UNIVERSITÀ DEGLI STUDI DI CATANIA

Corso di Laurea Magistrale in Giurisprudenza

Claudia Cassarino

RISERVATEZZA INFORMATICA, *CYBERSECURITY* E RESPONSABILITÀ DA REATO DEGLI ENTI

IL RUOLO DEL *COMPLIANCE PROGRAM* NELLA PREVENZIONE DEI REATI INFORMATICI E PROSPETTIVE FUTURE

TESI DI LAUREA

RELATORE:
Chiar.ma Prof.ssa Anna Maria Maugeri

A N N O A C C A D E M I C O 2 0 2 0 / 2 0 2 1

INDICE

Introduzione

Il presente lavoro si propone di intersecare le tematiche legate ai reati informatici posti a tutela dei beni giuridici di nuovo conio, la riservatezza informatica e sicurezza informatica, con la disciplina della responsabilità da reato degli enti. Il decreto 231 del 2001 che ha sancito il superamento del principio *societas delinquere non potest*, a vent'anni dalla sua introduzione ancora anima il dibattito tra gli studiosi. Con la l. 48/2008 sono stati inseriti alcuni reati informatici nel decreto e da ultimo con il d. l. 105/2019 (convertito con la l. 133/2019) è stata inserita una nuova fattispecie riguardante la sicurezza cibernetica. Tali reati fanno, ora, parte dell'art. 24-bis d.lgs. 231/2001.

Le motivazioni che ci spingono ad intraprendere un simile percorso si rintracciano, in primo luogo, nei timori diffusi nella società iper-connessa. La tecnologia se da un lato ci consente, e ne abbiamo avuto la prova durante la recente pandemia da Covid-19, di svolgere la nostra vita economica, professionale e relazionale attraverso *computer* e telefoni, dall'altro mette in serio pericolo la nostra *privacy*. Nel *cyber-space* sono nati nuovi modi di delinquere sempre più frequenti. Le statistiche, infatti, ci dicono che in Italia nel 2021 sono stati compiuti 800 reati informatici al giorno[1].

Questa nuova criminalità, tuttavia, non riguarda in maniera esclusiva le persone fisiche. L'elevata digitalizzazione degli enti accresce il rischio che questi rimangano vittima di reati informatici, ma anche che si sviluppi al loro interno l'occasione per delinquere.

Le ricerche sono state condotte partendo dagli strumenti normativi per poi analizzare la dottrina e giurisprudenza, indispensabili per fare luce sulle complesse questioni legate all'oggetto dell'indagine. Prezioso il contributo della giurisprudenza della Corte EDU e della Corte di giustizia per contestualizzare le problematiche legate alla *privacy* nella società moderna. L'apporto della dottrina ci ha permesso, in particolare, di riflettere sulle possibili riforme future ma anche di fare luce su complesse questioni laddove la giurisprudenza era contraddittoria o carente. Infatti, il decreto 231 non ha trovato una

[1] Indagine condotta dal il Sole24ore: https://www.ilsole24ore.com/art/boom-reati-web-sono-800-giorno

cospicua applicazione da parte dei giudici e i reati di cui ci occupiamo sono stati introdotti di recente. Il nostro lavoro, pertanto, è stato complicato dall'assenza di sentenze che si occupano di responsabilità da reato degli enti e reati informatici. In questa fase ci siamo serviti del lavoro di esperti del settore *privacy*, *cybercrime* e *cybersecurity* e di recenti episodi di cronaca per comprendere le reali problematiche ed esigenze delle società con riferimento alla prevenzione dei reati informatici.

L'obiettivo ultimo dell'indagine è quello di comprendere:

1) Il ruolo del modello di organizzazione, gestione e controllo nella prevenzione dei reati informatici.
2) In che modo potrebbe essere costruito in concreto un Modello organizzativo idoneo ed efficace alla luce delle caratteristiche dei reati informatici da noi analizzati.
3) Quali ricadute potrebbe avere la disciplina nazionale e sovranazionale in materia di *cybersecurity* sulla costruzione del Modello 231.

Tali riflessioni saranno condotte con uno sguardo al futuro. Nuove avanzate tecnologie, ci riferiamo alla Intelligenza artificiale e ai reati informatici, verranno impiegate sempre più spesso all'interno delle società, fornendo un ausilio anche all'attività svolta all'interno degli enti in materia di *compliance*. Tali strumenti, tuttavia, comportano nuovi rischi, ad esempio in materia di *privacy* e aprono nuove complesse questioni giuridiche. Ci soffermeremo su tali tematiche non con la pretesa di fornire un'analisi esaustiva, ma per aprire nuovi spunti di riflessione sulle questioni da noi affrontate.

La tesi si articola in tre capitoli, mentre dedicheremo le conclusioni per fare il punto della situazione e allargare la prospettiva ad un futuro non più così lontano. Di seguito mi soffermerò brevemente su ogni singolo capitolo per comprendere il lavoro che verrà svolto.

Il primo capitolo affronta il tema dell'emersione del diritto alla riservatezza e della sicurezza nella società moderna. Seguiremo l'evolversi del diritto alla *privacy*, dall'originario *right to be alone* alla visione della riservatezza come potere sui propri dati personali. L'indagine verrà effettuata principalmente nella prospettiva sovranazionale, attraverso l'analisi della giurisprudenza della Corte di giustizia dell'Unione Europea e

della Corte Edu. Soprattutto a seguito delle rivelazioni di Edward Snowden il rischio di una sorveglianza di massa si fa concreto. Le Corti prendono sul serio la protezione della *privacy* digitale, consentendo il progresso per via giurisprudenziale. Fondamentale il bilanciamento tra tutela della riservatezza e sicurezza che tornerà più volte nelle varie pronunce.

In seguito, analizzeremo gli strumenti normativi sovranazionali nella lotta al *cybercrime*. Partiremo dall'emersione della categoria dei reati informatici, per poi analizzare la Convenzione *cybercrime* di Budapest, la decisione 2005/222/GAI sugli attacchi informatici e infine la direttiva 2013/40/UE. Le parole chiave nella strategia dell'UE e che più volte vengono ribadite in questi lavori sono: cooperazione e armonizzazione delle differenze, necessarie per contrastare queste nuove forme di criminalità che non conoscono confini. Importante rilevare l'esigenza espressa dall'UE di estendere la responsabilità da reato degli enti a questo tipo di crimini.

L'ultima parte del capitolo sarà dedicata agli interventi in materi di *cybersecurity* volti a costruire un'Unione Europea più resiliente: la direttiva NIS, il *Cybersecurity Act*, ma anche la proposta di direttiva NIS 2.0. Questa analisi sarà funzionale a comprendere nel terzo capitolo le ricadute di tali atti nella costruzione del Modello di organizzazione, gestione e controllo volto a prevenire i reati informatici.

Nel secondo capitolo ci caliamo nel piano nazionale. Questa parte della tesi si incentra sullo studio dei reati informatici in senso stretto e tra questi quelli posti a tutela della riservatezza e sicurezza informatica ma anche della integrità, autenticità e genuinità delle comunicazioni informatiche o telematiche. Ci riferiamo ai reati previsti agli artt. 615- ter; -quater; quinquies c.p. e artt. 617- quater, -quinquies e -sexies c.p. Queste fattispecie introdotte nel 1993 da un legislatore previdente che è riuscito talora ad anticipare le mosse poi effettuate al livello sovranazionale, sono state oggetto di modifica recentemente con la l. 238 del 2021. L'analisi verrà condotta tendendo conto delle modifiche introdotte ma anche delle possibili riforme che autorevole dottrina prospetta per il futuro. Un'attenzione particolare verrà dedicata ai beni giuridici di nuovo conio: la riservatezza e sicurezza informatica, vagliandone le peculiarità in ragione delle fattispecie trattate. I rischi per questi beni giuridici ci hanno spinto a delimitare il campo d'indagine a questi reati.

Protagonista inevitabile di questa parte del lavoro sarà la fattispecie di accesso abusivo ai reati informatici che ha dato luogo a questioni giurisprudenziali rilevanti a cui cercheremo di rispondere. In particolare, ci chiediamo se il c.d. *insider*, legittimato all'ingresso nel sistema informatico possa essere imputato per tale tipo di reato, qualora si introduca o si mantenga al suo interno per uno scopo diverso da quello consentito. Tale interrogativo animerà il dibattito in giurisprudenza e in dottrina. Nonostante l'intervento delle sezioni unite della Corte di Cassazione prima nel 2012[2] e successivamente nel 2017[3], relativo al secondo comma, n.1 dell'art. 615- ter, non possono dirsi dissipati tutti i dubbi e c'è chi ha prospettato anche il rischio di un *overruling* sfavorevole. Ripercorreremo criticamente tali complesse vicende, valutando le possibili riforme che potrebbero aiutare a dirimere definitivamente la questione.

Altra complessa tematica su cui cercheremo di fare luce è l'individuazione del *locus commissi delicti* nel caso dei reati informatici. Una delle caratteristiche di tali reati è il fatto che l'agente possa trovarsi a molta distanza dal luogo in cui si estrinseca l'accadimento materiale. Seguiremo, pertanto, le varie tesi che si sono avvicendate in giurisprudenza e dottrina intorno a questo dibattito.

L'obiettivo di tale parte del lavoro è comprende le peculiarità di tali reati, per riflettere criticamente sulle ricadute in materia di responsabilità da reato degli enti e in particolare, sulla loro prevenzione attraverso il modello di organizzazione, gestione e controllo.

Le riflessioni svolte in questi primi capitoli convergeranno nel terzo ed ultimo capitolo di questo lavoro in cui tenteremo di intersecare i temi affrontati con la responsabilità da reato degli enti. Con legge 48 del 2008, i reati di cui ci siamo occupati in precedenza (ad eccezione dell'art. 617- sexies c.p.) sono entrati a far parte del catalogo dei reati presupposto del decreto 231/2001. In questa fase, tuttavia, ci siamo dovuti scontrare con l'assenza di giurisprudenza in materia che ha inevitabilmente complicato la nostra indagine. Consultando i codici con giurisprudenza commentata e le varie banche dati presenti sul *web*, non è stato possibile rintracciare una sola sentenza che avesse ad oggetto la commissione di un reato informatico da parte di un ente. Chiarito che i motivi di tale

[2] Cass. Sez. un., 7 febbraio 2012 n. 4694, consultabile sul sito www.dirittopenalecontemporaneo.it
[3] Cass., sez. unite, sent. 18 maggio 2017 n. 41210, in diritto penale contemporaneo, fasc. 10/2017

mancanza non sono da rintracciare nella scarsa rilevanza pratica dell'indagine, ma piuttosto in una certa reticenza da parte degli uffici di Procura nella elevazione di addebiti agli enti collettivi e nelle peculiarità connesse a questo tipo di reati che rendono difficile l'individuazione dell'autore materiale, abbiamo dato concretezza al nostro lavoro, traendo spunto da episodi di cronaca e avvalendoci degli studi degli esperti del settore.

Ci soffermeremo, quindi, su alcune zone d'ombra della disciplina del decreto 231/2001 e sulle riforme che ci possiamo aspettare dal futuro, valutando anche le ricadute che l'impiego di avanzate tecnologie, come l'IA e i *Big Data* potrebbero avere sulla colpa organizzativa.

L'intrinseca transnazionalità del reato informatico ci ha spinto ad occuparci della responsabilità del soggetto giuridico estero per i reati commessi in Italia. Tale questione risulta di particolare interessa data l'assenza di riferimenti all'interno del decreto 231 che invece si occupa della situazione inversa in cui una società italiana commetta un reato all'estero. In particolare, ci siamo chiesti se anche le società straniere operanti in Italia debbano dotarsi del modello di organizzazione, gestione e controllo così come previsto dalla disciplina italiana e se possano essere chiamate a rispondere ai sensi del d.lgs. 231/2001 per reati commessi sul nostro territorio. Anticipiamo che il dibattito è particolarmente accesso e ha diviso dottrina e giurisprudenza. La risoluzione del secondo interrogativo, una volta vagliati i vari orientamenti, risentirà del recente intervento della Corte di Cassazione, pronunciata nell'ambito del disastro di Viareggio[4].

L'introduzione dei reati informatici tra gli illeciti in grado di determinare la responsabilità dell'ente apre una ulteriore questione circa un potenziale contrasto tra la necessità di prevenire la criminalità d'impresa e l'aspettativa di riservatezza del lavoratore di cui si occupa il c.d. Statuto dei lavoratori (l. 20 maggio 1970, n. 70) e il c.d. Codice *Privacy* (d.lgs. 30 giugno 2003 n. 196). Ci occuperemo, pertanto, anche del tema relativo ai controlli dei lavoratori, riflettendo sulle possibili ricadute in tema di responsabilità da reato degli enti.

Il cuore di questo lavoro si rintraccia, tuttavia, nell'analisi dell'istituto del modello di organizzazione, gestione e controllo con riferimento ai reati informatici. Cercheremo,

[4] Cass., Sez. IV, sent. 8 gennaio 2021 (dep. 6 settembre 2021), n. 32899 in sistemapenale.it

quindi, di delineare un modello ideale che consenta di prevenire in concreto i reati informatici, coniugando le conoscenze tecniche a quelle giuridiche. Fondamentale l'apporto degli interventi normativi sovranazionali e nazionali in materia di *cybersecurity*, che, come abbiamo anticipato nel capitolo primo, possono avere importanti ricadute sulla formulazione del modello e sulla prevenzione dei reati informatici.

Da ultimo, faremo il punto della situazione del nostro lavoro, dando uno sguardo ad un futuro non più lontano. Così come accaduto per il *Computer* e *Internet*, oggi l'Intelligenza artificiale e i *Big Data* aprono nuovi interrogativi con cui il diritto deve confrontarsi. Le novità che si annunciano imminenti ci portano a riflettere sulle possibili intersezioni tra l'oggetto della nostra indagine e le tecnologie più avanzate. Data la crescente digitalizzazione delle società risulta interessante passare al vaglio i possibili impieghi dell'IA e dei *Big data* all'interno delle aziende: nella costruzione dei modelli organizzativi, nella realizzazione dei controlli dei lavoratori e ancora nell'assunzione delle decisioni. Se da un lato si prospettano indubbi vantaggi, dall'altro lato potrebbero aprirsi delle domande in ordine al rischio per la *privacy* degli individui. Infine, vedremo quali interrogativi si pongono con riferimento alle ricadute dell'impiego di tali tecnologie sulla responsabilità penale delle persone fisiche e sulla responsabilità da reato degli enti.

