni all'interno del codice penale sono numerose, e non è possibile analizzarle tutte in questa sede. Pare dunque opportuno soffermarsi su quelle più significative, rinviando ovviamente al capitolo successivo l'analisi della fattispecie che maggiormente rileva ai fini della tesi, ossia la frode informatica. Prima, però, è necessario inquadrare il ruolo delle Agenzie.

5.1. Il ruolo dell'ENISA

L'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) lavora per rendere l'Europa sicura dal 2004. L'Agenzia ha sede ad Atene, in Grecia, e ha un secondo ufficio a Heraklion, in Grecia[51].

L'Agenzia lavora a stretto contatto con gli Stati membri e il settore privato per fornire consulenza e soluzioni e migliorare le loro capacità. Questo supporto include tra l'altro:

a) gli esercizi paneuropei di cibersicurezza;

b) lo sviluppo e la valutazione delle strategie nazionali in materia di cibersicurezza;

c) Cooperazione CSIRT e sviluppo delle capacità;

[50] Cfr. V. De Rosa, *La formazione di regole giuridiche per il "cyberspazio"*, cit., pag. 369.
[51] Sul ruolo dell'ENISA si v. A. Contaldo, *L'ENISA e le competenze comunitarie per la cibersicurezza*, in *Rivista di polizia*, 6-7, 2018, pagg. 655 ss.

d) studi su IoT e infrastrutture intelligenti, affrontando questioni di protezione dei dati, tecnologie per il miglioramento della privacy e privacy su tecnologie emergenti, eID e servizi fiduciari, identificando il panorama delle minacce informatiche e altro.

L'ENISA sostiene inoltre lo sviluppo e l'attuazione della politica e della legge dell'Unione europea in materia di sicurezza delle reti e dell'informazione (NIS) e assiste gli Stati membri e le istituzioni, gli organismi e le agenzie dell'Unione europea nell'elaborazione e attuazione delle politiche di divulgazione delle vulnerabilità su base volontaria.

Dal 2019, in seguito all'entrata in vigore della legge sulla cibersicurezza (regolamento 2019/881), l'ENISA è stata incaricata di preparare gli "schemi europei di certificazione della cibersicurezza" che fungono da base per la certificazione di prodotti, processi e servizi a supporto del mercato unico digitale.

L'*European Cybersecurity Act* introduce processi che supportano la certificazione di cybersecurity di prodotti, processi e servizi ICT. In particolare, stabilisce norme a livello UE e schemi europei per la certificazione della cibersicurezza di tali prodotti, processi e servizi TIC.

L'obiettivo della valorizzazione dei compiti dell'ENISA, dunque, è quello di garantire la sicurezza dei prodotti e dei servizi nel mondo digitale. Si è osservato, in proposito, che «tale esigenza nasce senza dubbio dall'intento di creare un ciberspazio aperto, libero, sicuro e dalla consapevolezza che nessun Paese può affrontare da solo le nuove sfide della cybersecurity, ma è necessario promuovere ed applicare norme di comportamento responsabile da parte degli Stati, nonché incrementare iniziative di cooperazione. A ciò si aggiunge il non meno importante intento di rafforzare la fiducia dei cittadini e delle imprese nel mondo digitale, per affermare lo sviluppo di un Mercato unico digitale; considerata l'ormai incontrollata diffusione di ciberattacchi su vasta scala, standard di cibersicurezza elevati sono necessari e devono diventare il nuovo vantaggio competitivo delle imprese. Senza tralasciare poi

l'evidenza che l'uso delle reti e dei sistemi informativi da parte di cittadini, organizzazioni e imprese di tutta l'Unione è attualmente molto diffuso e che svolge un ruolo essenziale nella crescita economica e sociale. Peraltro, con l'avvento dell'Internet of Things, nel prossimo decennio sarà disponibile in tutta l'Unione un numero estremamente elevato di dispositivi digitali connessi, ma la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che li rende inadeguati sotto il profilo della cibersicurezza»[52].

In un contesto siffatto emerge il ruolo dell'ENISA che contribuisce con la sua attività da elaborare la politica e la normativa dell'Unione in materia di sicurezza delle reti e dell'informazione, ruolo indispensabile per garantire la crescita del mercato interno, soprattutto del mercato digitale.

L'ENISA aveva inizialmente solo un ruolo di consulenza tecnica, ma la situazione è cambiata a seguito dell'approvazione del *Cybersecurity Act*. Essa, infatti, svolge ormai attività di supporto agli Stati membri nella gestione operativa di tutti gli incidenti informatici, fornendo in tal modo un sostegno assai più concreto che in passato.

Tra i diversi compiti dell'ENISA rileva quello di fornire pareri e competenze in materia di sicurezza informatica per tutte le istituzioni e gli organismi dell'Unione europea, nonché per tutti gli altri soggetti che sono portatori di interessi. Essa, inoltre, è tenuta a fornire suggerimenti strategici alla Commissione europea ed agli Stati membri, ed è destinata a diventare un vero e proprio punto di riferimento politico per la futura normativa dell'Unione europea in materia di sicurezza informatica.

Da non sottovalutare, poi, è il ruolo di sensibilizzazione dell'ENISA: essa, infatti, avrà il compito di informare l'opinione pubblica in merito ai rischi della sicurezza informatico, contribuendo in maniera decisiva alla formazione

[52] R. Celella, *Il Cybersecurity Act e le nuove sfide del Mercato Unico Digitale*, in *Rivista di diritto dell'Unione europea*, 15 giugno 2020.

di una vera e propria cultura della cybersecurity che, allo stato attuale, in molte realtà è del tutto assente.

L'ENISA, inoltre, dovrà contribuire all'istituzione ed all'attuazione del quadro di certificazione diretto a garantire che i prodotti ed i servizi del mercato unico digitale siano sicuri dal punto di vista della sicurezza informatica. In particolare, l'art. 46 del *Cybersecurity Act* riguarda l'istituzione del quadro europeo di certificazione della cibersicurezza, previsto «al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC».

L'obiettivo di questo quadro normativo in materia di certificazione, dunque, è quello di rendere più sicuro il mercato unico digitale, garantendo che tutti i prodotti, i servizi ed i dati che passano attraverso il web siano immuni da attacchi informatici[53].

Si è sottolineato, ancora, che «con il *Cybersecurity Act*, quindi, si persegue un altro obiettivo importante e allo stesso tempo sfidante, ossia quello di accrescere la consapevolezza dei cittadini, delle organizzazioni e delle imprese circa le questioni riguardanti la cibersicurezza, nella consapevolezza che essa non attiene esclusivamente alla tecnologia di sistemi, reti o prodotti, ma anche al comportamento umano: le imprese e i singoli consumatori

[53] Si è osservato invero che «gli schemi di certificazione non rappresentano una novità assoluta, in quanto in alcuni Stati dell'UE – e anche in Italia– già esistevano, pur non essendo riconosciuti all'estero e inibendo, pertanto, la possibilità per molte imprese di operare a livello transnazionale. Il Cybersecurity Act intende ovviare a tali problemi attraverso l'armonizzazione degli schemi europei di certificazione della sicurezza informatica. È opportuno precisare, però, che il Cybersecurity Act non istituisce schemi di certificazione direttamente operativi, ma crea un "quadro" generale per la loro istituzione. Gli schemi europei di certificazione saranno predisposti dapprima dall'ENISA e successivamente adottati dalla Commissione europea. A seguito di questa adozione, le aziende interessate potranno presentare domanda di certificazione dei propri prodotti o servizi agli organismi accreditati. Il ricorso alla certificazione è volontario, a meno che specifiche norme di settore non lo rendano obbligatorio limitatamente a determinate categorie di prodotti o servizi»: R. Celella, *Il Cybersecurity Act e le nuove sfide del Mercato Unico Digitale*, cit.

dovrebbero disporre di informazioni precise sul livello di affidabilità con cui è stata certificata la sicurezza dei prodotti utilizzati e/o acquistati; i produttori o i fornitori coinvolti nella progettazione e nello sviluppo di prodotti IT dovrebbero essere incoraggiati ad implementare misure di sicurezza già nelle prime fasi di progettazione e sviluppo»[54].

Pare evidente, in conclusione, che l'ENISA è stata posta al centro di un progetto finalizzato a garantire la sicurezza cibernetica del nuovo mercato unico digitale, ed è dunque destinata a diventare il vero e proprio fulcro della politica in materia di cybersicurezza nel corso dei prossimi anni.

5.2. L'istituzione dell'Agenzia per la cybersicurezza nazionale

Il report Clusit 2022[55] segnala la recrudescenza del fenomeno dei crimini informatici. Secondo il rapporto, negli ultimi 11 anni sono stati realizzati, ogni mese, 106 attacchi gravi di dominio pubblico. La media, tuttavia, è aumentata in maniera significativa negli ultimi 4 anni: 129 nel 2018, 137 nel 2019, 156 nel 2020 e 171 nel 2021. Dati tutto sommati analoghi a livello mondiale: si sono registrati 14010 attacchi gravi tra gennaio 2011 e dicembre 2021, di cui oltre la metà (7144) registrati dal 2018 in poi.

Con lo scopo di tutelare gli interessi nazionali nel campo della cybersicurezza, garantire un più efficace coordinamento istituzionale, rendere più razionali le competenze amministrative e introdurre mezzi che permettano di fronteggiare con efficacia e tempestività le situazioni di emergenza che coinvolgano profili di sicurezza cibernetica, il Governo ha recentemente istituito con decreto-legge l'Agenzia per la cybersicurezza nazionale[56]. L'intervento normativo riguarda una pluralità di settori e riguarda interessi pubblici e privati di grande

[54] R. Celella, *Il Cybersecurity Act e le nuove sfide del Mercato Unico Digitale*, cit.
[55] https://clusit.it/rapporto-clusit/.
[56] D.L. 14 giugno 2021, n. 82D.L. 14/06/2021, n. 82 recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, convertito con modificazioni dalla L. 4 agosto 2021, n. 109.

rilevanza, giacché le interdipendenze derivanti dalla diffusa digitalizzazione e dal crescente ricorso all'intelligenza artificiale hanno rivelato un'aumentata e generalizzata esposizione al rischio di attacchi cibernetici. Il decreto-legge s'inserisce in un contesto normativo variegato, destinato a variare anche negli anni a venire; ciò in considerazione, da un lato, del collegamento tra la cybersicurezza e una molteplicità di settori ad essa connessi (in parte attratti nelle competenze del legislatore europeo) e, dall'altro, della complessità tecnica che connota tale materia.

L'istituzione dell'Agenzia per la cybersicurezza nazionale ha il merito di avvicinare l'ordinamento italiano a numerosi Paesi europei e agli Stati Uniti, colmando quella che, secondo il Governo, avrebbe rappresentato una grave lacuna nell'architettura istituzionale nazionale in materia di cybersicurezza. L'Agenzia funge anzitutto da coordinamento tra le autorità pubbliche competenti in questo settore. Oggetto di coordinamento sono sia le attività di prevenzione delle minacce cibernetiche di rilievo meramente nazionale, sia quelle relative alla cooperazione internazionale in materia di cybersicurezza, sebbene in quest'ultimo caso l'Agenzia debba raccordarsi con il Ministero degli esteri.

L'Agenzia è inoltre designata quale centro nazionale di coordinamento nell'ambito della neo-istituita rete europea dei centri nazionali di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e partecipa al gruppo di coordinamento propedeutico all'esercizio dei poteri speciali da parte del Presidente del Consiglio. Per assicurare tali esigenze di coordinamento e l'unità dell'azione amministrativa, l'Agenzia predispone la strategia nazionale di cybersicurezza, la quale è adottata dal Presidente del Consiglio.

In secondo luogo, sono affidate all'Agenzia le funzioni di qualificazione dei servizi cloud per la pubblica amministrazione[57] e di certificazione della

[57] Art. 7, comma 1, lett. m)-ter, D.L. n. 82/2021.

sicurezza cibernetica previste dall'art. 58 del regolamento UE 2019/881, assorbendo - sia sotto questo specifico profilo, sia in relazione a tutti gli aspetti concernenti la cybersicurezza - le funzioni già assegnate al Ministero dello sviluppo economico (di seguito MISE), incluse la vigilanza, l'attività ispettiva e l'esercizio di poteri sanzionatori[58]. A tale proposito l'Agenzia accredita inoltre, quali organismi abilitati a certificare la conformità dei sistemi di rispettiva competenza, le strutture specializzate del Ministero della difesa e del Ministero dell'interno, le quali sono delegate a rilasciare il certificato europeo di sicurezza cibernetica[59].

L'Agenzia assume in terzo luogo le funzioni di vigilanza - e l'esercizio dei relativi poteri sanzionatori - attribuite alla Presidenza del Consiglio dei ministri e al Dipartimento delle informazioni per la sicurezza (di seguito DIS) nell'ambito del perimetro di sicurezza nazionale cibernetica di cui al D.L. n. 105/2019 39. Inoltre, per quel che riguarda nello specifico la sicurezza delle reti e dei sistemi informativi ai sensi del D.Lgs. NIS, essa è Autorità nazionale competente e punto di contatto unico, svolgendo, anche in quest'ambito, funzioni di vigilanza e sanzionatorie[60].

Oltre a ciò, l'Agenzia deve svolgere una rilevante funzione consultiva, esprimendo il proprio parere sulle iniziative legislative o regolamentari concernenti - anche solo parzialmente - la cybersicurezza, al fine di promuovere la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente. In tale prospettiva è da segnalare anche l'attribuzione del potere di adottare linee guida contenenti regole tecniche di cybersicurezza - funzione che precedentemente era stata affidata all'Agenzia per l'Italia digitale.

[58] Art. 7, comma 1, lett. e)-f), D.L. n. 82/2021. Sono state trasferite all'Agenzia anche le funzioni precedentemente attribuite al MISE in materia di sicurezza e integrità delle comunicazioni elettroniche di cui agli artt. 16-bis e 16-ter, D.Lgs. 1° agosto 2003, n. 259.
[59] Art. 7, comma 1, lett. e), nn. 1 e 2, D.L. n. 82/2021 e artt. 60, comma 1, e 56, comma 6, lett. b) reg. (UE) 2019/881.
[60] Art. 7, comma 1, lett. b), D.L. n. 82/2021.

Infine, allo scopo di prevenire e gestire incidenti di sicurezza informatica, l'Agenzia promuove lo sviluppo delle capacità di prevenzione, monitoraggio, rilevamento, analisi e risposta agli attacchi cibernetici, insistendo, in particolare, sulla crittografia come strumento di cybersicurezza. A tal fine essa organizza - o prende parte - a esercitazioni e simulazioni nazionali e internazionali, promuove attività formative e lo sviluppo di algoritmi proprietari, partecipando inoltre a progetti di ricerca internazionali e coinvolgendo enti universitari, di ricerca e imprese, con i quali può concludere accordi e altre forme di partenariato pubblico-privato.

6. I reati informatici: un allarme crescente

Le tecniche di incriminazione dei programmi informatici che possono essere utilizzati per finalità illecite si stanno diffondendo sempre più, agendo sul tessuto economico, privato nonché istituzionale dei Paesi.
Le conseguenze delle azioni criminose che si possono attivare tramite gli strumenti informatici possono essere molto gravi andando ad imporsi, trasversalmente, in ogni ambito e superando i limiti apposti dalla normativa sula privacy. Dietro a tale agire si nascondono intenti spesso dolosi che richiedono un intervento idoneo a reprimerli, soprattutto in fase preventiva.
Poco convincente sembra essere la teoria che individua nei programmi informatici l'oggetto dell'incriminazione, venendo superata dal più condivisibile fine di perseguire i soggetti responsabili fattivamente dei reati in commento.
Ed in questo senso condivisibile è la tecnica di formulazione normativa impiegata dal nostro legislatore che, accanto alla punizione dei dispositivi idonei a commettere accessi abusivi ad un sistema informatico protetto da misure di sicurezza (art. 615-quater c.p.) persegue i soggetti, anche quelli con personalità giuridica, responsabili delle attività descritte. La natura virtuale

delle attività in oggetto richiede, però, un'attenta ricostruzione teorica della disciplina penale che regola il tema. Di seguito, tale approfondimento.

6.1. Accesso abusivo a un sistema informatico o telematico (615 ter c.p.)

Il reato di accesso abusivo ad un sistema informatico o telematico è previsto dall'art. 615 ter c.p.[61]. Il bene giuridico tutelato dal reato in esame è piuttosto controverso, anche a causa della sua ambigua collocazione sistematica.
Secondo un primo orientamento, il reato in esame, essendo collocato tra i reati contro il domicilio, tutelerebbe il c.d. domicilio informatico, da intendersi come una un'are idealmente coincidente con il domicilio fisico, ma avente ad oggetto, in realtà, il luogo informatico, all'interno del quale il soggetto è libero di svolgere qualunque attività lecita, senza subire intromissioni[62].
Sostanzialmente, quindi, secondo questo orientamento il legislatore avrebbe inteso estendere la tutela prevista per il domicilio fisico anche all'ambito informatico. Il domicilio informatico, pertanto, costituirebbe non un nuovo bene giuridico, ma una specificazione ulteriore del bene giuridico "domicilio fisico".

[61] Secondo cui «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 esso contenuti. 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 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».
[62] Cfr., in tal senso, M. Alma, C. Perroni, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. proc.*, 1997, pag. 505.

Di questo avviso si è mostrata anche la giurisprudenza, secondo cui «con la previsione dell'art. 615 ter c.p., 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 della sfera individuale, quale bene anche costituzionalmente protetto. Tuttavia 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 titolare dello *jus excludendi* sia persona fisica, sia giuridica, privata o pubblica, o altro ente»[63].

La dottrina prevalente[64], tuttavia, ha criticato questa impostazione, sottolineando la diversità tra il domicilio fisico e quello informatico, e l'impossibilità di procedere ad una associazione tra le due diverse figure, anche perché, diversamente, vi sarebbe il rischio di una estensione eccessiva della tutela penale.

Si sostiene, pertanto, che la norma in esame presenta una collocazione del tutto inopportuna dal punto di vista sistematico, considerato che non vengono in rilievo «modalità di violazione dei luoghi di privata dimora bensì forme di offesa alla *privacy* che vengono ad interferire su strumenti capaci di favorire tecniche di lavoro intellettuale»[65].

Questo orientamento, nel criticare la tesi secondo cui oggetto di tutela sarebbe il domicilio informatico, ritiene, diversamente, che il bene giuridico tutelato sarebbe la necessità di godere in maniera indisturbata del sistema informatico,

[63] Cass. pen., 4 ottobre 1999, n. 3067, in *Cass. pen.*, 2000, pag. 2990.
[64] Cfr., *ex multis*, F. Pazienza, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Riv. it. dir. proc. pen.*, 1995, pag. 750
[65] A. Merli, *Il diritto penale dell'informatica: legislazione vigente e prospettive di riforma*, in *Giust. pen.*, 2, 1993, pag. 127.

così come l'art. 637 c.p. prevede a favore della proprietà del fondo: come il proprietario di un terreno non deve essere disturbato da nessuno che voglia entrare nel proprio fondo, allo stesso modo il proprietario di un sistema informatico non deve subire intromissioni non gradite[66].

Secondo un diverso orientamento, invece, ad essere tutelata sarebbe la tutela della riservatezza dei dati e dei programmi contenuti in un sistema informatico, i quali sono esposti al rischio di essere facilmente catturati una volta che sono state superate le barriere virtuali poste a protezione dei sistemi informatici stessi[67].

Per quanto concerne l'oggetto fisico della tutela, si tratta del sistema informatico, che è stato definito dalla giurisprudenza come «una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche, che sono caratterizzate - per mezzo di un'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 esprimere un particolare significato per l'utente. Pertanto non lo è 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»[68].

Quanto, infine, alla condotta penalmente rilevante, essa consiste, in alternativa nell'introdursi abusivamente, ossia senza il consenso del titolare

---

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

[67] Cfr. M. Alma, C. Perroni, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, cit., pag. 505.

[68] Così Trib. Milano, 19 marzo 2007, in *Dir. ind.*, 1, 2008, pag. 85. I giudici di merito hanno escluso dunque il reato nel caso di riproduzione di dati di una banca dati contenuta in un sito non protetto da alcun sistema di sicurezza e in relazione al quale non risulta essersi verificata alcuna intrusione.

dello *jus excludendi*, in un sistema protetto, ovvero nel permanervi sebbene il medesimo titolare abbia esercitato, sia pure in maniera tacita, lo *jus excludendi*[69].

6.2. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quiquies c.p.)

Il reato in esame è previsto dall'art. 615 quinquies c.p., secondo cui «chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329»[70].

Nella sua versione originaria tale disposizione si era rivelata del tutto inidonea ad essere applicata in giurisprudenza: essa era diretta ad assicurare la

[69] La giurisprudenza ha osservato che «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»: così Cass. pen., 6 febbraio 2006, n. 11689, in *www.dejure.it*. Fattispecie in cui il reato è stato ravvisato nella condotta degli imputati, che si erano introdotti in una centrale Telecom ed avevano utilizzato apparecchi telefonici, opportunamente modificati, per allacciarsi a numerose linee di utenti, stabilendo, all'insaputa di costoro, contatti con utenze caratterizzate dal codice 899.

[70] Articolo prima aggiunto dall'art. 4, L. 23.12.1993, n. 547, e successivamente così modificato dall'art. 4, L. 18.3.2008, n. 48 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica). Il testo precedentemente in vigore era il seguente: «Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329.». Per l'aumento della pena per i delitti non colposi di cui al presente titolo commessi in danno di persona portatrice di minorazione fisica, psichica o sensoriale, vedi l'art. 36, 1° co., L. 5.2.1992, n. 104, come sostituito dall'art. 3, 1° co., L. 15.7.2009, n. 94.

protezione della funzionalità dei sistemi informatici da una specifica fonte di rischio costituito dai c.d. virus, sanzionando una serie di condotte oggettivamente considerate come pericolose ed intrinsecamente insidiose per il corretto funzionamento di sistemi, dati o programmi[71].

A seguito della riforma del 2008, l'ambito di applicazione della norma è stato esteso, prevedendo la protezione nei confronti di una gamma di rischi più ampia: non solo il *software*, ma anche apparecchiature e dispositivi. Sono state inoltre ampliate le condotte sanzionate anche alle ipotesi di procurarsi, produrre, riprodurre, importare o, comunque, mettere a disposizione di altri detti oggetti.

Ancora, il legislatore ha espressamente previsto che le fonti di rischio devono avere come obiettivo quello di danneggiare o alterare il funzionamento dei sistemi informatici o telematici. La rilevanza penale delle condotte, comunque, prescinde dall'effettivo danneggiamento di tali sistemi, in quanto il legislatore, vista la delicatezza del bene giuridico protetto, ha optato per un'anticipazione della tutela.

Oggetto di tutela, dunque, sono i sistemi informatici e telematici nel loro complesso, oltre che i dati, le informazioni e i programmi che in essi sono contenuti. A tal fine, è necessario che l'autore "inoculi" o cerci di inoculare dei programmi in grado di alterare effettivamente i sistemi informatici della vittima, ossia dei "programmi virus infetti" a tutti gli effetti, capaci di riprodurre sé stessi e di propagarsi, con effetti lesivi e dannosi, in tutto il sistema.

In definitiva, le condotte penalmente sanzionate sono le seguenti: diffondere, comunicare, consegnare o comunque mettere a disposizione programmi e hardware portatori di virus. Vengono, inoltre, incriminate con la riforma del 2008 le condotte di procurarsi, produrre, riprodurre, importare, chiaramente

[71] In tal senso C. Parodi, *Profili penali dei virus informatici*, in *Dir. pen. proc.*, 2000, pag. 632.

orientate a colpire il mercato dei programmi o dispositivi illeciti alimentato dalle condotte sanzionate.

6.3. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)

Altra fattispecie di reato rilevante è quella contenuta nell'art. 617 quater c.p., avente ad oggetto l'intercettazione, l'impedimento e l'illecita interruzione di comunicazioni informatiche o telematiche[72].

Tale previsione estende alla segretezza, libertà e riservatezza delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi la medesima cornice sanzionatoria già prevista dall'art. 617 c.p. per le comunicazioni telefoniche e telegrafiche.

La dottrina[73] ha segnalato che le condotte sanzionate dal legislatore sono idonee ad incidere sulle comunicazioni relative ad un sistema informatico o telematico, o che intercorrono tra più sistemi, nel momento dinamico della loro trasmissione.

Il primo comma dell'art. 617 quater c.p. prevede tre diverse ipotesi: intercettazione, interruzione e impedimento di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi. Laddove l'autore del reato commetta due o più condotte, si avrà comunque sempre un solo reato.

---

[72] Il testo dell'art. 617 quater c.p. è il seguente: «chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) 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, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato».

[73] Cfr. C. Pecorella, *Il diritto penale dell'informatica*, Padova, 2006, pag. 297.

Quanto alla nozione di intercettazione, la Cassazione ha chiarito che rappresenta una intercettazione a tutti gli effetti la cattura dei codici alfanumerici che permettono di accedere al c.d. bancomat. Ciò di solito avviene facendo ricorso ad appositi apparecchi in grado di acquisire illecitamente i codici. Una volta che il codice è stato illegittimamente acquisito, infatti, il suo utilizzo mette in contatto il soggetto con il sistema informatico, integrando un reato informatico[74].

L'intercettazione deve essere effettuata con intento e modalità fraudolenti, nel senso che deve essere realizzata con strumenti in grado di nascondere a coloro che stanno comunicando o al sistema informatico stesso l'intromissione abusiva e, quindi, del tutto illegittima, da parte del soggetto agente.

Quanto alle condotte di interruzione e impedimento esse consistono nella realizzazione di atti tecnicamente idonei, rispettivamente, a far cessare una comunicazione in corso tra due soggetti oppure ad impedirne che una nuova abbia inizio.

6.4. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies c.p.)

Tale disposizione, prevista dall'art. 617 *sexies* c.p.[75], riproduce pedissequamente, in materia di comunicazioni informatiche e telematiche, la

[74] Così Cass. pen., 2 novembre 2007, in *www.dejure.it*, secondo cui «integra la condotta di "intercettazione", rilevante ai sensi dell'art. 617 quater c.p., la condotta di colui che utilizza apparecchiature idonee a copiare i codici alfanumerici di accesso degli utenti, mediante applicazione ai terminali automatici delle banche. La digitazione del codice di accesso costituisce, invero, la prima comunicazione dell'utente con il sistema informatico, con la conseguenza che la copiatura di detti codici rientra nel concetto di intercettazione di comunicazioni telematiche preso in considerazione dalla citata disposizione normativa».

[75] Secondo cui «chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa». L'ultimo comma è stato inserito dall'art. 4, 1° co., D.Lgs. 10.4.2018, n. 36, a decorrere dal 9 maggio 2018

medesima che l'art. 617 ter c.p. ha previsto in tema di comunicazioni telefoniche o telegrafiche[76].

Anche in questo caso il bene giuridico tutelato è la libertà delle comunicazioni informatiche o telematiche, sotto il particolare profilo della sicurezza, genuinità e veridicità delle stesse, nel quale ripone fiducia la collettività.

L'unica peculiarità della disposizione in esame rispetto ai più comuni reati di falso risiede nella natura informatica o telematica del mezzo che forma i documenti oggetto dell'aggressione. Invero, la disposizione in esame sembra essere superflua, in quanto il bene giuridico tutelato poteva essere coperto già dal combinato disposto degli artt. 617 ter e 623 bis c.p.

7. La tutela dei minori al cospetto dei reati sessuali commessi online

Uno dei fenomeni che più si è diffuso con l'avvento di Internet è rappresentato dalla cyber-pedopornografia che trova la sua tutela all'interno dell'articolo 600 quater c.p. contenente il reato di pedopornografia. In questo caso il reato viene utilizzato tramite l'utilizzo di internet. Questa fattispecie è spesso legata alla pratica di adescamento dei minori.

Il pedofilo è un soggetto che normalmente è convinto che, in virtù delle sue competenze informatiche, può restare invisibile sul web, esercitando il comportamento prepotente nel più totale anonimato. Spesso l'illusione dell'anonimato può dare coraggio a soggetti che hanno subito atti di pedofilia nella vita reale, inducendoli a commettere atti di pedofilia virtuale.

In un contesto siffatto, il pedofilo non si rende conto di essere tale, a causa soprattutto dell'alterazione della percezione della gravità delle sue azioni. Le azioni richieste per compiere i soprusi, infatti, sono estremamente semplici, a portata di un click; il contesto nel quale le azioni vengono compiute, poi, è normalmente confortevole, al riparo da occhi indiscreti.

[76] In tal senso G. Corasaniti, *La tutela della comunicazione informatica e telematica,* in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), *Profili penali dell'informatica*, Milano, 1994, pagg. 125 ss.

In tal modo, viene a ridursi in maniera significativa la percezione della gravità delle proprie azioni, e viene a crearsi un contesto ideale per favorire la reiterazione dei comportamenti pedofili. Diventa poi difficile anche comprendere le conseguenze negative che i propri comportamenti hanno sulle vittime. Il fatto che il proprio comportamento possa assumere i contorni di un reato è spesso una rappresentazione del tutto lontana dalla realtà e dalla mente del minore[77].

Il pedofilo online viene favorito dall'assenza di limiti spaziali e temporali: mentre la pedofilia reale si verifica in luoghi ben definiti, ossia in contesti scolastici o casalinghi, quello virtuale non ha potenzialmente confini. Per compiere atti di pedofilia online è necessario collegarsi ad un dispositivo in grado di connettersi ad internet: la semplicità di questi gesti favorisce la probabilità che si verifichino.

Un altro fenomeno che viene favorito dal contesto virtuale è poi costituito dall'assenza di compassione nei confronti della vittima: se gli atti di pedofilia reale presuppongono un contatto diretto con la vittima, la cui sofferenza sovente potrebbe indurre il pedofilo a fermarsi, l'assenza di un contatto fisico finisce con l'allungare il lasso temporale delle persecuzioni e, dunque, della sofferenza della vittima, perché il pedofilo non la concepisce come tale.

La pedofilia online, poi, può manifestarsi in diversi modi: il più diffuso consiste nella diffusione online di comportamenti di pedofilia perpetrati nella vita reale: in tal modo la pedofilia si trasforma in pedofilia online, amplificando la sofferenza della vittima e la denigrazione della sua identità personale, oltre che, ovviamente, di quella virtuale.

Ciò, ad esempio, si verifica spesso quando comportamenti pedofili vengono ripresi attraverso telefonini e diffusi poi sul web per mostrare a tutti gli amici e conoscenti della vittima quello che essa ha subito, oltre che per mostrare ai propri amici ed ai propri conoscenti la propria superiorità nella vita reale.

---

[77] Cfr. F. Novario, *Pornografia minorile e file sharing: l'influenza della tecnologia informatica sull'asse probatorio*, in *Dir. pen. proc*., 10, 2009, pag. 1290.

Sempre concernente i minori e più in generale gli adolescenti, con l'evoluzione tecnologica il bullismo ha assunto vesti cyber, le condotte hanno iniziato ad essere perpetrate sempre più tramite i sistemi informatici.
Nel 2019, con la legge numero 69, è stato inserito l'articolo 612 ter nel codice penale con l'obiettivo di combattere il fenomeno del revenge porn. Questo fenomeno consiste nella diffusione di materiale intimo condiviso nell'ambito di una relazione privata con lo scopo di vendetta. Accanto a questa fattispecie si situa quella dell'estorsione sessuale perpetrata attraverso minacce di diffusione di immagini e video nel web[78].
Del resto anche la prostituzione minorile *online* si è diffusa molto nel corso degli ultimi anni. La Cassazione, in proposito, ha chiarito che «rientra nella nozione di prostituzione ogni attività sessuale, posta in essere dietro corrispettivo, anche se priva di contatto fisico tra i due soggetti, i quali si possono anche trovare in luoghi diversi per mezzo di apparecchiature di comunicazione elettronica o a mezzo telefono, essendo richiesta unicamente la possibilità per gli stessi di poter interagire fra loro. L'elemento caratterizzante il reato di specie, non è quindi, necessariamente costituito dal contatto fisico tra le parti del rapporto, ma rileva la correlazione atto sessuale-corrispettivo, e che tale atto sia finalizzato, in via diretta e immediata a soddisfare la libidine di colui che ha richiesto la prestazione e ne è destinatario, quindi, anche l'attività di chi esegue atti sessuali di qualsiasi natura su se stesso in presenza di chi ha chiesto la prestazione, dietro un compenso»[79].
Il problema, oggi, è posto dal nuovo fenomeno noto come *sexting*. L'art. 612 *ter* c.p. dispone che «Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere

[78] Cfr. M. Fabozzo, *Analisi normativa e profili problematici del reato di diffusione illecita di immagini o video a contenuto sessualmente esplicito (c.d. revenge porn) ex art. 612-ter c.p.*, in *Riv. pen.*, 2, 2020, pag. 150.
[79] Cass. pen., 19 dicembre 2013, n. 16207, in *Guid. Dir.*, 2014, pag. 78.

privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con la multa da euro 5.000 a euro 15.000. La stessa pena si applica a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento. La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici. La pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza. Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. La remissione della querela può essere soltanto processuale. Si procede tuttavia d'ufficio nei casi di cui al quarto comma, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio».

L'art. 10 del Codice Rosso ha inserito nel codice penale l'art. 612 *ter* e, con esso, il delitto di diffusione illecita di immagini o video sessualmente espliciti[80].

Sembrerebbe trattarsi del contrasto penalistico al fenomeno ormai generalmente conosciuto come "*revenge porn*": letteralmente, "vendetta porno" o "vendetta pornografica", o anche "porno vendicativo" o "pornografia vendicativa"[81].