Capitolo I: Il timore di una sorveglianza orwelliana tra tutela della *privacy* e *cybersecurity*

1.La nascita del diritto alla *privacy*

Durante il corso della vita quotidiana è sempre più frequente sentire parlare di *privacy*[1] e varie sono le questioni giuridiche implicate che riguardano da vicino ciascun individuo. Dare, tuttavia, una definizione a tale termine è un'opera tutt'altro che semplice, in quanto, si tratta di un concetto in evoluzione[2]. A tal proposito Philippe Ariès[3], storico francese, si chiedeva se fosse possibile una storia del concetto di diritto alla vita privata e aggiungeva "o forse questa nozione di privato ci rimanda a situazioni e valori troppo eterogenei da un'epoca all'altra perché si possa stabilire tra loro un rapporto di continuità e differenza?". È all'Ottocento che si fa risalire la fondazione del *right of privacy* da parte degli statunitensi Warren e Brandeis. La *privacy* assume, adesso, una connotazione giuridica e viene identificata nel diritto ad essere lasciato solo. Nel celebre articolo pubblicato sull'*Harvard law review* [4] si legge: "*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops*'". La definizione data a questo diritto viene rintracciata nella società del tempo. La rivoluzione industriale aveva portato al trasferimento di numerose persone dalle campagne alle città e questo aveva reso sempre più forte il desiderio di riservatezza, così, infatti i due autori scrivono: "*Political, social and economic changes entail the*

[1] La nostra trattazione si sofferma, in questa fase, sull'analisi della *privacy* come diritto. Questo ci darà modo di avere una visione d'insieme di questo concetto, attraverso gli studi dottrinali e gli interventi della giurisprudenza. Nel capitolo seguente, ci occuperemo del bene giuridico della riservatezza.
[2] S. NIGER, Le nuove dimensioni della *privacy*: dal diritto alla riservatezza alla protezione dei dati personali, CEDAM, Padova, 2006.
[3] Philippe Ariès fu uno storico francese, autore di cinque volumi dal titolo "*Histoire de le vie privée*".
[4] L'articolo apparve il 15 dicembre 1890 sulla *Harvard Law Review* ed è una precisa e articolata ricostruzione del rapporto tra diritto di informare ed essere informati e il diritto alla riservatezza.

recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society". Il diritto alla *privacy* venne pertanto definito come *right to be let alone*, riprendendo la logica proprietaria e lo *ius excludendi alios.* Nonostante il prezioso lavoro svolto da Warrein e Brandeis, la giurisprudenza faticherà a riconoscere la *privacy* come bene meritevole di tutela. Sarà la *Supreme court of Georgia* nel 1905, a riconoscere definitivamente la *privacy* come derivante dal diritto naturale nel noto caso *Pavesich v. New England Life Insurance Company*[5]. Dopo tale sentenza il diritto alla *privacy* acquisì uno stabile riconoscimento, venendo inserito dall'*American Law Institute nel Restatement of Torts* del 1939, ma anche una progressiva estensione. Negli Stati Uniti la tecnologia comportò significativi mutamenti nella società molto prima rispetto a quanto accaduto in Italia. Dal lontano 1890, anno in cui venne elaborato per la prima volta il diritto alla *privacy*, i progressi tecnologi hanno consentito a questo diritto di evolversi e mostrare una veste adeguata alle nuove esigenze[6]. "L'evoluzione della tecnologia e dei metodi di comunicazione commerciale rendono i dati personali assimilabili a vere e proprie merci che vengono messe a disposizione delle imprese interessate a conoscerli e a sfruttarli dietro pagamento di corrispettivi".[7] La dottrina statunitense prese atto dei differenti interessi che ruotavano intorno alla tutela alla *privacy* e giunse alla conclusione che non si potesse dare una definizione unitaria a questo diritto. Venne assunta, pertanto, una prospettiva multidimensionale in base alla quale gli interessi che vengono in gioco sono eterogenei e variano da caso a caso. In Italia le riflessioni sul diritto alla *privacy* arrivarono solo mezzo secolo dopo lo studio di Warren e Brandeis, a causa anche del ritardo nello sviluppo industriale. L'elaborazione italiana prese a prestito il concetto di *privacy* elaborato negli Stati Uniti come diritto ad essere lasciati soli, ma incontrò numerose difficoltà. Quest'ultime erano dovute da un lato alla mancanza di riferimenti normativi espliciti e dall'altro al trasferimento di un istituto tipico del *common law* nel nostro sistema di *civil law*. È in questo contesto che la dottrina italiana fece ricorso al termine "riservatezza" per tradurre il termine "*privacy*", non idoneo però ad esaurire tutti i possibili significati del termine inglese. Le differenze tra *privacy* e riservatezza

[5] Il testo della sentenza è reperibile sul sito casetext.com

[6] Per una dettagliata ricostruzione storica e analisi del diritto alla privacy in via esemplificativa: A. CATAUDELLA, *La vita civile della vita privata*, Giuffrè, Milano, 1972; D. CALDIROLA, *Il diritto alla riservatezza*, CEDAM, Padova, 2006; S. NIGER, *Le nuove…, cit.*; T. UBERTAZZI, *Il diritto alla privacy: natura e funzioni giuridiche,* Cedam, Padova, 2005.

[7] T. UBERTAZZI*, Il diritto*…, cit., pag. 45

attengono ai sistemi giuridici di provenienza, l'uno di *common law*, l'altro di *civil law*, ma soprattutto al rapporto tra persona e informazione. "Nella riservatezza ciò che viene in considerazione è la posizione dell'individuo rispetto alle informazioni che lo riguardano, in quanto gli interessi protetti sono quelli della non divulgazione di fatti privati e della non intromissione nella sfera privata, attraverso la *privacy*, invece, viene tutelata la libertà rispetto alle informazioni circolanti, nel senso che la protezione si dilata a tutto ciò che rende possibile il formarsi di una persona libera: per questo vi rientrano una fascia di interessi e di beni che vanno ben oltre il rispetto del riserbo e dell'intimità, come l'identità personale e l'autodeterminazione."[8] Altri, tuttavia, hanno ritenuto inutile tradurre la parola *privacy*, visto il suo comune utilizzo nella nostra lingua e non essendovi altro termine in grado di includere tutti i molteplici aspetti di tale termine. Questo spiega come il diritto alla riservatezza, nel linguaggio comune ma non solo, non sia riuscito a sostituire il più ben noto termine *privacy*. Nel nostro ordinamento la mancanza di un espresso riferimento normativo che riconoscesse il diritto alla riservatezza portò la dottrina a proporre diverse soluzioni. Alcuni studiosi rintracciarono un possibile fondamento normativo nell'art. 8 della Convenzione Europea dei diritti dell'uomo[9] [10]. "L'ampiezza della formula adottata fa riferimento al diritto al segreto e alla segretezza, tutelando l'individuo sia da indebite intromissioni nella vita privata, sia dalla divulgazione di notizie lecitamente conosciute da parte dei privati[11]". Questa norma ha la finalità di difendere l'individuo da ingerenze arbitrarie dei pubblici poteri. Sebbene fosse pacifico che la CEDU facesse sorgere in capo agli stati membri l'obbligo di riconoscere i diritti in essa proclamati, la questione circa il valore e la forza della convenzione diede luogo nel nostro ordinamento ad un acceso dibattito. In particolare, mentre alcuni ritenevano che la disposizione avesse valore programmatico, altri come T. Auletta ne affermavano il valore precettivo. "Se da una parte si riteneva che la Convenzione avesse

[8] D. CALDIROLA, *Il diritto alla riservatezza*, Cedam, Padova, 2006

[9] La CEDU è la convenzione europea per la salvaguardia dei diritti dell'uomo e del cittadino, firmata a Roma il 4 Novembre 1950, è stata resa esecutiva nel nostro paese con la legge di attuazione del 4 agosto 1955, N. 848. Il testo è consultabile sul sito: echr.coe.int

[10] Articolo 8 CEDU: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui.».

[11] S. NIGER*, Le nuove dimensioni…*, cit., pp. 50

un valore programmatico, volta a sollecitare l'azione pubblica, ma non fosse suscettibile di dar luogo a situazioni giuridiche soggettive direttamente azionabili dai singoli, dall'altra vi era chi sosteneva il dispiegarsi dell'efficacia della Convenzione nei confronti dei pubblici poteri e dei privati".[12] L'art. 8 venne spesso criticato per la sua eccessiva genericità dovuta al ricorso alla tecnica legislativa "per clausole generali", ma, autorevole dottrina individuava gli aspetti positivi di questa formulazione: "Il ricorso alla tecnica per clausole generali ha inteso assicurare un maggiore ambito di tutela della riservatezza. Infatti, se nella norma fossero stati elencati i possibili modi di violazione del diritto le incertezze si sarebbero moltiplicate di fronte al verificarsi di un caso non espressamente contemplato".[13] Ben presto gli studiosi volsero la loro attenzione alle norme costituzionali. In particolare, venne richiamato l'art. 2 della costituzione[14], il quale tende a preservare l'ambiente nel quale l'individuo svolge la sua personalità immune da intrusioni altrui. Nell'art. 2 possono rientrare gli interessi rilevanti in un determinato periodo storico[15]. Questo è possibile, grazie alla particolare elasticità delle disposizioni costituzionali che consentono la tutela di quelle posizioni soggettive implicitamente riconosciute nel testo e ricavabili in via interpretativa[16]. Altra norma costituzionale richiamata all'interno del dibattito era l'art 3 Cost.[17], il quale al primo comma garantirebbe il rispetto della vita privata attraverso la pari dignità sociale. Il concetto di dignità, proprio perché garantito dalla Carta costituzionale ed essenziale per il libero sviluppo della persona, secondo l'art 2 Cost., rientra tra i diritti inviolabili. "La dignità umana costituisce uno dei valori fondativi della riservatezza, destinato ad assumere un rilievo sempre più grande per il diffondersi e il rafforzarsi di tendenze che espongono, usando l'espressione di Bloustein, la vita privata a un *public scrutiny*".[18] In base al secondo comma, la riservatezza viene in rilievo non in qualità di diritto costituzionale,

[12] D. CALDIROLA, *Il diritto alla riservatezza*, cit., pp.16.
[13] T. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978, pagg. 53-54.
[14] Articolo 2 Cost: «La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale».
[15] Si veda T. AULETTA, *Riservatezza e tutela*…, cit., pp. 42-43.
[16] In tal senso S. Niger, *Il diritto*…, cit., pp.49.
[17] Articolo 3 Cost: «Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese».
[18] Si veda S. NIGER, *Il diritto…,* cit., pp. 47.

bensì come principio che consente a ciascun individuo il pieno godimento dei diritti sanciti dalla costituzione. "Dal secondo comma veniva desunta, come ostacolo di ordine economico e sociale, capace di impedire il pieno sviluppo della persona, la divulgazione dei fatti."[19] Il diritto alla riservatezza veniva da taluni ricostruito come libertà negativa rispetto al diritto di manifestare il proprio pensiero ex art 21 della costituzione[20]. In tal senso la norma riconoscerebbe anche il diritto di non manifestare il proprio pensiero e quindi di escludere la collettività dalla conoscenza di taluni fatti e vicende[21]. Mentre la dottrina aveva già formulato molteplici teorie, il diritto alla riservatezza non aveva, tuttavia, trovato riconoscimento nelle aule dei tribunali. Le prime pronunce che negli anni '50 accesero la questione tra le corti, furono originate dalla pubblicazione di opere riguardanti persone note che invocavano l'autorità giudiziaria a tutela del loro diritto alla riservatezza, ma non giunsero mai ad affermare espressamente questo diritto. È solo negli anni Settanta che venne definitivamente riconosciuto il diritto alla riservatezza da parte della Corte di cassazione nel caso che coinvolse la principessa Soraya Esfandiar. Nella sent. N. 2129 del 27 maggio 1975[22] la corte affermava: "Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti". La corte, tuttavia, precisava che non fosse opportuno dare alla riservatezza una definizione rigida vista la multiformità del suo contenuto che deve

[19] D. CALDIROLA*, Il diritto alla riservatezza*, cit., pp.21.

[20] Articolo 21 Cost: «Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure. Si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili. In tali casi, quando vi sia assoluta urgenza e non sia possibile il tempestivo intervento dell'Autorità giudiziaria, il sequestro della stampa periodica può essere eseguito da ufficiali di polizia giudiziaria, che devono immediatamente, e non mai oltre ventiquattro ore, sporgere denunzia all'Autorità giudiziaria. Se questa non lo convalida nelle ventiquattro ore successive, il sequestro s'intende revocato e privo di ogni effetto. La legge può stabilire, con norme di carattere generale, che siano resi noti i mezzi di finanziamento della stampa periodica. Sono vietate le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume. La legge stabilisce provvedimenti adeguati a prevenire e a reprimere le violazioni».

[21] A. CATAUDELLA, *La tutela civile della vita privata,* Giuffrè, Milano, 1972, pp.36.

[22] La sentenza è consultabile sul sito jstor.org

adattarsi al contesto storico e ambientale. Secondo la corte il diritto sarebbe riconosciuto sia in base alle norme ordinarie e costituzionali "che tutelando aspetti peculiari della persona, non possono non riferirsi alla sfera privata di essa", sia nelle norme contenute nelle leggi speciali "nelle quali si richiama espressamente la vita privata del soggetto o addirittura la riservatezza". La sentenza venne salutata con favore in dottrina, sebbene, come la stessa corte ha notato, concetti come quello di riservatezza siano in evoluzione e pertanto i confini siano incerti. "Prima degli anni '70, quando si parlava di riservatezza ci si riferiva solo alle intrusioni nella vita personale e familiare, poste in essere con metodi e strumenti semplici, quali macchine fotografiche o audiovisive, cannocchiali, pubblicazioni sui giornali di notizie riservate. Le definizioni elaborate in quegli anni, pur rivestendo notevole importanza, non appaiono più consone, però, a descrivere la nozione di privacy attuale[23]."

2. Il diritto alla riservatezza di fronte alle nuove tecnologie

L'incessante sviluppo delle tecnologie ha impattato sull'originario diritto alla riservatezza come diritto ad essere lasciati soli, trasformandolo e adeguandolo a nuove esigenze. "Così, le tecnologie sfidano i vecchi diritti e ne esigono impetuosamente di nuovi. Intorno ad esse si ridefinisce l'identità stessa del soggetto, a partire dalle modalità della procreazione fino alla rete di relazioni interpersonali costruita attraverso le varie categorie di informazioni[24]." L'elaboratore elettronico appare il simbolo più rappresentativo della società tecnologica di massa. Durante la vita quotidiana ciascun individuo conferisce informazioni che singolarmente considerate non avrebbero alcuna rilevanza, ma, se connesse tra di loro, consentono la valutazione e il controllo degli individui. Grazie all'uso di *internet* e dei *computer* è divenuto possibile non solo archiviare, ma anche accedere e far circolare grandi masse di dati. Le polemiche che andremo analizzare, riguardo le intercettazioni telefoniche e la conservazione dei dati relativi al traffico, proprio in relazione al rischio di una sorveglianza di massa, ci rivelano i profondi cambiamenti vissuti dalla nostra società. Non è solo la sfera privata ad essere modificata, ma anche i rapporti tra il cittadino e lo Stato, tra le imprese e i consumatori[25].

[23] Si veda S. NIGER, *Il diritto*…, cit., pag.61.
[24] Si veda S. RODOTÀ*, Tecnologie e diritti, Mulino*, Bologna, 1995, pag.15.
[25] S. NIGER, Il diritto…, cit., pag. 72.

Clive Humby, *data scientist* e matematico inglese, nell'ormai lontano 2006, del resto, ha coniato lo *slogan* "I dati *sono* il nuovo petrolio". Le informazioni rappresentano, infatti, un enorme potere per chi le detiene e gli individui, in questo contesto, sono sottoposti ad un controllo sempre più incisivo. "Si tratta, come ha segnalato Foucault, di un controllo virtuale, cioè preventivo e pertanto generalizzatore, che può materializzarsi in qualsiasi istante e che prescinde dal rapporto personale diretto fra chi controlla e chi è controllato. Insomma, il terrificante "campo di concentramento mondiale" descritto dalla penna di Orwell nel suo "1984" può diventare realtà, se nel seno delle società postindustriali non si apre un profondo dibattito sul controllo dell'uso dell'informatica" [26]. In questa società sorvegliata occorre ripensare il concetto di riservatezza e approntare gli strumenti necessari a tutela dell'intimità di ciascuno. Il precedente *right to be let alone*, elaborato da Warrein and Brandeis e trapiantato in Italia, risultava inadeguato alle nuove esigenze degli individui e pertanto il concetto venne esteso fino ad intenderlo come "possibilità di ciascuno di controllare l'uso delle informazioni che lo riguardano"[27]. In particolare, l'elaborazione di tale teoria si deve a Rodotà, che partendo dagli sviluppi avvenuti negli Stati Uniti sul tema, tentò di trapiantare nel nostro ordinamento la teoria del controllo. "Non è più possibile considerare i problemi della *privacy* solo seguendo il pendolo tra riservatezza e divulgazione; tra l'uomo prigioniero dei suoi segreti e l'uomo che non ha nulla da nascondere; tra la casa fortezza, che glorifica la *privacy* e favorisce l'egocentrismo, e la casa-vetrina, che privilegia gli scambi sociali".[28] Si passa, quindi, da una visione della *privacy* "individualistica e negativa" ad un'impostazione "collettiva e positiva"[29]. La definizione proposta da Rodotà "ha il merito di attribuire alla persona il potere necessario per rendere effettivo il diritto alla *privacy* a fronte delle nuove tecnologie"[30]. Dopo Rodotà la dottrina italiana ha abbandonato la visione della riservatezza come *right to be alone* per approdare alla visione della riservatezza come potere sui propri dati personali[31]. Anche la giurisprudenza ha progressivamente recepito la teoria del controllo, seppure molto lentamente. Nei venti anni successivi al caso Soraya

[26] F. MORALES PRATS, *Presupposti politico criminali per una tutela penale della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo),* in Diritto dell'informazione e dell'informatica, II, aa.1986, pp.41 ss.
[27] S. RODOTÀ, *Tecnologie e diritti*, cit., pag.19.
[28] S. RODOTÀ, *Tecnologie e diritti*, cit., pag.21.
[29] T. UBERTAZZI, *Il diritto…*, cit., pag. 61.
[30] T. UBERTAZZI, *Il diritto…*, cit., pag., 63.
[31] T. UBERTAZZI*, Il diritto…*, cit., pag. 61.

le corti italiane hanno emesso una serie di provvedimenti che vietavano la circolazione di dati personali e riconoscevano quindi all'individuo un potere di controllo a tutela della propria *privacy,* fino al riconoscimento del diritto all'oblio, uno dei molteplici aspetti in cui si manifesta il diritto alla riservatezza. In questa nuova veste la riservatezza è stata declinata, pertanto, come potere di vietare qualsiasi circolazione di informazioni ed in particolare di rettificare e all'occorrenza di cancellare i dati anche dopo la pubblicazione. "Si coglie così il passaggio da una impostazione negativa e passiva ad una positiva e dinamica della protezione dei dati individuali. La tecnica giuridica adoperata non è più quella dell'attribuzione al privato di un diritto azionabile davanti ad un organo ad hoc solo nel caso di una sua violazione. Ora al privato viene attribuito un potere di controllo diretto e continuo sui raccoglitori delle informazioni, indipendentemente dalla esistenza attuale di una violazione. Muta così la *privacy* e l'attenzione si sposta verso la messa a punto di regole sulla circolazione delle informazioni"[32]. Abbiamo seguito la lenta e progressiva evoluzione del diritto oggetto della nostra trattazione, ma non siamo ancora giunti al termine di questo percorso, le nuove tecnologie ed in particolare *internet* hanno portato a nuove declinazioni del diritto alla riservatezza. L'avvento degli elaboratori elettronici e la loro crescente diffusione hanno, infatti, fornito al tema della *privacy* una nuova e più concreta attualità. La nozione di *privacy* è quindi una nozione fortemente dinamica, "esiste infatti una constante relazione tra mutamenti delle tecnologie, delle informazioni e mutamenti del concetto di *privacy*. Tale concetto è infatti soggettivo e variabile in funzione dei soggetti, dei momenti storici, dei luoghi. È inoltre un concetto culturale: dipende, cioè, dalla cultura della società in cui viene invocato. I limiti della privacy, pertanto, sono elastici, ossia dipendono dalle circostanze e dal contesto in cui si trova un determinato soggetto"[33]. In questo contesto, l'evoluzione del concetto di *privacy* richiede la formulazione di regole aggiornate, adeguate alle innovazioni tecnologiche. Questa problematica, per essere affrontata necessita di un approccio globale, "e quindi della costruzione di un sistema armonico di regole, di un quadro di principi generali entro il quale possono trovare posto norme specifiche e codici di autoregolamentazione"[34]. Solo attraverso una sapiente opera di cooperazione possiamo ridurre le disarmonie e i rischi di disparità nel riconoscimento del diritto alla *privacy*. In questa fase sarà indispensabile

[32] S. RODOTÀ, Tecnologie e diritti, cit., pag. 64.
[33] S. NIGER*, Le nuove dimensioni della privacy*, cit., pag. 69.
[34] S. NIGER, Le nuove dimensioni della privacy, cit., pag. 77.

analizzare gli interventi normativi sovranazionali e il ruolo propulsore della Corte di giustizia, per avere una visione completa di questo complesso diritto, tanto sul versante del diritto all'oblio, quanto sul versante del contrasto alla creazione di una società sorvegliata. Tanti sono stati, infatti, gli sforzi fatti dagli organismi sovranazionali per tutelare la riservatezza e garantire uno spazio virtuale sicuro.

3. Il caso *Google Spain*: un rafforzamento del diritto alla riservatezza

Nell'ambito della nostra indagine risulta interessante soffermarci su una sentenza della Corte di giustizia europea. Si tratta della pronuncia della Grande Sezione del 13 maggio 2014, che ha riconosciuto il diritto all'oblio nel famoso caso *Google Spain*. Roberto Flor[35] sottolinea tutti i profili toccati da questa pronuncia: la responsabilità del fornitore di un servizio nella società dell'informazione di internet, la tutela della riservatezza e il suo bilanciamento con altri diritti fondamentali ma anche la globalizzazione del crimine. Si tratta pertanto di una controversia rilevante sia sul piano del diritto penale sostanziale sia sul piano sociale. Con questa sentenza la Corte afferma la prevalenza dei diritti tutelati dagli artt. 7[36] e 8[37] della Carta dei diritti fondamentali dell'UE[38] rispetto alla libertà di espressione e agli interessi economici dei *providers.* In questo modo, viene rafforzata la posizione giuridica della persona interessata da un trattamento di dati personali ma vengono anche posti dei limiti in quello che viene spesso definito il *far west* del *web*. La nostra analisi parte dai fatti che hanno originato la controversia. Il 5 marzo 2010, il sig. Costeja González, cittadino spagnolo, presentava un reclamo dinanzi all'*Agencia Espanola de Proteccion de Datos* (AEPD) contro *La Vanguardia Ediciones SL*, un

[35] R. FLOR, Cybercrime, cit.

[36] Art. 7 Carta dei diritti fondamentali dell'Unione Europea: Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

[37] Art. 8 Carta dei diritti fondamentali dell'Unione Europea: 1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole Ł soggetto al controllo di un'autorità indipendente.

[38] La carta dei diritti fondamentali dell'Unione Europea, nota anche come Carta di Nizza, è stata proclamata una prima volta il 7 dicembre 2000 a Nizza e una seconda volta, in una versione adattata, il 12 dicembre 2007 a Strasburgo da Parlamento, Consiglio e Commissione. La Carta ha il medesimo valore giuridico dei trattati, ai sensi dell'art. 6 del TUE ed è pienamente vincolante per gli Stati membri. Essa introduce una serie di diritti e di libertà, garantiti a tutti i cittadini dell'Unione. Il testo della Carta dei diritti fondamentali dell'UE è reperibile sul sito europarl.europa.eu.

quotidiano di larga diffusione in Spagna e contro *Google Spain* e *Google Inc.* Il reclamo si fondava sul fatto che cercando il nome del sig. Gonzalez nel motore di ricerca del gruppo *Google*, si ottenevano dei *link* che rimandavano a due pagine del quotidiano *La Vanguardia*. All'interno di tali pagine si faceva menzione di una vendita all'asta di un immobile connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali. Il sig. Costeja González chiedeva, da un lato, che fosse ordinato a *La Vanguardia* di sopprimere o modificare le pagine suddette affinché i suoi dati personali non vi comparissero più. Dall'altro lato, egli chiedeva che fosse ordinato a *Google Spain* o a *Google Inc.* di eliminare o di occultare i suoi dati personali, in modo che cessassero di comparire tra i risultati di ricerca e non figurassero più nei *link* di *La Vanguardia*. Il sig. Costeja González affermava in tale contesto che il pignoramento era stato interamente definito da svariati anni e che la menzione dello stesso era ormai priva di qualsiasi rilevanza. L'AEPD respinge il reclamo diretto verso *La Vanguardia* poiché la pubblicazione di quelle notizie era stata disposta su ordine del Ministero del Lavoro e degli Affari sociali. Viene, invece, accolto il reclamo nei confronti di *Google Spain* e *Google Inc*. sull'assunto che i gestori di motori di ricerca siano assoggettati alla normativa in materia di protezione dei dati. L'AEDP ritiene, pertanto, di essere autorizzata a chiedere la rimozione dei dati, qualora essa ritenga che la loro diffusione possa ledere il diritto fondamentale alla protezione dei dati e la dignità delle persone. *Google Spain* e *Google Inc*. hanno proposto due ricorsi separati contro la decisione menzionata dinanzi *l'Audiencia Nacional*, dei quali quest'ultima ha disposto la riunione. Tale controversia rimanda all'interrogativo su quali siano gli obblighi che incombano sui gestori di motori di ricerca per la tutela dei dati personali delle persone interessate. La risposta a tale quesito dipende dal modo in cui viene interpretata la direttiva 96/46/CE. Tale direttiva aveva cercato di garantire un livello alto ed equivalente di tutela della persona rispetto al trattamento dei dati e di armonizzare le normative degli stati membri dell'UE. In questa pronuncia andremo a verificare il suo adeguamento alle tecnologie apparse dopo la sua pubblicazione. L'*Audiencia Nacional*, pertanto, sottopone alla Corte di giustizia una serie di questioni pregiudiziali al fine di verificare se anche l'attività attuata dai *providers* debba essere sottoposta a questa disciplina. Le questioni di nostro interesse sono le seguenti: se l'attività dei motori ricerca possa essere qualificata come trattamento di dati personali e se gli stessi motori di ricerca possano essere considerati responsabili di tale

trattamento. Secondo *Google Spain* e *Google Inc*., l'attività dei motori di ricerca non può essere considerata come trattamento dei dati che appaiono sulle pagine *web* di terzi visualizzate nell'elenco dei risultati della ricerca, poiché i motori di ricerca trattano le informazioni nel loro insieme senza distinguere dati personali e altre informazioni. Inoltre, il gestore di un motore di ricerca non può essere considerato come responsabile del trattamento dei dati, dal momento che non ha conoscenza dei dati in questione e non esercita alcun controllo su di essi. La corte rileva, invece, nel paragrafo 26 che l'attività dei motori di ricerca, ove abbia ad oggetto anche dati personali, debba essere qualificata come trattamento di dati personali ai sensi dell'art. 2, lettera b della direttiva 95/46 CE del Parlamento e del Consiglio del 24 ottobre del 1995. Su questo punto la Corte aveva già avuto modo di pronunciarsi nella sentenza Lindqvist. "Pertanto, occorre constatare che, esplorando *Internet* in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca «raccoglie» dati siffatti, che egli «estrae», «registra» e «organizza» successivamente nell'ambito dei suoi programmi di indicizzazione, «conserva» nei suoi *server* e, eventualmente, «comunica» e «mette a disposizione» dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche. Poiché tali operazioni sono contemplate in maniera esplicita e incondizionata all'articolo 2, lettera b), della direttiva 95/46, esse devono essere qualificate come «trattamento» ai sensi di tale disposizione, senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali."[39]Inoltre, secondo i giudici, il gestore del servizio deve essere considerato responsabile del trattamento ai sensi dell'art.2 lettera d. Il motore di ricerca ha il ruolo di titolare del trattamento dei dati personali e di conseguenza ha lui il compito di eliminare i *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative alla persona interessata. Questo obbligo sussisterebbe anche nei casi in cui il sito *web* di origine si rifiutasse di cancellare le informazioni in questione. Affinché si possa procedere, occorre che vi sia un equo bilanciamento tra il legittimo interesse a reperire le informazioni e il diritto alla protezione dei dati personali dell'interessato. La corte ritiene che se il trattamento dei dati sia incompatibile con la direttiva 95/46, l'interessato possa

[39] Corte di giustizia dell'Unione europea, Grande sezione, sent. 13 maggio 2014, Google Spain SL e Google Inc. c. Agencia Espanola de Proteccion de Datos e Mario Costeja González, causa C-131/12, ECLI: EU:C: 2014:317, in curia.europa.eu, paragrafo 28.

esigere ai sensi dell'art. 12[40] la cancellazione dei dati. L'incompatibilità può derivare non soltanto dal fatto che tali dati siano inesatti, ma anche dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alla finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici. La corte, inoltre, nel paragrafo 97 rileva come bisogna tener conto del ruolo ricoperto da tale persona nella vita pubblica. In tale ipotesi l'ingerenza nei suoi diritti fondamentali, sanciti dagli artt. 7 e 8 della Carta sarebbe legittimata dall'interesse preponderante del pubblico ad avere accesso all'informazione. Viene pertanto annunciato il diritto all'oblio, seppure la pronuncia non sia andata esente da critiche. Le maggiori difficoltà risiedono nel bilanciamento dei diritti in gioco. A differenza di quanto fatto dall'Avvocato generale, che aveva operato un bilanciamento tra, da una parte, gli articoli 7 e 8 della Carta e, dall'altra parte, le disposizioni della Carta rilevanti in tema di libertà di espressione (art. 11) e di libertà di iniziativa economica (art. 16), nell'apparato argomentativo della Corte entrambe le previsioni normative appena richiamate scompaiono. Nessun riferimento agli artt. 11 e 16 è rinvenibile e il campo è lasciato interamente libero alle numerosissime citazioni presenti, invece, degli artt. 7 e 8 della Carta. I giudici sottolineano, inoltre, le differenze tra l'attività di un motore di ricerca e editori e siti *web* giornalistici. L'attività dei primi può essere molto più incisiva nei diritti fondamentali. Del resto, come rileva la Corte: " …tenuto conto della facilità con cui informazioni pubblicate su un sito *web* possono essere riprodotte su altri siti, nonché del fatto che i responsabili della loro pubblicazione non sempre sono assoggettati alla normativa dell'Unione, non sarebbe possibile realizzare una tutela efficace e completa delle persone interessate nel caso in cui queste dovessero preventivamente o in parallelo

[40] Art 12 direttiva 95/46: Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi: — la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono comunicati i dati; — la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati; — la conoscenza della logica applicata nei trattamenti automatizzati dei dati che lo interessano, per lo meno nel caso delle decisioni automatizzate di cui all'articolo 15 , paragrafo 1 ; b) a seconda dei casi , la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva , in particolare a causa del carattere incompleto o inesatto dei dati ; c) la notificazione ai terzi, ai quali sono stati comunicati ì dati , di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato.

ottenere dagli editori di siti web la cancellazione delle informazioni che le riguardano."[41] L'art. 9 della direttiva[42] consente il bilanciamento tra, da un lato, la tutela della vita privata e, dall'altro, la libertà di espressione. Tuttavia, i giudici concludono che il motore di ricerca non può beneficiare di tale deroga. La corte sembra mossa dall'intento di garantire la massima protezione possibile agli articoli della Carta che compongono lo statuto della *privacy* digitale. Tuttavia, alcuni studiosi ritengono che una simile differenziazione comporti una deresponsabilizzazione degli editori dei siti *web* ed una responsabilizzazione eccessiva dei motori di ricerca.[43] Risulta particolarmente interessante la lettura delle conclusioni dell'Avvocato generale Nillo Jääskinen, il quale sottolinea la rivoluzione attuata da Internet. "Al centro del presente rinvio pregiudiziale è il fatto che *Internet* amplifica e facilita in modo inedito la diffusione di informazioni. Come l'invenzione della stampa nel XV secolo ha consentito di riprodurre un numero illimitato di copie che prima dovevano essere scritte a mano, così caricare materiali su *Internet* permette un accesso di massa a informazioni che prima potevano essere reperite solo dopo faticose ricerche e in posti fisicamente limitati. L'accesso universale all'informazione *online* è possibile ovunque, con l'eccezione di quei paesi le cui autorità hanno limitato l'accesso a *Internet* con diversi mezzi tecnici (come i *firewall* elettronici) o nei quali l'accesso alle telecomunicazioni è controllato o scarso."[44] In merito alla qualificazione del gestore del motore di ricerca come titolare del trattamento, l'Avvocato generale ha una posizione diversa. Nella direttiva il titolare del trattamento viene definito come colui il quale determina le finalità e gli strumenti del trattamento. Secondo l'Avvocato generale, il motore di ricerca si limita ad indicare dove può essere reperito un contenuto già esistente e diventa titolare del trattamento solo nel caso in cui venga a conoscenza di dati personali. "Il ragionamento operato dall'Avvocato in questo punto crea un bilanciamento più equilibrato tra il diritto alla tutela dei dati personali e il diritto a una

[41] Corte di giustizia dell'Unione europea, Grande sezione, sent. 13 maggio 2014, Google Spain SL e Google Inc. c. Agencia Espanola de Proteccion de Datos e Mario Costeja González, causa C-131/12, ECLI: EU:C: 2014:317, in curia.europa.eu, paragrafo 84.