---

[80] Sul tema si v. G.M. Caletti, *Libertà e riservatezza sessuale all'epoca di internet. L'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale*, in *Riv. it. dir. proc. pen.*, 2019, pagg. 2045 ss.; A. Cisterna, *Reclusione a sei anni con la sola circolazione di filmati sui social*, in *Guid. Dir.*, 37, 2019, pag. 77; G. Pavich, *Le modifiche al codice penale*, in A. Marandola, G. Pavich (a cura di), *Codice rosso l. n. 69/2*019, Milano, 2019, pag. 21; B. Romano, *L'introduzione dell'articolo 612-ter del codice penale in materia di diffusione illecita di immagini o video sessualmente espliciti (art. 10, l. 19 luglio 2019, n. 69*), in B. Romano, A. Marandola (a cura di), *Codice rosso. Commento alla l. 19 luglio 2019 n. 69, in materia di tutela delle vittime di violenza domestica e di genere*, Roma, 2020, pag. 105

[81] Cfr. G.M. Caletti, *"Revenge porn". Prime considerazioni in vista dell'introduzione dell'art. 612-ter c.p.: una fattispecie "esemplare", ma davvero efficace?*, in *Dir. pen. cont.*, 29 aprile 2019. Prima della riforma, G.M. Caletti, *"Revenge porn" e tutela penale. Prime riflessioni*

Nella accezione più diffusa, è l'odiosa pratica consistente nel vendicarsi di qualcuno (spesso l'*ex partner*) diffondendo materiale sessualmente connotato che lo ritrae. In realtà, il delitto di cui all'art. 612 *ter* presenta una disciplina complessa, articolata in due differenti ipotesi, previste rispettivamente ai commi 1° e 2° della disposizione, corredate di numerose circostanze aggravanti, alle quali sono dedicati i successivi commi 3° e 4°, e completata dalla regolazione della materia della procedibilità.

Per comprendere, dunque, ruolo e funzione della disposizione introdotta, occorrerà esaminare distintamente tutti gli aspetti appena indicati.

Il 1° co. dell'art. 612 *ter* prevede che, salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con la multa da euro 5.000 a euro 15.000.

Dunque, il reato di diffusione illecita di immagini o video sessualmente espliciti è un reato comune, poiché commissibile da "chiunque".

Tuttavia, nel 1° co. dell'art. 612 *ter* ci si riferisce al soggetto che ha realizzato le immagini o i video, ma anche a chi ha sottratto detti contenuti. Sennonché, mentre il soggetto che ha realizzato tali immagini o video solitamente può essere chi ha partecipato direttamente alla scena rappresentata o comunque ha scattato le foto o effettuato le riprese, il soggetto che le ha sottratte può essere qualunque soggetto che se le sia procurate, invito domino, dalla stessa persona offesa o in qualsiasi altro modo o da qualsiasi altro soggetto.

Dal punto di vista dell'elemento soggettivo, l'ipotesi di cui al 1° co. dell'art. 612 *ter* è punita a titolo di dolo generico. Dunque, qui non si è, a ben vedere, in presenza di condotte necessariamente riconducibili a vendette o ritorsioni, come invece nello schema del *revenge porn*.

---

sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane, in *Dir. pen. cont.*, 3, 2018, pagg. 65 ss.

La condotta si dettaglia in cinque modalità alternative di integrazione del delitto, appunto realizzabile da chiunque "invia", "consegna", "cede", "pubblica" o "diffonde" le immagini o i video a contenuto sessualmente esplicito.

Al riguardo, si è notato come, mentre le prime tre condotte si basano su un contatto diretto tra un soggetto ed un altro (o altri, ma determinati), le ultime due modalità realizzative riguardano attività destinate ad una cerchia indeterminata di destinatari, con una potenziale "viralità" della pubblicità e della diffusione delle immagini o dei video[82].

Dunque, nonostante il plurale della rubrica, il delitto, almeno nelle prime tre modalità realizzative, punisce già l'invio, la consegna o la cessione da un soggetto ad un altro: con un tasso di severità comparativamente maggiore rispetto alla repressione della pubblicazione o della diffusione delle immagini o dei video a contenuto sessualmente esplicito.

Oggetto della condotta devono essere «immagini o video a contenuto sessualmente esplicito». La locuzione utilizzata dal legislatore non è né chiara né precisa: da un contenuto minimo relativo alla rappresentazione di atti sessuali, che rimanda alla definizione propria del delitto di violenza sessuale di cui all'art. 609 bis, ci si può spingere sino a concetti più ampi, quale quello di pornografia minorile, che vi comprende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali[83].

Sarà la giurisprudenza a dovere ricostruire la nozione di «immagini o video a contenuto sessualmente esplicito», anche se, probabilmente, la definizione

---

[82] Cfr. M. Fabozzo, *Analisi normativa e profili problematici del reato di diffusione illecita di immagini o video a contenuto sessualmente esplicito (c.d. revenge porn) ex art. 612-ter c.p.*, cit., pagg. 149 ss.

[83] Cfr. A. Valsecchi, *Codice rosso e diritto penale sostanziale: le principali novità. Commento a legge 19 luglio 2019 n. 69 (Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica o di genere)*, in *Dir. pen. proc.*, 2, 2020, pagg. 165 ss.

che si ricava dal delitto di pornografia minorile potrebbe rappresentare un ragionevole punto di equilibrio.

Si deve trattare, poi, di contenuti «destinati a rimanere privati». Qui, certamente, ci si riferisce a immagini o video nati nel quadro di rapporti di coppia; tuttavia, può ipotizzarsi anche una creazione sin dall'inizio destinata a nuclei più ampi, ma comunque determinati, di soggetti (si pensi a chi assiste, con il consenso dei "protagonisti", a condotte sessualmente esplicite poste in essere da altri).

Inoltre, l'invio, la consegna, la cessione, la pubblicazione o la diffusione delle immagini o dei video a contenuto sessualmente esplicito deve avvenire «senza il consenso delle persone rappresentate». Si noti che, opportunamente, il legislatore ha fatto riferimento alla mancanza di consenso.

Quindi, è sufficiente che la condotta avvenga "all'insaputa" della persona rappresentata, poiché si tratta di immagini o video, come detto, «destinati a rimanere privati». Si ritiene che la presenza del consenso ovviamente determinerà la persona offesa a non sporgere querela; mentre un consenso tardivo potrà condurre ad una remissione della querela[84].

Nei casi di procedibilità d'ufficio, invece, il consenso avrà ancora maggior peso, facendo venir meno *ab origine* il reato, nonostante l'immediata possibile procedibilità, o proiettando delicati problemi sul piano dell'accertamento probatorio, ove il consenso si manifesti successivamente.

Il 2° co. dell'art. 612 ter prevede che si applichi la stessa pena prevista dal comma precedente a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento.

Rispetto alla ipotesi disciplinata nel 1° co., rimane fermo il riferimento alle immagini o ai video a contenuto sessualmente esplicito, destinati a rimanere

[84] Cfr. A. Valsecchi, *Codice rosso e diritto penale sostanziale: le principali novità. Commento a legge 19 luglio 2019 n. 69 (Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica o di genere)*, cit., pagg. 167 s.

privati, l'elencazione delle cinque modalità realizzative della condotta (inviare, consegnare, cedere, pubblicare o diffondere), nonché il requisito della mancanza di consenso delle persone rappresentate.

Invece, costituiscono elementi differenziali l'individuazione del soggetto attivo del reato e la finalità ulteriore che deve muovere la condotta di tale soggetto.

Sotto il primo profilo, il 2° co. dell'art. 612 *ter* si riferisce a chi ha ricevuto o comunque acquisito le immagini o i video a contenuto sessualmente esplicito, cioè a soggetti "terzi" rispetto a quelli menzionati nel 1° co. della medesima disposizione. Peraltro, mentre nella generalità dei casi il soggetto attivo dell'ipotesi disciplinata dal 2° co. dell'art. 612 ter avrà ricevuto le immagini o i video dal primo distributore o da altri o le avrà comunque acquisite (magari scaricandole dalla rete), in taluni casi potrebbe avere ricevuto tali dati anche dalla stessa persona rappresentata, come avviene nel c.d. "*sexting*".

In entrambe le eventualità la condotta deve essere realizzata al fine di recare nocumento alle persone rappresentate: si tratta del c.d. *revenge porn* o, comunque, di condotte finalizzate a recare nocumento[85].

Ora, si è notato come la presenza del dolo specifico si comprenderebbe in relazione a condotte poste in essere da soggetti realmente "terzi", ma meno nel caso del *partner*, che potrebbe agire anche in assenza di finalità vendicative.

In ogni caso, la individuazione della finalità ulteriore che deve muovere il soggetto attivo del reato potrebbe presentare difficoltà sul piano dell'accertamento probatorio.

I commi 3° e 4° dell'art. 612 ter disciplinano una serie di circostanze aggravanti.

---

[85] Cfr. A. Valsecchi, *Codice rosso e diritto penale sostanziale: le principali novità. Commento a legge 19 luglio 2019 n. 69 (Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica o di genere)*, cit., pagg. 169 ss.

In particolare, ai sensi del 3° co. della disposizione citata, la pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici[86].

Si tratta di circostanze speciali ad effetto comune, con aumento di pena, ex art. 64, 1° co., fino ad un terzo.

Inoltre, in base all'art. 612 ter, 4° co., la pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza.

In tali ipotesi, siamo in presenza di circostante speciali ad effetto speciale, poiché l'aumento di pena è da un terzo alla metà.

Da notare che tali ultime aggravanti, pur se parzialmente corrispondenti a quelle previste dal 3° co. dell'art. 612 *bis*, in materia di atti persecutori (c.d. *stalking*), non fanno riferimento al minore (né, ma rileva meno, a persona travisata).

Ciò, probabilmente, perché il legislatore ha immaginato che, in tale eventualità, potrebbero rilevare altre fattispecie. Sennonché, la norma che potrebbe "coprire" tali ipotesi, e cioè quella disciplinata dall'art. 600 ter, 3° co., nel quadro della pornografia minorile, non sembra concretamente poter rilevare. Innanzitutto, perché l'art. 612 ter prevede una pena più severa e quindi opererebbe la clausola di riserva di cui all'incipit di tale delitto («salvo che il fatto costituisca più grave reato»)[87].

E poi anche perché la Corte di cassazione ha escluso che la divulgazione di immagini autoprodotte dal minore possa integrare la fattispecie di «distribuzione, divulgazione, diffusione, pubblicizzazione di materiale pedopornografico»[88]: con la conseguenza che il delitto di diffusione illecita

---

[86] Ivi, pagg. 171 ss.

[87] Cfr. M. Fabozzo, *Analisi normativa e profili problematici del reato di diffusione illecita di immagini o video a contenuto sessualmente esplicito (c.d. revenge porn) ex art. 612-ter c.p.*, cit., pagg. 151 ss.

[88] Cfr. Cass. pen., 18 febbraio 2016, n. 11675. Per un commento, M. Bianchi, *Il "Sexting minorile" non è più reato*?, in *Dir. pen. cont.*, 1, 2016, pagg. 138 ss.

di immagini o video sessualmente espliciti si applicherà, ma nella forma semplice (cioè, non aggravata), nelle ipotesi di pornografia non consensuale in ambito minorile.

L'ultimo comma dell'art. 612 ter si occupa della procedibilità.

In particolare, si prevede che, ordinariamente, il delitto sia punito a querela della persona offesa. Tuttavia, si procede d'ufficio nei casi di cui al quarto comma, e cioè se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio.

Quest'ultima previsione si pone in armonia sia con quanto previsto dall'ultimo comma dell'art. 612 *bis* c.p. per il delitto di atti persecutori, sia con quanto stabilito dal 4° co., n. 4, dell'art. 609 *septies* per i delitti di violenza sessuale, anche aggravati ai sensi dell'art. 609 *ter*, e di atti sessuali con minorenne.

Analogamente a quanto previsto per lo *stalking* dall'art. 612 *bis* c.p. e, prima del raddoppio dovuto all'art. 13, 4° co., lett. b, del Codice Rosso, dall'art. 609 septies, 2° co., c.p., il termine per la proposizione della querela è di sei mesi.

E, sempre come per il delitto di cui all'art. 612 bis (al 4° co.), ma non anche per l'art. 609 *septies*, che al 3° co. dispone che la querela disposta è irrevocabile, si prevede che la remissione della querela possa essere soltanto processuale.

Al riguardo, va segnalato che la Cassazione[89], in relazione al delitto di atti persecutori, ha recentemente affermato che la remissione di querela può essere effettuata non soltanto davanti all'autorità giudiziaria, ma anche davanti ad un ufficiale di polizia giudiziaria, poiché rileverebbe la disciplina risultante dal combinato disposto degli artt. 152 e 340 c.p.p.

[89] Cass. pen., 21 aprile 2016, n. 16669, in www.dejure.it.

Il delitto di diffusione illecita di immagini o video sessualmente espliciti, di cui all'art. 612 ter, come anticipato, si apre con la clausola di riserva «salvo che il fatto costituisca più grave reato». Si tratta, più precisamente, di una clausola di riserva relativamente indeterminata leggibile quale clausola di consunzione[90].

La presenza di detta clausola indica la scelta del legislatore di evitare che il concorso tra norme diventi effettivo, individuando quale sia la norma che debba prevalere.

Un altro profilo che mette a rischio i minori è la sottrazione dei dati. Il rischio, in particolare, è il fenomeno del c.d. *digital kidnapping*: utilizzando le informazioni che sono presenti in rete, spesso condivise dagli stessi genitori, un soggetto finisce con il duplicare l'identità di un minore per finalità diverse. La Cassazione ha riconosciuto la colpevolezza di un imputato reo di aver creato un falso profilo Facebook grazie all'utilizzo dell'identità digitale di un minore per adescare delle ragazzine, convincerle a mandargli foto erotiche di sé e arrivare, in alcuni casi, anche a minacciarle. La Cassazione, nell'occasione, ha infatti affermato che tale condotta rientra nel delitto di sostituzione di persona, punita dal codice penale all'art. 494[91]. Si tratta di un fenomeno che non deve essere sottovalutato in quanto, facendo ricorso al *digital kidnapping*, è anche possibile che il minore rimanga vittima di una truffa patrimoniale, soprattutto quando utilizza risorse per giocare ad alcuni giochi online.

[90] Cfr. M. Fabozzo, *Analisi normativa e profili problematici del reato di diffusione illecita di immagini o video a contenuto sessualmente esplicito (c.d. revenge porn) ex art. 612-ter c.p.*, cit., pagg. 153 ss.

[91] Cass. pen., 8 giugno, 2018, n. 33862.

CAPITOLO II
LA FRODE INFORMATICA

Sommario: 1. La frode informatica: origini della fattispecie; 2.1. La condotta nell'interpretazione della dottrina; 2.2. La condotta nell'applicazione della giurisprudenza; 3. La nozione di phishing come più tipica manifestazione della frode informatica; 3.1. Le diverse tecniche di attacco mediante phishing; 3.2. Phishing tra truffa e frode informatica 4. Il profitto ingiusto; 5. L'elemento soggettivo; 6. Le circostanze aggravanti; 7. La confisca obbligatoria; 8. Frode informatica e truffa: una riflessione conclusiva; 9. L'attività di prevenzione

1. La frode informatica: origini della fattispecie

Il reato di frode informatica è previsto dall'art. 640 ter c.p. e sanziona chiunque, «alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno».

Introdotta con la legge 23.12.1993, n. 547, la fattispecie era da tempo invocata dalla dottrina[92]. Prima che la frode informatica fosse introdotta, la giurisprudenza accertava, caso per caso, se i dati che venivano manipolati fossero stati successivamente oggetto di un controllo da parte dell'uomo, al fine di integrare il reato di truffa. Solo in questi casi, infatti, si poteva configurare il reato di truffa, in quanto il risultato dell'elaborazione era la conseguenza di aver indotto una determinata persona in errore.

Si comprende, pertanto, quanto fosse importante introdurre il reato di frode informatica, giacché era piuttosto complicato far ricadere all'interno della

[92] In particolare, come sottolinea G. Minicucci, *Le frodi informatiche*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), *Cybercrime*, Torino, 2019, pag. 828, era «invocata dai teorici e dai pratici del diritto soprattutto allo scopo di emarginare il dibattito intorno all'applicabilità del delitto di truffa in campo informatico, osteggiata in particolare da chi non riteneva in alcun modo assimilabile all'induzione in errore di un uomo la manomissione e/o l'impiego truffaldino di una macchina»

sfera di punibilità della truffa tutte quelle fattispecie in cui vi fosse la manomissione di un elaboratore e non l'induzione in errore di una persona fisica.

A seguito dell'introduzione da parte del legislatore per frode informatica si intende, dunque, un reato in cui un comportamento penalmente rilevante ha, nella stessa formulazione dell'incriminazione, beni informatici (programmi o macchine), quali oggetto della condotta ovvero strumenti o cose sui quali la condotta riverbera le sue conseguenze; un reato che non abbia nella sua descrizione tali elementi e che venga concretamente posto in essere con l'ausilio di mezzi informatici.

Il reato di frode informatica è collocato tra i delitti contro il patrimonio mediante frode: ciò significa che il legislatore del 1993 ha inteso attribuire una tutela ulteriore al bene "patrimonio"[93]. A tal proposito, bisogna necessariamente effettuare alcune considerazioni. La tutela che il codice Rocco appresta al patrimonio si rivela, allo stato attuale, del tutto inadeguata, considerato che la disciplina in esame è stata fortemente condizionata dal contesto giuridico, economico e sociale nel quale fu elaborata.

In particolare, lascia perplessi la risposta sanzionatoria in materia, connotata da un intento repressivo deterrente che pare francamente eccessivo per il suo rigore. Il patrimonio, nel codice vigente, è sostanzialmente tutelato oltre ogni ragionevolezza: se è vero, infatti, che esso è pur sempre un bene costituzionalmente rilevante, allo stesso tempo bisogna considerare che, nella scala gerarchica dei beni costituzionalmente rilevante, esso è sicuramente subordinato alla tutela della persona.

Parte della dottrina ha osservato che, al di là della tendenziale riduzione dell'ambito di operatività del diritto penale, conseguente all'azione dei postulati garantistici dello stato sociale di diritto, «appare evidente l'incongruità di una tutela penale, che tanto macroscopicamente incide sulla

[93] Cfr. F. Mucciarelli, *Commento all'art.10 della legge 547 del 1993*, in *Leg. Pen.*, 1996, pag. 136

libertà dell'individuo, nel momento in cui si pervenga alla piena consapevolezza del superamento, al livello di legge fondamentale, di una considerazione privilegiata della proprietà privata e, a fortiori, del patrimonio»[94].

In tale prospettiva, dunque, il bene-patrimonio deve essere considerato in chiave dinamica e non statica, ossia nel suo rapporto con la tutela della persona. In tanto la tutela penale dovrà essere più rigorosa in quanto la lesione del patrimonio abbia una diretta incidenza anche nei confronti della sfera intima della persona, secondo una concezione personale del patrimonio, affinché si appresti tutela non alla integrità di un astratto valore in denaro, ma al bene in quanto espressione della potenzialità economica della persona e del suo rapporto diretto con il bene.

Va segnalato, tuttavia, che secondo altra dottrina[95] il delitto in esame non avrebbe carattere monooffensivo bensì plurioffensivo: in altri termini, ad essere tutelato non sarebbe solo il patrimonio in quanto tale, ma anche il corretto funzionamento dei sistemi informatici e della riservatezza che deve caratterizzare l'utilizzazione di tali sistemi. In tale prospettiva, dunque, si ritiene che la fattispecie in esame abbia carattere plurioffensivo.

Secondo un altro orientamento ancora, invece, oggetto giuridico di tutela sarebbe anche la libertà negoziale. La tecnica di redazione del legislatore richiama, infatti, le modalità temporali con cui normalmente si verifica la truffa, considerato che le condotte di alterazione e di intervento sono in realtà veri e propri artifizi o raggiri[96].

Come è stato opportunamente osservato, una puntualizzazione del genere sarebbe superflua se non si assistesse, come accade da tempo soprattutto nella

---

[94] S. Moccia, *Il diritto penale tra essere e valore. Funzione della pena e sistematica teleologica*, Napoli, 1992, pag. 257.

[95] Cfr. G. Fiandaca, F. Musco, *Diritto penale. Parte speciale* II. *I delitti contro il patrimonio*, Bologna, 2012, pag. 198.

[96] Cfr. G. Marra, *Truffa (art. 640)*, in AA.VV., *Trattato breve dei delitti contro il patrimonio*, Torino, 2010, pagg. 477 ss.; A. Fanelli, *La truffa*, Milano, 2009, pagg. 199 ss.; A. Pagliaro, *Truffa e danno patrimoniale*, in *Rivista italiana di diritto e procedura penale*, 1963, pag. 1202 ss.

prassi applicativa, a un processo di svalutazione interpretativa delle specifiche caratteristiche modali della truffa, con connessa dilatazione della sua sfera di operatività[97].

Ancora, parte della dottrina[98] si è spinta oltre, sostenendo che, nonostante non debba essere messa in discussione la sua natura privatistica, il bene protetto nel delitto di frode informatica si atteggerebbe comunque in maniera composita: oggetto della tutela, in tale prospettiva, non sarebbe solo il patrimonio, ma anche la libertà della vittima di disporre del consenso al riparo da qualunque fraudolenta intromissione di terzi. Oltre al patrimonio, dunque, ad essere tutelato sarebbe anche il bene giuridico della libertà del consenso. Si tratta di una impostazione che richiama la summenzionata visione costituzionalmente orientata del patrimonio, da intendersi non come mero ed astratto insieme di beni, ma nella sua stretta relazione con la capacità di disporne del titolare.

Tuttavia non tutta la dottrina condivide questa impostazione, che finisce pur sempre con lo scomporre l'unitarietà della fattispecie, rendendola complessa. Altra dottrina[99], in particolare, ha osservato che il legislatore, mediante l'art. 640 ter c.p., non ha intenzione di proteggere esclusivamente l'integrità del patrimonio, né, tantomeno, il processo di formazione della volontà contrattuale, limitandosi piuttosto a tutelare l'integrità del patrimonio solo ed unicamente se messa in pericolo da un atto che si concretizza in una determinazione della volontà artificiosa del soggetto che esercita il potere di disposizione.

Egli, dunque, richiama la teoria secondo cui gli interessi ricevono una tutela diversa a seconda dell'aggressione cui sono soggetti. Del resto, appare utile ricordare che il patrimonio non viene difeso in quanto tale, ma con riguardo

[97] G. Fiandaca, E. Musco, *Diritto penale. Parte speciale* II. *I delitti contro il patrimonio*, cit., pag. 181.
[98] Ivi, pag. 164.
[99] L. Violante, *L'atto di disposizione patrimoniale nella truffa e la frode fiscale*, in *Ind. Pen.*, 1980, pag. 566.

alle diverse tipologie di aggressione cui è esposto. Per tale ragione, «può ricondursi l'interesse tutelato dell'art. 640 ter c.p. nell'ambito di quel gruppo di interessi complessi configurati in modo tale che la lesione di uno per essere giuridicamente rilevante da un certo titolo, deve verificarsi accompagnata dalla contemporanea (e necessaria) offesa all'altro o degli altri. Qui oggetto della tutela è un interesse unico, la cui struttura però si presenta costituita dalla fusione di più interessi semplici: l'offesa in tali ipotesi sorge con la lesione dell'interesse in tutte le sue componenti»[100].

Quanto, poi, alla giurisprudenza, di recente essa si è così pronunciata: «il bene giuridico tutelato dal delitto di frode informatica non può essere iscritto esclusivamente nel perimetro della salvaguardia del patrimonio del danneggiato, come pure la collocazione sistematica lascerebbe presupporre, venendo chiaramente in discorso anche l'esigenza di salvaguardare la regolarità di funzionamento dei sistemi informatici - sempre più capillarmente presenti in tutti i settori più importanti della vita economica, sociale, ed istituzionale del Paese - la tutela della riservatezza dei dati, spesso sensibili, ivi gestiti, e, infine, aspetto non trascurabile, la stessa certezza e speditezza del traffico giuridico fondata sui dati gestiti dai diversi sistemi informatici. Un articolato intessersi, dunque, di valori tutelati, tutti coinvolti nella struttura della norma, che indubbiamente ne qualifica, al di là del tratto di fattispecie plurioffensiva, anche i connotati di figura del tutto peculiare, e quindi "speciale", nel panorama delle varie ipotesi di "frode" previste dal codice e dalle varie leggi di settore»[101].

[100] Ibidem.

[101] Cass. pen., SS.UU., 15 aprile 2011, n. 17748, in *dejure.it*, secondo cui «integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua».

Pare evidente, dunque, in conclusione, che l'oggetto della norma ha carattere plurioffensivo, non potendo essa tutelare solo ed esclusivamente il patrimonio, a pena di ridimensionarne la portata.

2.1. La condotta nell'interpretazione della dottrina

Per quanto riguarda, in concreto, cosa si intende per alterare ed intervenire, pare opportuno partire dalla prima condotta. L'alterazione può essere effettuata in due diversi modi: agendo direttamente sul software, ossia sulla componente logica del computer, in pratica su dati, informazioni personali, programmi installati e memorizzati in una macchina che abbia capacità di elaborazione; oppure agendo sull'hardware, ossia sulle parti elettroniche, ottiche, magnetiche, meccaniche che permettono alla macchina di funzionare, in modo tale da costringerla a compiere azioni diverse da quelle che avrebbe fatto in assenza dell'intervento di alterazione[102].

La seconda condotta è quella di "intervento", da intendersi come qualunque azione in grado di incidere su dati, programmi o informazioni, modificandoli abusivamente[103]. Per quanto riguarda i dati, deve intendersi ogni registrazione elementare di un elaboratore elettronico codificato in modo tale da non essere

---

[102] Cfr., sul punto, quanto osservato da G. Marini, *Truffa*, in *Digesto delle discipline penalistiche*, XVIII, Torino, 1999, p. 141, secondo cui «l'alterazione» di un sistema informatico o telematico si abbia tanto operando sulla «parte fisica del sistema» (il c.d. hardware) quanto operando sui complessi di istruzioni che ne consentono il funzionamento (il c.d. software). Il primo caso si verifica allorché il soggetto opera sulla «parte fisica» della macchina, modificandone la struttura o i collegamenti «interni» (sia questa l'«unità centrale» o uno qualsiasi dei «terminali» utili ai fini perseguiti dall'agente) o modificando le caratteristiche delle parti «hardware» da inserirsi nella macchina (o nei suoi «terminali») per provocarne il funzionamento («bancomat», «carte di credito abilitate al prelievo» ecc.), sì da causarne un funzionamento anomalo. Va solo notato, per completezza, che l'«alterazione del funzionamento», traducentesi in un danneggiamento del sistema (sia nella sua parte fisica sia nella parte relativa ai programmi, dati ecc.), con conseguente necessità, ad esempio, di ripristinarne la funzionalità iniziale, è riportabile, in regime di concorso formale, al reato di cui all'art. 635 bis c.p.».

[103] Cfr. V.S. Destito, G. Dezzan, C. Santoriello, *Il diritto penale delle nuove tecnologie*, Padova, 2007, pag. 18, secondo cui l'espressione utilizzata dal legislatore, "senza diritto", intende sia senza il consenso dell'avente diritto che qualunque condotta «non consentita da norme giuridiche, né da altre fonti»

visivamente percepibile. Le informazioni, invece, sono costituite da un insieme di dati organizzati in modo tale che sia possibile attribuire loro un determinato significato. I programmi, infine, sono sequenze di istruzioni. Intervenendo sui programmi è possibile ordinare al computer di effettuare attività del tutto diverse da quelle programmate dal titolare.

Per quanto concerne l'espressione del legislatore, "senza diritto", la dottrina ha molto dibattuto sul significato. Appare chiaro che deve trattarsi di un intervento illegittimo, ma non vi è unanimità sull'interpretazione dell'espressione. Secondo un primo orientamento, il legislatore, facendo ricorso a tale espressione, avrebbe inteso «richiamare l'attenzione dell'interprete sul momento dell'antigiuridicità»[104].

Secondo altra dottrina, invece, si tratterebbe di un'ipotesi di «antigiuridicità speciale non reale ma apparente perché non fa che richiamarsi all'assenza giuridica di agire, di cui all'art. 51»[105].

Altra interpretazione[106] ha considerato l'inciso del tutto superfluo, se non addirittura pericoloso, in quanto vi è «il rischio che si crei una sacca di impunità proprio tra gli addetti ai lavori»[107]. Effettivamente, appare tutto sommato abbastanza inutile l'inciso, in quanto, trattandosi di un reato che presuppone un illecito profitto, è del tutto indifferente se il soggetto era legittimato ad intervenire o ad alterare i dati, i programmi e le istruzioni del sistema informatico. Va segnalato, ancora, che entrambe le condotte, quella di alterazione e quella di intervento, sono a forma libera, essendo per il legislatore del tutto indifferente circa le concrete modalità con cui l'agente intervenga o alteri senza diritto un sistema informatico.

---

[104] G. Delitala, *Raccolta degli scritti*, I, Milano, 1976, pag. 40.

[105] F. Mantovani, *Diritto penale, Parte speciale*. II. *Reati contro il patrimonio*, Padova, 2012, pag. 218.

[106] M. Alma, C. Perroni, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, cit., pag. 506.

[107] G. Pica, *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. Pen. Economia*, 1995, pag. 146.

Non è certo, invece, che sia possibile compiere tali condotte in modo omissivo: si ritiene che ciò sia possibile solo al cospetto di un obbligo di intervenire imposto dal legislatore, finalizzato ad evitare il verificarsi dell'evento, in capo all'agente. In altri termini, si ritiene necessaria la sussistenza di una posizione di garanzia[108].

Alla luce di ciò pare opportuno distinguere la frode informatica dall'accesso abusivo a sistema informatico. Tale reato sanziona, come si è visto, chiunque si introduce abusivamente 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.

Diversamente da quanto previsto per la frode informatica, l'accesso abusivo non prevede alcuna manipolazione del sistema, ma esclusivamente un accesso "non autorizzato" dal proprietario dello stesso. Per il configurarsi di tale reato, dunque, è necessario che il reo entri o si mantenga nel sistema senza autorizzazione e soprattutto che si tratti di un sistema oggetto di un accesso protetto. Nella frode informatica, invece, non è richiesto il sistema sia protetto. In come le due fattispecie hanno il fatto che qualcuno agisca attraverso l'uso di software nella vita cibernetica altrui.

2.2. La condotta nell'applicazione della giurisprudenza

Quanto alla condotta di alterazione, la giurisprudenza ha chiarito che integra il reato in esame «l'introduzione, in apparecchi elettronici, per il gioco di intrattenimento senza vincite, di una seconda scheda, attivabile a distanza, che li abilita all'esercizio del gioco d'azzardo, trattandosi dell'attivazione di un diverso programma con alterazione del funzionamento di un sistema informatico»[109].

[108] G. Marini, *Truffa (frode informatica)*, cit., pagg. 148 ss.

[109] Cass. pen., 1° dicembre 2016, n. 54715, in *dejure.it*, secondo cui «risponde del reato di ricettazione chi acquisti una macchina da gioco elettronico il cui sistema telematico sia stato alterato ex art. 640-ter c.p., senza aver concorso nel suddetto reato. Ove, il suddetto soggetto,

E ancora, altra giurisprudenza ha chiarito che «integra il reato di frode informatica l'utilizzazione di sistemi di blocco od alterazione della comunicazione telematica tra apparecchi da gioco del tipo slot-machine e l'amministrazione finanziaria, trattandosi di alterazione dell'altrui sistema telematico, finalizzato all'indebito trattenimento della quota di imposta sulle giocate»[110].

Va segnalato che prima che il legislatore introducesse il reato di frode informatica, tali condotte venivano, non senza difficoltà e forzature, ricondotte nell'ambito della truffa. Si pensi, ad esempio, all'ipotesi di frode nei confronti dell'INPS con riguardo alla condotta di alcuni soggetti che erano riusciti ad entrare nei sistemi informatici dell'ente previdenziale per

successivamente, utilizzi quella macchina, risponde anche del reato di frode informatica posto che la condotta di alterazione del sistema telematico si realizza ogni volta che si attivi il meccanismo fraudolento da altri installato consentendo, quindi, all'agente di procurare a sé un ingiusto profitto con altrui danno».

[110] Cass. pen., 13 settembre 2017, n. 41767, in *dejure.it*. Cfr. anche la più recente Cass. pen., 6 aprile 2018, n. 24634, in dejure.it, secondo cui «integra il reato di frode informatica, previsto dall'art. 640-ter cod. pen., - e non quello di peculato - la modifica di apparecchi elettronici di gioco idonea ad impedire il collegamento con la rete dell'Agenzia monopoli di Stato ed il controllo sul flusso effettivo delle giocate e delle vincite totalizzate, di modo che il titolare della concessione si appropri delle somme spettanti allo Stato a titolo di imposta». Nel caso di specie vi era stata l'alterazione del funzionamento di un sistema informatico, finalizzata a procurarsi fraudolentemente la "percentuale" di danaro, pari al 13,5%, corrispondente al tributo da versarsi allo Stato per ciascuna giocata. Per la configurabilità del delitto di truffa, in caso di fatto commesso senza alterare il sistema telematico di collegamento di tali apparecchi con l'Azienda Autonoma dei Monopoli di Stato, occultando la reale entità delle giocate effettuate, inserendo una scheda "clone" per la loro contabilizzazione, cfr. Cass. pen., 5 aprile 2018, n. 21318, in dejure.it, secondo cui «integra il reato di truffa aggravata ai danni dello Stato, e non quello di peculato o di frode informatica, la condotta dell'amministratore della società gerente apparecchi per le vincite in denaro che, senza alterare il sistema telematico di collegamento di tali apparecchi con l'Azienda Autonoma dei Monopoli di Stato, occulta la reale entità delle giocate effettuate, inserendo una scheda "clone" per la loro contabilizzazione, ed omette di versare all'amministrazione finanziaria le somme dovute a titolo di prelievo unico erariale (PREU), nella misura del 12% degli importi delle giocate». In motivazione, la Corte ha precisato che, «poiché l'imposta va corrisposta con riferimento a ciascun anno solare ed è dovuta anche per le giocate effettuate tramite apparecchi gestiti in assenza di autorizzazione ed estranei alla rete telematica, il denaro incassato all'atto della giocata deve ritenersi interamente di proprietà della società che dispone del congegno, configurandosi alla stregua di un ricavo di impresa sul quale è calcolato l'importo da corrispondere a titolo di debito tributario».

immettere falsi contributi previdenziali, inducendo in errore, con artifizi e raggiri, i funzionari dell'ente previdenziali preposti[111].