[42] Art 9 direttiva 95/46: "Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione."

[43] O. POLLICINO, *Interpretazione o manipolazione..., cit., pag. 23.*

[44] Punto 28 delle Conclusioni dell'Avvocato generale reperibili sul sito curia.europa.eu

libera informazione."[45] Altra criticità rilevata dall'Avvocato generale è la seguente: "quando la direttiva è stata adottata, il *World Wide Web* era una realtà appena comparsa e i motori di ricerca su Internet erano ancora agli inizi. Le disposizioni della direttiva semplicemente non tengono conto del fatto che masse ingenti di documenti e di *files* elettronici ospitati in maniera decentralizzata sono accessibili da qualsiasi parte del mondo e che i loro contenuti possono essere copiati, analizzati e diffusi da persone che non hanno alcuna relazione con i rispettivi autori o con quanti li hanno caricati in un *server host* connesso a Internet. "[46] Inoltre, sembra difficile attribuire a *Google Inc*. il compito di valutare l'opportunità di concedere il diritto all'oblio, trattandosi di una società privata. Altra lacuna della sentenza è determinata dall'assenza di coordinate precise che possano guidare nella concessione del diritto all'oblio. Ad esempio, non è indicato il lasso di tempo che deve trascorrere prima che una notizia possa essere rimossa. Altri dubbi attengono alla ingente dose di richieste che potrebbe generare. Per questi motivi, secondo taluni studiosi il bilanciamento tra diritto all'oblio e diritto all'informazione non dovrebbe essere affidato a un privato ma all'autorità giudiziaria[47]. Questa sentenza ha avuto un importante ruolo propulsore nell'affermazione del diritto all'Oblio nel Regolamento europeo della privacy[48]. L'art. 17 GDPR[49] chiarisce i motivi

[45] F. MELIS, Il diritto all'oblio e i motori di ricerca nel diritto europeo in Giornale di diritto amministrativo 2/2015

[46] Paragrafo 78 delle Conclusioni dell'Avvocato generale.

[47] F. MELIS, Il diritto all'oblio e i motori di ricerca nel diritto europeo cit.

[48] Il regolamento generale sulla protezione dei dati (RGPD) o in inglese *General Data Protection Regulation* (GDPR), ufficialmente regolamento (UE) n. 2016/679, è un regolamento dell'Unione Europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato nella gazzetta ufficiale dell'Unione Europea il 4 maggio 2016 ed entrato in vigore in 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018. Con questo regolamento la commissione europea si propone come obiettivo quello di rafforzare la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'UE, sia all'interno che all'esterno dei confini dell'UE, restituendo ai cittadini il controllo dei propri dati personali, semplificando il contesto normativo che riguarda gli affari internazionali, unificando e rendendo omogenea la normativa privacy dentro l'UE. Essendo un regolamento, ai sensi dell'art. 288 TFUE, ha portata generale, è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri. Il testo del Regolamento è reperibile sul sito eur-lex.europa.eu

[49] Art 17 GDPR: 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

per i quali si può richiedere la cancellazione: i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso su cui si fonda il trattamento oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati; l'interessato si oppone al trattamento di dati personali; un tribunale o autorità di regolamentazione dell'Unione ha deliberato in maniera definitiva e assoluta che i dati in questione devono essere cancellati; i dati sono stati trattati illecitamente. Inoltre, sempre l'art. 17 chiarisce che il responsabile del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, prende le misure ragionevoli, anche tecniche, per informare i responsabili del trattamento che stanno trattando la richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali. In conclusione, è interessante notare come tale pronuncia comporti un rafforzamento del diritto alla riservatezza, sia perché viene affermato il diritto all'oblio, sia perché viene affermata la sottoposizione dei *services providers* alla disciplina europea dei dati personali. "Considerata la potenziale gravità dell'ingerenza nell'area di riservatezza pertinente alla persona, il trattamento dei dati da parte del gestore di un motore di ricerca non può essere giustificato sulla base di interessi di natura

---

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

economica."[50] Il diritto all'oblio (*right to be forgotten*), può pertanto essere considerato una riviviscenza del diritto all'essere lasciati soli (*right to be left alone*). Un diritto che appartiene alle ragioni e alle regioni della riservatezza ovvero come pretesa a riappropriarsi della propria storia personale.[51] "Diritto all'oblio e diritto alla *privacy* possono ben rappresentare due facce di una stessa medaglia, che affondano nella dignità della persona la loro rilevanza costituzionale."[52]

4. L'intricato rapporto tra tutela della riservatezza e sicurezza

L'analisi del concetto di sicurezza, alla luce dell'incessante progresso tecnologico, risulta essere indispensabile all'interno della nostra trattazione, tanto per l'importanza che assume a livello nazionale e sovranazionale in una società esposta a nuovi e sempre più numerosi rischi quanto per il rapporto con la *privacy*. Thomas Hobbes nella sua opera "Il leviatano" individuava la sicurezza come giustificazione al potere dello Stato. È il bisogno di sicurezza che induce gli individui ad affidare i loro diritti naturali al sovrano, il solo in grado di garantire la pace. "Il compito di un sovrano rappresentativo, sia esso un monarca o un'assemblea, sta tutto nel fine per la realizzazione del quale il potere sovrano gli è stato affidato, cioè nel garantire la sicurezza del popolo, verso cui quello è obbligato per legge di natura, e per renderne conto di fronte a Dio e solamente a lui che è autore di essa"[53]. Locke condivide l'idea di Hobbes, è lo Stato a garantire la pace e la sicurezza, ma aggiunge che questo costituisce un pericolo per libertà dei cittadini[54]. Per Montesquieu, invece, la sicurezza è intesa come libertà politica. Quest'ultima esiste laddove non c'è abuso di potere e di conseguenza diviene anche sicurezza giuridica ossia osservanza dei principi fondamentali dello Stato di diritto. "La libertà politica consiste nella sicurezza, o almeno nell'opinione che si ha della propria sicurezza. Questa sicurezza non è mai tanto minacciata come nelle accuse pubbliche o private. Dunque, dalla bontà delle leggi penali dipende principalmente la libertà del cittadino"[55]. Queste sono le premesse delle prime codificazioni sui diritti fondamentali che collocavano la sicurezza

[50] R. FLOR, Cybercrime…, cit., pag. 130.
[51] T.E. FROSINI, Diritto all'oblio e Internet in federalismi.it n.1/2014
[52] T.E. FROSINI, Diritto…, cit.
[53] T. HOBBES*, Il leviatano*, 1651.
[54] J. LOCKE, *Secondo trattato sul governo*, 1689.
[55] MONTESQUIE, *Lo spirito delle leggi*, 1748.

tra i diritti innati dell'uomo. Tra di esse citiamo la Dichiarazione dei diritti dell'uomo e del cittadino, che nell'art. 2 afferma: "Il fine di ogni associazione politica è la conservazione dei diritti naturali ed imprescrittibili dell'uomo. Questi diritti sono la libertà, la proprietà, la sicurezza e la resistenza all'oppressione." Secondo tale articolo la sicurezza costituisce garanzia dei diritti e pertanto protezione dagli abusi della monarchia e sicurezza dei rapporti giuridici. Nel costituzionalismo contemporaneo la sicurezza è intesa come interesse collettivo alla tenuta complessiva dello Stato di diritto, viene infatti riconosciuto il valore costituzionale della sicurezza dello Stato, della sicurezza nazionale, dell'incolumità pubblica e dell'ordine pubblico. Tali interessi si affermano nella giurisprudenza costituzionale e in quella delle Corti internazionali dei diritti come cause legittime di restrizione dei diritti individuali. Questo naturalmente nel rispetto di rigide regole formali, tra cui, la riserva di legge, la riserva di giurisdizione, l'obbligo di motivazione, e di regole sostanziali consistenti nel principio del bilanciamento o di contestuale tutela dei beni costituzionalmente rilevanti, nel limite del contenuto minimo o essenziale del diritto fondamentale, nel principio di proporzionalità o di ragionevolezza[56]. Nonostante il termine ricorra frequentemente all'interno della nostra Carta costituzionale, non viene enunciato espressamente un diritto alla sicurezza. Questo ha indotto i giuristi a interrogarsi sulla sussistenza di un diritto costituzionale alla sicurezza. Tradizionalmente, nella nostra costituzione, la sicurezza ha rappresentato la garanzia dei diritti stessi, possiamo pertanto tradurla come diritto alla sicurezza dei diritti[57]. È tale teoria che consente, da un lato di rompere il rapporto tra sicurezza e coercizione e dall'altro rimanda al bilanciamento tra tutti i beni costituzionali e all'individuazione di beni di cui è vietata la compressione[58]. Il bisogno di sicurezza nell'attuale società del rischio è fortemente sentito e tanto a livello sovranazionale che nazionale gli interventi sul tema sono stati numerosi. "La sicurezza si impone sia come attività statale per tutelare il cittadino da rischi e pericoli sociali, sia come diritto fondamentale, quale condizione per l'esercizio delle libertà e per la riduzione delle disuguaglianze, come afferma la legge francese sulla sicurezza quotidiana del 15

[56] M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza*, in medialaws.eu, 2018
[57] T. FENUCCI, *Quanto spazio c'è per un diritto individuale della sicurezza nell'ordinamento costituzionale italiano?* in federalismi.it, 2015.
[58] M.DOGLIANI, *Il volto costituzionale della sicurezza*, in astrid-online.it

novembre 2001."[59] Tuttavia occorre tenere presenti i pericoli di un uso generalizzato dell'espressione diritto alla sicurezza, in nome del quale potrebbero essere legittimate azioni repressive specie a sfavore delle minoranze. Infatti, la sicurezza e l'incolumità dello Stato, pur dovendo essere garantita, non può mai spingersi fino a ledere i diritti fondamentali della persona. Il diritto alla sicurezza vive all'ombra di pericoli, di cui non si può parlare con leggerezza. Si pensi ad esempio alla limitazione della libertà di domicilio in forza delle perquisizioni domiciliari in assenza di autorizzazione dell'autorità giudiziaria, effettuate in Francia nell'ambito delle misure attuative dello stato d'urgenza[60]. O ancora basta far riferimento alla compressione potenziale della libertà di manifestazione del pensiero, determinata dal blocco amministrativo dei siti internet inneggianti al terrorismo, ancora una volta resa possibile dalle scelte del legislatore francese[61], così come le limitazioni alla libertà di circolazione determinate dall'obbligo di dimora per soggetti ritenuti pericolosi per l'ordine pubblico e la sicurezza (*assignation à résidence*)[62]. Si tratta di provvedimenti assunti in Francia in un clima di paura concretizzatosi a seguito dell'attacco alle torri gemelli dell'11 settembre e degli attacchi terroristici realizzati nel corso del 2015. Casi in cui è stata affermata la conformità a costituzione degli atti ma che tuttavia ci possono fare riflettere sull'incisività dei provvedimenti spesso assunti in nome della sicurezza. Il rischio di discriminazioni e intimidazioni deve essere sempre tenuto presente. Nel nostro ordinamento ai fini prettamente esemplificativi si potrebbe menzionare l'art. 13 comma 2 e 3, e l'art. 14 commi 2 e 3 Cost. dove viene richiamata la libertà personale e domiciliare; in questo caso il limite stabilito dalla "sicurezza" non è esplicito ma si può ricavare dalla lettura della disposizione. In particolare, l'art. 13, terzo comma, ammette una compressione della libertà personale "in casi eccezionali di necessità ed urgenza, indicati tassativamente dalla legge"; inoltre possono essere adottate misure temporanee necessariamente soggette alla convalida del giudice in veste di "autorità di pubblica sicurezza". In altre parole, la compressione di un diritto tanto rilevante quanto la libertà personale e/o domiciliare, può

[59] T.E. FROSINI, *Il diritto costituzionale della sicurezza*, in forumcostituzionale.it
[60] Introdotte con la l. 20 novembre 2015, n. 1501.
[61] Articolo 9 della legge n. 2014/1353. Per un commento si veda C. GAZZETTA, Sicurezza, terrorismo e cittadinanza: la nuova legislazione francese antiterrorismo e l'impegno internazionale contro i cd. *foreign fighters*, in Democrazia e sicurezza, n. 3/2015.
[62] Il *Conseil constitutionnel* ha stabilito la conformità a Costituzione di tale misura, perché proporzionata rispetto ai benefici che derivano in termini di tutela dell'ordine e della sicurezza pubblica (Décision n. 2015-527 QPC del 22 dicembre 2015)

avvenire esclusivamente quando questa sia assolutamente necessaria e limitatamente ai casi previsti dal legislatore; a sua volta, detta garanzia va intesa nella sua accezione più ampia. Come sottolineato dalla Corte Costituzionale in una fondamentale decisione riguardante l'espulsione dello straniero dal territorio dello Stato[63], la verifica del giudice deve "estendersi a tutti i presupposti del trattenimento" presso i centri di permanenza temporanea e assistenza, avendo riguardo, dunque, a tutti "i motivi che hanno indotto l'amministrazione procedente a disporre quella peculiare modalità esecutiva dell'espulsione (l'accompagnamento alla frontiera) che è causa immediata della limitazione della libertà personale dello straniero". Ma ciò che più rileva è che il controllo in esame non può mai venire meno, neanche laddove ricorrano motivi di ordine pubblico e sicurezza. In proposito, giova ribadire quanto affermato dalla Corte medesima in un'altra fondamentale decisione[64] concernente ancora una volta l'espulsione dello straniero. In particolare, la disposizione impugnata prevedeva che il provvedimento del questore col quale veniva disposto l'accompagnamento alla frontiera dello straniero fosse immediatamente esecutivo e, dunque, da eseguire prima della convalida da parte dell'autorità giudiziaria. Insomma, lo straniero poteva essere allontanato coattivamente dal territorio nazionale senza che il giudice avesse potuto pronunciarsi sul provvedimento restrittivo della sua libertà personale. Secondo i giudici della Corte, detta disciplina andava a contrastare proprio con l'art.13, terzo comma, Cost., che, come visto, impone la convalida. Pertanto, per quanto concerne la libertà personale, va sottolineato che tale diritto è riconosciuto anche agli stranieri irregolari, in quanto diritto della persona e non del cittadino. In estrema sintesi: nel potenziale "conflitto" tra la tutela (collettiva) della sicurezza pubblica e i diritti (individuali e inviolabili) alla difesa e alla libertà personale deve essere accordata prevalenza a questi ultimi. Ciò non significa che ragioni di ordine pubblico e sicurezza non possano mai comportare una menomazione della libertà in esame, semplicemente è necessario individuare quella soluzione che, sempre a dire della Corte costituzionale, "riduca al minimo il sacrificio per la libertà personale" medesima. Dunque, anche se in via approssimativa, questa ricostruzione generale mette in luce il rischio che le esigenze primarie della sicurezza possano rappresentare un limite all'esercizio di specifiche libertà. Quello che conta per rompere il nesso tra sicurezza e