Quanto alla condotta di "intervento", in uno dei primi casi in cui è stato punito un intervento su un sistema informatico, i giudici hanno ritenuto che fosse da condannare per frode informatica un dipendente Telecom che, intervenendo sui codici di protezione interni all'azienda, aveva sfruttato gli apparecchi telefonici dell'azienda per effettuare chiamate internazionali. Intervenendo sui dati, infatti, egli era stato capace di disattivare i meccanismi di controllo[112].

La Cassazione ha anche chiarito la differenza tra frode informatica e accesso abusivo ad un sistema informatico, di cui si parlava in precedenza, affermando che «il delitto di accesso abusivo ad un sistema informatico può concorrere con quello di frode informatica, diversi essendo i beni giuridici tutelati e le condotte sanzionate, in quanto il primo tutela il cosiddetto domicilio informatico sotto il profilo dello "ius excludendi alios", anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente

[111] Cfr. Trib. Roma, 20 giugno 1985, in *Diritto dell'informazione e dell'informatica*, 1986, p. 166, secondo cui «*il doppio artificio delle false registrazioni nella memoria magnetica del calcolatore e del* rilascio di false quietanze bancarie nei mod. DM 10/M è idoneo ad eludere, a vasto raggio, l'accertamento automatico delle evasioni; di conseguenza deve ritenersi, nella fattispecie, consumato il reato di truffa aggravata ricorrendone tutti gli elementi essenziali quali: 1) l'artifizio delle false memorizzazioni di denunce contributive mai saldate e la esibizione, nei casi di controllo, dei mod. DM 10/M con le false attestazioni di pagamento; 2) l'induzione in errore di quei dipendenti che erano preposti al controllo del versamento dei contributi e alla esazione degli stessi; 3) l'ingiusto profitto, avendo le aziende per anni evaso il loro obbligo contributivo, che solo un evento eccezionale ha fatto rivivere; 4) il danno per l'Inps, privato della riscossione dei contributi». Cfr. anche Pretura Palermo, 10 giugno 1996, in Diritto dell'informazione e dell'informatica, 1996, p. 962, secondo cui «la cessione al pubblico di informazioni contenute su una banca dati, duplicate senza autorizzazione, è suscettibile di configurare il reato di frode informatica previsto e punito dall'art. 640 ter c.p. sicchè si giustifica ex art. 252 c.p.p. il sequestro dei sistemi e supporti informatici utilizzati per la duplicazione».

[112] Cfr. Trib. Lecce, 12 marzo 1999, in *Foro italiano*, 2, 1999, p. 608, secondo cui «integra il delitto di frode informatica - e non anche quello di accesso abusivo ad un sistema informatico o telematico - la condotta di chi, mediante la digitazione, su apparecchi telefonici collegati a linee interne di una filiale Telecom, di una particolare sequenza di cifre, effettui una serie di chiamate internazionali in danno della Telecom, tenuta a versare agli enti gestori della telefonia nei paesi di destinazione l'importo corrispondente al suddetto traffico telefonico, procurandosi un ingiusto profitto consistente nel ricevere una parte di tali somme da detti enti gestori».

abilitati, mentre il secondo contempla e sanziona l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto»[113].

3. Il phishing come più tipica manifestazione della frode informatica

Diverse sono le modalità di manifestazione delle frodi informatiche: phishing (attività fraudolenta diretta ad indurre la vittima a rivelare informazioni personali grazie ad un'e-mail o ad un sito web), vishing (termine che deriva da "voice" e "phishing", in quanto un attacco di vishing è simile al phishing, solo che si verifica per telefono o tramite messaggio vocale), smishing (ossia una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco, attraverso SMS, da cui il nome "SMiShing").

Tra le tipologie di frode informatica che destano maggiore interesse merita una particolare attenzione, per la sua diffusione nella prassi, il phishing. L'esplosione del fenomeno del c.d. phishing[114] ha messo in luce tutte le difficoltà di adeguamento del diritto penale all'evoluzione dei crimini informatici, al cospetto dei quali, in alcuni casi, lo stesso diritto penale ha mostrato tutte le sue numerose lacune.

Il phishing, in concreto, è un'attività fraudolenta finalizzata ad indurre gli utenti a rivelare informazioni personali e dati sensibili grazie ad un'e-mail o ad un sito web, anche se negli ultimi tempi stanno proliferando i tentativi di phishing tramite social network.

La giurisprudenza ha definito il phishing come «quell'attività in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici e malware) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (user e password) di un utente, codici che, poi, utilizza per frodi informatiche

[113] Cassazione penale sez. V, 19/02/2020, n.17360.

[114] Per la definizione di *phishing*, si v. R. Flor, *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, pagg. 899 ss.

consistenti, di solito, nell'accedere a conti correnti bancari o postali che vengono rapidamente svuotati»[115].

Un esempio tipico di phishing si verifica nel momento in cui l'utente riceve un'e-mail, oppure è portato a cliccare su un link inviato tramite social network o ancora su un banner pubblicitario che viene artificiosamente collocato in applicazioni molto diffuse presso gli utenti.

Si tratta, normalmente, di una notifica che appare proveniente da una fonte o da un sito attendibile, quale una banca, una posta, ecc., ed anche la grafica, nel momento in cui l'utente sprovveduto vi accede, è molto simile a quella del sito ufficiale che vuole emulare, soprattutto agli occhi di un utente assai poco esperto del web.

Il link è sempre diretto ad indurre l'utente a lasciare informazioni personali sul sito, solitamente numeri di carte di credito o di password di accesso ai conti correnti, con l'obiettivo di carpire le informazioni e accedere ai conti riservati dell'utente stesso. Il phishing, dunque, è diretto a violare l'identità digitale del soggetto che, nel corso degli ultimi tempi, ha progressivamente ottenuto grande dignità, tanto da essere considerata a tutti gli effetti come una proiezione dell'identità personale.

Essa può essere considerata, secondo una prima accezione, come un sinonimo dell'identità utilizzata dall'individuo in rete, ossia come una sorta di identità virtuale[116].

Secondo una diversa accezione, ben più ristretta, l'identità digitale è da considerarsi sinonimo di identità informatica, utilizzata nel settore per indicare «l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto. Queste informazioni sono di norma protette da un sistema di autenticazione. L'autenticazione può essere effettuata tramite parola-chiave (password), caratteristiche biologiche

[115] Cass. pen., sez. II, 11 marzo 2011, n. 9861, in *dejure.it*.

[116] In tal senso S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004, pagg. 139 ss.

(iride, impronta digitale, impronta vocale, riconoscimento del volto, ecc.) o attraverso un particolare oggetto (tessera magnetica, smart card, ecc.)»[117].

Va segnalato che la tutela dell'identità digitale risulta essere, oggi, assai problematica. Esse deve giocoforza vertere su due aspetti fondamentali: da un lato la tutela dell'identità personale nella rete, tenendo presente il punto di vista dell'onore e della reputazione; dall'altro, il profilo delle tecniche identificative del soggetto, mediante l'utilizzo di strumenti di carattere telematico.

Trattati di due profili assai diversi, ma allo stesso tempo strettamente collegati tra loro. Si pensi che l'idoneità ad assumere identità multiple in Internet è soggetta alla condizione di poter conservare l'anonimato e, quindi, alla condizione di non essere identificati con quella che è la propria identità reale. Di contro, la legittimazione della protezione dell'identità prescelta, ossia di una vera e propria maschera virtuale come ad esempio si verifica con gli avatar (si pensi al sito Second Life, molto diffuso), come di frequente si verifica con gli pseudonimi, oppure quella del diritto alla pubblicità o di altri diritti in materia di pubblicità intellettuale, lascerebbe presupporre giocoforza una certa stabilità nell'utilizzo dei segni di distinzione che potrebbe essere assicurata mediante sofisticati meccanismi di identificazione[118].

Il phishing è capace di ledere in maniera significativa l'identità digitale del soggetto: del resto è l'etimologia del termine a suggerire la sua capacità lesiva, in quanto l'espressione deriva dall'inglese fishing, che può essere tradotto con "pescare", per indicare, appunto, la caduta nella rete (criminale) non di un pesce, ma di un utente sul web.

Il fenomeno ha cominciato a diffondersi sul finire degli anni Novanta del secolo scorso, parallelamente allo sviluppo della rete, ma nel corso degli

---

[117] Questa la traduzione testuale di quanto riportato da G. Hornung, *Die Digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, Job-Card-Verfahren*, Baden Baden, 2005, pag. 14.

[118] P. Masneri, *Identità personale e identità digitale: nuove regole per tutelare la personalità individuale dalle insidie del web*, su internet all'indirizzo web *http//www.francoabruzzo.it*, 8 gennaio 2008.

ultimi anni ha raggiunto livello di sofisticatezza maggiore, non essendo più diretto solo ed esclusivamente al perseguimento di finalità di carattere economico, ma anche a mettere in allarme i sistemi della sicurezza informativa di enti quali aziende, banche, ecc.
Pare dunque opportuno verificare quali sono le tecniche di attacco di phishing più diffuse.

3.1. Attacco informatico mediante phishing

Il phishing nasce prevalentemente come fenomeno che si concretizza nell'invio di una serie di e-mails esca a potenziali vittime, scelte spesso in maniera casuale da mailing list trovate sul web, con la speranza che qualcuna di esse cada nella rete criminale, lasciando i suoi dati al fine di riuscire ad ottenere informazioni riservate ed approfittarne immediatamente.
Inizialmente, almeno in Italia, il fenomeno era molto circoscritto ed abbastanza grossolano, incapace di creare problemi reali ed effettivi ad un utente anche inesperto: le mails, infatti, erano solitamente scritte in lingua straniera, oppure tradotte in un italiano talmente grossolano da essere incomprensibili e poco pericolose.
A partire dalla seconda metà della prima decade del secolo in corso la situazione è progressivamente cambiata. Le nuove tecniche di diffusione, infatti, prevedono l'invio di e-mails che hanno come referente siti istituzionali accreditati e prestigiosi, come poste, banche ed altri istituti di una certa affidabilità.
Sono solitamente scritte in un italiano impeccabile (o quasi), rimandano a siti assai simili a quelli istituzionali, e colpiscono soprattutto i detentori di conti correnti postali e postepay: la scelta non è affatto casuale, trattandosi dei conti e delle carte prepagate più diffuse soprattutto presso la fascia medio-bassa della popolazione, nella quale i criminali nutrono una maggiore speranza di individuare utenti poco esperti.

Il fenomeno, nel corso degli ultimi tempi, è diventato ancora più pericoloso a causa del fatto che si sono diffusi i c.d. software all inclusive, ossia software caratterizzati da meccanismi di reboot che possono essere agevolmente utilizzati anche da utenti poco esperti, i quali devono semplicemente limitarsi a lanciare il programma e sperare che qualche vittima abbocchi lasciando i propri dati personali riservati[119].

Nel corso degli ultimi tempi, poi, le tecniche di phishing si sono fatte ancora più sofisticate: consapevoli della grossolanità di alcuni tentativi di reindirizzo a siti pseudo-istituzionali, i criminali hanno cominciato ad inviare nelle mails link o programmi scaricabili ad un primo click che, sfruttando la vulnerabilità del computer dell'utente, permettono di acquisire dati personali dello stesso ottenendone vantaggi economici.

Molto spesso, poi, i tentativi di phishing avvengono pubblicizzando sui motori di ricerca prodotti e servizi (individualizzati a seconda delle preferenze dell'utente, sfruttando i famosi cookies) ambiti dall'utente, a prezzi assai vantaggiosi, inducendo l'utente a collegarsi ed a rilasciare i propri dati personali per effettuare l'acquisto.

Un'altra tecnica di phishing che si è diffusa nel corso degli ultimi anni è quella man in the middle, con la quale, sostanzialmente, il phisher si interpone tra l'utente ed un sito legittimo al quale il primo sta rilasciando (o meglio crede di rilasciare) i suoi dati, carpendoli illecitamente. Si tratta di un tipo di attacco molto sofisticato che l'utente difficilmente riesce a scoprire perché è assai poco invasivo rispetto a quelli tradizionali.

[119] Cfr., sul punto, quanto osservato da G.R. Massa, *Il phishing*, in *pmi.it*, 25 gennaio 2008: «dalla metà degli anni 90, periodo in cui ufficialmente ha esordito il phishing, ad oggi, la frode si è notevolmente affinata e diffusa, non limitandosi necessariamente al perseguimento di un lucro pecuniario e investendo tecniche e forme sempre più varie e sofisticate; si parla infatti di phishing tramite email, VoIP, fax, sms etc., varianti che fanno più vittime di ieri grazie anche all'inflazionamento del fenomeno e alla diffusione di kit software "all inclusive" che permettono ai malviventi più inesperti di cimentarsi in tentativi abbastanza credibili di truffa».

Nel corso degli ultimi tempi, poi, si sono diffuse tecniche ancora più evolute: ci si riferisce, in particolare, al pharming[120], ossia una tecnica che consente di manipolare gli indirizzi di DNS utilizzati dall'utente, al fine di fare in modo che le pagine web visitate da quest'ultimo, pur essendo sostanzialmente identiche a quelle originali, sono in realtà pagine fittizie.

3.2. Phishing tra truffa e frode informatica nell'interpretazione della dottrina e della giurisprudenza

Trattandosi di un fenomeno tutto sommato abbastanza recente, l'ordinamento giuridico italiano è stato costretto ad individuare la fattispecie penale più adeguata per dare una risposta al phishing. Non essendovi una fattispecie *ad hoc* che inquadri ed incrimini il fenomeno, esso viene di volta in volta ricondotto dall'interprete alla fattispecie di riferimento, a seconda dell'effettivo modus operandi dell'agente.

Va segnalato, invero, che a seguito della recrudescenza del fenomeno, a partire dal 2005, molto si è discusso, anche in Parlamento, in ordine all'opportunità di introdurre una norma ad hoc in grado di incriminare il phishing e, in generale, tutte quelle azioni ingannevoli poste in essere sul web con tecniche affini al phishing stesso[121].

---

[120] Sulla quale si v. A.G. Imbesi, *Phishing and pharming on the net*, in *Il Nuovo diritto*, 7-8, 2006, p. 797 ss.

[121] In una interrogazione parlamentare del 5 dicembre 2006, l'onorevole Urso sottolineava che «in Italia, inoltre, desta particolare preoccupazione l'incremento delle segnalazioni che lamentano l'invio di e-mail riconducibili al fenomeno denominato phishing, consistente nell'uso di messaggi di posta elettronica e nella creazione di pagine web progettate per simulare comunicazioni ufficiali da parte soprattutto di istituti di credito, con la finalita` di raggirare gli ignari utenti internet e carpire loro dati personali o acquisire fraudolentemente informazioni riguardanti la carta di credito (numero, scadenza, codice numerico) o il conto corrente bancario»: Camera dei Deputati, Resoconto stenografico seduta n. 82 del 5 dicembre 2006. Cfr. anche Camera dei Deputati, Resoconto stenografico seduta n. 100 del 30 gennaio 2007, secondo cui «è da tempo in atto da parte della criminalità organizzata una subdola azione di truffa telematica mediante l'invio di false (ma verosimili) e-mail, con le quali in realtà si carpiscono a ignari risparmiatori le password di accesso ai propri conti correnti bancari, propedeutiche alla successiva rapina telematica; tale insidiosa e non facilmente identificabile azione di phishing sembrava essere stata sufficientemente denunciata alla pubblica opinione, messa in grado di proteggersi mediante la divulgazione, attraverso organi

Resta il fatto che, nonostante le discussioni intervenute, il fenomeno non è mai stato regolamentato, lasciando all'interprete il compito di individuare la norma più idonea. A tal proposito, appare indispensabile distinguere le diverse fasi del phishing, la prima in cui vi è l'invio dei messaggi di posta elettronica che contengono i link di indirizzamento alle pagine "esca", la seconda in cui vengono raccolti i dati personali della vittima e la terza in cui questi dati vengono utilizzati per accedere indebitamente ai conti correnti, alle carte di credito e in generale a tutti i profili dell'utente.

Per quanto concerne la prima fase del phishing, parte della dottrina[122] ha ipotizzato l'applicabilità dell'art. 494 c.p., che sanziona la sostituzione di persona: tale disposizione, in particolare, punisce «chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno».

Tale fattispecie potrebbe essere applicata nel caso in cui vengano utilizzati via web i dati di un mittente reale, integrando dunque le modalità tassativamente previste dall'art. 494 c.p. Anche nel corso della terza fase, invero, è possibile astrattamente applicare tale disposizione, in quanto si accede a dati altrui con un profilo altrui.

Parte della giurisprudenza si è espressa in tal senso, non considerando di ostacolo all'applicazione della fattispecie in esame la presenza dello

di stampa e televisivi, di consigli di difesa a favore dei cittadini possessori di conti correnti on line, e, soprattutto, sembrava stroncata ad opera della competente polizia postale; ciononostante, a tutt'oggi, risulta all'interrogante che e-mail trabocchetto, perfettamente simili a quelle della banca di riferimento, continuano impunemente ad essere inviate a cittadini incolpevoli e non sempre in grado – magari per motivi di età – di difendersi adeguatamente –: se non intenda verificare i risultati dell'azione di prevenzione intrapresa dalla polizia postale, in particolare con la predetta campagna anti-phishing, e quali iniziative intenda assumere e in che tempi, ove il pericolo risultasse persistente, per debellare alla fonte la predetta azione delittuosa dei pirati informatici».

[122] Cfr., in particolare, V. Di Lembo, *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, pagg. 11 ss.

strumento informatico, privilegiando, piuttosto, la lesione della pubblica fede in considerazione della capacità, delle informazioni diffuse sul *web*, di raggiungere una platea potenzialmente sterminata di persone: «oggetto della tutela penale è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la stretta cerchia di un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome. […] nel caso in esame il soggetto indotto in errore non è tanto l'ente fornitore del servizio di posta elettronica, quanto piuttosto gli utenti della rete i quali, ritenendo di interloquire con una determinata persona, in realtà inconsapevolmente si sono trovati ad avere a che fare con una persona diversa»[123].

Parte della dottrina[124], tuttavia, ha criticato questa impostazione, per diversi motivi. Si è sostenuto, anzitutto, che inviare *mails* che richiamano siti e mittenti reali non significa necessariamente sostituirsi a questi ultimi; in secondo luogo, utilizzare credenziali di autenticazione per accedere ad un sistema informatico non corrisponderebbe all'attribuzione in un falso nome, un falso stato o una qualità cui la legge attribuisce effetti giuridici ai sensi dell'art. 494 c.p.[125]

---

[123] Cass. pen., 11 luglio 2014, n. 25774, in *dejure.it.*

[124] Cfr. P. Cipolla, *"Social network", furto di identità e reati contro il patrimonio*, in *Giur. mer.*, 12, 2012, pagg. 2672 ss.

[125] Altra dottrina, tuttavia, ha ritenuto che tali argomentazioni siano potenzialmente aggirabili, «distogliendo l'attenzione dall'elaboratore elettronico e ripiegando sulla persona fisica effettivamente tratta in inganno. Invero, considerando il sistema informatico semplicemente come strumento dell'attività illecita e, in quanto tale, astrattamente assimilabile ad una missiva cartacea, una telefonata o ad un qualsiasi altro espediente, ne consegue che l'evento consumativo del reato di sostituzione di persona appare a tutti gli effetti sussistente: l'agente trae in inganno l'ignaro utente della rete, destinatario ad esempio di un messaggio inviato per posta elettronica, sostituendosi al legittimo mittente grazie all'utilizzo fraudolento dei suoi elementi distintivi quali il logo, il marchio, lo stile, i colori di scrittura e il nome. Pertanto delle due condotte che caratterizzano l'art. 494 c.p. la prima – l'induzione «di taluno in errore, sostituendo illegittimamente la propria all'altrui persona» – può considerarsi indipendente ed autonomamente rilevabile dalla seconda, in quanto non necessita di essere integrata anche dagli estremi dell'attribuzione di un falso nome, o un falso

In generale, comunque, quello che più lascia perplessi è il fatto che obiettivo principale di chi compie atti di phishing è quello di ottenere un vantaggio patrimoniale, mentre l'inganno della vittima è solo una conseguenza inevitabile, ma non il fine principale, come invece si verifica nell'ipotesi della sostituzione di persona.

Per tale ragione, altra parte della dottrina[126] ha proposto di ricondurre il *phishing* alla truffa ed all'accesso abusivo al sistema informatico, soprattutto con riguardo alla seconda fase, quella in cui i dati della vittima vengono abusivamente carpiti.

Anche parte della giurisprudenza ha sposato questa impostazione, ritenendo che «chi avvalendosi delle tecniche del c.d. phishing, mediante artifici e raggiri realizzati attraverso l'invio di false e-mail e la creazione di false pagine web in tutto simili a quelle di primari istituti di credito, dopo aver indotto in errore l'utente ed essersi fatto rivelare le credenziali di accesso, si introduca nel servizio di home banking della vittima per effettuare operazioni di prelievo o bonifico online non autorizzate risponde dei delitti di sostituzione di persona (art. 494 c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), truffa (art. 640 c.p.)»[127].

Con riguardo all'applicabili dell'accesso abusivi al sistema informatico, effettivamente, non paiono esserci molti dubbi. Diverso invece il discorso con riguardo alla truffa. Gli artifizi e raggiri vengono solitamente individuati nel ricorso ad *e-mails* intestate nelle quali vengono riprodotte in maniera pressoché pedissequa e con grandi abilità loghi, colore, marchi ed altre caratteristiche tipici di siti istituzionali ed affidabili.

In tal senso si è espresso parte della giurisprudenza, sottolineando che il phishing rientra nella truffa e non nella frode informatica: «integra il delitto

---

stato, ovvero una qualità a cui la legge attribuisce effetti giuridici»: F. Capone, *Le problematiche di disciplina dei phishing attacks*, in *Cyberlaws.it*, 21 settembre 2018.

[126] Cfr. G. Modesti, *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali*, in *Ragiusan*, 335-337, 2012, pagg. 328 ss.

[127] Trib. Milano, 7 ottobre 2011, in *dejure.it*.

di truffa, e non quello di frode informatica, il conseguimento di un ingiusto profitto ottenuto attraverso l'invio di e-mail contraffatte nel mittente e tramite siti civetta (c.d. phishing) finalizzato al conseguimento di credenziali per il dirottamento dei fondi degli utenti di siti di home banking su carte prepagate o conti nella disponibilità di un'organizzazione criminale»[128].

Questa interpretazione, che si fonda su una interpretazione letterale del disposto di cui all'art. 640 c.p., è stata criticata dalla dottrina prevalente[129], secondo cui è indispensabile, per il configurarsi della truffa, che l'atto di disposizioni patrimoniale sia realizzato dalla vittima e non dal soggetto che realizza gli artifizi e i raggiri, mentre nel caso di specie è quest'ultimo che utilizza poi i dati personali.

Per tale ragione, si ritiene che il phishing rientri nell'ambito della frode informatica. In tal senso si è espressa anche la giurisprudenza, secondo cui «in molti attacchi di phishing sussistono gli estremi del delitto di frode informatica allorquando, ad esempio, si ponga in essere una condotta di alterazione in qualsiasi modo del sistema informatico o telematico con l'installazione fraudolenta di un malware o di un trojan horse in grado di funzionare in background e carpire in tal modo i dati, ovvero, intervenendo senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico si effettui, successivamente alla captazione fraudolenta delle informazioni altrui, operazioni di home banking o acquisti online»[130].

Per il configurarsi della frode informatica è sufficiente che sia stato manipolato il computer o il sistema telematico e che tale manipolazione permetta all'agente di acquisire quei dati fondamentali per ottenere un vantaggio patrimoniale in danno della vittima. In tal caso, il delitto sarà

[128] Trib. Milano, 10 dicembre 2007, in *dejure.it*.

[129] Cfr. F. Agnino, *Computer crime e fattispecie penali tradizionali: quando il phishing integra il delitto di truffa. Nota a Trib. Milano 29 ottobre 2008*, in *Cor. Mer.*, 3, 2009, pagg. 288 ss.

[130] Cass. pen., sez. II, 24 febbraio 2011, n. 9891, in *dejure.it*.

commesso in concorso con la sostituzione di persona, in quanto l'azione è illecita proprio in quanto realizzata da una persona che non è legittimata a farlo.

Si è osservato, comunque, che non è possibile escludere che vi siano anche gli estremi per la truffa: «vi sarà in questo caso una contestazione caratterizzata da uno spazio d'intervento residuale, essendo riscontrabile nelle ipotesi di *deminutio patrimonii* realizzate con artifizi e raggiri»[131], ma senza manipolazione o intervento non autorizzato con riguardo ad un sistema telematico o informatico.

In tal senso si è espressa anche parte della giurisprudenza, secondo cui «il phisher si rende responsabile anche del delitto di truffa, di cui ricorrono tutti gli elementi costitutivi: l'artificio o il raggiro, consistente, appunto, nell'invio di false e-mail e nella creazione di false pagine web; l'errore in cui cade il destinatario della mail, il quale ritiene provengano dalla banca di cui è cliente, così fornendo inconsapevolmente i dati di accesso del proprio conto corrente; l'ingiusto profitto con correlativo altrui danno, rappresentato dalle somme di denaro illecitamente sottratte dal conto corrente della vittima»[132].

Va segnalato, in conclusione, che, a seguito dell'entrata in vigore del d.lgs. n. 93/2013, è entrata in vigore l'aggravante ad effetto speciale del delitto di frode informatica, che sanziona con la pena «della reclusione da due a sei anni e della multa da euro 600 a euro 3.000» la frode informatica commessa con «furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti». Con l'introduzione di tale aggravante il legislatore ha voluto apprestare una tutela maggiore alle vittime di truffe e sottrazione di dati sensibili *online*: tale novella normativa sembra anzi essere stata introdotta soprattutto per colpire il phishing, almeno laddove esso si concretizzi nella sottrazione di dati dal computer della vittima.

[131] F. Capone, *Le problematiche di disciplina dei phishing attacks*, cit.
[132] Trib. Milano, 7 ottobre 2011, cit.

Del resto, l'invio massimo di mail, la produzione di virus da inviare alle vittime e tutte le altre condotte tipiche del phishing sono sicuramente attività propedeutiche a quel «furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti» richiesto dal legislatore per il perfezionamento dell'aggravante in parola.

È evidente, in conclusione, come ciò consente una contestazione che appare assai più coerente con le caratteristiche dell'offesa e una cornice sanzionatoria più adeguata rispetto al disvalore della condotta. Non si tratta, infatti, di due reati commessi in concorso, né, tantomeno, di una truffa sic et simpliciter, ma di un'offesa che aggredisce un unico bene giuridico, dunque un unico reato commesso facendo ricorso a modalità particolarmente subdole e insidiose che richiedono una maggiore severità[133].

Tale aggravante, in definitiva, consente di dare una risposta sanzionatoria più adeguata in quanto risulta essere maggiormente calata nel fenomeno del phishing.

4. Il profitto ingiusto

Il profitto costituisce un altro elemento della struttura della frode informatica. La prima questione che rileva, specularmente ai problemi che reca il concetto di danno, è se esso debba essere inteso necessariamente in senso economico o meno. La giurisprudenza ha inteso il profitto in senso molto ampio, sostenendo che non necessariamente esso deve tradursi in termini meramente economici.

[133] F. Capone, *Le problematiche di disciplina dei phishing attacks*, cit., secondo cui «il delitto di sostituzione di persona potrà allora trovare applicazione residuale in tutti quei casi nei quali la sottrazione o l'utilizzo fraudolento di informazioni altrui avvenga al fine di procurare a sé o ad altri un vantaggio di qualsiasi altra natura, recando contemporaneamente offesa alla fede pubblica, connotata da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi speciali. Poiché si tratta di artifizi che possono superare la ristretta cerchia di un determinato destinatario, il legislatore ha ravvisato in essi una costante minaccia alla fede pubblica e non soltanto alla fede privata o alla tutela civilistica del diritto al nome».

La Cassazione, in particolare, ha evidenziato proprio, sotto tale profilo, la differenza tra profitto e danno (con riguardo al delitto di truffa, ma le considerazioni sono analoghe anche con riguardo al delitto di frode informatica): «nel delitto di truffa, mentre il requisito del profitto ingiusto può comprendere in sé qualsiasi utilità, incremento o vantaggio patrimoniale, anche a carattere non strettamente economico, l'elemento del danno deve avere necessariamente contenuto patrimoniale ed economico, consistendo in una lesione concreta e non soltanto potenziale che abbia l'effetto di produrre - mediante la "cooperazione artificiosa della vittima" che, indotta in errore dall'inganno ordito dall'autore del reato, compie l'atto di disposizione - la perdita definitiva del bene da parte della stessa; ne consegue che in tutte quelle situazioni in cui il soggetto passivo assume, per incidenza di artifici e raggiri, l'obbligazione della dazione di un bene economico, ma questo non perviene, con correlativo danno, nella materiale disponibilità dell'agente, si verte nella figura di truffa tentata e non in quella di truffa consumata»[134].

Bisogna, tuttavia, considerare che il profitto non è sempre e comunque l'esatta conseguenza del danno, ben potendo sussistere un danno e non un profitto, e viceversa: al giudice, in ogni caso concreto, spetta il compito di verificare che, effettivamente, sussistano entrambi gli elementi[135]. La giurisprudenza, dunque, accoglie una nozione molto estesa di profitto, non limitandolo all'aspetto meramente patrimoniale, ma a qualsiasi altra utilità o situazione di vantaggio che sia propedeutica al conseguimento di un successivo vantaggio di natura economica.

Addirittura, la Cassazione ha sostenuto che il profitto può anche essere morale o psicologico[136]. Parte della dottrina[137], tuttavia, ha criticato questa impostazione, in quanto anche il profitto dovrebbe essere inteso o come un

[134] Cass. pen., 19 gennaio 1999, n. 1, in dejure.it.
[135] Cfr. G. Fiandaca, E. Musco, *Diritto penale. Parte speciale*. II. *Reati contro il patrimonio*, cit., pag. 75.
[136] Cfr. Cass. pen., 2 maggio 1959, n. 2214, in *dejure.it*.
[137] Cfr. G. Fiandaca, E. Musco, *Diritto penale. Parte speciale*. II. *Reati contro il patrimonio*, cit., pagg. 183 ss.

aumento di ricchezza effettivo, o comunque come una omessa riduzione della stessa, e non come un vantaggio morale o psicologico.

Cerca di conciliare le posizioni estreme Mantovani[138], il quale, per un verso, critica l'idea di un profitto anche solo morale o spirituale, in quanto, in tal modo, sarebbe del tutto dematerializzato il requisito in esame, che, invece, già dal punto di vista etimologico, è strettamente connesso ad una idea di accrescimento patrimoniale; in secondo luogo, sarebbe eccessivamente allargato l'ambito della punibilità, che finirebbe con il ricomprendere fatti che, per il loro minimo disvalore, non dovrebbero rientrare nella sfera del penalmente rilevante, ma essere sanzionati esclusivamente nelle forme dell'illecito civile; in terzo luogo, una interpretazione siffatta finirebbe con lo svuotare del tutto di significato il requisito del profitto, ritenendolo coincidente con il movente dell'azione, e, dunque, sostanzialmente, si tratterebbe di un vero e proprio profitto *in re ipsa*.

Per altro verso, tuttavia, Mantovani sostiene che anche l'interpretazione opposta, che privilegia un profitto in termini esclusivamente economici, presenta qualche rilievo critico, in quanto una interpretazione del genere tende ad escludere la sussistenza del profitto anche quando si verifichi un incremento strutturale del patrimonio, anche se non di carattere economico. L'idea di Mantovani, in definitiva, è che il profitto coincida con ogni incremento della capacità strumentale del patrimonio in grado di soddisfare un bisogno umano, materiale e spirituale.

Il profitto deve essere ingiusto: in tal senso si è espressa la giurisprudenza, secondo cui «ai fini dell'applicazione del 640 ter, si richiede che il profitto sia stato realizzato attraverso una ingiusta modalità di ottenimento, dovendosi intendere che il soggetto si sia mosso in un ambito di illiceità, che abbia cioè

[138] Cfr. F. Mantovani, *Diritto penale. Parte Speciale*, II. *Reati contro il patrimonio*, cit., pagg. 43 ss.

agito in posizione di contrarietà rispetto all'ordinamento giuridico traendo una utilità che non gli era dovuta per legge»[139].

Questo orientamento è stato criticato da una parte della dottrina secondo cui in tal modo si estenderebbe in maniera eccessiva l'ambito di applicazione della fattispecie, facendovi rientrare anche comportamenti diretti ad ottenere un profitto non dovuto secondo la legge, ma tuttavia non illecito e nemmeno contrario all'ordinamento giuridico.

In particolare, si è fatto l'esempio delle obbligazioni naturali «le quali, come tutti sanno, se non autorizzano l'azione giudiziaria per l'adempimento, tuttavia escludono la facoltà di ripetere quanto sia stato spontaneamente prestato in esecuzione di esse»[140].

Di recente, comunque, la Cassazione ha ribadito che «il reato si consuma nel momento in cui l'agente consegue l'ingiusto profitto, con correlativo danno patrimoniale altrui, e che il carattere dell'ingiustizia è attribuito al profitto per il fatto di essere realizzato sine jure, tanto che l'arricchimento in cui esso si risolve, risulta conseguito sine causa»[141].

L'ingiustizia del profitto, tuttavia, non va confusa con l'ingiustizia della condotta, per cui l'attività di accertamento del giudice deve essere diversa, finalizzata ad accertare prima l'ingiustizia della condotta e poi quella del profitto, pena una interpretazione sostanzialmente abrogatrice del requisito in esame, come testimonia un risalente precedente giurisprudenziale. La Cassazione[142], infatti, in una pronuncia che poi, non a caso, è rimasta isolata, dopo aver premesso che la *ratio* della frode informatica non è solo la tutela del patrimonio ma anche quella della libertà del consenso, ha ritenuto sussistente il reato in ogni circostanza in cui la frode posta in essere dalla parte leda la libertà del consenso altrui.

---

[139] Cass, pen., 30 marzo 2009, n. 6477, in *dejure.it*.
[140] F. Antolisei, *Diritto penale. Parte speciale*. I, *Delitti contro il patrimonio*, Milano, 1966, pag. 194.
[141] Cass. pen., 14 dicembre 1999, p. 11257, in *dejure.it*.
[142] Cass. pen., 20 marzo 1964, n. 1142, in *dejure.it.*

Secondo la Corte, infatti, in un caso del genere, essendo stato perseguito con una condotta illecita, il profitto dovrebbe giocoforza essere considerato anch'esso illecito. Superato questo remoto precedente, oggi dottrina[143] e giurisprudenza sono abbastanza concordi sulla nozione di ingiustizia che deve riguardare il profitto: ingiusto non è solo quel profitto generato dalla percezione di utilità *contra ius*, ma anche *sine iure*, ossia prive di meritevolezza secondo l'ordinamento giuridica.

Manzini, in particolare, sebbene con riguardo al delitto di truffa, ha ritenuto non configurabile tale reato «se il profitto, ancorché ottenuto fraudolentemente, risulti oggettivamente legittimo. Per aversi questa legittimità obiettiva è necessario che l'agente avesse diritto a ottenere la prestazione o l'equivalente. In tal caso neppure può sussistere il delitto di esercizio arbitrario di ragioni, per mancanza del requisito della violenza reale o personale o della minaccia. Ma, per ammettere la legittimità del profitto ed eliminare la truffa, occorre necessariamente che rimanga esclusa l'ingiustizia del danno; e ciò importa che il diritto, che l'agente ha fatto valere con l'uso dei mezzi propri della truffa, sia da lui preteso ed esercitato in rapporto a chi gli doveva la prestazione di cui si tratta. Se invece egli, per conseguire ciò che giuridicamente gli spetta, danneggia un terzo, la truffa sussiste, perché ad un danno evidentemente ingiusto, non può corrispondere che un ingiusto profitto»[144].

In poche parole, dunque, una azione fraudolenta, finalizzata a realizzare una pretesa che si atteggia astrattamente come giusta, ma nei confronti di un soggetto non tenuto a fornire all'agente l'utilità avuta di mira, diviene di per sé soggettivamente ingiusta ed idonea a perfezionare il delitto di truffa. La giurisprudenza condivide l'impostazione della dottrina, sostenendo che l'ingiustizia del profitto va valutata al momento in cui l'agente consegue la disponibilità di beni altrui, e che in tal caso il profitto deve essere considerato

[143] Cfr. sul punto U. Lucarelli, *La truffa*, Padova, 2002, pagg. 87 ss.
[144] V. Manzini, *Trattato di diritto penale italiano*, cit., pag. 732.

ingiusto nel momento in cui l'agente consegue ciò che non è dovuto e che lo stesso non può ritenere come a lui dovuto[145].

La Cassazione ha statuito che «il requisito della "ingiustizia" del profitto, termine di qualificazione dell'evento riflettentesi nel dolo dell'agente, avendo natura di elemento normativo integrativo della fattispecie, va individuato aliunde in modo autonomo rispetto all'illiceità del fatto offensivo, essendo già frutto della scelta di repressione penale della condotta criminosa - mediante le altre indicazioni dell'ordinamento extrapenale. L'ingiusto profitto va ravvisato quando un vantaggio, un'utilità o un incremento patrimoniale (che, nei reati nei quali è previsto come elemento costitutivo anche il danno, rappresenta concettualmente sul versante del soggetto attivo l'aspetto speculare dell'arricchimento ingiusto, in una un'accezione economica - conseguito dall'autore a fronte del pregiudizio subito dalla vittima)»[146].

Oltre il profitto ingiusto, il legislatore richiede, per il perfezionamento della frode informatica, anche il configurarsi di un danno. Sussistono, tuttavia, due diverse concezioni del danno, una economica ed una giuridica. La concezione giuridica, che è invero minoritaria, ricalca la nozione di patrimonio in senso giuridico, come mera somma di rapporti giuridici relativi ai beni di pertinenza di un soggetto: in tale prospettiva, il danno si concretizza nella perdita di un diritto o nella assunzione di un obbligo[147].

L'opinione prevalente, tuttavia, è quella che attribuisce rilevanza ad una nozione economica di danno, in quanto l'accettazione di una nozione giuridica "altererebbe" la struttura della frode, rendendola non più un delitto lesivo del bene patrimonio, ma di un bene diverso, ossia semplicemente della libertà di disposizione del soggetto passivo[148].

---

[145] Cass. pen., 5 novembre 1969, n. 10558, in *dejure.it.*

[146] Cass. pen., 13 novembre 2009, n. 43347, in *dejure.it.*

[147] Su tale interpretazione si v. Cass. pen., 15 giugno 1982, in *Foro it.*, Rep. 1984, s.v. Truffa, n. 7.

[148] Così G. Fiandaca, E. Musco, *Diritto penale. Parte speciale.* II. *Delitti contro il patrimonio*, cit. pagg. 178 ss.

L'adesione ad una concezione piuttosto che ad un'altra non è priva di conseguenze sul piano pratico: aderendo alla concezione economica, infatti, il danno rilevante sotto il profilo giuridico sarebbe unicamente quello che fa riferimento al patrimonio in senso stretto, ad eccezione di altre valutazioni di carattere meramente soggettivo come quelle relative all'utilità individuale di una determinata prestazione oppure al valore effettiva che può attribuire una persona a una cosa.

Aderendo alla concezione giuridica, invece, avrebbero rilevanza giuridica anche gli affetti e, in generale, tutti quei profili psichici che solitamente legano le persona a determinati beni. Secondo questa impostazione, infatti, sarebbe del tutto irragionevole non considerare il valore di affezione, giacché è lo stesso diritto penale ad essere finalizzata alla tutela della persona umana e solo in via strumentale alla salvaguardia del patrimonio da intendersi nella sua dimensione economica.

Pertanto, la ratio della disposizione in esame dovrebbe riposare nell'ingiustizia della condotta, capace di incidere su posizioni giuridiche costituzionalmente tutelate, per cui la protezione della dignità della persona, «non vi potrebbe essere tutela della persona umana negando rilevanza giuridica al c.d. valore di affezione»[149].

Nonostante l'opinione prevalente sia indubbiamente quella che considera il danno in una prospettiva economica, alcuni studiosi hanno avvertito l'esigenza di apportare alcuni correttivi, al fine di evitare alcune aporie: Heinitz[150], in particolare, ha optato per la valorizzazione di criteri di tipo soggettivo per valutare il danno, ponendo l'accento sull'utilità personale della controprestazione per il soggetto passivo, arrivando a sostenere che in alcune ipotesi è possibile prescindere dalla sussistenza di un effettivo danno economico, sempre che, ovviamente, vi sia l'ingiusta perdita di un diritto.

---

[149] L. Viola, *Ingiusto profitto e danno altrui nella cd. truffa contrattuale*, in *Diritto&Diritti*, settembre 2003.

[150] Cfr. H. Heinitz, *Il danno patrimoniale nella truffa*, in *Archivio penale*, 1953, pagg. 365 ss.

Una questione che è strettamente dipendente dalla diatriba concezione economica/giuridica del danno attiene alla possibilità di considerare un danno penalmente rilevante la mera assunzione di obbligazioni, oppure se anche in tal caso è necessario comunque che si verifichi un pregiudizio economicamente rilevante.

La giurisprudenza prevalente[151], tuttavia, sostiene che il danno debba essere effettiva, e che quindi non è sufficiente una mera assunzione di obbligazioni. Anche la dottrina[152] è convinta di questa soluzione, in quanto, diversamente, la truffa si trasformerebbe da reato di danno in reato di pericolo. Il danno comprende sia il danno emergente che il lucro cessante.

Parte della dottrina[153] ha sostenuto che il danno vada personalizzato, attraverso il ricorso a criteri di tipo oggettivo, per cui oggetto della truffa potrebbero essere anche beni che hanno un valore puramente affettivo e non economico, avuto riguarda alla situazione concreta in cui versa il proprietario. Questa impostazione è stata tuttavia criticata da altra dottrina[154], che non concorda con l'idea di una soggettivazione del danno, che esporrebbe il diritto penale ai capricci dei singoli individui

5. L'elemento soggettivo

L'elemento soggettivo richiesto per la configurazione della fattispecie non pone particolari problemi, trattandosi di un dolo generico, in particolare è richiesta la coscienza e volontà di realizzare le condotte richieste dalla norma con l'obiettivo di procurare a sé o ad altri un ingiusto profitto con conseguente danno a carico della vittima.

---

[151] Cfr. Cass. pen., 13 maggio 2003, in *Guida al diritto*, 2003, p. 79 ss.
[152] Così G. Fiandaca, E. Musco, *Diritto penale. Parte speciale.* II. *Delitti contro il patrimonio*, cit., pagg. 369 ss.
[153] In tal senso F. Antolisei, *Manuale di diritto penale*, cit., pagg. 362 ss.
[154] Cfr. Così G. Fiandaca, E. Musco, *Diritto penale. Parte speciale*. II. *Delitti contro il patrimonio*, cit., pagg. 180 ss.

6. Le circostanze aggravanti

Per quanto concerne, invece, le circostanze aggravanti, esse sono previste dai commi 2 e 3 dell'art. 640 ter c.p. Per quanto riguarda, anzitutto, il comma 2, esso disciplina due ipotesi: a) l'ipotesi in cui la frode informatica sia posta in essere a danno dello Stato o di altro ente pubblico, con l'obiettivo di esonerare qualcuno dal servizio militare; b) l'ipotesi in cui la frode informatica sia realizzata abusando delle qualità di operatore del sistema informatico.

Quanto all'ipotesi sub a), la giurisprudenza ha chiarito che «l'elemento distintivo tra il delitto di peculato e quello della frode informatica aggravata ai danni dello Stato è costituito dalle modalità di possesso del denaro o d'altra cosa mobile altrui oggetto di appropriazione, ricorrendo il reato di peculato se il pubblico ufficiale o l'incaricato di pubblico servizio se ne appropri avendone già il possesso o comunque la disponibilità per ragione del suo ufficio o servizio, ricorrendo, al contrario, la frode informatica allorché il soggetto agente, non avendo tale possesso, se lo procuri fraudolentemente, facendo ricorso ad artifici o raggiri per procurarsi un ingiusto profitto con altrui danno»[155].

Sempre con riguardo a tale prima ipotesi, in alcune circostanze è possibile anche una responsabilità dell'ente a danno del quale la frode informatica è stata realizzata, almeno in presenza dei presupposti per la responsabilità dell'ente di cui al d.lgs. n. 231/2001.

Ancora, sempre in presenza di tali circostanze l'art. 640 *quater* c.p. impone la confisca obbligatoria dei beni che sono stati ottenuti come prezzo o profitto del reato. Ci si chiede se alla stessa conclusione deve giungersi anche in presenza di entrambe le circostanze aggravanti. La giurisprudenza ha risposto positivamente a tale quesito[156].

[155] Cass. pen., 10 aprile 2013, n. 18909, in *Diritto penale e processo*, 6, 2013, p. 649.
[156] Cfr. Cass. pen., 11 marzo 2009, n. 16669, in *dejure.it*.

Per quanto riguarda, invece, la seconda circostanza aggravante, che prevede l'aumento di pena per chi abusa della sua qualità di operatore del sistema, la *ratio* è piuttosto evidente: si vuole infatti responsabilizzare chi ricopre un ruolo così importante e che, dunque, più di ogni altro ha la possibilità di alterare o intervenire sui sistemi informatici.

Si è osservato, in particolare, che l'operatore si viene a trovare in una «particolare pericolosità sociale in considerazione del suo rapporto privilegiato con il sistema»[157].

La giurisprudenza ha applicato questa circostanza nell'ipotesi in cui l'imputato, dopo aver abusivamente acquisito una password di un terzo, nel caso di specie responsabile di zona di una compagna assicurativa, ha attuato un'alterazione dei dati del sistema, elaborando, in tal modo, delle attestazioni fasulle finalizzate ad ottenere, in maniera del tutto illecita e indebita, delle somme di denaro a titolo di risarcimento del danno[158].

Del resto l'operatore del sistema, abusando della sua qualità, rompe anche un rapporto di fiducia e di fedeltà nei confronti del titolare del sistema informatico, oltre che procurargli un grave danno economico considerato che l'archivio informatico custodisce normalmente dati molto rilevanti dal punto vista economico per i terzi.

Non è chiaro, tuttavia, cosa si intenda per operatore del sistema, trattandosi di un'espressione molto generica e vaga. Pare dunque opportuno partire dalla *ratio* della norma, intesa a punire chiunque, per la sua posizione, è titolare di un accesso al sistema informatico ed è dotato di particolari competenze che lo rendono operatore dello stesso.

Secondo una parte della dottrina[159], invero, operatore del sistema sarebbe qualunque tecnico che ha il titolo per operare sul computer; secondo un

---

[157] Cfr. R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti, *Profili penali dell'informatica*, Milano, 1994, pagg. 39 ss.

[158] Cfr. Cass. pen., 11 novembre 2009, n. 11447, in *dejure.it*.

[159] Cfr. R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti, *Profili penali dell'informatica*, cit., pag. 27.

diverso orientamento, invece, assumerebbe rilevanza «la posizione del tecnico che abbia il controllo su varie fasi di elaborazione dei dati, escludendo sia del semplice operatore addetto a funzioni meramente esecutive sia del programmatore che possiede solo una conoscenza settoriale dei dati relativi alla macchina»[160].

Un orientamento intermedio[161], invece, che appare preferibile, ha interpretato l'espressione in maniera funzionale, ritenendo che il legislatore abbia inteso fare riferimento a tutti coloro che sono legittimati ad operare nel sistema e che sono dotati delle competenze e delle qualifiche professionali e specifiche rispetto ad un qualunque altro operatore del sistema.

Infine, il comma 3 dell'art. 640 *ter* c.p., introdotto dall'art. 7 del d.l. 14 agosto 2013, n. 93, convertito in legge 15 ottobre 2013, n. 119, ha disciplinato una ulteriore ipotesi, a commissione del fatto con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti, prevedendo una pena della reclusione da due a sei anni e della multa da euro 600 a euro 3.000. La *ratio* di tale aggravante è quella di inasprire il trattamento sanzionatorio in tutti quei casi in cui l'alterazione o l'intervento in un sistema informatico altrui avviene attraverso un furto dell'identità digitale della vittima[162].

A tal proposito la giurisprudenza ha chiarito che «integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, essendogli stata revocata la delega ad operare sul conto corrente on line, attraverso l'utilizzazione dei codici di accesso telematici

[160] G. Pomante, *Internet e criminalità*, Torino, 1999, pag. 11.
[161] F. Mucciarelli, *Commento all'art.10 della legge 547 del 1993*, cit., pag. 102.
[162] Va segnalato che il testo originario del decreto legge faceva riferimento alla "sostituzione dell'identità digitale", espressione considerata ambigua, poiché «formalmente evoca, piuttosto che l'indebito utilizzo dell'identità, la sua surrogazione con altra al fine di accedere ai dati raggiungibili con quella sostituita e cioè fattispecie diversa e ben più specifica di quella ipotizzata in precedenza, ma di dubbia rilevanza»: L. Pistorelli, *Relazione dell'Ufficio Massimario della Corte di Cassazione*, n. III/1/2013.

penetri abusivamente nel sistema informatico bancario ed effettui la ricarica del telefono cellulare»[163].

7. La confisca obbligatoria

L'art. 640 quater c.p., nel richiamare le disposizioni contenute nell'art. 322 ter c.p.[164], dispone l'obbligatoria confisca dei beni che sono il profitto e/o il prezzo della frode informatica realizzata ai danni dello Stato, prevista dal n. 2 dell'art. 640 ter c.p., fatta eccezione per l'aggravante che si riferisce a chi è operatore del sistema.

Ancora, è prevista un'altra ipotesi di confisca obbligatoria, introdotta dall'art. 1 della legge 15 febbraio 2012, n. 12, che, per effetto dell'inserimento, all'interno del comma 2 dell'art. 240 c.p., del n. 1 bis, ha disposto l'obbligatoria confisca dei beni e degli strumenti, sia informatici che

[163] Cass. pen., 13 maggio 2015, n. 50140, in *dejure.it*. Cfr. anche Cass. pen., 9 maggio 2017, n. 26229, in *dejure.it*, secondo cui «integra il delitto di frode informatica la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua», e Cass. pen., 24 ottobre 2018, n. 48553, in dejure.it, secondo cui «integra il reato l'accesso abusivo a conti correnti on line cui segua il prelievo di somme fatte confluire su carte prepagate appositamente attivate a tale scopo a nome e da persone in condizioni economiche disagiate, materialmente estranee all'accesso abusivo»

[164] Secondo cui «Nel caso di condanna, o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale, per uno dei delitti previsti dagli articoli da 314 a 320, anche se commessi dai soggetti indicati nell'articolo 322bis, primo comma, è sempre ordinata la confisca dei beni che ne costituiscono il profitto o il prezzo, salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a tale prezzo o profitto. Nel caso di condanna, o di applicazione della pena a norma dell'articolo 444 del codice di procedura penale, per il delitto previsto dall'articolo 321, anche se commesso ai sensi dell'articolo 322bis, secondo comma, è sempre ordinata la confisca dei beni che ne costituiscono il profitto salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a quello di detto profitto e, comunque, non inferiore a quello del denaro o delle altre utilità date o promesse al pubblico ufficiale o all'incaricato di pubblico servizio o agli altri soggetti indicati nell'articolo 322bis, secondo comma Nei casi di cui ai commi primo e secondo, il giudice, con la sentenza di condanna, determina le somme di denaro o individua i beni assoggettati a confisca in quanto costituenti il profitto o il prezzo del reato ovvero in quanto di valore corrispondente al profitto o al prezzo del reato».

telematici, che sono stati utilizzati, in tutto o in parte, per commettere una serie di reati, tra i quali anche quello di frode informatica[165].

Infine, in attuazione della direttiva n. 2014/42/UE, che ha ad oggetto la confisca e il congelamento dei beni utilizzati per la commissione dei reati e dei profetti da reato nell'Unione europea ed in attuazione della delega prevista dalla legge 7 ottobre 2014, n. 154, il d.lgs. 29 ottobre 2016, n. 202, nell'introdurre un secondo periodo all'art. 240, comma 2, n. 1 bis, c.p., ha optato per l'estensione di tale confisca obbligatoria anche al prodotto e al profitto dei delitti che ivi sono previsti, stabilendo, poi, in via subordinata, la confisca per equivalenti di beni che abbiano un valore equipollente al prodotto o profitto di tali reati.

8. Frode informatica e truffa: una riflessione conclusiva

Chiarito cosa si intende per frode informatica, è necessario individuare le differenze con la truffa. Il reato di truffa[166], anche se dal punto di vista statistico è assai meno frequente rispetto al furto, sta divenendo sempre più diffuso negli ultimi anni, «essendo aumentate le occasione di fraudolenta captazione patrimoniale, parallelamente alla evoluzione dei rapporti economici sia nell'ambito del libero mercato, sia soprattutto nell'ambito dell'economia sorretta dalle molteplici forme di intervento statale e comunitario»[167].

Nonostante la sua configurazione giuridica sia piuttosto recente, la nozione di truffa è nota da tempo. Etimologicamente il termine deriva dal termine tedesco "*trug*", da intendersi nel senso di "inganno, frode", evidenziando per

[165] Si tratta, in particolare, dei reati contenuti nei seguenti articoli: 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.

[166] La bibliografia sul tema è veramente sterminata; si v., senza pretesa di completezza, G. Marra, *Truffa (art. 640)*, cit., pagg. 477 ss.; G. Marini, *Truffa*, cit., pagg. 353 ss.; A. Fanelli, *La truffa*, cit..

[167] G. Fiandaca, E. Musco, *Diritto penale. Parte speciale.* 2/II. *I delitti contro il patrimonio*[6], cit., pag. 179.

tale via l'elemento chiave della fattispecie in esame, che presuppone, appunto, una attività fraudolenta, truffaldina, appunto.

Il reato di truffa è previsto dal vigente codice penale all'art. 640, all'interno dei reati contro il patrimonio[168]. Il reato di truffa rappresenta un vero e proprio reato manifesto della categoria dei reati connotati dalla cooperazione artificiosa della vittima. La truffa, infatti, nella sua manifestazione esteriore, si snoda in due momenti diversi: da un lato vi sono gli artifizi e i raggiri della parte, finalizzati ad indurre in errore la vittima; dall'altro vi è proprio l'errore della vittima, che si concretizza in un atto di disposizione patrimoniale lesivo dei propri interessi ed a vantaggio del terzo.

La cooperazione artificiosa della vittima, poi, deriva anche del fatto che la truffa costituisce un classico esempio di reato in contratto, in cui ad essere illecito non è il contratto considerato nella sua essenza, ma le modalità aggressive della condotta altrui. La fattispecie del reato di truffa è quasi prevalentemente incentrata sull'attività ingannatoria del reo, e quindi sulla nozione di artifizi e raggiri. Anche su questo profilo la dottrina, nel corso degli anni, si è estremamente divisa. Quella più risalente[169], ormai, sosteneva che l'attività truffaldina poteva costituire il frutto di qualunque strumento ritenuto idoneo, nel caso di specie, ad indurre la vittima in errore.

Sostanzialmente, quindi, il profilo fondamentale del delitto di truffa non sarebbe costituito dagli artifizi o raggiri, ma solo dal conseguimento di un ingiusto profitto provocando un danno ad altri, ricorrendo a qualsiasi mezzo fraudolento.

Questa impostazione, tuttavia, non è assolutamente condivisibile, in quanto svilisce il ruolo degli artifizi o raggiri all'interno della fattispecie, finendo con il banalizzarli e ponendosi, in tal modo, del tutto in contrasto con il

---

[168] Sulla tutela penale del patrimonio, in senso critico, si v. A. Carmona, *Tutela penale del patrimonio individuale e collettivo*, Bologna, 1996, pagg. 235 ss.; C. Pedrazzi, *La riforma dei reati contro il patrimonio e contro l'economia*, in AA.VV., *Verso un nuovo codice penale*, Milano, 1993, pagg. 350 ss.; F. Grosso, *Interessi protetti e tecniche di tutela*, in AA.VV., *Beni e tecniche della tutela penale*, Milano, 1987, pagg. 163 ss.

[169] Così D. Angelotti, *Delitti contro il patrimonio. Trattato di diritto penale* IV, Milano, 1936.

fondamentale principio di tassatività e determinatezza. La formula in esame, pertanto, può sicuramente essere interpretata diversamente, ma certamente non nel senso che ogni condotta può integrare un artifizio o un raggiro. Una diversa scuola di pensiero, oggi dominante, sostiene che, per il verificarsi del reato di truffa, deve sempre sussistere una messa in scena da parte dell'autore di una condotta delittuosa.

Ora, per quanto riguarda la condotta del reato di frode informatica, essa è sostanzialmente identica a quella del reato di truffa, in quanto il legislatore punisce l'attività di procurare a sé o ad altri un ingiusto profitto con altrui danno. Tuttavia, sono differenti le modalità di realizzazione del vantaggio economico che, nel caso specifico della truffa, avvengono con artifizi e raggiri che sono idonei ad indurre in errore la vittima; diversamente, invece, nel caso della frode informatica il legislatore ha deciso di optare per una descrizione meno generica, indicando modalità tassative di realizzazione del reato.

In particolare, il legislatore ha utilizzato le seguenti formule: «alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico» o «intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti».

Il legislatore, pertanto, ha introdotto due diverse ipotesi, la condotta di alterazione e quella di intervento, che sono nient'altro che quegli artifizi o raggiri del reato di truffa calati tuttavia nel peculiare ambito della frode informatica, in quanto condotte idonee ad alterare il regolare funzionamento del sistema telematico o informatico al fine di porre in essere azioni che arrecano un vantaggio a chi le compie a svantaggio della vittima. Il fatto che il legislatore abbia inserita una "o" disgiuntiva tra le due ipotesi induce a pensare che si tratti di condotte alternative le quali, poste in essere in modalità separata, sarebbero entrambe in grado di configurare il perfezionamento del reato.

Tuttavia, secondo una parte della dottrina[170] le due ipotesi difficilmente possono essere distinte l'una dall'altra considerato che la seconda modalità di condotta, ossia l'intervento, finisce con il ricadere, sia dal punto di vista logico che tecnico, nella prima ipotesi, quella di alterazione, in quanto sarebbe impensabile che un terzo intervenga in un sistema informatico altrui senza in qualche modo alternarne il funzionamento.

Va segnalato che, tuttavia, la giurisprudenza di merito ha riconosciuto un'autonomia concettuale alle due ipotesi: si è osservato, infatti, che l'intervento è cosa ben diversa dall'alterazione, come del resto lascia intendere il legislatore nel momento in cui usa la disgiuntiva "o"[171].

In particolare, la giurisprudenza ha chiarito che «il reato ex art. 640-ter c.p. prevede due distinte condotte; la prima consiste nell'alterazione, in qualsiasi modo, del funzionamento di un sistema informatico o telematico; la seconda è rappresentata dall'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un dato sistema informativo o telematico. Tale ipotesi, finalizzata pur sempre all'ottenimento di un ingiusto profitto con altrui danno, si concretizza in un'illecita condotta intensiva ma non alterativa del predetto sistema»[172].

Alla luce di queste considerazioni, è chiara la differenza tra truffa e frode informatica: nella truffa assumono rilevanza decisiva gli artifizi e i raggiri, mentre nella frode informatica vi è il ricorso a mezzi fraudolenti, senza alcun riferimento ai raggiri. La truffa è diretta a far cadere in errore la vittima,

---

[170] Cfr. G. Pica, *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, cit., p. 144.

[171] Cfr. Trib. Milano, 19 marzo 2007, in *Diritto industriale*, 1, 2008, p. 85, con nota di A. Musso, secondo cui «non commetta il reato di cui all'art. 640-ter c.p. (che punisce la frode informatica) chi abbia effettuato la copiatura di alcuni contenuti di un sito perché la frode informatica suppone una alterazione del funzionamento di un sistema informatico oppure un intervento abusivo sul sistema stesso o su dati o informazioni o programmi ivi contenuti o ad esso pertinenti e la fattispecie criminosa è configurata sullo schema della truffa, mediante la sostituzione della condotta umana artificiosa ed ingannatoria con la manipolazione o l'intervento su sistemi informatici e cioè con una forma di interferenza sul processo di elaborazione dei dati pur non assimilabile ad una vera e propria alterazione».

[172] Cass. pen., 6 marzo 2013, n. 13475, in *dejure.it*.

mentre la frode informatica interviene direttamente sul dispositivo telematico che viene manipolato.

Non vi è alcun dubbio, pertanto, circa l'autonomia del delitto di frode informatica rispetto a quello di truffa: in tal senso si è espressa la giurisprudenza, secondo cui «è indubbio che la fattispecie di cui all'art. 640 ter integri senz'atro un'autonoma figura di reato, a differenza di quanto si è invece ritenuto in giurisprudenza a proposito della ipotesi di truffa aggravata per il conseguimento di erogazioni pubbliche, prevista dall'art. 640-bis cod. pen., ormai pacificamente ricondotta nel novero delle circostanze aggravanti rispetto al reato "base" di truffa ex art 640 cod. pen.»[173].

Va segnalato, ancora, che vi è differenza anche tra truffa online e frode informatica. La Cassazione, in proposito, ha chiarito che «il delitto di frode informatica ha la stessa struttura e i medesimi elementi costituivi della truffa, dalla quale si differenzia solo per il fatto che l'attività fraudolenta non investa la persona inducendola in errore ma il sistema informatico di sua pertinenza attraverso una manipolazione»[174].

Dunque, il fatto che la truffa venga commessa ingannando la persona online non tramuta automaticamente il fatto in una frode informatica, considerato che quest'ultima manipola direttamente il sistema informatico e non la persona.

9. L'attività di prevenzione

Il profilo della prevenzione nei confronti degli atti di *phishing* presenta diversi profili, a seconda del punto di vista tenuto in considerazione. Sotto il profilo dell'utente, sebbene sia paradossalmente quello più importante, non esistono

[173] Cass., Sez. un., 26 giugno 2002.

[174] Cass. pen., sez. II, 24 novembre 2020, n. 32894. Ne consegue che la fattispecie si consuma nel momento e nel luogo in cui l'agente consegue l'ingiusto profitto con relativo danno patrimoniale altrui. Laddove il profitto sia conseguito mediante accredito su carta di pagamento ricaricabile, come nel caso di specie, il tempo e il luogo di consumazione della truffa sono quelli in cui la persona offesa ha effettuato il versamento di denaro.

particolari indicazioni da dare: è evidente che qualunque persona un minimo esperta dovrebbe utilizzare internet in maniera accorta, evitando di cliccare su link e banner sospetti, che non provengono da siti ufficiali, analizzando in maniera accorta il testo della mail, per verificare se viene utilizzato un linguaggio sgrammaticato o sospetto, e soprattutto non lasciando mai propri dati personali quando la richiesta proviene via mail, perché nella maggior parte dei casi si tratta di truffe. In caso di richiesta di dati via mail, dunque, è opportuno contattare sempre il sito ufficiale autonomamente al fine di verificare se effettivamente la richiesta è veritiera o si tratta di phishing.

Un altro profilo è quello che coinvolge le banche e gli altri istituti, come ad esempio le poste, che sono quelli più imitati per realizzare attacchi di phishing, trattandosi delle istituzioni presso le quali si detengono solitamente le somme di denaro. Inoltre, sono anche i soggetti che subiscono più attacchi, e sono potenzialmente più invasivi e devastanti di quelli che possono subire i privati, considerando la mole di dati che tali istituti contengono.

Sebbene i media raccontino spesso di attacchi informatici diretti alle aziende, di hacker che hanno colpito i grandi colossi della tecnologia quali Google, Apple ecc., le aziende hanno ancora dei tentennamenti nell'investire in maniera significativa sul tema della cybersecurity.

Eppure una strategia aziendale mirata è necessario per fronteggiare pericoli che diventano sempre più invasivi con il passare del tempo e l'evolvere della tecnologia. Il primo aspetto che deve essere considerato, infatti, nel momento in cui viene elaborata una strategia di cybersecurity, è che tale strategia deve essere flessibile, pronta ad essere rivista in ogni momento, in continuo aggiornamento, perché le tecniche elaborate dagli hacker sono sempre avanti rispetto a quelle difensive che vengono elaborate in sede di cybersecurity[175].

Tra le aziende più colpite vi sono soprattutto quelle bancarie, o comunque quelle che si occupano di intermediazione finanziaria, nei confronti delle

[175] Cfr. R.S. Cheung, J.P. Cohen, H.Z. Lo, F. Elia, *Challenge Based Learning in Cybersecurity Education*, in *josephcohen.com*, 2018.

quali, soprattutto nel corso degli ultimi anni, sono aumentati gli attacchi, specie a seguito della diffusione dei nuovi sistemi di pagamento e dei nuovi prodotti finanziari, quali il bitcoin.

La crescita della percentuale di attacchi, dunque, ha riguardato le categorie della salute (+102%), della grande distribuzione organizzata e del retail (+70%) e della finanza (+64%). Il picco di attacchi ha riguardato SWIFT, ossia il sistema che gestisce le operazioni finanziarie internazionali tra gli istituti bancari, considerato da sempre un sistema inattaccabile.

L'attacco a tale sistema ha prodotto perdite per centinaia di milioni di dollari: si riteneva, infatti, che le transazioni fossero vere e legittima ma, nella sostanza, si sono rivelate transazioni fasulle, che hanno prodotto effetti devastanti[176].

Le tecniche di attacco informatico sono piuttosto variegate, ma sono caratterizzate dall'essere spesso molto semplici. Le più diffuse, infatti, si basano su *malware* semplici, Ddos e vulnerabilità note. Nel corso degli ultimi tempi, poi, hanno progressivamente trovato larga diffusione il *Phishing* e il *social engineering*.

I cyberattacchi, negli ultimi anni, stanno quindi diventando sempre più insistenti, ma soprattutto hanno completamento mutato la propria natura. Fino a qualche anno fa, infatti, gli attacchi informatici erano finalizzati soprattutto a forme di autocompiacimento, per esaltare l'ego di chi provava grande soddisfazione nell'essere entrato nel sistema informatico di una grande azienda, riuscendo nell'impresa di scardinare un sistema considerato inattaccabile.