[63] Corte cost. 10 aprile 2001, n. 105, punto 5 del Considerato in diritto, in Giur. cost., 2001, pag. 675 ss.
[64] Corte cost. 15 luglio 2004, n. 222, in Giur. cost., 2004, pag. 2340 ss.

coercizione è non intendere la sicurezza in senso soggettivo, inteso come percezione di una condizione di sicurezza. Non si può usare la coercizione per soddisfare il bisogno di percepire una condizione soggettivamente soddisfacente di sicurezza[65]. "Bisogna procedere a più complessi bilanciamenti tra gli interessi in gioco, per assicurare insieme la garanzia dei diritti individuali e la progressiva apertura della società"[66]. In poche parole, non ci può essere sicurezza senza il rispetto della legge, altrimenti si sconfinerebbe in repressioni arbitrarie, comportando un *vulnus* alla democrazia. Dopo aver introdotto, seppur in maniera sintetica, il concetto di sicurezza ci soffermiamo sul rapporto con il diritto alla riservatezza, che ha assunto negli ultimi anni particolare rilevanza. Abbiamo già avuto modo di vedere come il progresso tecnologico abbia messo in luce il multiforme volto della *privacy* e come l'infinito scorrere dei dati sul *web* abbia esposto ciascuno di noi a nuovi rischi e attività illecite. In particolare, la possibilità di archiviare, organizzare e mettere in correlazione grandi masse di dati personali, traendo dai medesimi nuove informazioni grazie anche all'utilizzo dell'intelligenza artificiale, consente di ricostruire l'identità, le abitudini, i desideri di un individuo. Come spesso accade quando si parla di tecnologia, questo fenomeno ha una duplice natura. Da un lato positiva, consente lo svolgimento di attività di tipo economico, politico, sociale e facilita la prevenzione, l'accertamento e la persecuzione dei reati. Dall'altro lato, il trattamento dei dati personali e la profilazione agevola la commissione delle attività criminose. I reati informatici, l'utilizzo di captatori informatici, il tracciamento delle ricerche effettuate dal consumatore ai fini della vendita di un prodotto sono solo alcuni degli esempi che possono essere fatti. Tali fattori insieme alla generalizzata percezione di un rischio per la sicurezza individuale hanno aperto il dibattito intorno al rapporto tra *privacy*[67] e sicurezza. In un primo momento la questione è stata semplificata nella opposizione tra *privacy* e sicurezza. Questo è stato determinato sia dai timori di una sorveglianza di massa legati alla rivelazione del programma PRISM, sia ai fenomeni terroristici. Questa semplificazione, però, non tiene conto dell'ampiezza del concetto di *privacy* e di sicurezza[68], termini che è necessario contestualizzare. All'inizio di questo paragrafo, abbiamo infatti esposto i

[65] M. DOGLIANI, Il volto costituzionale della sicurezza in astrid-online.it
[66] S. RODOTÀ, Tecnologie e diritti, cit., pag. 49
[67] Il termine *privacy* viene qui inteso in senso ampio come protezione dell'intimità, della riservatezza e dell'autodeterminazione.
[68] Si veda DOGLIANI M., *Il volto costituzionale della sicurezza* in astrid-online.it, il quale mette in evidenzia tutti i possibili significati che possono essere assunti dal termine sicurezza.

rischi di un'affermazione generalizzata del diritto alla sicurezza. Rischi che possono tradursi anche in violazioni della *privacy* degli individui. Il filo conduttore delle pronunce che andremo analizzare è proprio il rapporto tra *privacy* e sicurezza , dalle quali emergerà che esse invece "rappresentano due facce della stessa medaglia, ovverosia quella della protezione dei diritti essenziali dell'individuo nel più ampio quadro dei bisogni di tutela di una società globale interessata da gravi minacce alla sua stessa esistenza: minacce che impongono, quindi, di riconsiderare ragionevolmente i confini e i contenuti delle stesse libertà del singolo e delle esigenze di protezione della sicurezza collettiva"[69]. In taluni casi, esigenze di sicurezza nazionale e di sicurezza pubblica, richiedono limitazioni specifiche del diritto alla riservatezza e alla protezione dei dati personali. Questa dinamica appartiene, però, alla normale dialettica che il bilanciamento dei diritti e degli interessi costituzionalmente rilevanti impone. In proposito, la giurisprudenza delle Corti europee ha dimostrato che tale bilanciamento non può mai comportare l'integrale sacrificio dell'uno o dell'altra posizione giuridica tutelata. Questa prospettiva in cui *privacy* o protezione dei dati e sicurezza sono complementari e non alternative esce ulteriormente rafforzata se si guarda alla protezione dei dati come interesse collettivo della società. Se infatti la protezione dei dati è non solo un diritto individuale ma ormai compiutamente un interesse primario della società, lo è proprio perché esso appare strumentale, da un lato, alla garanzia dei diritti e, dall'altro lato, alla tenuta complessiva degli ordinamenti democratici. In questo senso, la protezione dei dati è necessaria sia a garantire la sicurezza declinata come sicurezza dei diritti sia la sicurezza come percezione soggettiva di sicurezza e collante ultimo delle società. Per cui sembra di poter concludere che l'espressione "*privacy* vs. sicurezza" sia in realtà molto meno idonea a descrivere la realtà di quanto non possa farlo piuttosto l'affermazione contraria e cioè che "*privacy* è sicurezza". Tutti gli atti normativi dello storico corpus europeo di protezione dati (la direttiva 95/46, c.d. direttiva madre, la direttiva 58/2002, c.d. direttiva e-privacy e la decisione 2008/977/GAI) specificano che le norme europee lasciano inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato e l'applicazione della legge penale. In particolare, la direttiva

[69] M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza*, cit.

58/2002[70], specifica, in ossequio a quanto già affermato dalla giurisprudenza della corte di giustizia dell'Unione Europea, che eventuali limitazioni al diritto di protezione dei dati debbano essere conformi alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali. La Cedu, infatti, ha tradizionalmente rappresentato la fonte da cui desumere le tradizioni comuni a cui occorre conformarsi. Il Regolamento 679/2016 e la Direttiva 680/2016, intervenuti successivamente alle sentenze che andremo ad analizzare, confermano la possibilità di prevedere restrizioni alla protezione dei dati personali per esigenze di sicurezza, ma delimitano questa fattispecie in maniera stringente. In particolare, l'art. 23 del Regolamento[71] prevede una serie di limitazioni specifiche ai diritti di protezione dei dati garantiti dalla normativa. Tra i fini che possono giustificare restrizioni figurano specificamente la sicurezza nazionale, la difesa, la sicurezza pubblica, la prevenzione, l'indagine, l'accertamento di reati e l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Innanzitutto, è chiarito che la restrizione debba essere necessaria e proporzionata in una società democratica, come previsto dalla CEDU e dalla carta dei diritti fondamentali dell'Unione Europea. Inoltre, è previsto che la restrizione debba

[70] La direttiva 58/2002 del Parlamento europeo e del Consiglio del 12 luglio 2002, pubblicata in Gazzetta Ufficiale nel 31 luglio 2002 si occupa del trattamento dei dati personali e della tutela della vita privata nel settore delle comunicazioni elettroniche

[71] Art 23 GDPR: 1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare: a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica; d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g); i) la tutela dell'interessato o dei diritti e delle libertà altrui; j) l'esecuzione delle azioni civili. 2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso: a) le finalità del trattamento o le categorie di trattamento; b) le categorie di dati personali; c) la portata delle limitazioni introdotte; d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti; e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari; f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento; g) i rischi per i diritti e le libertà degli interessati; e h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

contenere alcune disposizioni specifiche circa: a) le finalità del trattamento o le categorie di trattamento; b) le categorie di dati personali; c) la portata delle limitazioni introdotte; d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti; e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari; f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento; g) i rischi per i diritti e le libertà degli interessati; e h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa. "Come si evince dal tenore delle norme qui citate, il test di legittimità circa future restrizioni si preannuncia assai severo, in linea però con la più recente giurisprudenza della Corte CEDU e della Corte di giustizia che rappresenta, pur nella diversità di portata, un riferimento ineludibile per evidenziare i confini entro cui eventuali restrizioni alla protezione dei dati personali sono oggi e saranno domani ritenute legittime."[72] Ci soffermiamo adesso sulla, direttiva 680/2016 del Parlamento e del Consiglio, del 27 aprile 2016, in cui ricorre questo bilanciamento tra diritti e interessi che consente di fare coesistere la *privacy* da un lato e la sicurezza dell'altro. Essa si occupa della protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Una volta fissati gli obiettivi della direttiva, alcune importanti definizioni e i principi applicabili al trattamento dei dati personali (art.4[73]),

[72] M.OROFINO, *Diritto alla protezione dei dati personali e sicurezza,* cit.

[73] Art. 4 direttiva 680/2016: 1. Gli Stati membri dispongono che i dati personali siano: a) trattati in modo lecito e corretto; b) raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità; c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati; d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; f) trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. 2. Il trattamento da parte dello stesso o di un altro titolare del trattamento per una qualsiasi delle finalità di cui all'articolo 1, paragrafo 1, diversa da quella per cui sono raccolti i dati personali, è consentito nella misura in cui: a) il titolare del trattamento è autorizzato a trattare tali dati personali per detta finalità conformemente al diritto dell'Unione o dello Stato membro; e b) il trattamento è necessario e proporzionato a tale altra finalità conformemente al diritto dell'Unione o dello Stato membro. 3. Il trattamento da parte dello stesso o di un altro titolare del trattamento può comprendere l'archiviazione nel pubblico interesse, l'utilizzo scientifico, storico o statistico per le finalità di cui all'articolo 1, paragrafo 1, fatte salve le garanzie adeguate per i diritti e le libertà degli interessati. 4. Il titolare del trattamento è competente per il rispetto dei paragrafi 1, 2 e 3 e in grado di comprovarlo.

viene disposto che gli Stati membri fissino adeguati termini per la cancellazione dei dati personali (art. 5[74]). Inoltre, il titolare del trattamento è tenuto, ai sensi dell'art. 6[75], ad operare una distinzione tra i dati personali delle diverse categorie di interessati. Si fa in particolare riferimento a: a) le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato; b) le persone condannate per un reato; c) le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato, e d) altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b). Anche in questo caso si interviene per evitare le generalizzazioni e mettere in relazione il trattamento dai dati con gli individui a cui questi dati appartengono. In questa ottica sarà necessario mettere a disposizione dell'interessato una serie di informazioni per potergli garantire la contezza circa l'uso che il titolare del trattamento farà dei dati ma anche dei diritti esercitabili dall'interessato[76]. Tuttavia, recita il terzo comma dell'art. 3: "Gli Stati membri possono adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 nella misura e per il tempo in cui ciò

[74] Art. 5 direttiva 680/2016: Gli Stati membri dispongono che siano fissati adeguati termini per la cancellazione dei dati personali o per un esame periodico della necessità della conservazione dei dati personali. Misure procedurali garantiscono che tali termini siano rispettati

[75] Art. 6 direttiva 680/2016: Gli Stati membri dispongono che il titolare del trattamento, se del caso e nella misura del possibile, operi una chiara distinzione tra i dati personali delle diverse categorie di interessati, quali: a) le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato; b) le persone condannate per un reato; c) le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato, e d) altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b).

[76] Art. 13 direttiva 680/2016: 1. Gli Stati membri dispongono che il titolare del trattamento metta a disposizione dell'interessato almeno le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento; b) i dati di contatto del responsabile della protezione dei dati, se del caso; c) le finalità del trattamento cui sono destinati i dati personali; d) il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano. 2. In aggiunta alle informazioni di cui al paragrafo 1,gli Stati membri dispongono per legge che il titolare del trattamento fornisca all'interessato, in casi specifici, le seguenti ulteriori informazioni per consentire l'esercizio dei diritti dell'interessato: a) la base giuridica per il trattamento; b) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; c) se del caso, le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali; d) se necessario, ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato.

costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui". Pertanto, vengono in rilevo le esigenze di sicurezza nazionale e pubblica, in nome delle quali si possono sacrificare le garanzie sancite dall'art. 13, tenendo pur sempre conto dei diritti fondamentali. Ai fini della nostra indagine risulta interessante quanto disposto dall'art. 15[77]. Tale norma consente, infatti una limitazione del diritto di accesso dell'interessato per il perseguimento di taluni scopi, quali quello di sicurezza o ancora per esigenze legate all'accertamento dei reati. Questa misura, tuttavia deve essere sempre necessaria e proporzionata. La società democratica in cui viviamo, infatti, esige che limitazione di un diritto sia sempre opportunatamente giustificata. Infine, l'art. 16[78]

[77] Art. 15 direttiva 680/2016: 1. Gli Stati membri possono adottare misure legislative volte a limitare, in tutto o in parte, il diritto di accesso dell'interessato nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui. 2. Gli Stati membri possono adottare misure legislative al fine di determinare le categorie di trattamenti cui possono applicarsi, in tutto o in parte, le lettere da a) a e) del paragrafo 1. 3. Nei casi di cui ai paragrafi 1 e 2, gli Stati membri dispongono che il titolare del trattamento informi l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione. Detta comunicazione può essere omessa qualora il suo rilascio rischi di compromettere una delle finalità di cui al paragrafo 1. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato della possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale. 4. Gli Stati membri dispongono che il titolare del trattamento documenti i motivi di fatto o di diritto su cui si basa la decisione. Tali informazioni sono rese disponibili alle autorità di controllo.