Oggi, tuttavia, non è più così. Gli attacchi informatici sono diretti ad ottenere risultati ben precisi, ed in particolare ad acquisire grosse somme di denaro. Sono anche mutate le tecniche: si preferisce infatti ricorrere ad attacchi di lungo periodo, ossia diretti ad un controllo duraturo del sistema informatico

[176] Cfr. *clusit.it.*

dell'azienda senza che la *cybersecurity* sia in grado di rilevarlo con i meccanismi interni predisposti[177].

Gli attacchi, poi, nella maggior parte dei casi sono automatizzati, non richiedendo dunque un grande sforzo da parte dell'*hacker*. Si richiede, tuttavia, la partecipazione della vittima, puntando sulla sua scarsa cultura informatica.

Gli attacchi informatici sono aumentati anche perché esiste un vero e proprio mercato che, a basso costo, consente di imparare le tecniche e di comprare illegalmente codici malevoli da sfruttare per preparare il cyberattacco.

Al cospetto di tutto questo, dunque, diventa indispensabile cercare di elaborare strategie in grado di fronteggiare gli attacchi informatici in maniera adeguata.

L'aumento dei dispositivi digitali utilizzati all'interno delle aziende ha reso necessario implementare il livello di sicurezza al fine di proteggere i dati aziendali.

Questo è il motivo per cui gli investimenti dei privati e delle aziende nel settore della cybersecurity sono aumentati in maniera esponenziale. Addirittura le microimprese, tradizionalmente restie a investire nel settore in esame, hanno compreso l'importanza di attivarsi al fine di evitare danni irreparabili[178].

Va segnalato, tuttavia, che la totale sicurezza dei dati è un obiettivo irraggiungibile: non vi sono, infatti, possibilità di garantire che, anche con un elevato investimento nel settore, i dati aziendali siano sicuri senza alcun dubbio.

Piuttosto, è necessario procedere con una analisi dei costi-benefici, verificando quale è l'investimento adeguato tenendo conto dell'impossibilità di garantire il risultato. La cybersecurity costituisce la risposta ai rischi

---

[177] Cfr. R. Paglia, P. Iezzi, *Hotel Cybersecurity: le minacce e le soluzioni. Security*, Milano, 2018, pagg. 11 ss.

[178] Cfr., sul tema, A.M. Cavadini, G. Lucietto, *Risk management. Conoscenze e competenze in un unico processo*, Bari, 2014, pagg. 252 ss.

derivanti da attacchi ai sistemi informatici aziendali. Nel corso degli ultimi anni, il numero di attacchi cui le aziende vengono coinvolte è aumentato in maniera esponenziale[179].

Il maggior numero di attacchi aziendali che riesce ad andare a buon fine è dovuto alla scarsa competenza dei dipendenti, che non sono preparati in maniera sufficiente a fronteggiare attacchi informatici.

Una ricerca effettuata da Kaspersky Lab[180], dal titolo piuttosto significativo, *Human Factor in IT Security*, ha infatti chiarito che il fattore umano rappresenta a tutti gli effetti un pericolo per l'azienda. Secondo lo studio, circa il 28% degli attacchi diretti alle aziende avvengono attraverso *phishing* o ingegneria sociale, ossia mediante tecniche che richiedono una collaborazione da parte dei dipendenti, in assenza della quale non potrebbero andare a buon fine.

Si pensi, in particolare, al *phishing*, tecnica la quale, per produrre effetti negativi, richiede necessariamente che il dipendente apra il *link* dannoso inviato solitamente via mail, oppure anche un allegato. Il problema risiede nel fatto che solo una minima parte dei dipendenti sono accorti, attenti e soprattutto preparati a comprendere che dietro un link o un allegato si cela una minaccia.

Molto spesso, infatti, le tattiche utilizzate dai pirati informatici sono piuttosto semplici se il dipendente fosse capace di comprendere il reale intento di chi attacca.

Un altro aspetto piuttosto preoccupante, rivelato sempre dallo studio in esame, risiede nel fatto che la buona parte dei dipendenti, circa il 40%, non riferisce agli addetti alla sicurezza che l'azienda è rimasta vittima di un attacco informatico[181]. Ciò, invero, non deve sorprendere: molti dipendenti hanno paura di ritorsioni, o semplicemente di essere giudicati negativamente

[179] Cfr. P. Iezzi, R. Puglia, *AI CyberSecurity e AI-powered Cyber Attack*, cit., pagg. 31 ss.
[180] Cfr. *https://www.kaspersky.com/blog/the-human-factor-in-it-security/.*
[181] Cfr. *https://www.kaspersky.com/blog/the-human-factor-in-it-security/.*

per essere ingenuamente caduti nella rete del pirata informatico. Tuttavia, ciò rischia di produrre danni ulteriori all'azienda, considerato che, non sapendo di essere stata attaccata, non può difendersi nella maniera giusta, e molti dati potrebbero essere in pericolo.

Molti dipendenti, ancora, non essendo esperti, o semplicemente non pensando seriamente che i loro gesti e comportamenti possono compromettere la sicurezza dell'azienda, pongono in essere azioni che possono provocare delle falle significative nei sistemi informatici interni all'azienda.

Si pensi all'utilizzo, molto diffuso, di chiavette USB e altri supporti esterni nei computer aziendali: il dipendente che si comporta in questo modo mette a rischio l'azienda perché tali supporti potrebbero essere infatti da *malware* o altri virus.

Non va sottovalutato un altro aspetto, che chiama direttamente in causa le aziende: esse, infatti, molto spesso sono colpevoli almeno quanto i propri dipendenti, perché non riescono ad inculcare una vera e propria cultura della sicurezza informatica.

Si tratta, infatti, di una tematica che viene ancora oggi considerata una incombenza cui assolvere malvolentieri, un vero e proprio investimento da evitare. Ciò è dovuto in parte alla scarsa percezione del rischio informatico cui è esposto l'azienda, in parte alla scarsa fiducia nei confronti della cybersecurity[182]. Ne deriva che qualunque approccio, qualunque

[182] Cfr. quanto osservato da S. Dal Grande, *Sicurezza informatica, le fatiche di chi la "evangelizza" in azienda*, in *agendadigitale.eu*, 12 novembre 2018, secondo cui «una delle non poche difficoltà di chi si è messo in mente di evangelizzare le aziende e le organizzazioni (ovviamente PMI) presenti sull'italico suolo sui temi della cybersecurity, negli ultimi mesi confusi e sovrapposti (a torto) al tema GDPR, è quella di trovarsi spesso in situazioni nelle quali ci si sente degli alieni. Per quanto ci sforziamo di "tradurre" il linguaggio tecnico dei manuali e il linguaggio formale delle norme e dei framework, il nostro interlocutore, spesso ben posizionato nella piramide gerarchica aziendale, ci guarda con occhio sghembo, e dopo qualche secondo di riflessione, che in cuor nostro speriamo preluda ad una accettazione di tutto (o quasi) ciò che abbiamo esposto, se ne esce con un laconico "non ho capito niente se non che volete farmi spendere dei soldi", con la variante, esplosa nelle ultime settimane, che suona come "voi e l'Europa volete farci spendere un sacco di soldi anche dove non serve". Lo snodo cruciale, indipendentemente dalla versione esposta dal nostro interlocutore, sta proprio qui: la percezione che i denari spesi per l'informatica siano un esborso necessario, ma da evitare o procrastinare il più possibile nel tempo».

investimento, anche quello più costoso, rischia di rivelarsi cosa vano in mancanza di una vera e propria cultura aziendale della cybersecurity.

Si è opportunamente osservato, in proposito, che al fine di ridurre i rischi degli hacker non è sufficiente adottare soluzioni di IT security invasive né, tantomeno, rispettare policy aziendali più rigida, essendo indispensabile modificare l'approccio culturale alla sicurezza informatica da parte di tutti i membri dell'azienda[183].

Pare evidente, in conclusione, che nel momento in cui si parla di centralità della cybersecurity nel panorama aziendale si intende la necessità di costruire, prima ancora che un sistema idoneo a fronteggiare attacchi informatici, anzitutto una vera e propria cultura della cybersecurity che, allo stato attuale, soprattutto nelle aziende di dimensioni più piccole, sembra mancare del tutto.

[183] M. Santini, *Cyber security in azienda, diffondere la cultura della sicurezza informatica: ecco perché*, in *cybersecurity360.it*, 20 novembre 2018, secondo cui «fondamentale il ruolo del board aziendale, in cui il CIO, e sempre più il CISO (Chief Information Security Officer) ha un sempre più alto livello di responsabilità rispetto alle implicazioni etiche e legali relative alla sicurezza informatica e, in generale, agli obiettivi di business, e diventa parte integrante della catena di valore della governance aziendale. Anche da parte dei professionisti della sicurezza è fondamentale apprendere il linguaggio del business, poiché qualsiasi decisione presa dai CEO o dai manager aziendali a proposito di nuovi processi, responsabilità e strumenti da adottare è motivata da obiettivi organizzativi ed economici».

CAPITOLO III
LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI PER I REATI INFORMATICI

Sommario: 1. La responsabilità amministrativa degli enti; 1.1. La nascita del d.lgs. 231/2001; 1.1.1. Il profilo sanzionatorio del d.lgs. n. 231/2001; 1.1.2. I soggetti destinatari della disciplina; 1.1.3. I criteri di imputazione; 1.1.4. Gli autori del reato presupposto: soggetti in posizione apicali e soggetti sottoposti all'altrui direzione e controllo; 1.1.5. Criteri oggettivi: l'interesse o vantaggio dell'ente; 1.1.6. Criteri soggettivi: la colpa di organizzazione. Esonero della responsabilità dell'ente e modelli organizzativi; 2. Il reato di frode informatica ai sensi del d.lgs. 231/2001; 3. Frode informatica: modello di organizzazione, gestione e controllo nella prevenzione dei reati informatici; 4. Punti di contatto tra la normativa in materia di tutela della privacy ex GDPR e il d.lgs. n. 231/2001 alla luce della frode informatica; 5. Organismo di Vigilanza e Data Protection Officer

1. La responsabilità amministrativa degli enti

L'ordinamento giuridico italiano è stato caratterizzato dall'adozione del principio di irresponsabilità penale delle persone giuridiche, ritraibile dal brocardo "*societas delinquere non potest*". Sebbene manchi una norma specifica che disponga il suddetto principio, esso è ricavabile dall'art.27 Cost., in cui è indicato il carattere personale della responsabilità penale[184].
D'altronde, anche il codice penale italiano assume come punto di riferimento dell'accezione "delinquente", la persona fisica, come si evince dalla richiesta dell'elemento soggettivo del reato, rinvenibile nella presenza di dolo o colpa, ed i cui connotati psicologici non possono che fare riferimento ad una persona fisica, dotata di una propria "coscienza".
Nell'ambito del diritto civile alle persone giuridiche viene riconosciuta una capacità giuridica, intesa come il centro di imputazione diretta di atti o fatti giuridici; tuttavia, in quello penale, nella sua evoluzione storica, diviene

[184] In tal senso si v. A. Traversi, S. Gennai, *Diritto penale commerciale*, Padova, 2017, pag. 295.

difficile immaginare che l'ente possa esprimersi manifestando una intenzionalità psichica criminosa. Anche nelle ipotesi di reati colposi, l'assunzione di un atteggiamento negligente, imprudente o caratterizzato da imperizia, non può che riguardare le persone fisiche.

Tuttavia, nell'evoluzione storica, l'irresponsabilità penale delle persone giuridiche è stata rivisitata considerando, in particolare, due ragioni: in primis, la crescita delle attività di impresa e, con essa, lo sviluppo delle sue manifestazioni criminose; in secondo luogo, a seguito dell'armonizzazione delle normative degli Stati membri dell'UE, ha coinvolto anche gli aspetti penali, il che ha imposto un ripensamento della normativa in oggetto, considerato sia che l'accezione di Stato unionale impone obblighi di tutela nei confronti di interessi ritenuti di rilievo, tra i quali quelli di natura economica e finanziaria hanno assunto un significato sempre più incisivo; e dall'altro che molti Paesi membri detengono una disciplina in cui la responsabilità penale delle persone giuridiche è prevista.

A ciò si aggiunga che, in assenza di una disciplina finalizzata a punire direttamente le società e gli altri enti superindividuali ha come conseguenza il ricorso alla costituzione di enti dotati di personalità giuridica da parte della criminalità organizzata, finalizzata all'ottenimento dell'impunità o, almeno, di un sanzioni attenuate. Ciò ha indotto il legislatore a superare alcuni limiti posti alla responsabilità delle persone giuridiche, pensando al d.lgs. n. 231/2001.

Il limite normativo che si è frapposto alla statuizione della responsabilità penale delle persone giuridiche, è sempre stato l'art. 27 Cost. che prevede, come ampiamente illustrato, il carattere "personale" della responsabilità penale, mentre al terzo comma, prevede che le pene non siano contrarie al senso di umanità né che impediscano la rieducazione del condannato: da tale disposizione, è ritraibile il principio in base al quale la responsabilità penale non può coinvolgere gli enti dotati di personalità giuridica.

Nell'attribuire natura "personale" alla responsabilità di matrice penale, anche la Corte Costituzionale[185], ha ritenuto che il costituente avesse inteso sottolineare che si dovesse trarre l'elemento della colpevolezza, ossia la presenza del dolo o della colpa, sottraendo, in tal senso, i profili di responsabilità oggettiva.

In basa a tale ricostruzione, sembrava difficile che una persona giuridica potesse agire con il dolo o la colpa, ossia con "colpevolezza". Per aggirare il problema, la colpevolezza avrebbe dovuto essere intesa non in accezione psicologica, ma normativa: secondo tale impostazione, le persone giuridiche, essendo in grado di mettere in atto illeciti extrapenali, sono anche idonee a commettere reati servendosi degli organi, ossia tramite il rapporto di immedesimazione organica che si determina e che vede l'organo medesimo creare un'osmosi con la persona giuridica.

Se si considera il terzo comma dell'art. 27 Cost., ovvero l'impossibilità di sanzionare le persone giuridiche, essa va considerata di minore rilevanza. Nel nostro ordinamento giuridico, infatti, la sanzione penale non assume solo le

[185] Cfr., tra le tante pronunce, Corte Cost., 24 marzo 1988, n. 364, in *www.giurcost.org*, nella quale si legge, tra l'altro, che «la colpevolezza costituzionalmente richiesta, come avvertito dalla più recente dottrina penalistica, non costituisce elemento tale da poter esser, a discrezione del legislatore, condizionato, scambiato, sostituito con altri o paradossalmente eliminato. Limpidamente testimonia ciò la stessa recente, particolare accentuazione della funzione di garanzia (limite al potere statale di punire) che le moderne concezioni sulla pena attribuiscono alla colpevolezza. Sia nella concezione che considera quest'ultima "fondamento", titolo giustificativo dell'intervento punitivo dello Stato sia nella concezione che ne accentua particolarmente la sua funzione di limite allo stesso intervento (garanzia del singolo e del funzionamento del sistema) inalterato permane il "valore" della colpevolezza, la sua insostituibilità». In tale prospettiva, «il principio di colpevolezza è, pertanto, indispensabile, appunto anche per garantire al privato la certezza di libere scelte d'azione: per garantirgli, cioè, che sarà chiamato a rispondere penalmente solo per azioni da lui controllabili e mai per comportamenti che solo fortuitamente producano conseguenze penalmente vietate; e, comunque, mai per comportamenti realizzati nella "non colpevole" e, pertanto, inevitabile ignoranza del precetto». Ad avviso della Consulta, quindi, i «Costituenti mirarono, sul piano dei requisiti d'imputazione del reato, ad escludere che si considerassero costituzionalmente legittime ipotesi carenti di elementi subiettivi di collegamento con l'evento e, sul piano politico, a non far ricadere su "estranei" "colpe altrui". E mai, in ogni caso, venne usato il termine fatto come comprensivo del solo elemento materiale, dell'azione cosciente e volontaria seguita dal solo nesso oggettivo di causalità: anzi, sempre venne usato lo stesso termine come comprensivo anche d'un minimo di requisiti subiettivi, oltre a quelli relativi alla coscienza e volontà dell'azione».

sembianze della pena detentiva (non applicabile, oggettivamente, alle persone giuridiche), ma altresì di sanzioni interdittive e soprattutto pecuniarie, che senza alcun problema possono essere estese alle persone giuridiche.
Il legislatore, con il d.lgs. n. 231/2001, ha, dunque, provare ad "aggirare" l'ostacolo descritto costruendo un sistema sanzionatorio a carico degli enti che risulta gemmato dalla commissione di reati al proprio interno.

1.1. La nascita del d.lgs. 231/2001

Tramite il d.lgs. 8 giugno 2001, n. 231, l'Esecutivo ha dato attuazione alla delega ricevuta dall'art.11 della legge 29 settembre 2000, n.300, finalizzata ad individuare la disciplina della responsabilità amministrativa delle persone giuridiche e delle società, degli enti e delle associazioni prive di personalità giuridica (esentando solo quelle che svolgono funzioni di rilievo costituzionale).
Dall'osservazione dottrinale è stato desunto che «il modello prescelto è stato quello della responsabilità per l'omessa adozione delle cautele organizzative idonee ad impedire la commissione di reati da parte dei dipendenti o degli amministratori. L'ente risponde per la perpetrazione del reato presupposto ad opera del vertice aziendale o da soggetto sottoposto alla vigilanza dello stesso; non risponde laddove abbia elaborato idonei *compliance programs* (mutuati dall'esperienza anglosassone)»[186].
In base alla norma le persone giuridiche possono essere considerate destinatarie di una sanzione penale, adottando un sistema sanzionatorio ad hoc, ovvero esse riservato, e non più, come accadeva in passato, in via sussidiaria, nell'eventualità di inadempienza della persona fisica colpita dalla sanzione penale in via diretta.

[186] R. Garofoli, *Il contrasto ai reati di impresa nel d.lgs. n. 231 del 2001 e nel d.l. n. 90 del 2014: non solo repressione, ma prevenzione e continuità aziendale*, in *www.penalecontemporaneo.it*, 2015, pag. 3.

Una ricostruzione della possono in base ai principi in essa contenuti può essere utile. In *primis*, la responsabilità della persona giuridica si perfeziona tramite connessione con la realizzazione di un reato, che deve rientrare tra quelli previsti dal legislatore e che deve essere commesso da una persona fisica legata all'ente da un rapporto funzionale, sia esso di rappresentanza o di mera subordinazione.

Inoltre, il nesso tra reato e persona giuridica si basa su un piano oggettivo, in quanto il reato deve produrre un vantaggio dell'ente oppure essere stato commesso con take intento e nel suo interesse. L'interesse e l'obiettivo vantaggio costituiscono i due criteri che il legislatore richiede in via alternativa e non cumulativa, essendo bastevole la presenza di uno solo dei due. L'esistenza dell'interesse, deve essere accertato dal giudice penale tramite una valutazione *ex ante*, indipendentemente dagli esiti raggiunti a seguito della condotta delittuosa dell'agente. L'esistenza del vantaggio, invece, richiede una valutazione *ex post*, essendo il giudice chiamato a verificare che l'ente abbia tratto vantaggio dalla condotta delittuosa in maniera effettiva.

Infine, anche il tipo di rapporto che lega la persona giuridica ed il soggetto agente ha una sua rilevanza. Infatti, il legislatore ha individuato il rapporto di rappresentanza e quello di determinazione: nel primo caso, laddove il reato sia stato commesso da un soggetto che occupa una posizione apicale, la persona giuridica dovrà rispondere del reato nella misura in cui non dimostri l'adozione, a scopo preventivo, dei modelli organizzativi idonei a prevenirlo; laddove, infine, esso sia commesso da un soggetto legato all'ente da un rapporto di subordinazione, la persona giuridica risponde penalmente solo in caso di deficit di sorveglianza o organizzativa, da cui si possa evincere che vi sia stato un omesso controllo del responsabile del fatto delittuoso[187].

[187] Al quale è stata sostanzialmente lasciata "via libera" per la commissione del reato.

In merito alla natura giuridica della responsabilità dell'ente (amministrativa, penale, o di un *tertium genus*) è stata avanzata anche l'ipotesi di responsabilità speciale. La questione ha notevoli risvolti pratici[188].

Quella della responsabilità speciale è un'ipotesi che deriva dalla Relazione di accompagnamento al d.lgs. n. 231/2001, nella quale trae che il modello scelto dal legislatore, in riferimento alla responsabilità, «coniuga i tratti essenziali del sistema penale e di quello amministrativo nel tentativo di contemperare le ragioni dell'efficacia preventiva con quelle, ancor più ineludibili, della massima garanzia»[189].

La responsabilità dell'ente munito di personalità giuridica risulta espressione del nuovo diritto penale di impresa, un modello ibrido che coinvolge il diritto penale e quello amministrativo.

In ambito dottrinario si propende per la natura amministrativa della responsabilità basando le argomentazioni di sostegno soprattutto sul carattere formale della qualificazione normativa che parla di responsabilità amministrativa degli enti[190]. Tuttavia, va ricordato che il *nomen iuris*, per quanto inequivocabile, non è mai sufficiente in assenza di un dato

---

[188] Sul punto si v. G. De Simone, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) di imputazione*, in *www.penalecontemporaneo.it*, 2012, pagg. 5 ss., secondo il quale «non è una questione solo accademica e nominalistica, perché qui sono in gioco i "referenti costituzionali" della disciplina tratteggiata nel d.lgs. n. 231. È chiaro, infatti, che, qualora si ritenga sostanzialmente penale siffatta responsabilità, la legittimità di questa disciplina non potrà che essere valutata alla luce di quelle norme che la costituzione dedica alla materia penale. Entrerebbero in gioco, pertanto, sia gli artt. 25, commi 1 e 2, e 27, commi 1, 2 e 3, cost., sia gli artt. 111 e 112 cost.; ed i principi ivi sanciti diventerebbero giustiziabili da parte della Corte costituzionale al fine di vagliare la legittimità delle singole disposizioni normative che compongono il d.lgs. n. 231. Senza contare che potrebbe anche porsi, prima o poi, la necessità di un'eterointegrazione delle lacune della disciplina che dovessero emergere via via nella prassi applicativa. Ma quale dovrà essere il quadro normativo di riferimento? Il codice penale, i "Principi" codificati nella "689" dell'81, oppure lo statuto civilistico della responsabilità extracontrattuale?»; in tal senso si v. anche G. Marelli, *Profili pratici della questione sulla natura giuridica della responsabilità degli enti*, in *Rivista italiana di diritto e procedura penale*, 2016, pagg. 151 ss.

[189] Relazione al d.lgs. 8 giugno 2001, n. 231, cit., p. 12, § 1.1.

[190] Sostengono la natura amministrativa della responsabilità delle persone giuridiche, tra gli altri, G. Marinucci, *"Societas puniri potest": uno sguardo sui fenomeni e sulle discipline contemporanee*, in *Rivista italiana di diritto e procedura penale*, 2002, pagg. 1201 ss.; M. Romano, *La responsabilità amministrativa degli enti, società o associazioni: profili generali*, in *Rivista delle società*, 2002, pagg. 398 ss.

"sostanziale"; basti pensare a alle misure di sicurezza, che il codice penale considera sanzioni amministrative ma che, in sostanza, sono penali a tutti gli effetti.

A favore della natura amministrativa della responsabilità degli enti contribuiscono altre considerazioni: *in primis*, il regime della prescrizione, differente da quello previsto nell'ambito penale, e più vicino al regime previsto dalla legge sugli illeciti amministrativi, n. 689/1981; a ciò si aggiunga il richiamo alle vicende modificative dell'ente, improntato ad una logica civilista e non penalistica (basti pensare al caso della fusione, che prevede una responsabilità per fatto altrui che non appartiene al diritto penale); inoltre, è assente un meccanismo di sospensione condizionale della risposta sanzionatoria, anche se tale argomento non ha trovato accoglimento da altra dottrina, secondo la quale esso risulta «difficilmente compatibile con la complessiva strategia preventiva (e premiale) perseguita dal legislatore, fondata sulla valorizzazione delle condotte riparatorie e riorganizzative, a cui è collegata quella "flessibilità regressiva" che caratterizza le sanzioni interdittive»[191].

Non mancano coloro i quali[192] sostengono che la responsabilità descritta dal d.lgs. n. 231/2001 sia di tipo penale, mettendo in luce che il legislatore abbia richiesto, per il perfezionarsi della responsabilità in oggetto, la commissione di un reato, ovvero di un fatto tipico ed antigiuridico, nell'interesse o a vantaggio dell'ente. Pertanto, essendo l'illecito di natura penale, tale dovrebbe essere anche la responsabilità dell'ente, poiché «a decidere della qualificazione giuridica di un comportamento illecito è la natura

[191] G. De Simone, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) di imputazione*, cit., pag. 14.

[192] Si v., in particolare, L. Conti, La *responsabilità amministrativa delle persone giuridiche. Abbandonato il principio societas delinquere non potest?*, in Id. (a cura di), *Il diritto penale dell'impresa*, Padova, 2001, pag. 866; C. Piergallini, *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, in *Rivista trimestrale di diritto penale dell'economia*, 2002, pagg. 578 ss.; G. Amarelli, *Profili pratici della questione sulla natura giuridica della responsabilità degli enti*, in *Riv. it. dir. proc. pen.*, 1, 2006, pagg. 151 ss.

dell'interesse violato, non la natura del soggetto che ha commesso la violazione»[193].

Inoltre, il soggetto legittimato a condurre le indagini preliminari e ad esercitare l'azione penale nei confronti della persona giuridica è il pubblico ministero, mentre, in ambito amministrativo, la cognizione di un illecito appartiene al giudice del reato presupposto.

Assume rilievo anche la cornice sanzionatoria estremamente afflittiva e repressiva nei confronti dell'ente, argomento sminuito da chi ha ritenuto che «un analogo coefficiente di afflittività è dato riscontrare in non poche sanzioni amministrative, sulla loro valenza stigmatizzante e sulla loro caratterizzazione in chiave personalistica, essendo i medesimi in grado di incidere su beni essenziali dell'ente, quali il patrimonio e, soprattutto, la sua libertà di azione, che verrebbe ad essere compressa in modo significativo dall'applicazione delle temibili sanzioni interdittive. Ed anche l'inedito sistema di commisurazione per quote, mutuato dal diritto penale, andrebbe considerato come un indice parimenti sintomatico in tal senso»[194].

La ricostruzione della responsabilità dell'ente in un'ottica penalistica rimanda anche al fatto che sia prevista una sanzione anche per l'ipotesi del delitto tentato, istituto che non appartiene al diritto amministrativo; il rilievo extraterritoriale che si attribuisce all'illecito dell'ente, che ha natura penalistica; infine, il profilo relativo alla successione delle leggi nel tempo, con riguardo al principio della retroattività della legge più favorevole al reo, che costituisce un principio fondamentale del diritto penale.

Per quanto osservato, il panorama dottrinale non sembra trovare un campo di intesa: la natura giuridica della responsabilità dell'ente permane controversa, anche se sembra avvicinarsi più al diritto penale che a quello amministrativo,

---

[193] A. Falzea, *La responsabilità penale delle persone giuridiche*, in AA.VV., *La responsabilità penale delle persone giuridiche in diritto comunitario*, Milano, 1981, pag. 141.

[194] G. De Simone, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) di imputazione*, cit., pag. 18.

pur identificandosi di un diritto penale diverso, adattatosi alle specificità della persona giuridica.

Si è parlato di altro diritto penale, differente da quello pensato per le persone fisiche: «è un diritto penale diverso – con categorie sistematiche e criteri d'imputazione suoi propri – ritagliato, ovviamente, sulle specifiche fattezze dei soggetti metaindividuali. È un *secundum genus* penalistico, se si vuole»[195].

Anche la giurisprudenza si è espressa sul tema della natura della responsabilità degli enti, configurandola, inizialmente, in termini di responsabilità amministrativa a tutti gli effetti. In particolare, si è ritenuto che «com'è noto, il d.lgs. 231/01 ha introdotto nell'ordinamento il principio della responsabilità amministrativa degli enti collettivi, con esclusione degli enti pubblici non economici, in conseguenza di reati commessi in loro favore. Nonostante l'indiscusso elemento di novità introdotto nel sistema da tale normativa, va evidenziato come la responsabilità in questione rivesta, per espressa scelta legislativa, natura amministrativa, fungendo la commissione del reato come mero presupposto per la sua attivazione»[196].

L'elemento che i giudici di merito hanno richiamato per ancorare la responsabilità dell'ente al diritto amministrativo è stato quello letterale, richiamando l'espressione del legislatore che rimanda alla "responsabilità amministrativa" degli enti.

La giurisprudenza della Suprema Corte di Cassazione, inizialmente, ha manifestato una ricostruzione che ha portato ad una individuazione di una responsabilità amministrativa "da reato", evidenziando la peculiare natura amministrativa di una responsabilità da reato[197].

---

[195] *Ivi*, pag. 20.

[196] Trib. Milano, ord. 9 marzo 2004, in *Rivista italiana di diritto e procedura penale*, 2004, p. 1333, con nota di C.F. Grosso, *Sulla costituzione di parte civile nei confronti degli enti collettivi chiamati a rispondere ai sensi del d.lgs. n. 231 del 2001 davanti al giudice penale*, pagg. 1335 ss.

[197] In tal senso Cass. pen., SS.UU., 23 giugno 2011, n. 34476, in *www.penale.it*, secondo cui «il d.lgs. 27 gennaio 2010, n. 39, nell'abrogare e riformulare il contenuto precettivo dell'art. 174-bis T.U.F. (Falsità nelle relazioni o nelle comunicazioni delle società di revisione), non

In altre occasioni, però, sia la giurisprudenza di merito[198] che quella di legittimità hanno individuato un *tertium genus* di responsabilità. Ad esempio, ad avviso della Suprema Corte «il d.lgs. n. 231 del 2001 ha introdotto un *tertium genus* di responsabilità rispetto ai sistemi tradizionali di responsabilità penale e di responsabilità amministrativa, prevedendo un'autonoma responsabilità amministrativa dell'ente in caso di commissione, nel suo interesse o a suo vantaggio, di uno dei reati espressamente elencati nella sezione 3° da parte un soggetto che riveste una posizione apicale, sul presupposto che il fatto-reato "è fatto della società, di cui essa deve rispondere»[199].

In altre pronunce la Corte ha preferito non prendere posizione sul tema: ««il sistema sanzionatorio proposto dal d.lgs. 231 fuoriesce dagli schemi tradizionali del diritto penale – per così dire – "nucleare", incentrati sulla distinzione tra pene e misure di sicurezza, tra pene principali e pene accessorie, ed è rapportato alle nuove costanti criminologiche delineate nel citato decreto»[200].

è intervenuto sulla responsabilità amministrativa da reato dettata dall'art. 25-ter d.lgs. n. 231 del 2001, in quanto le relative fattispecie non sono richiamate da questo testo normativo e non possono conseguentemente costituire fondamento di siffatta responsabilità».

[198] Cfr., in particolare, Tribunale di Milano, ordinanza 24 gennaio 2008, secondo cui «Non vi è dubbio perciò che l'illecito amministrativo conseguente da reato disciplinato dal d.lgs. n. 231/2001 obbliga direttamente l'ente al risarcimento e/o alle riparazioni del danno a norma delle leggi civili. É evidente che l'art. 185 c.p. deve essere interpretato estensivamente alla luce dei principi sopra richiamati e ricomprendere anche il *tertium genus* disciplinato dalla legge in esame. La stessa difesa dell'ente riconosce che il danneggiato dall'illecito amministrativo conseguente da reato può adire il giudice civile e chiedere il risarcimento del danno ex art. 2043 c.c.».

[199] Cass. pen., 16 luglio 2010, n. 27735, in *www.dejure.it*, secondo cui «conclusivamente, in forza del citato rapporto di immedesimazione organica con il suo dirigente apicale, l'ente risponde per fatto proprio, senza coinvolgere il principio costituzionale del divieto di responsabilità penale per fatto altrui (art. 27 Cost.). Né il d.lgs. n. 231 delinea un'ipotesi di responsabilità oggettiva, prevedendo, al contrario, la necessità che sussista la c.d. "colpa di organizzazione" dell'ente, il non avere cioè predisposto un insieme di accorgimenti preventivi idonei ad evitare la commissione di reati del tipo di quello realizzato; il riscontro di un tale deficit organizzativo consente una piana e agevole imputazione all'ente dell'illecito penale realizzato nel suo ambito operativo».

[200] Cass. pen., SS.UU., 27 marzo 2008, n. 26654, in *Rivista italiana di diritto e procedura penale*, 2008, p. 1746, con note di V. Mongillo, *La confisca del profitto nei confronti dell'ente in cerca d'identità: luci e ombre della recente pronuncia delle Sezioni Unite*, pagg.

In alcuni casi la Cassazione ha criticato la scelta del legislatore, ritenuto reo di aver mascherato tramite il *nomen iuris* una responsabilità di natura chiaramente penale: «è noto che il d.lgs. n. 231 del 2001, sanzionando la persona giuridica in via autonoma e diretta con le forme del processo penale si differenzia dalle preesistenti sanzioni irrogabili agli enti, così da sancire la morte del dogma "*societas delinquere non potest*". E ciò perché, ad onta del "*nomen iuris*", la nuova responsabilità, nominalmente amministrativa, dissimula la sua natura sostanzialmente penale; forse sottaciuta per non aprire delicati conflitti con i dogmi personalistici dell'imputazione criminale, di rango costituzionale (art. 27 Cost.); interpretabili in accezione riduttiva, come divieto di responsabilità per fatto altrui, o in una più variegata, come divieto di responsabilità per fatto incolpevole»[201].

Tale è l'orientamento più diffuso presso la giurisprudenza della Corte di Cassazione, confermato anche dalla pronuncia delle Sezioni Unite del 2009, nella quale si trae che «la responsabilità degli enti così come strutturata nella normativa 231/01, ancorché formalmente denominata "amministrativa", ricalca poi nella sostanza, *mutatis mutandis*, la falsariga della responsabilità penale, come già riconosciuto dalla stessa dottrina che predica ormai quasi unanimemente il principio per cui *societas delinquere potest*, così sovvertendo l'opposta e radicata tradizione romanistica sotto l'impulso della normativa comunitaria»[202].

L'indirizzo prevalente, ad oggi, attribuisce rilevanza non solo al *nomen iuris* adottato dal legislatore, e al dato sostanziale delineato dal d.lgs. n. 231/2001, che sembra ispirato più ad una logica penalistica (anche se adeguata alle specifiche caratteristiche delle persone giuridiche) piuttosto che a quella amministrativistica.

1758 ss. e di E. Lorenzetto, *Sequestro preventivo contra societatem per un valore equivalente al profitto del reato*, pagg. 1788 ss.

[201] Cass. pen., 20 dicembre 2005, n. 3615, in *www.dejure.it.*

[202] Cass. civ., SS.UU., 30 settembre 2009, n. 20936, in *Foro Italiano*, 2010, II, c. 3127 ss.

1.1.1. Il profilo sanzionatorio del d.lgs. n. 231/2001

La cornice sanzionatoria predisposta dal legislatore a carico degli enti per illeciti amministrativi dipendenti da reato è abbastanza specifico e peculiare, caratterizzandosi in sanzioni amministrative (sanzioni pecuniarie e sanzioni interdittive) e sanzioni speciali, sebbene di matrice penalistica, quali la confisca e la pubblicazione della sentenza.

L'obiettivo del legislatore è quello di creare un apparato sanzionatorio in grado di fungere da dissuasore nei confronti delle persone giuridiche, atteggiandosi come incisivo senza però assumere i contorni di regime eccessivamente repressivo.

La dottrina ha osservato che le sanzioni previste per gli enti collettivi «attingono direttamente (sanzione pecuniaria e confisca) o indirettamente (sanzioni interdittive) al profitto, o comunque all'utile economico dell'ente, e sono dirette a perseguire esigenze di prevenzione, generale e speciale, attraverso la tecnica del *carrot and stick*. Il sistema, se da un lato cerca di distogliere gli enti da propositi criminosi mediante la minaccia di pene severe e, in caso di recidiva, di inasprimenti sanzionatori, dall'altro, valorizzando in funzione premiale il postfatto, concede cospicui abbattimenti di pena — fino a due terzi dell'entità della sanzione pecuniaria — laddove l'ente medesimo ponga in essere attività riparatorie efficacemente dirette a rimuovere le conseguenze del reato e/o adotti i *compliance programs*, ovvero modelli organizzativi idonei a prevenire reati della stessa specie di quelli, rispetto ai quali, si è configurata la responsabilità dell'ente»[203].

Esistono, dunque, diverse tipologie di sanzioni. Le sanzioni pecuniarie sono previste dagli artt. 10, 11 e 12 del d.lgs. n. 231/02001, e sono sanzioni

[203] M. Lottini, *Il sistema sanzionatorio*, in G. Garuti (a cura di), *Responsabilità degli enti per illeciti amministrativi*, cit., pag. 130. Nello stesso senso, valutando favorevolmente l'intervento del legislatore, R. Guerrini, *Le sanzioni a carico degli enti nel d.lgs. n. 231/2001*, in G. De Francesco (a cura di), *La responsabilità degli enti: un nuovo modello di giustizia "punitiva"*, Torino, 2004, pag. 89.

tipicamente amministrative. Si tratta di una sanzione indefettibile, nel senso che deve essere necessariamente applicata in caso di sussistenza di un illecito amministrativo derivante da reato.

Il legislatore, al fine di rendere più flessibile il sistema sanzionatorio, ha previsto un innovativo meccanismo di commisurazione della sanzione "per quote", che si articola in una doppia determinazione del giudice: la prima riguarda il numero di quote e si fonda sui comuni indici di gravità dell'illecito e, dunque, il grado di responsabilità dell'ente, la gravità del fatto commesso e l'attività esercitata al fine di eliminare oppure ridurre le conseguenze del fatto e per la prevenzione della commissione di illeciti ulteriori; la seconda, invece, ha ad oggetto il valore di mercato della singola quota, che deve essere determinato tenendo presente le condizioni economiche e patrimoniali dell'ente, al fine di garantire l'efficacia della sanzione[204]. Chiamato a rispondere della sanzione è esclusivamente l'ente con il suo patrimonio o fondo comune.

Per quanto concerne, invece, le sanzioni interdittive, esse sono previste dall'art. 9 del d.lgs. n. 231/2001, e sono caratterizzate da una afflittività piuttosto incisiva, in quanto sono idonee a generare delle limitazioni piuttosto significative all'attività di gestione e produttiva dell'ente, fino addirittura a determinarne la paralisi.

Le sanzioni interdittive sono infatti le seguenti: «a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di

[204] L'art. 12 del d.lgs. n. 231/2001 prevede, inoltre, che «la sanzione pecuniaria è ridotta della metà e non può comunque essere superiore a lire duecento milioni se: a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità; 2. La sanzione è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado: a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; b) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi. 3. Nel caso in cui concorrono entrambe le condizioni previste dalle lettere del precedente comma, la sanzione è ridotta dalla metà ai due terzi. 4. In ogni caso, la sanzione pecuniaria non può essere inferiore a lire venti milioni».

contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi».

Esse trovano applicazione insieme alle sanzioni pecuniarie, e possono essere comminate solo relativamente a quei reati per i quali il legislatore espressamente le prevede, ed in presenza di almeno una delle seguenti condizioni: «a) l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; b) in caso di reiterazione degli illeciti»[205].

Esse hanno una durata di minimo tre mesi e massimo due anni, e solo in casi eccezionali possono essere comminate in via definitiva. Il giudice, nella loro irrogazione, deve tenere conto del principio di proporzionalità, applicando la sanzione meno incisiva se adeguata.

Le sanzioni interdittive, infine, non possono essere applicate se: «a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; b) l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi; c) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca».

Altra sanzione, di matrice penalistica, è la pubblicazione della sentenza di condanna, prevista dall'art. 18 del d.lgs. n. 231/2001. La *ratio* di tale

[205] Cfr., sul punto, M. Panasiti, *Riparazione delle conseguenze del reato*, in M. Levis, A. Perini (diretto da), *La responsabilità amministrativa delle società e degli enti*, Bologna, 2014, pag. 357, secondo cui per evitare la sanzione interdittiva che, di regola, tende a paralizzare o condizionare la svolgimento dell'attività, non è sufficiente aver eliminato la conseguenze e aver risarcito il danno, considerato che il modello di esonero dalla sanzione interdittiva diventa pienamente cofunzionale agli scopi di tali sanzioni solo se la condotta compensativa post factum ricomprende anche l'eliminazione del fattore rischio che ha provocato o agevolato la commissione del reato da cui dipende l'esistenza dell'illecito amministrativo».

previsione è quella di creare all'ente un danno di immagine, ma anche di fare in modo che i terzi possano essere tutelati.

Ultima sanzione prevista, poi, è la confisca, che ha sempre carattere obbligatorio ed è disposta con la sentenza di condanna dell'ente. La *ratio* della confisca è quella di precludere all'ente la possibilità di beneficiare dei frutti dell'attività illecita commessa nel suo interesse o a suo vantaggio. La confisca ha ad oggetto il prezzo o il profitto del reato, fatta salva la parte acquistata dai terzi di buona fede e quella che può essere restituita al danneggiato.

Vi è poi anche l'ipotesi residuale della confisca per equivalente, avente ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato. La finalità di tale previsione è piuttosto chiara, ossia quella di evitare che l'ente possa godere dei frutti della sua attività criminosa anche quando il prezzo od il profitto della stessa sia ormai sostanzialmente non più disponibile. Va segnalato, inoltre, che le sanzioni amministrative si prescrivono in cinque anni[206].

Un aspetto peculiare del d.lgs. 231/2001, è l'aver previsto l'applicabilità delle misure cautelari, in relazione agli illeciti amministrativi commessi dell'ente, in presenza delle condizioni previste dall' art. 45 della summenzionata disciplina. In particolare, esse sono rappresentate da gravi indizi di responsabilità dell'ente per l'illecito amministrativo, rivelatore di un consistente *fumus* di colpevolezza, e dalla presenza di fondati e specifici elementi che fanno presumere la reiterazione di reati della medesima indole, espressione quest' ultime di *esigenze cautelari*[207]. Il giudice nel disporre le suddette misure, su richiesta del pubblico ministero, il quale è l'unico a detenere tale potestà, deve attenersi a specifici criteri di scelta, quali idoneità,

[206] Ai sensi dell'art. 22 del d.lgs. n. 231/2001, «interrompono la prescrizione la richiesta di applicazione di misure cautelari interdittive e la contestazione dell'illecito amministrativo a norma dell'articolo 59. Per effetto della interruzione inizia un nuovo periodo di prescrizione. Se l'interruzione è avvenuta mediante la contestazione dell'illecito amministrativo dipendente da reato, la prescrizione non corre fino al momento in cui passa in giudicato la sentenza che definisce il giudizio».

[207] A. Traversi, S. Gennai, *Diritto penale commerciale*, cit., pagg. 318 ss.

proporzionalità ed adeguatezza. E' il caso di ricordare come il giudice possa solo accogliere o respingere la suddetta richiesta del pm, ma non potrà in alcun caso applicare una misura più grave, mentre sarà consentita, nell'eventualità, l'applicazione di una misura cautelare meno grave.
Le tipologie di misure previste dall'art. 45 del d.lgs. 231/2001, sono le stesse di quelle previste dall'art. 9, comma 2[208].
La disciplina in esame, oltre all'applicazione delle misure cautelari di cui abbiamo appena discusso, prevede due ulteriori strumenti di tutela. Ci si riferisce al "sequestro preventivo" ex art. 53 ed il "sequestro conservativo" ex art 54 d.lgs. 231/2001, i quali hanno la funzione di «evitare la dispersione delle garanzie delle obbligazioni civili derivanti dal reato e di paralizzare o ridurre l'attività dell'ente quando la prosecuzione dell'attività stessa possa aggravare o protrarre le conseguenze del reato ovvero agevolare la commissione d altri reati»[209]. In riferimento a tali istituti vengono richiamate, in quanto compatibili, le norme processuali che regolano gli omologhi istituti di dritto penale.

1.1.2. I soggetti destinatari della disciplina

Il d.lgs. n. 231/2001 fa riferimento a tutte le persone giuridiche che esercitano attività di natura economica, una platea di destinatari piuttosto estesa: infatti all'art. 1, commi 2 e 3, del d.lgs. n. 231/2001, la disciplina si rivolge agli «enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica», escludendo, pertanto, gli enti dello Stato, quelli pubblici territoriali, ossia Regioni, Province e Comuni, gli enti pubblici non

[208] L'art. 9, comma 2, del d.lgs. n. 231/2001 prevede a) l'interdizione dall'esercizio dell'attività; b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; e) il divieto di pubblicizzare beni o servizi.
[209] A. Traversi, S. Gennai, *Diritto penale commerciale*, cit., pag. 316.

economici[210] nonché quelli che esercitano funzioni di rilevanza costituzionale, tra cui rientrano i partiti politici e i sindacati.
L'impresa individuale è stata considerata dalla giurisprudenza prevalente non rientrante nella disciplina in esame, non trattandosi di un ente collettivo, sebbene l'orientamento sul tema non è ampiamente condiviso[211].
In generale, la disciplina è finalizzata al contrasto dell'attività criminosa delle società commerciali, per cui è a queste ultime che il legislatore *in primis* fa riferimento.

1.1.3. I criteri di imputazione

Il legislatore ha delineato una fattispecie che presenta una struttura complessa, che si perfeziona quando il reato viene commesso nell'interesse dell'ente o a suo vantaggio, e sia stato realizzato da soggetti legati all'ente da uno specifico rapporto.
In base all'art. 5 del d.lgs. n. 231/2001, il reato in oggetto deve essere stato commesso «a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso»; «b) da

[210] Per quanto riguarda, in particolare, gli enti pubblici non economici, Cass. pen., 26 ottobre 2010, n. 234, in *www.cortedicassazione.it*, 2010, 248795, ha sostenuto che la natura pubblicistica di un ente è condizione necessaria ma non sufficiente per l'esonero dalla disciplina in questione, dovendo necessariamente essere presente anche la condizione dell'assenza di svolgimento di attività economica da parte dell'ente medesimo.
[211] Inizialmente, infatti, la Cassazione aveva escluso che l'impresa individuale fosse soggetta alla disciplina di cui al d.lgs. n. 231/2001, in quanto essa era riservata unicamente agli enti dotati di personalità giuridica strutturati in forma societaria o pluripersonale. Una estensione della disciplina, dunque, sarebbe incompatibile con il divieto di analogia tipico del diritto penale. In tal senso si era espressa Cass. pen., 3 marzo 2004, n. 18941, in *ww.,dirittoegiustizia.it*, n. 30, 2004, p. 25. Successivamente, però, Cass. pen., 15 dicembre 2010, n. 15657, in *Cassazione penale*, 2011, p. 2556, aveva stabilito che invece la normativa trovava applicazione anche per le imprese individuali. La giurisprudenza ha poi cambiato nuovamente orientamento, sostenendo che «la normativa sulla responsabilità da reato degli enti prevista dal d.lgs. n. 231/2001 non si applica alle imprese individuali, in quanto si riferisce ai soli soggetti collettivi»: così Cass. pen., 16 maggio 2012, n. 30085, in *www.cortedicassazione.it*, 2012, 252995.

persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lett. a)».

Tali criteri di imputazione hanno carattere oggettivo, ad essi si affianca un requisito soggettivo, essendo stato previsto che per il perfezionarsi della responsabilità della persona giuridica sia necessario un legame fra il reato ed il comportamento dell'ente, di cui occorre accertare quantomeno la colpa.

I criteri di imputazione hanno, pertanto, natura oggettiva e soggettiva.

1.1.4. Gli autori del reato presupposto: soggetti in posizione apicali e soggetti sottoposti all'altrui direzione e controllo

I soggetti la cui attività criminosa può far scattare la responsabilità penale dell'ente, vanno accertati, in base alla cd. teoria organica, riprodotta dalla Relazione al decreto n. 231, in base alla quale «l'identità tra autore dell'illecito e destinatario della sanzione viene assicurata quando la persona fisica autrice del reato è un soggetto che ha agito "nell'interesse o a vantaggio" dell'ente»[212].

Pertanto, laddove un soggetto che, all'interno dell'organizzazione dell'ente, ricopre una qualifica, pone in essere una fattispecie delittuosa a vantaggio o nell'interesse dell'ente, è lo stesso ente protagonista della vicenda criminosa, in quanto, in base alla Relazione citata «se gli effetti civili degli atti compiuti dall'organo si imputano direttamente alla società, non si vede perché altrettanto non possa accadere per le conseguenze del reato, siano esse penali o - come nel caso del decreto legislativo - amministrative».

I soggetti che possono provocare la responsabilità penale dell'ente vanno individuati utilizzando un criterio oggettivo-funzionale, non tenendo conto solo del *nomen iuris* del rapporto, ma anche all'attività esercitata in concreto.

[212] Sui presupposti oggettivi necessari per l'affermazione della responsabilità penale dell'ente si v. G. Forti, *Uno sguardo ai "piani nobili" del d.lgs. n. 231/2001*, in *Rivista italiana di diritto e procedura penale*, 4, 2012, pagg. 1249 ss.; P. Cipolla, *Il d.lgs. n. 231 del 2001 nella prassi giurisprudenziale, a dieci anni dall'entrata in vigore*, in *Giurisprudenza di merito*, 6, 2011, pagg. 1468 ss.

Ci si riferisce ai rappresentanti, agli amministratori, a quelli che esercitano attività di direzione dell'ente oppure di una sua unità organizzativa dotata di autonomia sotto il profilo funzionale o finanziario e, infine, ai soggetti che lo gestiscono o controllano.

I ambito dottrinario è stato rilevato che tra i soggetti che occupano posizioni apicali debbano rientrare i direttori generali che «non sono organi ma dipendenti (e possono, in casi particolari, anche non esserlo) della società, i cui poteri di gestione derivano dal contratto di lavoro, e sono sottoposti alle direttive del consiglio di amministrazione»[213]. Nelle imprese di grandi dimensioni, tuttavia, non è raro che tali soggetti detengano una notevole autonomia operativa, che può arrivare ad essere superiore a quella degli amministratori.

Per quanto attiene, invece, i soggetti che svolgono una posizione apicale, di fatto, ovvero in assenza di un'investitura, la dottrina ha stabilito che l'esercizio di tali funzioni non deve essere episodico, visto che il legislatore ha inteso fare riferimento a coloro che «esercitano un penetrante dominio sull'ente (è il caso del socio non amministratore ma detentore della quasi totalità delle azioni, che detta dall'esterno le linee della politica aziendale ed il compimento di determinate operazioni)»[214].

Ulteriore categoria di soggetti concerne coloro i quali si trovano in una posizione subordinata, esercitando la loro attività sotto la direzione o la vigilanza altrui che, pure, possono "spendere" il nome dell'ente.

La necessità «di prevenire il fenomeno c.d. dell'"irresponsabilità organizzata" e di evitare preordinati (e altrimenti prevedibili) scaricamenti verso il basso della responsabilità»[215] spiega il coinvolgimento di tali soggetti. Il legislatore

[213] G. De Simone, *I profili sostanziali della responsabilità c.d. amministrativa degli enti: la parte generale e la parte speciale del d.lgs. 8 giugno 2001 n. 231*, in G. Garuti (a cura di), *Responsabilità degli enti per illeciti amministrativi*, Padova, 2002, pag. 103.
[214] G. De Simone, *I profili sostanziali della responsabilità c.d. amministrativa degli enti: la parte generale e la parte speciale del d.lgs. 8 giugno 2001 n. 231*, cit., pag. 104.
[215] Ivi, pag. 105.

ha inteso, sostanzialmente, evitare che l'ente possa garantirsi l'impunità facendosi schermo con lavoratori non apicali.

1.1.5. Criteri oggettivi: l'interesse o vantaggio dell'ente

Oltre al dato soggettivo, appena descritto, il legislatore ha considerato fondamentale che il reato detenga un profilo oggettivo venendo posto in essere nell'interesse dell'ente, oppure comunque a suo vantaggio.
Sebbene i due requisiti paiano essere molto simili, la Suprema Corte ha chiarito la differenza tra "interesse" e "vantaggio" dell'ente: in particolare, il criterio dell'interesse «esprime una valutazione del reato apprezzabile "*ex ante*" e cioè al momento della commissione del fatto e secondo un metro di giudizio marcatamente soggettivo mentre quello del vantaggio ha una connotazione essenzialmente oggettiva e come tale valutabile "*ex post*" sulla base degli effetti concretamente derivanti dalla realizzazione dell'illecito»[216].
Occorre, dunque, accertare concretamente le modalità dell'accaduto.
In base alla giurisprudenza il requisito dell'interesse si muoverebbe su un piano soggettivo, riferendosi alla sfera psichica del soggetto che ha agito

[216] Cass. pen., 21 gennaio 2016, n. 2544, in *www.altalex.com*. Secondo i giudici, nel caso di specie, «ricorre il requisito dell'interesse quando la persona fisica, pur non volendo il verificarsi dell'evento morte o lesioni del lavoratore, ha consapevolmente agito allo scopo di conseguire un'utilità per la persona giuridica; ciò accade, ad esempio, quando la mancata adozione delle cautele antinfortunistiche risulti essere l'esito (non di una semplice sottovalutazione dei rischi o di una cattiva considerazione delle misure di prevenzione necessarie, ma di una scelta finalisticamente orientata a risparmiare sui costi d'impresa: pur non volendo il verificarsi dell'infortunio a danno del lavoratore, l'autore del reato ha consapevolmente violato la normativa cautelare allo scopo di soddisfare un interesse dell'ente (ad esempio far ottenere alla società un risparmio sui costi in materia di prevenzione). Ricorre il requisito del vantaggio quando la persona fisica, agendo per conto dell'ente, pur non volendo il verificarsi dell'evento morte o lesioni del lavoratore, ha violato sistematicamente le norme prevenzionistiche e, dunque, ha realizzato una politica d'impresa disattenta alla materia della sicurezza del lavoro, consentendo una riduzione dei costi ed un contenimento della spesa con conseguente massimizzazione del profitto; il criterio del vantaggio, così inteso, appare indubbiamente quello più idoneo a fungere da collegamento tra l'ente e l'illecito commesso dai suoi organi apicali ovvero dai dipendenti sottoposti alla direzione o vigilanza dei primi».

mentre, il requisito del vantaggio si atteggia su un piano oggettivo, essendo legato alle conseguenze nella sfera della persona giuridica.

L'ente è responsabile anche se l'autore del fatto ha inteso agire con il solo scopo di arrecare un vantaggio personale ma, di cui, se ne sia avvalso anch'esso. Se la persona fisica ha commesso il fatto al solo scopo di arrecare un vantaggio a sé o ad un terzo, l'ente non è considerato responsabile, venendosi ad "infrangere" il rapporto di immedesimazione organica.

In ambito dottrinario è stato sostenuto che «anche sull'assetto di questo requisito oggettivo sono altresì da segnalare le ricadute derivanti dell'allargamento dei reati presupposto. Ciò innanzi tutto con l'inclusione tra gli stessi di fattispecie che non costituiscono davvero espressione della criminalità di impresa e che, come tali, mal si attagliano alla logica della colpa da rischio di base lecito e, dunque, alle finalità di natura economica in senso stretto»[217].

Si fa riferimento all'ampliamento dei reati presupposti verificatosi soprattutto dopo che l'art. 9 della legge 3 agosto 2007, n. 123 ha introdotto nel d.lgs. n. 231 l'art. 25-septies, estendendo i reati presupposto «ai delitti di cui agli articoli 589 e 590, terzo comma, del codice penale, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sui lavoro».

Tuttavia, è stato sostenuto che «ben noto è il rilievo della difficoltà che il reato colposo di evento (morte o lesioni del lavoratore) possa essere commesso "nell'interesse dell'ente", vista la ritenuta incompatibilità di questo criterio con un delitto realizzato appunto "senza volizione"; ma anche il criterio del vantaggio è parso mal conciliabile con questa categoria di reati, a meno di riferire i due concetti di "interesse" e "vantaggio" non già all'evento delittuoso, bensì alla condotta che si ponga in contrasto con le regole cautelari a tutela della salute e dell'incolumità dei lavoratori, salve le ricadute in

[217] G. Forti, *Uno sguardo ai "piani nobili" del d.lgs. n. 231/2001*, cit., pag. 1251.

termini di anticipazione della tutela destinate a conseguirne (e peraltro incombenti su tutto l'impianto del d.lgs.)»[218].
Di tali questioni, dunque, il legislatore avrebbe dovuto tenere conto.

1.1.6. Criteri soggettivi: la colpa di organizzazione. Esonero della responsabilità dell'ente e modelli organizzativi

Come già detto in precedenza, non è sufficiente la presenza dei requisiti oggettivi, essendo indispensabile che sussista anche un criterio soggettivo, ossia la colpevolezza della persona giuridica. Avendo chiarito che la colpevolezza dell'ente non può muoversi secondo i canoni ordinari di tipo psichico, è chiaro che l'ente è responsabile per una vera e propria colpa "organizzativa".
L'ente, pertanto, può essere considerato colpevole del reato posto in essere determinate persone fisiche solo nel momento in cui tali reati siano stati agevolati da lacune organizzative e dall'assenza di un meccanismo di controllo[219].
Come è stato osservato, «i profili di tale colpa di organizzazione sono strutturati diversamente a seconda della tipologia di soggetti che hanno commesso il reato nell'interesse o a vantaggio dell'ente, ovvero a seconda che il reato sia stato posto in essere da un soggetto apicale o da un sottoposto, poiché in tali due casi sono diversi i tipi di cautele da adottare per evitare la violazione della legge penale»[220].

---

[218] G. Forti, *Uno sguardo ai "piani nobili" del d.lgs. n. 231/2001*, cit., pag. 1251.
[219] In tal senso S. Riondato, *Prevenzione dei reati riconducibili alla politica dell'ente e personalità della responsabilità penale dell'ente (d.lgs. 8 giugno 2001 n. 231)*, in *Rivista trimestrale di diritto penale dell'economia*, 2003, pag. 824. In senso critico nei confronti di tale requisito M. Romano, *La responsabilità amministrativa degli enti, società o associazioni: profili generali*, cit., pag. 407.
[220] Per questa ricostruzione C.E. Paliero, *Il d.lgs. 8 giugno 2001, n. 231: da ora in poi, societas delinquere (et puniri) potest*, in *Corriere Giuridico*, 2001, pagg. 845 ss.; G. De Simone, *I profili sostanziali della responsabilità c.d. amministrativa degli enti: la parte generale e la parte speciale del d.lgs. 8 giugno 2001 n. 231*, cit., pag. 106.

Per quanto riguarda, in particolare, l'ipotesi della fattispecie criminosa posta in essere da soggetti che si trovano in una posizione apicale, in tal caso l'ente è chiamato ad una prova contraria molto rigorosa, essendo tenuto a dimostrare che non ha avuto alcuna responsabilità nel verificarsi dell'episodio criminoso. Il fatto commesso dal soggetto posto in posizione apicale, infatti, è considerato alla stregua di un fatto commesso dall'ente stesso, per cui in capo a questi vi è una prova molto difficile.

In particolare, l'ente è tenuto a dimostrare, anzitutto, di aver adottato tutti i controlli necessari per impedire la commissione del reato; di aver istituito un organismo di controllo indipendente deputato alla verifica della commissione di tali reati; che gli autori materiali sono riusciti ad eludere il modello organizzativo. Infine, l'ente deve dimostrare che l'organo di controllo è stato vigile senza commettere negligenze, e nonostante questo il reato o i reati sono stati commessi.

Il *compliance programs*, pertanto, viene ad essere la chiave di volta che può esimere l'ente dall'addebito di responsabilità. L'adozione di tali programmi, invero, non ha carattere obbligatorio, costituendo, piuttosto, un vero e proprio onere per l'ente, che può andare esente da responsabilità penale solo dimostrando l'esistenza e l'efficacia dello stesso. Non basta, dunque, la mera adozione del programma, essendo necessario che esso funzioni correttamente, secondo le indicazioni del legislatore.

In particolare, i modelli di organizzazione e di gestione della società dovranno essere molto elastici e flessibili, nel senso che nella loro elaborazione si dovrà giocoforza tenere conto delle caratteristiche della società, in quanto non è possibile immaginare l'esistenza di un unico modello gestionale che sia valido per tutti.

Il legislatore, comunque, impone che il modello sia in grado di soddisfare le seguenti esigenze: a) individuare le attività nel cui ambito possono essere commessi reati; b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da

prevenire; c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati; d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli; e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello[221].

Per quanto riguarda, infine, i reati commessi da coloro i quali esercitano, all'interno dell'ente, una attività posta in posizione non apicale, dunque sotto il controllo e la direzione altrui, la responsabilità posta a carico dell'ente si presenta come meno rigorosa, verificandosi a tutti gli effetti una inversione dell'onere della prova. In tal caso, infatti, sarà il pubblico ministero a dover dimostrare che la commissione del reato è stata resa possibile dalla negligenza degli organi di controllo e vigilanza dell'ente, che non hanno funzionato correttamente.

L'ente risponde, in tal caso, in presenza di un vero e proprio *deficit* organizzativo. Tuttavia, il legislatore ha previsto una nuova via di fuga per l'ente, che può andare esente da responsabilità penale dimostrando di aver adottato un modello di organizzazione e gestione tale da prevenire in astratto l'ipotesi delittuosa in concreto commessa. Quindi nel caso di reato commesso da subordinati la responsabilità è legata all'inosservanza degli obblighi di direzione e vigilanza. Questa responsabilità è sicuramente esclusa in caso di adozione ed efficace attuazione da parte dell'ente di un modello di organizzazione, gestione e controllo, ma è ben possibile dare comunque dimostrazione di avere adempiuto ai propri obblighi di direzione in altro modo.

---

[221] Nel senso che l'adozione del *compliance programs* non si esaurisce in un unico momento, essendo l'ente tenuto ad un aggiornamento del modello a seconda dello sviluppo della propria attività. Sul punto si v. U. Lecis, *L'Organismo di vigilanza e l'aggiornamento del Modello organizzativo*, in *Rivista – La responsabilità amministrativa delle società e degli enti*, 4, 2006, pag. 40.Va ricordato che il legislatore ha comunque previsto la possibilità che tali modelli vengano adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti e comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli stessi.

Alla luce di quanto detto sinora, pare evidente che «il modello organizzativo, per risultare idoneo, deve stabilire, previo monitoraggio delle aree di attività soggette al rischio di commissione di reati, appositi paradigmi procedimentali per la formazione e l'attuazione delle decisioni dei vertici aziendali, per la gestione delle risorse finanziarie e per la trasmissione delle informazioni all'organismo di vigilanza. L'efficace attuazione del modello è infine assicurata dalla previsione di un sistema sanzionatorio di carattere disciplinare»[222].

2. Il reato di frode informatica ai sensi del d.lgs. 231/2001

Nel 2001 i reati informatici non erano contenuti nell'elenco originario del d.lgs. n. 231, fatta eccezione per il reato di frode informatica a danno di enti pubblici. Solo nel 2008 finalmente tali reati sono stati inseriti, per effetto della legge n. 48/2008 con la quale il legislatore ha deciso di ratificare la Convenzione di Budapest del Consiglio d'Europa sul cyber crime, con alcune modifiche.

A seguito di tale provvedimento legislatore sono entrati a far parte del d.lgs. n. 231/2008, tra i reati presupposto, i reati informatici. Questo, in particolare, è l'elenco dei reati informatici inclusi nel d.lgs. n. 231/2001: falsità in un documento informatico, accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche, intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di informazioni, dati e programmi

[222] A. Traversi, S. Gennai, *Diritto penale commerciale*, cit., pag. 308.

informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, danneggiamento di sistemi informatici o telematici, danneggiamento di sistemi informatici o telematici di pubblica utilità, frode informatica del certificatore di firma elettronica.

È chiaro che l'inserimento del reato di frode informatica tra i reati presupposto è finalizzato a valorizzare il concetto di sicurezza informatica. La sicurezza informatica può essere considerata come quell'insieme di misure di carattere tecnologico, organizzativo e procedurale indirizzate ad assicurare la protezione dei sistemi informatici e di tutti i dati in essi contenuti[223].

Inoltre, la sicurezza informatica è diretta a garantire l'autenticazione dell'utente, la disponibilità, l'integrità e la riservatezza di tutte le informazioni e dei servizi gestiti o erogati in modalità digitale, onde prevenire eventuali rischi o violazioni.

L'obiettivo della sicurezza informatica, quindi, è quello di garantire la riservatezza, l'integrità e la disponibilità dei dati. La riservatezza è da intendersi nel senso di garantire che i dati non vengano divulgati al di fuori del sistema informatico nel quale sono collocati. La riservatezza copre anche i dati nel momento della trasmissione, memorizzazione e conservazione[224].

Quanto all'integrità, la sicurezza informatica è finalizzata ad evitare che i dati non vengano modificati in maniera illegittima da parte di soggetti esterni del tutto privi di autorizzazione.

Quanto, infine, alla disponibilità, la sicurezza informatica deve garantire la reperibilità dei dati da parte dei legittimi titolari, ragion per cui sono opportuni sistemi di memorizzazione.

Questa visione della sicurezza informatica sarebbe tuttavia riduttiva: essa, infatti, non può essere intesa unicamente nel senso di insieme delle misure di

[223] In tal senso F. Cirinni, *La sicurezza informatica. Tra informatica, matematica e diritto*, Milano, 2017, pag. 1.

[224] Si v. P. Perri, *Privacy, diritto e sicurezza informatica*, Milano, 2007, pagg. 10 ss.

protezione e di contrasto ad eventuali tentativi di intromissione da parte di soggetti esterni.

Diversamente, la sicurezza informatica concerne anche quelle misure che vengono adottate per evitare che eventi accidentali, quali ad esempio interruzioni improvvise di corrente o altri eventi del genere, possano provocare effetti pregiudizievoli nei confronti dei dati contenuti nel sistema informatico.

Ne deriva cha la sicurezza informatica si muove su due piani del tutto diversi: su un piano tecnologico ed informatico, da un lato, e su un piano organizzativo, dall'altro. La nozione di sicurezza informatica, poi, distingue necessariamente i rischi dalle violazioni: quanto ai rischi, si tratta di eventi accidentali o utilizzi impropri del sistema da parte di soggetti accreditati[225].

Le violazioni, invece, sono solitamente accessi non autorizzati, che vengono di solito posti in essere attraverso Internet o mediante l'installazione di appositi programmi da memorie esterne per opera di un soggetto, il c.d. *cracker*, che si pone come obiettivo quello di modificare, catturare, eliminare o rendere del tutto inaccessibili i dati contenuti nel sistema.

La sicurezza informatica, in definitiva, si pone quindi l'obiettivo di prevenire i rischi e le violazioni elaborando opportuno politiche di sicurezza.

Proprio questo è il motivo per cui la sicurezza informatica e il d.lgs. n. 231/01 sono progressivamente diventati un binomio difficilmente scindibile. La legge n. 48/2008, mediante la quale ha trovato attuazione nell'ordinamento giuridico italiano la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001, ha modificato il codice penale ed il codice di procedura penale, nonché l'art. 24 del d.lgs. n. 231/01, aggiungendovi l'art. 24 *bis*, rubricato "Delitti informatici e trattamento illecito di dati quali reati presupposto"[226].

---

[225] Cfr. P. Iezzi, R. Paglia, F. D'Agostino, *Vulnerability Assessnent*, Milano, 2018, pagg. 1 ss.