[78] Art. 16 direttiva 680/2016: 1. Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, gli Stati membri dispongono che l'interessato abbia il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa. 2. Gli Stati membri impongono al titolare del trattamento di cancellare i dati personali senza ingiustificato ritardo e stabiliscono il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione di dati personali che lo riguardano senza ingiustificato ritardo qualora il trattamento violi le disposizioni adottate a norma degli articoli 4, 8 o 10 o qualora i dati personali debbano essere cancellati per conformarsi a un obbligo legale al quale è soggetto il titolare del trattamento. 3. Anziché cancellare, il titolare del trattamento limita il trattamento quando: a) l'esattezza dei dati personali è contestata dall'interessato e la loro esattezza o inesattezza non può essere accertata; o b) i dati personali devono essere conservati a fini probatori. Quando il trattamento è limitato a norma della lettera a), primo comma, il titolare del trattamento informa l'interessato prima di revocare la limitazione

afferma il diritto di rettifica o cancellazione di dati personali e limitazione di trattamento. L'interessato, facendone richiesta, ha il diritto di ottenere dal titolare del trattamento la rettifica o la cancellazione dei dati personali inesatti che lo riguardano. Eventualmente tale diritto potrà essere limitato, anche in questo caso, solo quando vengono in rilievo esigenze prioritarie relative alla sicurezza all'accertamento dei reati o alla protezione dei diritti e delle libertà altrui. Da questo quadro normativo si evince le esigenze di un continuo bilanciamento tra i diritti in gioco. Nel testo della direttiva ricorre spesso il termine sicurezza, il quale viene in rilievo proprio per limitare esigenze legate alla privacy, questo tuttavia sempre attraverso una compressione proporzionata del diritto alla riservatezza. Abbiamo finora guardato al contesto normativo utile a comprendere il rapporto tra *privacy* e sicurezza; tuttavia, il discorso non può essere esaurito alla luce di questi importanti interventi normativi sovranazionali, visti anche gli scarsi interventi dei singoli stati membri. Occorre pertanto osservare la giurisprudenza che a livello sovranazionale si è occupata del tema. Del resto, tutte le volte in cui gli stati membri dell'UE si dimostrano restii ad intervenire per via legislativa, la Corte di giustizia ha indossato le vesti del *judge made law*, consentendo il progresso per via giurisprudenziale.[79] In particolare, tanto nella sentenza *Google Spain*, già analizzata, quanto nella sentenza *Digital Rights Ireland*[80], che analizzeremo presto, la Corte di

del trattamento. 4. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato per iscritto di ogni rifiuto di rettifica o cancellazione dei dati personali o limitazione del trattamento e dei motivi del rifiuto. Gli Stati membri possono adottare misure legislative volte a limitare, in tutto o in parte, l'obbligo di fornire tali informazioni nella misura in cui tale limitazione costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata per: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato delle possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale. 5. Gli Stati membri dispongono che il titolare del trattamento comunichi le rettifiche dei dati personali inesatti all'autorità competente da cui i dati personali inesatti provengono. 6. Gli Stati membri dispongono che, qualora i dati personali siano stati rettificati o cancellati o il trattamento sia stato limitato a norma dei paragrafi 1, 2 e 3, il titolare del trattamento ne informi i destinatari e che i destinatari rettifichino o cancellino i dati personali o limitino il trattamento dei dati personali sotto la propria responsabilità.

[79] O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale in Federalismi.it*, n.3/2014, pag. 3.

[80] Corte di giustizia dell'Unione Europea, Grande sezione, Sent. 8 aprile 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Minister for justice, Equality and Law Reform e Commissioner of Garda Síochána e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a., cause riunite: C- 293/12 e C- 594/12, ECLI:EU:C:2014:238, il sito della sentenza è reperibile sul sito eur-lex.europa.eu

giustizia prende sul serio la protezione della *privacy* digitale e tali pronunce accelereranno l'adozione del Regolamento generale sulla protezione dei dati. "Un tentativo, in altre parole, da parte della Corte di giustizia, di adeguare, a legislazione invariata, alle caratteristiche tecniche del "mondo dei *bit*" quel *Right to Privacy* che Warren e Brandeis, per primi, nel 1890, avevano teorizzato sulla *Harvard Law Review*, pensando, ovviamente, ad un "mondo di atomi". Un diritto alla *privacy* digitale che, seppure mai esplicitamente, i giudici di Lussemburgo enucleano fondandolo sulle due colonne portanti costituite dai diritti al rispetto della vita privata e familiare ed alla protezione dei propri dati personali, previsti, rispettivamente, dagli artt. 7[81] ed 8[82] della Carta dei diritti fondamentali dell'Unione europea"[83]. Vedremo come al centro del dibattito si pone il tema della conservazione dei dati da parte dei servizi di comunicazione. Grazie alle potenzialità fornite dai *service providers* e dai servizi su *internet OTT*[84], nonché per il possibile uso di *virus* che trasformano *computer* e *smartphone* in strumenti di intercettazione ambientale diventa possibile l'ascolto e la visione degli individui in qualunque momento della loro vita. "La conoscenza/consapevolezza dell'esistenza di pratiche legali e illegali, in base alle quali possono essere registrati per anni i dati di persone che non sono sospettati di gravi reati, ha determinato una crescente richiesta di stringenti criteri di (ri)equilibrio tra diritti fondamentali e finalità di sicurezza"[85]. La questione giuridica consiste nel bilanciamento degli interessi in gioco da parte del giudice e del legislatore sia a livello europeo che interno agli stati membri.

4.1 Gli interventi della Corte EDU nei casi Roman Sacharov *v.* Russia e *Big Brother Watch & Others v. the UK*: sorveglianza di massa e violazione art. 8 CEDU

[81] Rinvio a pag. 10 per il testo completo dell'articolo.
[82] Rinvio a pag. 10 per il testo completo dell'articolo.
[83] O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale, cit.,* pag. 3.
[84] Sono definite OTT le imprese che agiscono al di sopra delle reti, da cui il termine *OVER THE TOP* che forniscono servizi, contenuti e applicazioni di tipo "*rich media*" (per esempio le pubblicità). Esse traggono profitto dalla vendita di contenuti e servizi tramite concessionari agli utenti finali o di spazi pubblicitari. Tra le maggiori imprese OTT troviamo Google, Facebook, iTunes, Amazon Prime, Netflix, YouTube, WhatsApp, Messanger, Skype, Gmail.
[85] G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione* in rivista di diritto dei media 2/2018

La nostra indagine, in cui i temi di tutela della *privacy* e sicurezza si intrecciano inesorabilmente, ha inizio con il caso Roman Sacharov v. Russia[86], affrontato dalla corte EDU. Il caso riguarda il sistema di intercettazioni segrete delle comunicazioni via cellulare in Russia. Roman Zakharov, redattore capo di una casa editrice e abbonato a vari *providers* di servizi di reti mobili, aveva denunciato al tribunale di San Pietroburgo la violazione del suo diritto alla riservatezza delle comunicazioni telefoniche. In base alla legge russa i fornitori di reti mobili sono obbligati ad installare apparecchiature che consentono ai servizi di sicurezza di eseguire attività di ricerca. Il 20 ottobre 2006 Zakharov aveva presentato un ricorso alla Corte EDU, affermando che il sistema delle intercettazioni segrete delle comunicazioni telefoniche mobili in Russia costituisce una violazione del diritto alla vita privata, così come tutelato dall'articolo 8 della Convenzione Europea sui Diritti Umani. La corte ha innanzitutto affermato che il ricorso era ammissibile, pur non essendo Zacharov in grado di provare di essere stato oggetto di sorveglianza. Nel caso di specie è la stessa legislazione russa a costituire una violazione dei diritti del soggetto ai sensi dell'art. 8 CEDU. La legge russa risponde a fini legittimi di protezione della sicurezza nazionale e della sicurezza pubblica, di prevenzione della criminalità e di protezione del benessere economico del paese. Questi fini sono idonei, ai sensi della CEDU, a giustificare restrizioni dei *privacy rights*, tuttavia, mancano le misure adeguate a proteggere gli individui dagli abusi. Le criticità che vengono evidenziate sono molte. Le disposizioni giuridiche che disciplinano la sorveglianza delle comunicazioni consentono ai servizi segreti e alla polizia un accesso diretto a tutte le comunicazioni telefoniche mobili. La legislazione non prevede la supervisione dell'intercettazione da parte di un giudice o di un'autorità pubblica. Inoltre, non sono specificate la durata massima delle misure, le circostanze in cui le autorità pubbliche possono fare ricorso a tali misure e le procedure per l'autorizzazione dell'intercettazione, per la memorizzazione e distruzione dei dati. Infine, i rimedi disponibili per contestare l'intercettazione delle comunicazioni, sono disponibili solo per coloro che sono in grado di presentare la prova dell'intercettazione, ma l'ottenimento di tale prova è di fatto impossibile mancando qualsiasi sistema di notifica. La corte ha concluso che la legge russa non soddisfaceva il criterio di "qualità della legge" e che non fosse in grado di limitare le intercettazioni delle

[86] Corte europea dei diritti dell'uomo, Grande camera, 4 dicembre 2015, caso Roman Zakharov v. Russia, 47143/06, in federalismi.it

comunicazioni a quanto "necessario in una società democratica". Di conseguenza c'è stata violazione dell'articolo 8 della Convenzione. Il requisito della qualità della legge non implica soltanto che la legge nazionale debba essere conosciuta e prevedibile nella sua applicabilità, ma che anche le misure di sorveglianza segreta dovrebbero essere applicate quando necessario in una società democratica, in particolare offrendo adeguate ed effettive tutele e garanzie contro l'abuso. Un altro recentissimo caso affrontato dalla Corte EDU in tema di sorveglianza di massa è il *Big Brother Watch & others v. the UK*[87]. Anche in questa occasione la Corte ha censurato la sorveglianza governativa di massa. In particolare, il 25 maggio del 2021 è giunto a conclusione il caso avviato nel 2013 da 16 organizzazioni per la difesa dei diritti individuali a seguito dello scandalo *Datagate* sollevato dall'ex tecnico della CIA Edward Snowden. I giudici hanno ritenuto che lo spionaggio di massa dei dati delle comunicazioni effettuato dal *Government Communication Headquarters* (GCHQ), come consentito dal *Regulation of Investigatory Powers Act* (RIPA) del 2000 comportasse una violazione del diritto fondamentale alla vita familiare e alla *privacy* sancito all'art. 8 della Convenzione. La legge in questione ha consentito all'*intelligenc*e britannica di intercettare gli immensi flussi di informazioni elettroniche che transitano nei cavi a fibra ottica, anche sottomarini. Questo sistema era l'asse portante del programma Tempora, svelato nel 2013 da Snowden, che prevedeva la condivisione delle informazioni intercettate con l'NSA americano (il quale sovraintendeva negli USA l'analogo *Project* PRISM andando così a costituire il più grande sistema di sorveglianza globale nella storia dell'umanità). I giudici hanno anche condannato l'acquisizione di dati attraverso gli *Internet Providers*. Il RIPA, che è stato sostituito dall'*Investigatory Powers Act* (IPA) nel 2016, avrebbe inoltre limitato il diritto di libertà di espressione e di libera stampa garantito dall'articolo 10 della Convenzione. La Corte, come emerge nella pronuncia, non demonizza la sorveglianza di massa, che anzi considera "*a valuable technological capacity to identify new threats in the digital domain*"[88], occorre tuttavia approntare le opportune garanzie. A tal fine la Corte ha idealmente suddiviso il procedimento di sorveglianza di massa in quattro fasi: a) intercettazione e conservazione iniziale dei dati (e metadati) delle comunicazioni; b)

[87] Corte europea dei diritti dell'uomo, Grande camera, 25 maggio 2021, caso Big Brother watch and others v. The United Kingdom, *58170/13, 62322/14 and 24960/15*. Il testo integrale della sentenza è reperibile sul sito hudoc.echr.coe.int

[88] Grande camera, sent. Big Brother & others…, cit., par. 323.

applicazione di specifici selettori ai dati (e ai metadati) delle comunicazioni; c) analisi dei soli dati (e metadati) delle comunicazioni precedentemente selezionati; d) conservazione dei dati definitiva- mente analizzati e successiva (eventuale) condivisione con Stati terzi[89]. Secondo il verdetto, ciò che è mancato è la "supervisione *end-to-end*", ossia la presenza di un organismo indipendente dall'esecutivo che fosse deputato a monitorare l'operato dell'*intelligence* e che decidesse in anticipo i perimetri d'indagine e le operazioni eseguibili. In altre parole, lo spionaggio governativo incontrollato, massivo ed indiscriminato è ciò che ha leso i diritti dell'uomo. Occorre pertanto che il regime di sorveglianza sia necessario e proporzionale. Inoltre, occorre sottoporre l'uso di tali misure ad una preventiva autorizzazione di un'autorità indipendente e prevedere una supervisione *ex post* sulle misure concretamente utilizzate. La Corte ha ampliato, rispetto al passato[90], il novero degli elementi che le legislazioni deli Stati dovrebbero prevedere per garantire la compatibilità con la Convenzione. Attualmente i criteri sono i seguenti: i) i motivi per i quali le intercettazioni di massa potrebbero essere autorizzate; ii) le circostanze in cui le comunicazioni di un individuo potrebbero essere intercettate; iii) la procedura da seguire per il rilascio dell'autorizzazione; iv) la procedura da seguire per la selezione, l'esame e l'utilizzo del materiale intercettato; v)le garanzie da adottare nella condivisione del materiale intercettato con altri soggetti; vi) i limiti circa la durata e la conservazione del materiale intercettato, nonché le circostanze in cui tale materiale deve essere cancellato; vii) le procedure e le modalità per il controllo da parte di un'autorità indipendente del rispetto delle precedenti garanzie e i poteri ad essa riconosciuti per far fronte ad eventuali inadempienze; viii) le procedure per la revisione ex poste i poteri riconosciuti in capo all'organo competente nel caso di non conformità[91]. Per quanto concerne la condivisione dei dati con le nazioni amiche, la maggioranza dei giudici non ha accolto la richiesta degli attivisti per i diritti civili di considerare come violazione dei diritti fondamentali gli accordi di interscambio informativo tra i cinque stati soprannominati come *"Five Eyes"* (Stati Uniti, Gran Bretagna, Canada, Australia e Nuova Zelanda) tra cui vige una sorta di alleanza dei servizi segreti. Sul punto, la *Grand Chamber* ha ritenuto che ci siano regole sufficientemente chiare per consentire un

[89] Grande camera, sent. Big Brother & others…, cit., par. 325.
[90] Facciamo riferimento a Corte europea dei diritti dell'uomo, terza sessione, 29 giugno 2006, Caso Weber e Saravia c. Germania 54934/00 in ilsa.org
[91] Grande camera, caso Big Brother & Others…, cit., par. 361

trasferimento di dati tra le rispettive *intelligence.* I giudici dissenzienti hanno, di contro, ammonito che la presenza di tali regole non è sufficiente essendo, anche qui, necessari meccanismi espliciti per controllare il potenziale uso improprio dei poteri di sorveglianza. La corte, pertanto non si spinge a dichiarare illegale l'intercettazione di massa, bensì ha ritenuto che occorressero maggiori garanzie per i cittadini, in modo da garantire un corretto bilanciamento tra *privacy* e sicurezza. In particolare, quello che emerge nella sentenza è che la Corte tra l'esigenza di tutela della *privacy* e sicurezza nazionale propenda a favore della prima sebbene sembri più preoccuparsi dei soli aspetti procedurali, senza prestare particolare attenzione al carattere sostanziale della tutela[92]. "In conclusione, la sentenza della Grande Camera, nonostante l'apprezzabile tentativo di sistematizzazione delle più recenti questioni relative alla sorveglianza di massa e all'*intelligence sharing*, non appare pienamente soddisfacente. Il nodo principale è la convinzione maturata dalla Corte che i regimi di sorveglianza di massa siano indispensabili nell'attuale sistema del Consiglio d'Europa. Di conseguenza, l'analisi è spesso condotta in modo parziale portando i giudici di Strasburgo ad interrogarsi esclusivamente sulla presenza di garanzie procedurali adeguate a giustificare l'interferenza nella vita privata dei cittadini"[93].

4.2 La sentenza *digital rights*: l'autonomia del diritto alla protezione dei dati personali

In merito al caso noto come *Digital Rights*[94], la Corte di giustizia, in verità, si pronuncia su due cause riunite: la causa C-293/12 (Digital Rights Ireland) e la causa C-594/12. Fondamentali, per comprendere la vicenda, sono le parole dell'Avvocato generale Cruz Villalon, il quale afferma: «nelle cause in esame la Corte è adita due volte in via pregiudiziale di una questione vertente sulla validità della direttiva 2006/24/CE, che le

[92] A. STIANO, *Ancora sul bilanciamento tra la tutela del diritto alla privacy e l'utilizzo di strumenti di sorveglianza di massa: tra garanzie procedurali e sostanziali* in rivista di diritto internazionale n.3/2021, pag. 904- 908

[93] A. STIANO, *Ancora sul bilanciamento tra la tutela del diritto alla privacy e l'utilizzo di strumenti di sorveglianza di massa: tra garanzie procedurali e sostanziali*, cit., pag. 909.

[94] Corte di giustizia dell'Unione Europea, Grande sezione, Sent. 8 aprile 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Minister for justice, Equality and Law Reform e Commissioner of Garda Síochána e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a., cause riunite: C- 293/12 e C- 594/12, ECLI:EU:C:2014:238 in eur-lex.europa.eu

offre l'occasione di pronunciarsi sulle condizioni alle quali è costituzionalmente possibile per l'Unione europea prevedere una limitazione all'esercizio dei diritti fondamentali nel senso particolare di cui all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, mediante una direttiva e i relativi provvedimenti nazionali di recepimento». La corte analizza, in primo luogo, il contesto normativo in cui si colloca la controversia. La corte cita la direttiva 95/46/CE del Parlamento europeo e del Consiglio, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Si tratta del primo testo sulla tutela dei dati personali, proposto nel 1990 quando *Internet* non esisteva ancora. In particolare, l'art 17 interviene sul tema della sicurezza del trattamento dei dati personali. La disposizione così recita: «Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere». Dall'altro lato, la direttiva 2002/58/CE assumeva come obiettivo "l'armonizzazione delle disposizioni degli stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno dell'Unione europea".[95] La direttiva venne adottata dopo la distruzione delle Torri gemelle, pertanto la questione circa il bilanciamento tra diritti fondamentali ed esigenze di sicurezza era ben presente. Le disposizioni della presente direttiva precisano e integrano la direttiva 95/46. La sentenza cita gli art. 4, 5, 6 e 15 della direttiva 2002/58/CE. L'art 4 interviene sul tema della sicurezza dei dati; l'art.5 si occupa della riservatezza delle comunicazioni

[95] Corte di giustizia dell'Unione Europea, Grande sezione, Sent. 8 aprile 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Minister for justice, Equality and Law Reform e Commissioner of Garda Síochána e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a., cause riunite: C- 293/12 e C- 594/12, ECLI:EU:C:2014:238 in eur-lex.europa.eu

e dei dati relativi al traffico; l'art 6, par.1, riguarda la cancellazione dei dati; l'art 15, par.1 dispone che gli stati membri possono limitare i diritti e obblighi di cui agli art.5 e 6 per la salvaguardia della sicurezza nazionale e pubblica. Infine, la corte cita la direttiva 2006/24/CE che aveva modificato la direttiva 2002/58/CE. La corte si occuperà di verificare la validità di tale testo. La direttiva 2006/24/CE era stata introdotta per ragioni di pubblica sicurezza. Essa si occupava della conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e consentiva la raccolta di metadati da parte dei *service provider* senza alcun collegamento con indagini in corso ma solo nell'eventualità di sopravvenute indagine collegate alla commissione di gravi reati. "Una disciplina, quella oggetto di esame da parte della Corte che, imbevuta della logica del controllo preventivo e del sospetto diffuso, deroga, come ricorda lo stesso Avvocato Generale nelle sue Conclusioni, al regime di tutela del diritto al rispetto della vita privata, istituito dalle direttive 95/46 e 2002/58, con riferimento al trattamento dei dati personali nel settore delle comunicazioni elettroniche. Le suddette direttive hanno previsto la riservatezza delle comunicazioni e dei dati relativi al traffico nonché l'obbligo di cancellare o di rendere anonimi i dati stessi quando non siano più necessari alla trasmissione di una comunicazione. La direttiva del 2006 dispone, che gli Stati membri prevedano, «*for the purposes of the investigation, detection and prosecution of serious crime*» un obbligo di conservazione dei dati stessi per un periodo non inferiore a sei mesi e non superiore a due anni"[96]. In merito al caso Digital Rights Ireland, nella controversia si opponeva la *Digital Rights Ireland Ltd* al *Minister for Communications, Marine and Natural Resources, al Minister for Justice, Equality and Law Reform, al Commissioner of the Garda Síochána*, all'Irlanda nonché *all'Attorney General*. Il ricorrente, una società avente come scopo statutario la protezione dei diritti umani nel contesto delle moderne tecnologie di comunicazione, mette in discussione la legittimità delle misure legislative e amministrative nazionali riguardanti la conservazione di dati relativi a comunicazioni elettroniche e chiede al giudice del rinvio di dichiarare la nullità della direttiva 2006/24 e della parte settima della legge del 2005 sulla giustizia penale. La seconda richiesta proviene dal *Verfassungsgerichtshof* austriaco e aveva ad oggetto la compatibilità della

[96] O. POLLICINO, *Interpretazione o manipolazione? La corte di giustizia definisce un nuovo diritto alla privacy digitale*, in federalismicostituzionali.it

legge di recepimento della Direttiva 2006/24 con la Costituzione austriaca. Viene, in entrambi casi, in rilievo il bilanciamento tra il diritto alla protezione dei dati personali e le esigenze di pubblica sicurezza. Sono i giudici a sottolineare l'importanza dei metadati: "Questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati"[97]. Un punto saliente della sentenza è la rilevanza autonoma data agli art. 7 e 8 della Carta di Nizza, un tempo considerati un binomio inscindibile. Nella Carta dei diritti fondamentali dell'Unione Europea trovano riconoscimento, per la prima volta, alcuni nuovi diritti, la cui tutela si è resa necessaria alla luce dei progressi tecnologi, si tratta degli artt. 7 e 8. L'art. 7 costituisce il nucleo originario del diritto alla riservatezza, intorno al quale dottrina e giurisprudenza hanno sviluppato un'ampia tutela della *privacy* e trova una corrispondenza nella disposizione di cui all'art. 8 della CEDU. Le differenze rispetto all'art 8 CEDU sono le seguenti. In primo luogo, il diritto al rispetto delle "comunicazioni" prende il posto del diritto al rispetto della "corrispondenza" allo scopo di tenere conto delle evoluzioni tecnologiche. In secondo luogo, l'art. 7 non riproduce il secondo comma dell'art. 8 CEDU, che individua i limiti del diritto al rispetto della vita privata. La disposizione più innovativa è l'art. 8 della Carta, che recepisce i principi sanciti dalla normativa europea in materia di trattamento dei dati personali. "L'introduzione di questo diritto risponde alla necessità di garantire una specifica tutela nei confronti di attività diffuse e potenzialmente pericolose per alcuni diritti fondamentali. L'utilizzo di mezzi automatizzati nella gestione delle informazioni ha, infatti, facilitato la possibilità di creare banche dati e di far circolare le informazioni in esse contenute, ponendo l'esigenza di una tutela della *privacy* e degli altri diritti della persona rispetto al trattamento dei dati personali"[98]. Il diritto alla *privacy* (art.7) si manifesta nella libertà "negativa" a non subire interferenze nella propria vita privata mentre il diritto della protezione dei dati personali (Art.8) nella libertà "positiva" ad

[97] Corte di giustizia dell'Unione Europea, Grande sezione, Sent. 8 aprile 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Minister for justice, Equality and Law Reform e Commissioner of Garda Síochána e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a., cause riunite: C- 293/12 e C- 594/12, ECLI:EU:C:2014:238 in eur-lex.europa.eu

[98] D. BLONDA, *La disciplina della privacy nel panorama internazionale* in jei.it, 1 agosto 2006

esercitare il controllo sul trattamento e sulla circolazione delle informazioni che riguardano la propria persona. Vi possono essere, quindi, dei casi in cui una normativa che restringe il diritto alla protezione dei dati di carattere personale rimanendo in conformità all'art. 8, possa, invece, procurare una lesione sproporzionata all'art. 7. Anche l'Avvocato generale Cruz Villalon afferma: «l'art. 8 della Carta sancisce il diritto alla protezione dei dati di carattere personale come diritto distinto dal diritto al rispetto della vita privata. Pur se la protezione dei dati è volta a garantire il rispetto della vita privata, essa è soprattutto soggetta a un regime autonomo». Questo riconoscimento rappresenta il punto di approdo di una lunga e complessa evoluzione della normativa europea che ha cercato di armonizzare le discipline dei paesi membri dell'Unione. La nostra vita sta sempre più diventando uno scambio continuo di informazioni, viviamo in un flusso continuo di dati e ciò ha attribuito un'importanza sempre crescente alla protezione dei dati, portandola sempre più verso il centro del sistema politico-istituzionale. Questo diritto consente di modernizzare il classico diritto alla riservatezza. La protezione dei dati personali può in senso lato, comprendere anche la *privacy*, ove questa sia intesa come il diritto di scegliere cosa, nel nostro spazio personale, vogliamo rendere conoscibile agli altri, ma non si esaurisce in ciò. Il diritto alla protezione dei dati personali è molto più ampio, non è il solo controllo delle informazioni private, la mera autodeterminazione informativa, come espressione della ridefinizione della riservatezza, ma si estende "alla tutela di ogni informazione riferita o riferibile a una persona identificata o identificabile, quale che ne sia il contenuto o l'oggetto" [99]. La Corte di Giustizia dell'Unione Europea mantiene distinte le due nozioni, inquadrando il diritto alla *privacy* come diritto ad avere uno spazio privato immune da ingerenze, mentre il diritto alla protezione dei dati personali come il diritto a un corretto trattamento dei propri dati personali, indipendentemente dal fatto che siano dati privati. È lecito pertanto affermare che, il *discrimen* tra le due nozioni si rinviene nel bene oggetto di tutela, la sfera privata, che ha una portata esclusivamente individualistica, nel diritto alla *privacy* e l'interesse generale alla correttezza e liceità del trattamento dei dati, nel diritto alla protezione dei dati personali, che ha la duplice natura di diritto dell'individuo e interesse della collettività. In tal senso, la dottrina osserva che la disciplina della raccolta e del trattamento dei dati

[99] Corte Giustizia UE (Grande Sezione), 6 ottobre 2015, C-362/14, nel celebre caso Maximilian Schrems c. Data Protection Commissioner.

personali si rivela irriducibile alla sola cifra individualistica, in quanto attinge alle garanzie di trasparenza e legalità quali presupposti di funzionamento del sistema democratico[100]. "Questa evoluzione è ben visibile nella Carta dei diritti fondamentali dell'Unione europea, dove si opera una distinzione tra il tradizionale diritto al rispetto della propria vita privata e familiare (art.7) e il diritto alla protezione dei dati personali (art.8), che si configura così come un diritto fondamentale, nuovo e autonomo. La distinzione non è di facciata. Nel diritto al rispetto, alla vita privata e familiare si manifesta soprattutto il momento individualistico, il potere si esaurisce sostanzialmente nell'escludere interferenze altrui: la tutela è statica, negativa. La protezione dei dati, invece, fissa regole sulle modalità del trattamento dei dati, si concretizza in poteri d' intervento: la tutela è dinamica, segue i dati nella loro circolazione. I poteri di controllo e di intervento, inoltre, non sono attribuiti soltanto ai diretti interessati, ma vengono affidati anche ad un'autorità indipendente. La tutela non è più soltanto nelle mani dei soggetti interessati, ma coinvolge permanentemente una specifica responsabilità pubblica. Siamo così di fronte anche ad una redistribuzione di poteri sociali e giuridici. Si coglie qui il punto di arrivo di una lunga evoluzione del concetto di *privacy* dall'originaria sua definizione come diritto ad essere lasciato solo fino al diritto di mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata. Si contribuisce in maniera determinante al processo di costituzionalizzazione della persona"[101]. Occorre qui rilevare, sebbene si tratti di una disciplina successiva alla sentenza in commento, che il presente diritto riceverà tutela grazie al Regolamento 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 e dal Codice in materia di protezione dei dati personali. Infatti, l'art. 1 del Codice *privacy* riproduce esattamente la disposizione contenuta nell'art. 8 della Carta di Nizza. In merito al rapporto tra sicurezza e *privacy,* la Corte ritiene che le misure in esame perseguissero interessi generali, quello della sicurezza internazionale e quello della sicurezza pubblica, meritevoli di tutela e idonei, ai sensi dei Trattati europei e della Carta dei diritti, a giustificare restrizioni dei diritti. "Sancendo di fatto l'ammissibilità di meccanismi di *data retention* e conseguente messa a disposizione delle autorità naturali, la Corte afferma altresì che tali meccanismi rispondono a obiettivi di interesse generale

[100] RODOTÀ S. *Tecnologie e diritti*, Bologna, 1995.
[101] S. RODOTÀ*, Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice della privacy,* in "*Europa e diritto privato*", 2004, p. 3

dell'Unione europea come la lotta al terrorismo finalizzata al mantenimento della pace della sicurezza internazionali, nonché, più in generale, all'obiettivo di contribuire al contrasto della criminalità grave e, con essa, alla sicurezza pubblica"[102]. Tuttavia, all'interno della sentenza leggiamo: "La direttiva 2006/24 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Pertanto, è giocoforza constatare che tale direttiva comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario[103]." La direttiva infatti riguardava qualsiasi persona, qualsiasi mezzo di comunicazione elettronica e l'insieme dei dati relativi al traffico senza operare distinzioni in merito al reato che doveva essere accertato. Dall'altro lato, mancavano limitazioni alla conservazione dei dati e non erano previsti criteri oggettivi per delimitare l'accesso a tali dati. Facciamo riferimento agli articoli da 1 a 9, 11 e 13 della direttiva. In particolare, l'obbligo imposto dall'art. 3[104] ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione elettronica, di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni, come quelli previsti dall'articolo 5[105] della suddetta direttiva,

[102] 0. POLLICINO, cit., pag.13.

[103] Corte di giustizia dell'Unione Europea, Grande sezione, Sent. 8 aprile 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Minister for justice, Equality and Law Reform e Commissioner of Garda Síochána e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a., cause riunite: C- 293/12 e C- 594/12, ECLI:EU:C:2014:238 in eur-lex.europa.eu

[104] Art. 3 direttiva 2006/24: 1. In deroga agli articoli 5,6e9della direttiva 2002/58/CE, gli Stati membri adottano misure per garantire che i dati di cui all'articolo 5 della presente direttiva, qualora siano generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati, da fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione nell'ambito della loro giurisdizione, siano conservati conformemente alle disposizioni della presente direttiva. 2. L'obbligo di conservazione stabilito al paragrafo 1 comprende la conservazione dei dati specificati all'articolo 5 relativi ai tentativi di chiamata non riusciti dove tali dati vengono generati o trattati e immagazzinati (per quanto riguarda i dati telefonici) oppure trasmessi (per quanto riguarda i dati Internet) da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione nell'ambito della giurisdizione dello Stato membro interessato nel processo di fornire i servizi di comunicazione interessati. La presente direttiva non richiede la conservazione dei dati per quanto riguarda le chiamate non collegate.