[226] Il testo integrale dell'art. 24 *bis* del d.lgs. n. 231/01 dispone che «In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-

Tale disposizione introduce numerosi reati informatici tra quelli presupposto previsti dal suddetto d.lgs. n. 231/01: si tratta, in particolare, dell'accesso a sistema informatico o telematico, dell'intercettazione, dell'impedimento e illegittima interruzione delle comunicazioni informatiche o telematiche, del danneggiamento di dati o informazioni contenuti in supporti informatici o telematici, ecc.

La riforma è stata considerata scarsamente efficace dalla dottrina[227], almeno per quanto concerne la salvaguardia dei dati telematici aziendali, considerato che non pare esservi attenzione per una mappatura delle aree di rischio, indispensabile per la protezione dei sistemi aziendali.

In secondo luogo, si è lamentata l'assenza di procedure preventive e adozione di modelli comportamentali idonei ad arrestare sul nascere qualsivoglia prassi lesiva dei dati informatici aziendali, dimenticando che agire sull'adozione di buone prassi e sull'informazione rappresenta lo strumento più semplice per ridurre il rischio del verificarsi dei reati presupposto.

L'altro fattore critico del d.lgs. n. 231/01 in materia di sicurezza informatica concerne la scelta di adottare dei protocolli rigidi, che non tengono conto delle specificità di ogni singola azienda, atteggiandosi come strumenti preconfezionati che, spesso, si rivelano del tutto inidonei a calarsi nel contesto aziendale di riferimento.

---

ter, 635-quater, 635-quinquies terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote. 2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote. 3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote. 4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)».

[227] Cfr. A. Giarda, *L'elenco dei reati presupposto ex D.Lgs. 231/2001 si ampli*, in *Il Corriere del Merito*, 6, 2008, pagg. 649 ss.

Per tale ragione, al fine di garantire al meglio l'effettiva salvaguardia dei dati informatici dell'azienda, è opportuno che ogni contesto aziendali si doti di un responsabile della sicurezza informatica cui incomba il compito di organizzare tutto l'apparato di salvaguardia dei dati aziendali verificando l'adozione dei protocolli e delle norme comportamentali previsti dal d.lgs. n. 231/01.

3. Frode informatica: il modello di organizzazione, gestione e controllo nella prevenzione dei reati informatici

La previsione di modelli organizzativi e gestionali idonei a prevenire il reato di frode informatica (così come invero altri reati del genre) rappresenta senza alcun dubbio la più grande novità del d.lgs. n. 231/2001. La dottrina, in proposito, ha osservato che «si tratta di un ennesimo derivato dell'ormai dominante cultura giuridica americana (che da tempo conosce i c.d. *compliance programs*), in forza del quale è da prevedere che almeno le più importanti società, allo scopo di ridurre il rischio derivante da comportamenti individuali illegittimi, provvederanno a dotarsi di un insieme di regole procedurali interne, i cui punti salienti sono sommariamente enunciati dall'art. 6, comma 2, per i dirigenti e, per quel che riguarda i dipendenti, dall'art. 7 della medesima legge»[228].

I modelli organizzativi e gestionali sono finalizzati alla prevenzione dei reati ma, come è ovvio che sia, essi non precludono in radice la possibilità che tali reati siano realizzati, essendo ben possibile che comportamenti individuali devianti, e dunque illegittimi, vengono comunque posti in essere, vanificando il modello organizzativo.

[228] R. Rodorf, *I criteri di attribuzione della responsabilità. I modelli organizzativi e gestionali idonei a prevenire i reati*, in *Le Società*, 11, 2001, pag. 1300. Cfr. sul tema anche S. Perini, *I modelli di organizzazione, gestione e controllo nel d.lgs. n. 231/2001. Profili applicativi e giurisprudenziali*, Vicalvi, 2015, pagg. 1 ss.

Tuttavia, la costruzione di tale modello è chiaramente finalizzata a responsabilizzare l'ente, ed a mostrare che esso si muove sulla linea della legalità. L'obiettivo, sostanzialmente, è quello di rendere l'eventuale reato posto in essere un fatto episodico ed eccezionale, che nulla ha a che vedere con l'attività propria dell'ente e la sua politica aziendale.

Il legislatore ha previsto che l'adozione preventiva dei modelli di organizzazione può escludere, in radice, la responsabilità dell'ente per i reati posti in essere dai propri rappresentati, dirigenti o dipendenti; se adottati prima dell'apertura del dibattimento del processo di primo grado, poi, il quale a tal fine può essere oggetto di un provvedimento di sospensione, l'ente può ottenere uno sconto di pena, in particolare evitando le gravi sanzioni interdittive di cui all'art. 16[229] del d.lgs. n. 231/2001, impedendo quindi anche la pubblicazione della sentenza; se adottati entro il medesimo termine possono implicare una sensibile riduzione delle pene pecuniarie.

Va segnalato, ancora, che anche la mera dichiarazione, da parte dell'ente, di volersi dotare in futuro dei modelli organizzativi, acquisisce rilevanza considerato che, in presenza degli altri requisiti di cui all'art. 17 del d.lgs. n. 231/2001, può consentire all'ente medesimo di ottenere la sospensione delle misure cautelari interdittive che eventualmente siano state adottata durante la causa. Tali misure poi saranno effettivamente revocate nel momento in cui l'ente attuerà in concreto i modelli.

Il ruolo dei modelli organizzativi, dunque, assume una rilevanza decisiva, in alcuni casi finanche eccessiva: si pensi che la loro adozione dopo il processo

[229] Secondo il quale «può essere disposta l'interdizione definitiva dall'esercizio dell'attività se l'ente ha tratto dal reato un profitto di rilevante entità ed è già stato condannato, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività. 2. Il giudice può applicare all'ente, in via definitiva, la sanzione del divieto di contrattare con la pubblica amministrazione ovvero del divieto di pubblicizzare beni o servizi quando è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni. 3. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità è sempre disposta l'interdizione definitiva dall'esercizio dell'attività e non si applicano le disposizioni previste dall'articolo 17».

può permettere all'ente, che già sia stato destinatario di una sentenza di condanna, di ottenere la conversione delle sanzioni interdittive ex art. 78 d.lgs. n. 231/2001, sempreché entro venti giorni dalla notifica della sentenza se ne dimostri l'attuazione congiuntamente agli altri requisiti previsti dal citato art. 17[230].

I modelli organizzativi, pertanto, assumono rilevanza non solo ai fini della prevenzione del reato, ma anche in un momento successivo, in quanto la loro attuazione in concreto può consentire all'ente di evitare, a posteriori, l'applicazione delle più gravi sanzioni interdittive. Il rischio della scelta del legislatore, tuttavia, è che tali modelli attuati *post factum* non possano essere valutati dal giudice, il quale non avrà gli strumenti per verificarne la bontà applicativa.

La conseguenza di ciò è che il giudice non avrà motivi per negare lo sconto di pena, ma ciò andrà inevitabilmente a discapito dell'efficacia dei modelli medesimi, i quali ben potranno essere costruiti unicamente ai fini dello sconto di pena, senza un reale impatto nella prassi.

Si è osservato, in proposito, che era preferibile «la diversa soluzione originariamente adombrata nel disegno di legge per la riforma del diritto societario (c.d. progetto Mirone), secondo cui l'adozione da parte della società di misure gestionali ed organizzative idonee ad evitare il rischio del ripetersi di reati non avrebbe dovuto incidere sull'entità della pena ma avrebbe consentito soltanto la sospensione condizionale della sanzione irrogata a carico della medesima società»[231].

---

[230] Infine, nel caso in cui, in luogo della sanzione interdittiva che determinerebbe la sospensione di un'attività, venga disposta la nomina di un commissario giudiziario, ai sensi dell'art. 15, costui dovrà tra l'altro provvedere a predisporre l'adozione dei modelli secondo la previsione del comma 3 del medesimo articolo.

[231] R. Rodorf, *I criteri di attribuzione della responsabilità. I modelli organizzativi e gestionali idonei a prevenire i reati*, cit., pag. 1304. In senso analogo si v. anche G. Forti, *Uno sguardo ai "piani nobili" del d.lgs. n. 231/2001*, cit., pag. 1254, secondo il quale «ai modelli compete in realtà una duplice funzione: sia esimente (oppure, a seconda delle diverse prospettive teoriche: scusante, o di esclusione della punibilità, o impeditiva della realizzazione degli elementi costitutivi della responsabilità), sia riparatoria. L'adozione post delictum di modelli idonei ha infatti come conseguenza, insieme ad altre condizioni (artt. 12 e 17 d.lgs.

In generale, però, la funzione principale del modello è quella di prevenire i reati, fungendo da vera e propria esimente per l'ente, il quale è dunque indotto dal legislatore a costruire il modello onde evitare di incorrere in responsabilità penale. Ne deriva, dunque, che l'adozione del modello non costituisce affatto un obbligo, ma esclusivamente un onere funzionale per le società, idoneo ad escludere, in presenza delle altre condizioni previste dalla legge, la responsabilità delle stesse.

Nella prassi, però, l'introduzione del modello organizzativo tende a coincidere con un vero e proprio obbligo, in quanto la giurisprudenza, in assenza di un modello organizzativo, è sostanzialmente unanime nell'addossare all'ente la responsabilità penale, sovente senza nemmeno ricorrere alle tipiche verifiche del caso[232].

Vi è tuttavia una differenza tra i reati posti in essere dai soggetti apicali e quelli posti in essere da altri dipendenti dell'azienda: la differenza risiede nel fatto che mentre nel primo caso il modello è l'unica possibilità riservata all'ente per evitare di incorrere a responsabilità penale, nella seconda ipotesi, invece, la responsabilità non sussiste laddove gli organi all'uopo deputati hanno correttamente esercitato la loro funzione di direzione e vigilanza sui subordinati.

La dottrina, in proposito, ha rilevato che «l'adozione del modello in tale ipotesi assicura una presunzione ex lege di corretto svolgimento degli obblighi di direzione o vigilanza. L'ordinamento attribuisce effetti premiali anche all'adozione successiva. L'adozione del modello successivo al verificarsi del reato può determinare infatti una riduzione della sanzione pecuniaria ovvero la non applicazione delle sanzioni interdittive»[233].

231/2001), una significativa riduzione della sanzione pecuniaria e l'inapplicabilità delle affilate sanzioni interdittive, con ciò esprimendosi « una significativa cofunzionalità con i criteri di ascrizione della responsabilità, atteso che viene valorizzato, in chiave specialpreventiva, il ruolo dei modelli in vista della minimizzazione del rischio-reato».

[232] Cfr. Tribunale di Milano, 13 febbraio 2008, n. 1774, in *www.iusexplorer.com.*

[233] L. Benvenuto, *Organi sociali e responsabilità amministrativa da reato degli enti*, in *Le Società*, 6, 2009, pag. 675.

Da un punto di vista classificatorio, sono state individuate «due tipologie di Modelli di organizzazione astrattamente attuabili sulla base del combinato disposto di cui agli artt. 6 e 7 d. lgs. n. 231/2001: l'uno, di tipo manageriale, l'altro, invece, di tipo imprenditoriale, i quali si differenziano per il fatto che, mentre il primo si caratterizza per una struttura decentrata, nella quale sono ben distinte le posizioni apicali rispetto a quelle ad esse subalterne, il secondo presenta un accentramento delle decisioni nel soggetto posto in posizione apicale; differenziazione che, come detto, trova la propria *ratio* nel sistema dualistico di responsabilità delineato dal d. lgs. n. 231/2001»[234].

Il legislatore, invero, nulla ha previsto circa il contenuto dei modelli di gestione, limitandosi unicamente ad individuare le esigenze cui esso deve fare fronte: in particolare, i modelli di organizzazione e di gestione devono «a) individuare le attività nel cui ambito possono essere commessi reati; b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire; c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati; d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli; e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello»[235].

In definitiva, da un punto di vista contenutistico, «il dettato legislativo individua – a guisa di contenuto minimo ed imperativo – tre aspetti peculiari ed imprescindibili, che costituiscono, per così dire, la base "normativa" del Modello: da un lato, l'individuazione del "rischio reato" a cui la società è maggiormente soggetta (lett. a) e b), ovvero un sistema di gestione dei rischi (cosiddetto *risk management*); dall'altro, la predisposizione di procedure

[234] C. Berti, *I "Modelli di organizzazione e gestione" previsti dal d.lgs. n. 231/01: natura ed inquadramento giuridico*, in *Contratto e impresa*, 4-2, 2012, pag. 1242

[235] In tal senso dispone l'art. 6, comma 2, del d.lgs. n. 231/01. Cfr. sul punto S. Pettinato, *I Modelli organizzativi e di gestione del d. lgs. n. 231/2001 e la responsabilità legale delle società e degli enti per i reati commessi dai loro appartenenti: note illustrative aggiornate*, in *Fisco*, 23, 2005, pagg. 3480 ss.

organizzative finalizzate a stabilire le modalità di gestione delle risorse finanziarie (lett. c), d)); nonché, un sistema sanzionatorio per la eventuale violazione delle misure previste (lett. e)»[236].

Ciò chiarito, sebbene i media raccontino spesso di attacchi informatici diretti alle aziende, di *hacker* che hanno colpito i grandi colossi della tecnologia quali Google, Apple ecc., le aziende, come già sottolineato in precedenza, hanno ancora dei tentennamenti nell'investire in maniera significativa sul tema della cybersecurity.

Eppure una strategia aziendale mirata è necessario per fronteggiare pericoli che diventano sempre più invasivi con il passare del tempo e l'evolvere della tecnologia. Il primo aspetto che deve essere considerato, infatti, nel momento in cui viene elaborata una strategia di cybersecurity, è che tale strategia deve essere flessibile, pronta ad essere rivista in ogni momento, in continuo aggiornamento, perché le tecniche elaborate dagli hacker sono sempre avanti rispetto a quelle difensive che vengono elaborate in sede di cybersecurity[237].

Tra le aziende più colpite vi sono soprattutto quelle bancarie, o comunque quelle che si occupano di intermediazione finanziaria, nei confronti delle quali, soprattutto nel corso degli ultimi anni, sono aumentati gli attacchi, specie a seguito della diffusione dei nuovi sistemi di pagamento e dei nuovi prodotti finanziari, quali il bitcoin.

Al fine di tenere sotto controllo il rischio aziendale e cercare di prevenirlo per quanto possibile è indispensabile che le aziende si dotino di un sistema di audit interno. L'attività di audit, termine di chiara matrice latina in cui l'auditor è il soggetto che ascolta, nonché il giudice istruttore, è molto diffusa nelle aziende italiane che sono caratterizzate dalla presenza di sistemi di gestione.

---

[236] C. Berti, *I "Modelli di organizzazione e gestione" previsti dal d.lgs. n. 231/01: natura ed inquadramento giuridico*, cit., pag. 3481.

[237] Cfr. R.S. Cheung, J.P. Cohen, H.Z. Lo, F. Elia, *Challenge Based Learning in Cybersecurity Education*, cit.

Va segnalato che l'attività di audit non è l'unica attraverso la quale le aziende effettuano delle verifiche sui rischi aziendali. Essa, infatti, si pone al vertice di un sistema molto articolato di controlli interni, finalizzati a ridurre il margine di rischio.

Per quanto concerne, nello specifico, il trattamento dei dati e la loro tutela al cospetto di attacchi hacker, il WP 29, con il parere 3/2010 ha indicato in maniera piuttosto chiara come deve essere strutturato un sistema di controlli interno: «esistono vari metodi a disposizione dei titolari del trattamento per valutare l'efficacia (o l'inefficacia) delle misure. Per il trattamento di dati di maggiori dimensioni, più complesso e ad alto rischio, gli audit interni ed esterni sono metodi comuni di verifica. Anche il modo in cui vengono condotti gli audit può variare, da audit completi ad audit negativi (che possono a loro volta assumere forme diverse)»[238].

Pare evidente, in definitiva, come non vi sia un modo standard per effettuare un audit interno adeguato. Quello che assume una rilevanza decisiva è la dimensione dell'azienda, in quanto ogni azienda presenta esigenze diverse, anche a seconda della mole di dati che è tenuta quotidianamente a salvaguardare.

Va segnalato, da ultimo, che anche il Regolamento generale sulla protezione dei dati (GDPR), regolamento (UE) n. 2016/679, si occupa di prevenzione contro la frode informatica. Va premesso che il Regolamento si pone come obiettivo l'unificazione della disciplina in tutti gli Stati membri, così come la Direttiva madre, la quale, tuttavia, non era stata in grado di impedire la frammentazione normativa nazionale.

[238] Del resto, lo stesso DPO (art. 39, paragrafo b del GDPR) è chiamato a svolgere fra i propri compiti una attività di verifica a vari livelli: b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

Va segnalato, in proposito, che tale rischio è piuttosto concreto anche alla luce della disciplina contenuta nel Regolamento in esame, considerato che esso lascia un ampio margine di discrezionalità ai singoli Stati membri in alcuni ambiti. L'obiettivo del Regolamento, tuttavia, non è tanto la mera armonizzazione, quanto piuttosto la uniformazione della disciplina dei diversi Stati membri in materia di dati personali.

Quanto ai principi generali fissati dallo stesso Regolamento, appare sicuramente meritevole il c.d. principio dell'*accountability*. Il principio in esame ha lo scopo di introdurre delle misure di sicurezza idonee a ridurre i rischi in materia di divulgazione o di perdita dei dati.

In tale prospettiva, il Regolamento chiarisce che è il titolare del trattamento dei dati personali a dovere valutare le misure tecniche e organizzative da adottare sulla base della natura dei dati, dell'oggetto, delle finalità di trattamento.

Tali misure non hanno carattere meramente teleologico, ma anche organizzativo, considerato che l'unico modo per affrontare in maniera costruttiva il problema della sicurezza dell'informazione è quello di avere una visione integrata, informatica-giuridica-organizzativa.

Sostanzialmente, quindi, bisogna comprendere che la questione della sicurezza non può riguardare una sola competenza, dovendo investire invece diversi settori professionali che devono collaborare in maniera sinergica[239].

[239] Come è stato osservato da G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, cit., 11, «la sicurezza deve garantire la protezione dei dati in ciascuna delle singole operazioni del trattamento. La sicurezza è un concetto dinamico e relazionale, da rapportarsi alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati personali oggetto di trattamento ed alle specifiche caratteristiche delle operazioni di trattamento compiute. Dunque sta al titolare individuare le misure di sicurezza da adottare dopo avere valutato la natura dei dati, il contesto, i rischi, i danni potenziali, i costi e lo stato dell'arte. Avendo definito le misure di sicurezza da adottare, il titolare deve compiere un'attività di continuo monitoraggio, per verificare che esse siano proporzionate e adeguate ai rischi, anch'essi in continuo mutamento. Occorre dunque una complessa attività di valutazione (tecnica, giuridica e organizzativa), un'analisi dei rischi e dei costi, una scelta sulle misure di sicurezza da adottare, l'istituzione di un presidio, l'emanazione di policy interne e quindi un'attività di monitoraggio continuo. Tutto ciò deve essere anche adeguatamente formalizzato e il titolare non soltanto deve attuare la normativa vigente, ma anche essere in grado di dimostrarlo».

In tale prospettiva, è stato dunque adottato il principio dell'*accountability*, che può essere tradotto come "principio di rendicontazione" o di "responsabilità", che consiste nell'obbligo di conformarsi e di dimostrare. In altri termini, il titolare del trattamento deve essere in grado di dimostrare che ha adottato un sistema di protezione dei dati personali idoneo ad evitare la loro divulgazione o la loro perdita[240].

Altro principio che rileva in questa sede è quello di ragionevolezza. Il trattamento dei dati deve avvenire, come in più occasioni sottolineato nel testo del Regolamento, secondo il principio di ragionevolezza, in quanto bisogna necessariamente utilizzare i dati nella misura strettamente necessaria secondo le finalità perseguite.

Altro principio fondamentale è quello del bilanciamento di interessi. Il considerando n. 4, infatti, chiarisce che «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità».

Lo stesso considerando cita «tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

[240] Come precisa il parere 3/2010 del Gruppo di lavoro art. 29, «l'architettura giuridica dei meccanismi di responsabilità prevedrebbe due livelli: il primo livello sarebbe costituito da un obbligo di base vincolante per tutti i responsabili (N.d.A.: titolari) (35) del trattamento. Tale obbligo comprenderebbe due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove. Questo primo livello potrebbe essere integrato da disposizioni specifiche. Il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure (norme di attuazione eccedenti il livello minimo)».

La disposizione, dunque, chiarisce espressamente che il diritto alla protezione dei dati personali non è in alcun modo un diritto assoluto, che deve essere tutelato sempre e comunque, pur in presenza di altri diritti altrettanto rilevanti. Tale diritto, infatti, va coordinato e bilanciato con gli altri diritti riconosciuti e tutelati dall'ordinamento (tra questi, l'interesse pubblico alla celerità, trasparenza ed efficacia all'attività amministrativa)[241].

Un altro principio rilevante, poi, è il principio della finalità del trattamento dei dati personali. In forza di tale principio, ogni trattamento dei dati è legittimo solo ed esclusivamente in ragione delle finalità dello stesso. I dati, infatti, devono essere raccolti per perseguire determinate finalità, le quali devono essere esplicitate all'utente in maniera chiara, al fine di consentire un consenso informato.

Laddove non venga precisata la finalità che si intende raggiungere con il trattamento dei dati, tale attività deve essere considerata illegittima. Altro corollario di tale principio è il fatto che non è possibile mutare la finalità del trattamento nel corso dello stesso, perché in tal modo verrebbe eluso il principio del consenso.

Con particolare riguardo alla sicurezza informatica, il GDPR ha il grande merito di aver superato un pregiudizio che ha da sempre caratterizzato la tematica in esame, ossia il fatto che la tutela e la salvaguardia dei dati informatici debba avere come obiettivo unicamente le minacce esterne, ossia gli attacchi di potenziali *hacker* interessati all'acquisizione dei dati per le finalità più disparate[242].

In realtà la situazione è assai diversa: in molti casi, infatti, la minaccia all'integrità dei dati informatici è frutto non di attacchi esterni, ma dell'adozione di comportamenti sbagliati da parte degli stessi dipendenti

[241] Cfr. ampiamente sul tema F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuov. leg. Civ. comm.*, 2, 2017, p. 369 ss.; A. Ricci, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2, 2017, p. 586 ss.

[242] Cfr., sul tema, N. Fabiano, *GDPR&Privacy. Consapevolezza e opportunità*, Milano, 2019, p. 65 ss.

dell'azienda, i quali, a causa di una scarsa cultura informatica, adottano modelli comportamentali idonei a porre in pericolo l'integrità dei dati informatici.

Nel GDPR un evidente riferimento alle misure di sicurezza si rinviene, anzitutto, nell'art. 22, disposizione che chiarisce che il titolare del trattamento deve prendere tutte le misure tecniche e organizzative adeguate per assicurare, ed essere capaci di dimostrare, che il trattamento dei dati personali viene effettuato in maniera conforme al Regolamento (principio di accountability).

Assume rilevanza, poi, l'art. 32 del GDPR, rubricato "Sicurezza del trattamento"[243]. Tale disposizione, diversamente da quanto si verificava in passato, comprende la necessità di tutelare non solo la riservatezza dei dati, ma anche la loro integrità e sicurezza, nonché la loro disponibilità. A tal fine all'interno di ogni azienda è necessario adottare buone pratiche e formare tutti coloro che hanno accesso ai dati informatici circa i corretti comportamenti da tenere al fine di evitare che i dati possano essere persi o danneggiati.

[243] Il testo integrale dell'art. 32 del GDPR è il seguente: «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

Il regolamento GDPR consiglia il ricorso alla crittografia, come strumento in grado di proteggere i dati attraverso la loro cifratura. In secondo luogo, è prevista l'esigenza di formare tutti gli operatori dell'azienda ad un utilizzo corretto della posta elettronica, considerato che la maggior parte dei dati "viaggia" attraverso la posta elettronica.

Ancora, assume rilevanza la necessità di procedere ad una corretta gestione e ad un continuo backup dei dati, indispensabile per evitare che le informazioni contenute nei files possano andare disperse o possano essere corrotte.

Un altro profilo molto importante è quello dell'autenticazione, che si basa normalmente sulla coppia username/password. Si tratta normalmente del primo ostacolo che si frappone a chi abbia intenzione di intromettersi in un sistema informatico aziendale. L'obiettivo di ogni responsabile aziendale della sicurezza informatica deve essere quello di sensibilizzare tutti i dipendenti dell'azienda a non sottovalutare il profilo dell'autenticazione, prediligendo un'autenticazione forte, se possibile anche biometrica, in grado di ridurre in maniera significativa il rischio di accessi abusivi ai sistemi informatici.

Più che le aziende, sono gli hacker a sembrare i grandi sconfitti della normativa europea, che negli ultimi due anni ha rallentato notevolmente la fragilità delle organizzazioni in termini di ransomware. I vincoli posti dal GDPR rendono più difficile il loro compito e hanno quindi messo in sicurezza le reti delle aziende, nonché i dati personali dei loro utenti e dipendenti.

Più la portata dei dati personali sfruttati dalle aziende è limitata (sia in termini di volume che di durata di conservazione), minori sono le opportunità per gli hacker di effettuare attacchi e prendere il controllo di database sensibili che potrebbero sfruttare a danno degli utenti.

Non è un caso che, secondo il rapporto Provider Lens Cyber Security - Solutions & Services 2020, realizzato da Information Services Group (ISG), le aziende europee abbiano aumentato la loro gamma e le loro competenze in

termini di cybersecurity da quando è stato introdotto il GDPR. Il web nel suo complesso è diventato più sicuro grazie al GDPR.

Nel complesso, il legislatore europeo l'accento sulla necessità di pseudonimizzazione da intendersi come un particolare trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a patto che tali informazioni aggiuntive vengano conservate in maniera separata e siano soggette a misure tecniche e organizzative finalizzate ad assicurare che tali dati personali non vengano attribuiti a una persona fisica identificata o identificabile.

Inoltre, per la prima volta in ambito europeo si parla di resilienza dei sistemi informatici, da intendersi come la capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da assicurare la disponibilità dei servizi erogati.

Notevole rilevanza, infine, viene attribuita dal legislatore comunitario anche al «disaster recovery, per cui diventa fondamentale predisporre uno specifico piano con il quale si intende fornire servizi volti all'analisi dei rischi di inoperatività del sistema EDP (informatico) e delle misure da adottare per ridurli, nonché la messa a punto del vero e proprio piano di emergenza informatica, che ricomprende, in particolare, procedure per l'impiego provvisorio di un centro di elaborazione dati alternativo o comunque l'utilizzo di macchine di soccorso da utilizzare in attesa della riattivazione»[244].

Pare evidente, in definitiva, come il GDPR abbia avvertito il bisogno di tutelare la sicurezza informatica non tanto e non solo sotto il profilo della riservatezza dei dati quanto, piuttosto, su quello, spesso sottovalutato, della disponibilità/integrità degli stessi. Si tratta di una prospettiva differente e sicuramente innovativa, che rende lo strumento utilizzato sicuramente assai pregevole.

[244] M. Iaselli, *Il concetto di sicurezza informatica nell'ottica del GDPR*, in *Rivista Informatica*, 2, 2017, p. 76.

4. Punti di contatto tra la normativa in materia di tutela della privacy ex GDPR e il d.lgs. n. 231/2001 alla luce della frode informatica

La frode informatica, come si è visto in precedenza, può avere ad oggetto il furto di dati sensibili. Ciò impone di verificare il puntuale coordinamento e i possibili elementi di sovrapposizione tra normativa a tutela della privacy ex GDPR e d.lgs. n. 231/2001. Bisogna però sottolineare che tali strumenti (D.lgs 231/2001 e GDPR) non sono totalmente sovrapponibili, essendo essi molto diversi. Infatti il d.lgs 231/2001 presente un campo di applicazione molto ristretto rispetto a quello del GDPR, dunque può recuperare diversi mezzi di tutela attraverso il ricorso a quest'ultimo.

Quanto ai reati informatici "presupposto", la rubrica dell'art. 24 bis del D.Lgs. n. 231/01 richiama, in maniera espressa, il "trattamento illecito di dati personali", anche se, poi, in concreto, l'elencazione, inserita all'interno della disposizione normativa in esame, non cita alcuna delle fattispecie previste dagli artt. 167 ss. del novellato D.Lgs. n. 296/2003 (Codice Privacy).

Si è osservato che «la *ratio* sottesa alla permanenza di tale richiamo risiede nell'oggettiva (ed inevitabile) circostanza che, in caso di commissione di un reato informatico, sussiste un evidente profilo di interdisciplinarietà con un trattamento illecito di dati personali: infatti, se si tiene a mente un qualsivoglia illecito illustrato nel decalogo di cui all'art. 24 bis del D.Lgs. n. 231/01 si verifica presumibilmente, appunto, anche un illecito trattamento di dati personali, tanto che la società, sia essa Titolare o Responsabile del trattamento, deve avviare le indagini interne al fine di verificare se vi sia stata anche una compromissione dei dati personali oggetto di trattamento, e, di conseguenza, intraprendere la procedura di gestione di una violazione dei dati personali (data breach) ex artt. 33 e 34 del GDPR»[245].

[245] G. Borghi, *Reati informatici e tutela dei dati personali: alcuni punti di contatto tra la normativa privacy e il d.lgs. N. 231/2001*, in *Salvis Juribus*, 2 maggio 2021.

I reati informatici presupposto sono già stati analizzati in precedenza. Quanto alla tutela penale nell'ambito della protezione dei dati personali, il Considerando n. 149), da leggersi, in combinato disposto, con l'art. 84 paragrafo 1) del GDPR, stabilisce che, tenuto conto della natura di ordine pubblico del precetto penale, ogni Stato deve avere la possibilità di stabilire le norme aventi ad oggetto le sanzioni penali applicabili per la violazione del GDPR e delle norme nazionali attuative dello stesso.

In particolare, l'art. 167 del novellato D.Lgs. n. 196/2003 dispone espressamente che: «Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 sexies e 2 octies, o delle misure di garanzia di cui all'articolo 2 septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2 quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni. 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato».

A tutti gli effetti si fa riferimento ad una norma penale in bianco, che non descrive le condotte oggetto di divieto in maniera esaustiva, ma, ai fini dell'individuazione del precetto vietato si rinviene un rinvio ad altre

disposizioni contenute nel Codice Privacy, che attribuiscono liceità ad un trattamento di dati personali la cui violazione integra la fattispecie in esame.
Va aggiunto, poi, anche il caso della comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (art. 167 bis). Il reato si propone di punire la comunicazione o la diffusione illecita (avvenuta anche senza il consenso) di un archivio automatizzato o di una sua parte consistente che contiene dati personali oggetto di trattamento su larga scala, allo scopo di trarre profitto o di danneggiare: anche tale previsione presenta elementi di che trovano una compatibilità poco riuscita con il principio di tassatività, mancando una definizione univoca di "parte sostanziale" di un archivio, sul quale ricade la condotta e la nozione di larga scala[246].
Anche l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167 ter) rientra tra le fattispecie innovative sanzionando l'acquisizione, in maniera fraudolenta, al fine di trarre profitto per sé (o per altri) di un archivio automatizzato o una parte sostanziale di esso contenente dati personali.
Risulta essere rilevante anche la violazione delle norme dettate in materia di controllo a distanza e indagini sulle opinioni dei lavoratori (art. 171), fattispecie penale volta alla repressione delle violazioni dell'art. 4 della Legge n. 300/1970 (Statuto dei Lavoratori), al fine di evitare (*rectius*, regolamentare) il controllo dell'attività dei lavoratori in modalità telematica.
Ai sensi del d.lgs. 231/2001 la compliance presuppone policy e protocolli aziendali, i quali assecondano l'esigenza di formalizzare e disciplinare un particolare processo aziendale, nonché di veicolare i comportamenti dei soggetti che, a diverso titolo, sono partecipi di quell'attività[247].

---

[246] Cfr. M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti*, in *JusOnline*, 1, 2017, p. 218 ss.

[247] Ciò in considerazione di un approccio fondato sulla responsabilizzazione dei soggetti (accountability) e sull'analisi del processo, in ragione di un preventivo *risk assessment* finalizzato a prevenire i reati (informatici) presupposto.

Il *risk base approach* viene impiegato anche nel GDPR, che disciplina una preventiva (e, non più, successiva) tutela dei dati personali, incentrata sulla responsabilizzazione del Titolare (e/o del Responsabile) del trattamento. In base a tale presupposto viene svolta un'analisi dei rischi su tutte le operazioni di trattamento effettuate, richiamando la valutazione d'impatto ex art. 35 del GDPR, laddove necessario.

Pertanto, «il *trade d'union* tra la protezione dei dati personali, la tutela della sicurezza informatica e la responsabilità amministrativa degli Enti si rinviene – oltre che nell'ipotesi patologica in cui si abbia un incidente di sicurezza, al quale può derivare una violazione dei dati personali (e la conseguente valutazione circa la necessità (o meno) di effettuare una notifica al Garante Privacy e una comunicazione ai soggetti interessati ex artt. 33 e 34 del GDPR) – senz'altro nell'art. 32 del GDPR, il quale impone l'adozione di adeguate misure di sicurezza tecnica ed organizzative, volte, di riflesso, a garantire la sicurezza informatica tesa a salvaguardare la protezione e l'intangibilità dei dati (informatici)»[248].

I profili di sovrapposizione risultano essere significativi: «se si pensa a qualunque delle fattispecie richiamate nel decalogo dei reati indicati all'art. 24 bis, si verifica anche un illecito trattamento di dati, tanto che, la società, sia essa titolare o responsabile del trattamento, deve avviare le indagini interne al fine di verificare se vi sia stata anche una compromissione dei dati personali trattati ed eventualmente aprire la procedura per la gestione dei casi di violazione dei dati personali ai sensi degli artt. 33 e 34 del Regolamento»[249].

Laddove un'azienda viene a conoscenza della commessione di un reato informatico avvenuto nell'ambito della propria attività, dovrà interrogarsi sulle ripercussioni sui dati personali trattati, e in particolare su quelli sensibili,

[248] G. Borghi, *Reati informatici e tutela dei dati personali: alcuni punti di contatto tra la normativa privacy e il d.lgs. N. 231/2001*, cit.

[249] L. Asti, *"Reati privacy" e "reati 231": ci sono profili di sovrapposizione?*, in www.privacygdpr.it, 23 febbraio 2021.

sia in qualità di titolare che di responsabile del trattamento. Nel caso in cui l'azienda dovesse accertare che il cybercrime è anche un *data breach*, scattano gli obblighi previsti dagli artt. 33 e 34 GDP.

L'articolo 33 del GDPR stabilisce che, entro le 72 ore dal momento in cui ne è venuto a conoscenza, il titolare del trattamento notifichi la violazione dei dati personali al Garante, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Inoltre, il responsabile del trattamento deve informare il Titolare senza ritardo dell'avvenimento di una violazione[250].

L'art. 34 del GDPR, interviene laddove la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. In tale evenienza sorge l'obbligo ulteriore per il titolare del trattamento di comunicare la violazione all'interessato senza ritardo ingiustificato. La violazione degli articoli 33 e 34 viene accompagnata da una sanzione amministrativa pecuniaria fino a 10.000 € o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83 (4) lett. a).

Le attività che hanno ad oggetto la sicurezza dell'infrastruttura IT, secondo il modello 231, ma anche al fine di osservare l'obbligo, ex art. 32 GDPR, devono adottare misure di sicurezza idonee ad assicurare un livello di sicurezza adeguato[251].

Un ulteriore aspetto da analizzare riguarda l'onere probatorio. Il d.lgs. 231/2001 distingue in base all'autore del reato: se soggetto apicale è prevista

[250] Cfr. M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti*, cit., p. 219.

[251] L'imprenditore, pertanto, attualmente deve comunque adottare modelli integrati di *compliance* che siano capaci di prevenire, allo stesso tempo, sia il verificarsi dei reati informatici che illeciti trattamenti dei dati personali.

l'inversione dell'onere della prova che, invece, ha una portata minore se trattasi di soggetto sottoposto all'altrui direzione.

In caso di commissione di un reato-presupposto da parte di un soggetto in posizione apicale, l'art. 6 d.lgs. 231/2001 prevede che la difesa provi che (i) l'ente ha adottato ed efficacemente attuato un Modello di Organizzazione idoneo a prevenire la consumazione di reati della specie di quello verificatosi e (ii) ha istituito un Organismo di Vigilanza dotato di poteri autonomi, (iii) che quest'ultimo ha adeguatamente svolto le sue funzioni e che (iv)il reo ha fraudolentemente eluso il Modello Organizzativo. In relazione alla prova della mancanza di lacune nelle verifiche dell'Organismo di Vigilanza, assume rilevo la documentazione attestante la relativa attività. Per quanto riguarda invece la prova dell'elusione fraudolenta, pare corretto ritenere che consista nella dimostrazione della "volontarietà" e "intenzionalità" dell'aggiramento delle procedure aziendali[252].

L'art. 7 d.lgs. 231/2001, invece, con riferimento al caso di consumazione di un illecito presupposto della responsabilità dell'ente da parte di un soggetto sottoposto all'altrui direzione, richiede alla difesa solo di dimostrare che l'ente ha adottato e attuato un Modello Organizzativo idoneo a prevenire reati della specie di quello verificatosi. L'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza". Pertanto, il Pubblico Ministero ha l'onere di provare l'omessa direzione o vigilanza e il collegamento fra questa e il reato commesso.

Nel caso del GDPR, l'articolo 7, par. 1, precisa che "il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali". L'azienda ha quindi l'onere della

[252] Cfr. M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti*,

prova: l'obbligo di dimostrare di aver ottenuto un consenso lecito per il trattamento dei dati personali[253].

Sotto il versante delle misure di sicurezza, nella prospettiva del GDPR si tratta delle pratiche tecniche e organizzative finalizzate a garantire la sicurezza dei dati personali che è tenuto ad adottare chi tratta i dati. Sono considerate misure di sicurezza tecniche gli strumenti che assicurano la protezione e la corretta conservazione dei dati (es. la cifratura dei dati). Sono misure di sicurezza organizzative le attività e gli adempimenti effettuati per garantire l'applicazione del GDPR e la riduzione dei rischi che derivano dal trattamento dei dati.

Le misure di sicurezza previste dal GDPR devono essere adottate dal titolare e dal responsabile del trattamento in maniera adeguata al caso concreto. Non esiste un elenco tassativo delle misure da adottare, tuttavia, il Regolamento europeo GDPR prevede le seguenti misure di sicurezza a titolo esemplificativo:

- cifratura e pseudonimizzazione: ad esempio, l'uso di algoritmi per la cifratura dei dati salvati e l'anonimizzazione dei dati per garantire la confidenzialità
- garanzia di riservatezza: ad esempio, con la restrizione degli accessi, monitoraggio degli accessi, firewall, password e credenziali sicure
- garanzia di integrità, disponibilità, resilienza e ripristino tempestivo: ad esempio, l'adozione di meccanismi di backup o particolari tipologie di archiviazione dei dati (archiviazione ridondante)
- procedure di verifica per testare l'efficacia delle misure adottate: ad esempio, audit indipendenti per la verifica e il controllo sulla compliance privacy.

[253] Cfr. M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti*, cit., p. 221.

Per quanto riguarda il modello 231, invece, deve trattarsi anch'esso di un modello adeguato ma anche in tal caso il legislatore non indica in maniera tassativa misure di sicurezza

5. Organismo di Vigilanza e Data Protection Officer

Un altro profilo da affrontare è quello relativo agli organismi di vigilanza e controllo previsti dalla normativa 231 e dal GDPR. La novella 231 ha introdotto l'OdV, Organismo di Vigilanza, mentre in materia di privacy è stato introdotto il DPO, Data Protection Officer. Entrambe le figure, in posizione di terzietà rispetto agli altri organi aziendali, hanno compiti di sorveglianza sulla corretta adozione e implementazione degli strumenti di compliance; inoltre, sono tenuti ad agire in maniera autonoma circa la gestione del flusso informativo di cui sono destinatari e che ha ad oggetto la violazione di MOG con conseguente aumento del rischio che vengano commessi reati (che rilevano ai fini dell'OdV ai sensi dell'art. 6, comma 2 lett. b) del D. Lgs. 231/2001), oppure di *data breach*, oggetto di valutazione del DPO (artt.37, 38 e 39 del GDPR).

Le due figure, però, a dispetto di quanto sembra, non sono del tutto sovrapponibili, ragion per cui non è possibile che i compiti vengano affidati alla stessa persona. Anzitutto, rileva, il dato normativo, in base al quale l'OdV, ai sensi dell'art. 6 del D. Lgs. 231/2001, è necessario ai fini dell'adeguamento delle prassi aziendali alla normativa in materia, mentre il DPO, in base all'art. 37 comma 1 del GDPR, deve essere individuato solo con riferimento a determinate circostanze espressamente indicate nella norma. In secondo luogo, la sovrapponibilità delle due figure deve essere esclusiva anche tenuto conto della necessità di salvaguardare la terzietà e autonomia dei ruoli.

Il DPO ha, tra l'altro, la funzione di tenere sotto controllo e verificare il corretto trattamento dei dati posto in essere dall'OdV, nell'esercizio delle sue funzioni, mentre quest'ultimo ha, a sua volta, il particolare compito di verificare il corretto adempimento, da parte del DPO, delle prescrizioni impartite dai MOG adottati in azienda: per tale motivazione, le due figure non possono concretizzarsi in un unicum operativo.

In conclusione, si può affermare che «proprio il confronto tra i ruoli dell'OdV e del DPO sintetizza il rapporto che lega le normative oggetto di analisi. Così come gli organi di vigilanza, pur cooperando tra loro al fine di garantire il rispetto delle prescrizioni tanto in materia di protezione dei dati personali quanto in materia di responsabilità degli Enti, sono sempre due ruoli distinti e non sovrapponibili, anche le normative, considerate nel loro complesso, pur sembrando complementari, non devono trarre in inganno l'imprenditore che, con l'obiettivo di contenere i costi derivanti dall'adozione di tali sistemi di compliance, può convincersi erroneamente che il modello organizzativo 231 esaurisca in maniera completa tutti gli aspetti di programmazione e di formazione imposti dal GDPR»[254].

In definitiva, tra le due normative le differenze sono più significative di quanto sembri. Il GDPR definisce in maniera meticolosa l'ambito applicativo dei modelli di organizzazione a tutela dei dati personali, è assente nel d.lgs. n. 231/2001, che lascia un margine di discrezionalità alla valutazione dell'ODV.

La differenza più significativa, in realtà, riguarda la *ratio* sottesa ad entrambe le normative: con la normativa 231/2001, il legislatore ha deciso di sancire la responsabilità amministrativa da reato per le aziende, limitando però la punibilità all'ente colpevole di non aver adottato ed attuato in maniera efficace modelli organizzativi con l'obiettivo di prevenire la commissione di

[254] G. Guglielmotti, *La privacy in azienda: GDPR e D. Lgs. 231/2001, punti di contatto e divergenze*, in https://www.riskmanagement360.it/compliance/la-privacy-in-azienda-gdpr-e-dlgs-231-2001-punti-di-contatto-e-divergenze/, 7 dicembre 2020.

reati commessi nel suo interesse oppure a suo vantaggio da soggetti che hanno posizioni di vertice nell'aziende oppure da chi è soggetto alla direzione dei primi, mentre non è prevista la punibilità degli illeciti commessi a danno dell'azienda stessa, ovvero nel suo interesse oppure vantaggio da soggetti estranei all'azienda.

Si tratta di una tutela assai ridotta rispetto a quella prevista dal GDPR il quale, nel prevedere la tutela dei dati personali delle persone fisiche nel suo complesso, non attua alcuna distinzione tra reati commessi nell'interesse o meno dell'ente, prevedendone la punibilità sia che vengano commessi a vantaggio che a danno dell'impresa, con condotte che provengono da soggetti interni o esterni ad essa, senza attuare alcuna differenza, e non attribuisce, inoltre, alcun valore scriminante all'adozione di modelli organizzativi da parte dell'ente.

In definitiva, l'armonizzazione delle due cornici normative può essere assicurata solo se si pensi a modelli di organizzazione e gestione integrati con le disposizioni in materia di privacy, considerato che l'adozione di soli modelli di compliance 231 non esenta l'azienda dai rischi legati alla violazione della privacy. Spetterà pertanto all'imprenditore decidere come comportarsi, a seconda delle dimensioni dell'azienda e della necessità di uniformare le prassi aziendali alle normative analizzate.

Conclusioni

La categoria dei reati informatici non individua un ambito di tutela dai contenuti omogenei, tanto è vero che la stessa autonomia di un diritto penale dell'informatica è in discussione. L'indagine ha messo in luce la continua rincorsa, del diritto penale, verso i nuovi reati informatici. Per lungo tempo l'ordinamento giuridico italiano è stato del tutto privo di una normativa in materia di reati informatici, situazione che ha costretto l'interprete a ricorrere alle fattispecie tradizionali che, però, erano state pensate e tradotte in pratica in un contesto storico cui era del tutto sconosciuto il fenomeno dei reati informatici.

La riforma legislativa è finalmente arrivata ma, come testimonia proprio l'esempio del *phishing*, risulta essere per certi versi già "indietro" rispetto all'affermarsi delle nuove tecniche, costringendo, dunque, l'interprete in quella rincorsa affannosa alla ricerca della norma applicabile foriera di numerose problematiche.

Sarebbe dunque opportuno, una volta delineata la cornice normativa di carattere generale, intervenire in maniera più pronta e solerte nel momento in cui si diffondono nuove tecniche di attacchi informatici che sfuggono alle maglie della legge o che, comunque, possono essere represse solo ricorrendo a forzature dei principi garantisti del diritto penale.

La tecnica legislativa ha cercato, nell'ambito del rispetto del principio di legalità, da un lato di aggiornare alcune fattispecie penali già esistenti per adattarle alla realtà di queste tecnologie, come la frode informatica; dall'altro di crearne di nuove, come l'accesso abusivo ai sistemi o la divulgazione di password.

Una particolarità che emerge osservando le fattispecie penali inserite nel quadro della legge 547/93 è l'assenza di reati colposi e la mancanza di reati omissivi. Sarebbe inoltre necessario regolamentare a fondo il concetto di

danno informatico, con le sue varianti e, soprattutto, separando i dati dai sistemi, e questi ultimi a loro volta dall'hardware.

Per quanto riguarda l'ambito procedurale, va notato che nell'ordinamento italiano si assiste a una proliferazione di reati soggetti ad azione privata a scapito della procedibilità d'ufficio, che si verifica nei casi in cui l'ordine pubblico è compromesso.

Si è visto che nel corso degli ultimi anni la produzione normativa in materia è stata assai significativa. Le ragioni tecnico-giuridiche che stanno a monte della significativa produzione normativa concernente la materia in esame sono da individuare, innanzi tutto, nel principio di stretta legalità (art. 25 Cost.) e nel divieto di analogia in malam partem (art. 14 preleggi), vigenti in materia penale. Sia il divieto di applicazione analogica delle norme penali, sia il principio di legalità - sotto il profilo della tassatività - comportano, come è noto, precisi doveri e divieti a carico del legislatore e del giudice.

In particolare, il legislatore ha l'obbligo di determinare con precisione, al momento della creazione della norma punitiva, la fattispecie legale, in modo che risulti chiaramente prestabilito ciò che è penalmente lecito e ciò che è penalmente illecito, mentre al giudice è fatto divieto di applicare la norma penale a casi da essa non espressamente preveduti. A causa di tali doveri (per il legislatore) e divieti (per il giudice), non sempre le nuove forme di criminalità informatica risultavano punibili alla stregua delle fattispecie di reato preesistenti.

Per quanto riguarda i modelli di tutela a disposizione del legislatore contro il fenomeno della frode informatica, va segnalato, anzitutto, che le ipotesi di frode informatica non possono essere ricondotte alla fattispecie di truffa, anche là dove la truffa sia concepita in termini più lassi e aperti: non v'è dubbio, infatti, che manca la cooperazione di una persona fisica. D'altra parte, in secondo luogo, le ipotesi di frode informatica non possono essere ricondotte nemmeno alla fattispecie di furto, in quanto manca la cosa mobile suscettibile di sottrazione. Certo si ha un arricchimento e un depauperamento,

tuttavia tali risultati vengono conseguiti in forma informatica, telematica, nella sostanza virtuale.

Il legislatore italiano ha forgiato una fattispecie dai tratti molto ambigui. In particolare, per quanto riguarda gli eventi, manca quello consistente nel risultato irregolare del processo di elaborazione di dati e quindi, conseguentemente e a rigore, dovrebbe mancare anche l'evento dell'atto di disposizione meccanico. Tuttavia, è presente l'evento dell'ingiusto profitto e dell'altrui inganno. Quindi si potrebbe dire che in ordine agli eventi la fattispecie si ispira per metà al modello del furto, là dove mancano gli eventi concernenti la macchina, e in parte al modello della truffa e del furto, là dove si prevede il profitto ingiusto con altrui danno.

Per quanto riguarda le modalità della condotta, anzitutto si fa riferimento ad espressioni "in qualsiasi modo" oppure "con qualsiasi modalità" davvero molto vaghe e dubbie. Si tratta di un profilo da non sottovalutare, in quanto, portando a confondere la generica descrizione di modalità della condotta, con l'assenza di una loro tipizzazione, ha indotto una parte della giurisprudenza e della dottrina a ritenere che si sarebbe in presenza di un reato a condotta libera.

In secondo luogo, ispirandosi al modello della truffa, la fattispecie prevede la condotta di "alterazione del funzionamento del sistema informatico o telematico", la quale di per sé non pone particolari problemi interpretativi, in quanto si tratta delle condotte di interferenza sull'hardware e sul software. Al contrario, pone problemi il riferimento all'"intervento senza diritto e con qualsiasi modalità su dati". Si tratta infatti di un'espressione alquanto ambigua perché non solo non distingue tra manipolazione (al di là dell'autorizzazione) e uso (connesso a questioni di autorizzazione), ma addirittura la fattispecie fa riferimento soltanto alla manipolazione (intervento su) e non anche all'uso. Inoltre, e soprattutto, la manipolazione, che di per sé dovrebbe essere del tutto indipendente dalla questione dell'autorizzazione, deve avvenire "senza

diritto", in presenza cioè di una caratteristica che è coerente con la condotta di uso dei dati che invece non è prevista.

Alla luce di queste considerazioni si può allora concludere che la fattispecie si ispira al modello della truffa, là dove fa riferimento alla manipolazione, ma non si ispira a tale modello quando richiede che la manipolazione avvenga senza diritto e quando non si prevedono gli eventi del risultato irregolare del processo di elaborazione di dati e dell'atto di disposizione. Si ispira invece al modello del furto là dove non si prevedono eventi e si fa riferimento all'assenza di legittimità, ma non si ispira a tale modello quando omette il riferimento all'uso dei dati o comunque di un servizio.

Bibliografia

F. Agnino, *Computer crime e fattispecie penali tradizionali: quando il phishing integra il delitto di truffa. Nota a Trib. Milano 29 ottobre 2008*, in *Cor. Mer.*, 3, 2009.

M. Alma, C. Perroni, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. proc.*, 1997.

G. Amarelli, *Profili pratici della questione sulla natura giuridica della responsabilità degli enti*, in *Riv. it. dir. proc. pen.*, 1, 2006.

G. Amarelli, *I nuovi reati ambientali e la responsabilità degli enti collettivi: una grande aspettativa parzialmente delusa*, in *Cassazione penale*, 2016.

A.C. Amato Mangiameli, G. Saraceni, *I reati informatici: elementi di teoria generale e principali figure criminose*, Milano, 2015.

S. Amore, V. Stanca, S. Staro, *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Milano, 2006.

D. Angelotti, *Delitti contro il patrimonio. Trattato di diritto penale* IV, Milano, 1936.

F. Antolisei, *Diritto penale. Parte speciale*. I, *Delitti contro il patrimonio*, Milano, 1966.

L. Benvenuto, *Organi sociali e responsabilità amministrativa da reato degli enti*, in *Le Società*, 6, 2009.

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

C. Berti, *I "Modelli di organizzazione e gestione" previsti dal d.lgs. n. 231/01: natura ed inquadramento giuridico*, in *Contratto e impresa*, 4-2, 2012.

M. Bianchi, *Il "Sexting minorile" non è più reato*?, in *Dir. pen. cont.*, 1, 2016.

Z. Bohm, S.J. *Shackelford, Securing Critical North American Infrastructure: A Comparatice Case Study in Cybersecurity Regulation*, in *School of Law*, 40, 2006.

G. Borghi, *Reati informatici e tutela dei dati personali: alcuni punti di contatto tra la normativa privacy e il d.lgs. N. 231/2001*, in *Salvis Juribus*, 2 maggio 2021.

R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti, *Profili penali dell'informatica*, Milano, 1994.

A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da), *Cybercrime*, Torino, 2019.

G.M. Caletti, *"Revenge porn" e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane*, in *Dir. pen. cont.*, 3, 2018.

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

G.M. Caletti, *"Revenge porn". Prime considerazioni in vista dell'introduzione dell'art. 612-ter c.p.: una fattispecie "esemplare", ma davvero efficace?*, in *Dir. pen. cont.*, 29 aprile 2019.

F. Capone, *Le problematiche di disciplina dei phishing attacks*, in *Cyberlaws.it*, 21 settembre 2018.

A. Carmona, *Tutela penale del patrimonio individuale e collettivo*, Bologna, 1996.

A.M. Cavadini, G. Lucietto, *Risk management. Conoscenze e competenze in un unico processo*, Bari, 2014.

R. Celella, *Il Cybersecurity Act e le nuove sfide del Mercato Unico Digitale*, in *Rivista di diritto dell'Unione europea*, 15 giugno 2020.

C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, Roma, 2014.

R.S. Cheung, J.P. Cohen, H.Z. Lo, F. Elia, *Challenge Based Learning in Cybersecurity Education*, in *josephcohen.com*, 2018.

P. Cipolla, *Il d.lgs. n. 231 del 2001 nella prassi giurisprudenziale, a dieci anni dall'entrata in vigore*, in *Giurisprudenza di merito*, 6, 2011.

P. Cipolla, *"Social network", furto di identità e reati contro il patrimonio*, in *Giur. mer.*, 12, 2012.

F. Cirinni, *La sicurezza informatica. Tra informatica, matematica e diritto*, Milano, 2017.

A. Cisterna, *Reclusione a sei anni con la sola circolazione di filmati sui social*, in *Guid. Dir.*, 37, 2019.

A. Contaldo, *L'ENISA e le competenze comunitarie per la cibersicurezza*, in *Rivista di polizia*, 6-7, 2018.

L. Conti, La *responsabilità amministrativa delle persone giuridiche. Abbandonato il principio societas delinquere non potest?*, in Id. (a cura di), *Il diritto penale dell'impresa*, Padova, 2001.

V. Contraffatto, *Reati informatici*, Milano, 2007.

G. Corasaniti, *La tutela della comunicazione informatica e telematica*, in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), *Profili penali dell'informatica*, Milano, 1994.

L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici*, Torino, 2009.

G. D'Aiuto, L. Levita, *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012.

S. Dal Grande, *Sicurezza informatica, le fatiche di chi la "evangelizza" in azienda*, in *agendadigitale.eu*, 12 novembre 2018.

G. Delitala, *Raccolta degli scritti*, I, Milano, 1976.

D. Denning, *Cyberterrorism*, in *http://palmer.wellesley.edu/*, 24 agosto 2004.

V. De Rosa, *La formazione di regole giuridiche per il "cyberspazio"*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2003.

G. De Simone, *I profili sostanziali della responsabilità c.d. amministrativa degli enti: la parte generale e la parte speciale del d.lgs. 8 giugno 2001 n. 231*, in G. Garuti (a cura di), *Responsabilità degli enti per illeciti amministrativi*, Padova, 2002.

G. De Simone, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) di imputazione*, in *www.penalecontemporaneo.it*, 2012.

V.S. Destito, G. Dezzan, C. Santoriello, *Il diritto penale delle nuove tecnologie*, Padova, 2007.

V. Di Lembo, *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013.

N. Fabiano, *GDPR&Privacy. Consapevolezza e opportunità*, Milano, 2019.

M. Fabozzo, *Analisi normativa e profili problematici del reato di diffusione illecita di immagini o video a contenuto sessualmente esplicito (c.d. revenge porn) ex art. 612-ter c.p.*, in *Riv. pen.*, 2, 2020.

A. Falzea, *La responsabilità penale delle persone giuridiche*, in AA.VV., *La responsabilità penale delle persone giuridiche in diritto comunitario*, Milano, 1981.

A. Fanelli, *La truffa*, Milano, 2009.

G. Fiandaca, F. Musco, *Diritto penale. Parte speciale* II. *I delitti contro il patrimonio*, Bologna, 2012.

G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuov. leg. civ. comm.*, 1, 2017.

G. Fioriglio, *Sorveglianza e controllo nella società dell'informazione. Il possibile contributo dell'etica "Hacker"*. Relazione alla Conferenza "La filosofia del diritto tra storia delle idee e nuove tecnologie", Ravenna, 19 settembre 2014, in *Nomos*, 2, 2014.

R. Flor, *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007.

R. Flor, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *Diritto penale contemporaneo*, 2012.

G. Forti, *Uno sguardo ai "piani nobili" del d.lgs. n. 231/2001*, in *Rivista italiana di diritto e procedura penale*, 4, 2012.

V. Frosini, *La criminalità informatica*, in *Dir. Inf.*, 1997.

A. Gammarota, *Lo scambio transnazionale di notizie di reati informatici: questioni di legittimità e di effettività dei diritti di difesa dell'indagato-imputato*, in *Inf. dir.*, 1-2, 2015.

R. Garofoli, *Il contrasto ai reati di impresa nel d.lgs. n. 231 del 2001 e nel d.l. n. 90 del 2014: non solo repressione, ma prevenzione e continuità aziendale*, in *www.penalecontemporaneo.it*, 2015.

A. Giarda, *L'elenco dei reati presupposto ex D.Lgs. 231/2001 si ampli*, in *Il Corriere del Merito*, 6, 2008.

F. Grosso, *Interessi protetti e tecniche di tutela*, in AA.VV., *Beni e tecniche della tutela penale*, Milano, 1987.

F. Grosso, *Sulla costituzione di parte civile nei confronti degli enti collettivi chiamati a rispondere ai sensi del d.lgs. n. 231 del 2001 davanti al giudice penale*, in *Rivista italiana di diritto e procedura penale*, 2004.

R. Guerrini, *Le sanzioni a carico degli enti nel d.lgs. n. 231/2001*, in G. De Francesco (a cura di), *La responsabilità degli enti: un nuovo modello di giustizia "punitiva"*, Torino, 2004.

G. Guglielmotti, *La privacy in azienda: GDPR e D. Lgs. 231/2001, punti di contatto e divergenze*, in https://www.riskmanagement360.it/compliance/la-privacy-in-azienda-gdpr-e-dlgs-231-2001-punti-di-contatto-e-divergenze/, 7 dicembre 2020.

H. Heinitz, *Il danno patrimoniale nella truffa*, in *Archivio penale*, 1953.

G. Hornung, *Die Digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, Job-Card-Verfahren*, Baden Baden, 2005.

M. Iaselli, *Il concetto di sicurezza informatica nell'ottica del GDPR*, in *Rivista Informatica*, 2, 2017.

P. Iezzi, R. Paglia, F. D'Agostino, *Vulnerability Assessnent*, Milano, 2018.

A.G. Imbesi, *Phishing and pharming on the net,* in *Il Nuovo diritto*, 7-8, 2006.

M. Lamanuzzi, *Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento 2016/679/UE e nuove responsabilità per gli enti,* in *JusOnline*, 1, 2017.

U. Lecis, *L'Organismo di vigilanza e l'aggiornamento del Modello organizzativo,* in *Rivista – La responsabilità amministrativa delle società e degli enti*, 4, 2006.

J.A. Lewis, *Aux Armes, Citoyens: Cyber Security and Regulation in the United States*, in *Elsevier's Telecommunications Policy*, Fall 2005.

E. Lorenzetto, *Sequestro preventivo contra societatem per un valore equivalente al profitto del reato,* in *Rivista italiana di diritto e procedura penale*, 2008.

M. Lottini, *Il sistema sanzionatorio,* in G. Garuti (a cura di), *Responsabilità degli enti per illeciti amministrativi*, Padova, 2002.

U. Lucarelli, *La truffa*, Padova, 2002.

L. Luparia, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, Milano, 2009.

F. Mantovani, *Diritto penale, Parte speciale*. II. *Reati contro il patrimonio*, Padova, 2012.

G. Marelli, *Profili pratici della questione sulla natura giuridica della responsabilità degli enti,* in *Rivista italiana di diritto e procedura penale,* 2016.

G. Marini, *Truffa,* in *Digesto delle discipline penalistiche,* XVIII, Torino, 1999.

G. Marinucci, *"Societas puniri potest": uno sguardo sui fenomeni e sulle discipline contemporanee,* in *Rivista italiana di diritto e procedura penale,* 2002.

G. Marra, *Truffa (art. 640),* in AA.VV., *Trattato breve dei delitti contro il patrimonio,* Torino, 2010.

P. Masneri, *Identità personale e identità digitale: nuove regole per tutelare la personalità individuale dalle insidie del web,* su internet all'indirizzo web *http//www.francoabruzzo.it,* 8 gennaio 2008.

A. Merli, *Il diritto penale dell'informatica: legislazione vigente e prospettive di riforma,* in *Giust. pen.,* 2, 1993.

M. Mignone, *I cybercriminali: rischi e limiti dei profili criminologici,* in *Ciber. e dir.,* 2001.

S. Moccia, *Il diritto penale tra essere e valore. Funzione della pena e sistematica teleologica,* Napoli, 1992.

G. Modesti, *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali,* in *Ragiusan,* 335-337, 2012.

V. Mongillo, *La confisca del profitto nei confronti dell'ente in cerca d'identità: luci e ombre della recente pronuncia delle Sezioni Unite,* in *Rivista italiana di diritto e procdura penale,* 2008.

F. Mucciarelli, *Commento all'art.10 della legge 547 del 1993,* in *Leg. Pen.,* 1996.

F. Novario, *Pornografia minorile e file sharing: l'influenza della tecnologia informatica sull'asse probatorio*, in *Dir. pen. proc*., 10, 2009.

R. Paglia, P. Iezzi, *Hotel Cybersecurity: le minacce e le soluzioni. Security*, Milano, 2018.

A. Pagliaro, *Truffa e danno patrimoniale*, in *Rivista italiana di diritto e procedura penale*, 1963.

C.E. Paliero, *Il d.lgs. 8 giugno 2001, n. 231: da ora in poi, societas delinquere (et puniri) potest*, in *Corriere Giuridico*, 2001.

A. Palma, *In tema di reati informatici. Nota a Cass. sez. un. pen. 7 febbraio 2012, n. 4694*, in *Stud. Iur*., 6, 2012.

M. Panasiti, *Riparazione delle conseguenze del reato*, in M. Levis, A. Perini (diretto da), *La responsabilità amministrativa delle società e degli enti*, Bologna, 2014.

C. Parodi, *Profili penali dei virus informatici*, in *Dir. pen. proc.*, 2000.

G. Pavich, *Le modifiche al codice penale*, in A. Marandola, G. Pavich (a cura di), *Codice rosso l. n. 69/2*019, Milano, 2019.

F. Pazienza, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Riv. it. dir. proc. pen.*, 1995.

C. Pecorella, *Il diritto penale dell'informatica*, Padova, 2006.

C. Pedrazzi, *La riforma dei reati contro il patrimonio e contro l'economia*, in AA.VV., *Verso un nuovo codice penale*, Milano, 1993.

S. Perini, *I modelli di organizzazione, gestione e controllo nel d.lgs. n. 231/2001. Profili applicativi e giurisprudenziali*, Vicalvi, 2015.

P. Perri, *Privacy, diritto e sicurezza informatica*, Milano, 2007.

S. Pettinato, *I Modelli organizzativi e di gestione del d. lgs. n. 231/2001 e la responsabilità legale delle società e degli enti per i reati commessi dai loro appartenenti: note illustrative aggiornate*, in *Fisco*, 23, 2005.

G. Pica, *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. Pen. Economia*, 1995.

L. Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id. (a cura di), *Il diritto penale dell'informatica nell'era di Internet*, Padova, 2004.

L. Picotti, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. mer.*, 12, 2012.

L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Torino, 2019.

C. Piergallini, *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, in *Rivista trimestrale di diritto penale dell'economia*, 2002.

F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuov. leg. Civ. comm.*, 2, 2017.

L. Pistorelli, *Relazione dell'Ufficio Massimario della Corte di Cassazione*, n. III/1/2013.

G. Pomante, *Internet e criminalità*, Torino, 1999.

A. Ricci, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2, 2017.

S. Riondato, *Prevenzione dei reati riconducibili alla politica dell'ente e personalità della responsabilità penale dell'ente (d.lgs. 8 giugno 2001 n. 231)*, in *Rivista trimestrale di diritto penale dell'economia*, 2003.

S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004.

M. Romano, *La responsabilità amministrativa degli enti, società o associazioni: profili generali*, in *Rivista delle società*, 2002.

B. Romano, *L'introduzione dell'articolo 612-ter del codice penale in materia di diffusione illecita di immagini o video sessualmente espliciti (art. 10, l. 19 luglio 2019, n. 69*), in B. Romano, A. Marandola (a cura di), *Codice rosso. Commento alla l. 19 luglio 2019 n. 69, in materia di tutela delle vittime di violenza domestica e di genere*, Roma, 2020.

R. Rodorf, *I criteri di attribuzione della responsabilità. I modelli organizzativi e gestionali idonei a prevenire i reati*, in *Le Società*, 11, 2001.

I. Salvadori, *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010. Profili di diritto comparato*, in *Ind. Pen*., 2, 2011.

I. Salvadori, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. proc. pen*., 1, 2012.

M. Santini, *Cyber security in azienda, diffondere la cultura della sicurezza informatica: ecco perché,* in *cybersecurity360.it*, 20 novembre 2018.

F. Scalia, *Energia sostenibile e cambiamento climatico*, Torino, 2008.

M.G. Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 4, 2016.

A. Traversi, S. Gennai, *Diritto penale commerciale*, Padova, 2017.

A. Valentini, *Dentro la NIS 2, più obblighi e regole per la cybersecurity europea*, in https://www.cybersecurity360.it/outlook/dentro-la-nis-2-piu-obblighi-e-regole-per-la-cybersecurity-europea/, 20 dicembre 2022.

A. Valsecchi, *Codice rosso e diritto penale sostanziale: le principali novità. Commento a legge 19 luglio 2019 n. 69 (Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica o di genere)*, in *Dir. pen. proc.*, 2, 2020.

L. Viola, *Ingiusto profitto e danno altrui nella cd. truffa contrattuale*, in *Diritto&Diritti*, settembre 2003.

L. Violante, *L'atto di disposizione patrimoniale nella truffa e la frode fiscale*, in *Ind. Pen.*, 1980.

G. Ziccardi, *Il giurista hacker e il corretto approccio alle tecnologie informatiche*, in *Ciber. e dir.*, 4, 2005.