[105] Art. 5 direttiva 2006/24: 1. Gli Stati membri provvedono affinché in applicazione della presente direttiva siano conservate le seguenti categorie di dati: a) i dati necessari per rintracciare e identificare la fonte di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero telefonico chiamante; ii) nome e indirizzo dell'abbonato o dell'utente registrato; 2) per l'accesso Internet, posta elettronica su Internet e telefonia via Internet: i) identificativo/i dell'utente; ii) identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica; iii) nome e indirizzo

costituisce di per sé un'ingerenza nei diritti garantiti degli artt. 7 e 8[106]. Dalla lettura dell'articolo 5, possiamo notare che la direttiva fa riferimento a una grande massa di informazioni, che consentono di trarre conclusioni molto precise riguardo la vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati[107]. Inoltre, il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi siano effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate, come rilevato dall'avvocato generale ai paragrafi 52 e 72 delle sue conclusioni, la sensazione che la loro vita privata sia oggetto di costante sorveglianza[108]. Per quanto riguarda l'accesso delle autorità nazionali competenti ai dati e al loro uso

dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico; b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: i) numero/i digitato/i (il numero o i numeri chiamati) e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i; 2) per la posta elettronica su Internet e la telefonia via Internet: i) identificativo dell'utente o numero telefonico del/dei presunto/i destinatario/i di una chiamata telefonica via Internet; ii) nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i e identificativo del presunto destinatario della comunicazione; c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione; 2) per l'accesso Internet, la posta elettronica via Internet e la telefonia via Internet: i) data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato; ii) data e ora del log-in e del log-off del servizio di posta elettronica su Internet o del servizio di telefonia via Internet sulla base di un determinato fuso orario; d) i dati necessari per determinare il tipo di comunicazione: 1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato; 2) per la posta elettronica Internet e la telefonia Internet: il servizio Internet utilizzato; e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature: 1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati; 2) per la telefonia mobile: i) numeri telefonici chiamanti e chiamati; ii) International Mobile Subscriber Identity (IMSI) del chiamante; iii) International Mobile Equipment Identity (IMEI) del chiamante; iv) l'IMSI del chiamato; v) l'IMEI del chiamato; vi) nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (Cell ID) dalla quale è stata effettuata l'attivazione; 3) per l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet: i) numero telefonico chiamante per l'accesso commutato (dial-up access); ii) digital subscriber line (DSL) o un altro identificatore finale di chi è all'origine della comunicazione; f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile: 1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione; 2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni. 2. A norma della presente direttiva, non può essere conservato alcun dato relativo al contenuto della comunicazione.

[106] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 34

[107] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 26

[108] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 37

ulteriore, la direttiva 2006/24 non contiene le condizioni sostanziali e procedurali ad esso relative. L'articolo 4 della direttiva[109], che regola l'accesso di tali autorità ai dati conservati, non stabilisce espressamente che tale accesso e l'uso ulteriore dei dati di cui trattasi debbano essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative, ma si limita a prevedere che ciascuno Stato membro definisca le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità[110]. Inoltre, non è previsto alcun criterio oggettivo che consenta di limitare il numero di persone che dispongono dell'autorizzazione di accesso e di uso ulteriore dei dati conservati a quanto strettamente necessario, né l'accesso ai dati è subordinato ad un previo controllo effettuato da un giudice o da un'autorità amministrativa esterna[111]. Per quanto attiene alla durata della conservazione dei dati, la direttiva 2006/24 impone, all'art. 6, la conservazione degli stessi per un periodo di almeno sei mesi senza che venga effettuata alcuna distinzione tra le categorie di dati previste all'art. 5 della direttiva a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate[112]. Non viene, inoltre, precisato che la determinazione della durata di conservazione debba basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario[113]. L'articolo 7 della direttiva 2006/24, non garantisce che sia applicato dai fornitori di servizi un livello particolarmente elevato di protezione e di sicurezza attraverso misure tecniche e organizzative, ma autorizza in particolare i suddetti fornitori a tener conto di considerazioni economiche nel determinare il livello di sicurezza da essi applicato. Inoltre, la direttiva 2006/24 non garantisce la distruzione irreversibile dei dati al termine della durata di conservazione degli stessi[114]. In secondo luogo, si deve aggiungere che tale direttiva non impone che i dati di cui trattasi siano conservati sul

[109] Art. 4 direttiva 2006/24: Gli Stati membri adottano misure per garantire che i dati conservati ai sensi della presente direttiva siano trasmessi solo alle autorità nazionali competenti, in casi specifici e conformemente alle normative nazionali. Le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità sono definite da ogni Stato membro nella legislazione nazionale, con riserva delle disposizioni in materia del diritto dell'Unione europea o del diritto pubblico internazionale e in particolare della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo.

[110] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 61

[111] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 62

[112] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 63.

[113] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 64.

[114] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 67

territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza, quali richiamati ai due punti precedenti[115]. La corte, invece, ritiene che misure limitative del diritto alla protezione dei dati personali e alla vita privata dovrebbero essere applicate solo quando necessario. Inoltre, il test della proporzionalità richiede che le misure debbano essere essenziali al raggiungimento delle finalità generali e meno intrusive possibile. Il sacrificio della protezione dei dati personali a tutela della sicurezza generale può essere legittimo, ma non generalizzato. In conclusione, la corte rileva che il legislatore dell'Unione europea abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli art. 7,8 e 52, paragrafo 1 della carta ed ha infine dichiarato invalida la direttiva 2006/24 *ex tunc*. I giudici, pertanto, arrivano alla conclusione di annullare un atto di diritto derivato dell'Unione Europea perché in contrasto con la Carta dei diritti fondamentali dell'Unione Europea, che viene utilizzata come parametro di costituzionalità.

4.3 Il caso Schrems: Il trasferimento di dati personali verso un paese terzo

La corte di giustizia coglie l'occasione per compiere un ulteriore passo avanti, in materia privacy e sicurezza, grazie al noto caso *Schrems*[116]. La controversia è stata originata da un'azione giudiziaria promossa da Maximilian Schrems, dottorando di ricerca austriaco, il quale lamenta il trasferimento di propri dati personali dall'Unione europea alle piattaforme di servizi su internet (*social network*), localizzate negli Stati Uniti. La questione è particolarmente complessa. Nel 2013 il giovane informatico Edward Snowden rivela documenti segreti riguardanti l'attività di spionaggio condotta dalla *National Security Authority* (Nsa). Il *whistleblower*[117] statunitense rende noti i dettagli di

[115] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 8 aprile 2014, cit., par. 68

[116] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 6 ottobre 2016, Maximillian Schrems c. Data Protection Commissioner, C-362/14, ECLI: EU:C: 2015:650 in eur-lex.europa.eu

[117] Il termine *whistleblower* risulta intraducibile in lingua italiana, tuttavia, l'accademia della Crusca ha dato la seguente definizione: "una persona che lavorando all'interno di un'organizzazione, di un'azienda pubblica o privata si trova ad essere testimone di un comportamento irregolare, illegale, potenzialmente dannoso per la collettività e decide di segnalarlo all'interno dell'azienda stessa o all'autorità giudiziaria o all'attenzione dei media, per porre fine a quel comportamento." Fonte: accademiadellacrusca.it

sofisticatissimi programmi, come il *Prism*[118], attraverso il quale sembrerebbe realizzarsi il rischio orwelliano della sorveglianza di massa. A seguito di tali rivelazioni, in Austria, Maximilian Schrems che aveva trascorso un periodo negli Stati Uniti per studiare i meccanismi di protezione della *privacy* nel caso *Facebook*, teme che i dati raccolti dal *social network* possano essere trasferiti negli Stati Uniti. Schrems solleva la questione dinanzi al *Data Protection Commissioner* irlandese, chiedendo che venga fatto il possibile affinché cessi il trasferimento dati oltreoceano. Il garante della *privacy* rigetta l'istanza poiché una decisione della Commissione europea aveva considerato conforme la disciplina in oggetto. Schrems si rivolge, allora, ai giudici nazionali. La Corte d'Appello irlandese ritiene che sebbene il trasferimento dei dati risponda a finalità di interesse pubblico ed in particolare di sicurezza pubblica, il controllo sia considerevolmente eccessivo. I giudici nazionali sono del parare che il Commissioner avrebbe dovuto istruire la causa al fine di verificare la lesione del diritto fondamentale alla riservatezza. "L'accesso massiccio e indifferenziato a dati personali sarebbe manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese. Affinché intercettazioni di comunicazioni elettroniche possano essere considerate conformi a tale Costituzione, occorrerebbe dimostrare che tali intercettazioni sono mirate, che la sorveglianza su talune persone o taluni gruppi di persone è oggettivamente giustificata nell'interesse della sicurezza nazionale o della repressione della criminalità, e che esistono garanzie adeguate e verificabili. Pertanto, secondo la *High Court* (Corte d'appello), qualora il procedimento principale dovesse essere definito sulla base del solo diritto irlandese, occorrerebbe constatare che, alla luce dell'esistenza di un serio dubbio sul fatto che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali, il commissario avrebbe dovuto compiere un'indagine sui fatti lamentati dal sig. Schrems nella sua denuncia e che il commissario ha erroneamente respinto quest'ultima."[119] Tuttavia, la materia è disciplinata dal diritto dell'Unione Europea. Vengono in rilievo le seguenti disposizioni della Carta dei diritti fondamentali dell'Unione Europea: l'art. 7 che si riguarda il rispetto della vita privata e

[118] Prism è un programma di sorveglianza elettronica, guerra cibernetica e *Signal Intelligence*, classificato come di massima segretezza e gestito dalla *United States National Security Agency (NSA*). Esso è utilizzato per la gestione di dati raccolti attraverso Internet e vari services providers tra cui: *Facebook, Microsoft, Yahoo, Skype e YouTube*. Tra tali dati rientrano *e-mail*, *chat, chat* vocali e *videochat*, foto e video.

[119] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 6 ottobre 2016, cit., par. 33.

della vita familiare; l'art. 8 che si occupa del diritto alla protezione dei dati personali e l'art. 47[120] che garantisce il diritto a un ricorso effettivo e a un giudice imparziale. Viene in rilievo, inoltre, l'art 25[121] della direttiva n. 95/46/CE ai paragrafi n. 1, 2 e 6 secondo cui i dati personali possono essere trasferiti in un paese terzo qualora garantisca un livello di protezione adeguato e l'art.28. La commissione europea ha il compito di constatare che il paese assicuri un livello di protezione adeguato. "Il diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili".[122] Nel caso di specie la decisione della Commissione del 26 luglio 2000 n. 2000/520/CE aveva attestato l'adeguatezza del livello di protezione dei dati previsto dall'accordo c.d. *Safe Harbour* ed aveva autorizzato il trasferimento dei dati personali dall'Unione europea agli Stati Uniti per le imprese americane che lo avessero sottoscritto. Tale accordo rappresentava la base legale che consentiva alle multinazionali del *web* di operare in Europa mantenendo i propri *server* principali negli Stati Uniti. La decisione attua quanto previsto dalla direttiva. La Corte

[120] Art. 47 Carta dei diritti fondamentali dell'UE: "Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo. Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni persona ha la facoltà di farsi consigliare, difendere e rappresentare. A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato, qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia."

[121] Art. 25 dir. n. 95/46/CE: 1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.
2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.
6. La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona.

[122] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 6 ottobre 2016, cit., par. 34.

d'appello irlandese rinvia la questione alla Corte di giustizia europea. La Grande sezione a cui è affidata la controversia dovrà interpretare la direttiva n. 95/46/CE agli art. 25, par.6 e 28[123] e verificare la validità della decisione della commissione. In merito alla prima questione la corte ritiene che in virtù dell'art. 28 le autorità nazionali possano esercitare una forma di controllo riguardo l'utilizzo e il trasferimento dei dati. Anche se gli Stati membri sono tenuti a dare attuazione alla decisione della Commissione, nulla può impedire che un'Autorità di controllo di uno Stato membro possa esaminare la domanda di una persona relativa alla protezione dei suoi dati personali. "Una decisione della Commissione che "constata" la presenza di un livello di protezione adeguato da parte di un paese terzo, destinatario del trasferimento di dati personali di un cittadino dell'Unione, non impedisce che l'autorità nazionale: a) esamini la denuncia del soggetto interessato; b) promuova un'azione giudiziaria, qualora ritenga sussistere una violazione della

[123] Art. 28, par.1, direttiva 95/46/CE: 1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite. amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali. 2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.
3. Ogni autorità di controllo dispone in particolare:
- di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
- di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;
- del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.
È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.
4. Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda.
Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo.
5. Ogni autorità di controllo elabora a intervalli regolari una relazione sulla sua attività. La relazione viene pubblicata. 6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro. Le autorità di controllo collaborano tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile.7. Gli Stati membri dispongono che i membri e gli agenti delle autorità di controllo sono soggetti, anche dopo la cessazione delle attività, all'obbligo del segreto professionale in merito alle informazioni riservate cui hanno accesso.

situazione giuridica soggettiva del singolo."[124] Tuttavia la sentenza conferma la competenza esclusiva della Corte di giustizia a dichiarare l'invalidità degli atti delle istituzioni dell'Unione. Le divergenze tra i giudici nazionali su tale validità potrebbero mettere in discussione la stessa unità dell'ordinamento giuridico comunitario e ledere il principio fondamentale della certezza del diritto. "La Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione".[125] I giudici entrano, successivamente, nel merito della decisione della Commissione, verificandone la validità. La corte ricorda che il diritto alla *privacy* è suscettibile di compressione per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia, purché sussistano le garanzie minime richieste nel continente europeo. La commissione con la propria decisione aveva ritenuto che gli Stati Uniti fornissero un livello adeguato di tutela. Dal punto di vista normativo manca una definizione di "livello adeguato di protezione", tuttavia la Corte compie il proprio giudizio di valutazione sulla base degli art. 7 e 8 della Carta. "È vero che il termine «adeguato» figurante all'articolo 25, paragrafo 6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, come rilevato dall'avvocato generale al paragrafo 141 delle sue conclusioni, l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta. Infatti, in assenza di un siffatto requisito, l'obiettivo menzionato al punto precedente della presente sentenza sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall'Unione verso paesi terzi ai fini del loro trattamento in tali paesi."[126] La corte ritiene che negli Stati

[124]B. CAROTTI, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa* in Giornale di diritto amministrativo 3/2016

[125] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 6 ottobre 2016, cit., par. 61.

[126] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 6 ottobre 2016, cit., par. 73.

Uniti manchino tali garanzie minime e non sia previsto un meccanismo di rimedio giudiziale per i cittadini europei in caso di violazione dei propri dati. Viene ricordata la sentenza *Digital Rights* e il test della necessità in base al quale deroghe e restrizioni alla *data protection* debbano essere limitate allo stretto necessario. "…la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario".[127] La legislazione americana, invece, consente una raccolta massiva di dati a cui le autorità pubbliche possono accedere in qualunque momento. "Le esigenze di sicurezza prevalgono sui principi del regime dell'approdo sicuro, rendendoli recessivi in caso di interferenza. In questo modo, le ragioni legate alla legislazione degli Stati Uniti o agli obblighi di questi ultimi prevalgono - si noti - sulla tutela di diritti e libertà fondamentali di cittadini dell'Unione. È proprio quello che la Commissione avrebbe dovuto evitare; invece, la decisione n. 2000/520 "non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura"[128]. La corte ha deciso di annullare la decisione 2000/520/CE della commissione, del 26 luglio 2000, nella quale era stato constatato che il paese terzo degli Stati Uniti garantisse un livello di protezione adeguato. Tale decisione è di importanza fondamentale per le sue conseguenze. Gli Stati Uniti, in seguito hanno adottato una nuova legge il *Freedom Act* sostitutiva del *Patriot Act*, che introduce maggiori garanzie riguardo l'attività di sorveglianza da parte delle autorità federali. A seguito di tale pronuncia è stato approvato, inoltre, dalla Commissione europea il nuovo accordo tra UE e USA, il 12 luglio 2016, sostitutivo del *Safe Harbour*, definito *Privacy Shield.* Tale accordo avrebbe dovuto prevede obblighi di protezione stringenti per le imprese che trasferiscono dati, misure di sicurezza in materia di accesso ai dati da parte del Governo degli Stati Uniti, e strumenti specifici per la tutela delle persone, tuttavia è stato messo recentemente in discussione dalla Corte di giustizia. In conclusione, riporto un passo di B. Carotti, il quale proprio in merito al seguente caso si pronuncia in questi termini: "…la prospettiva della pronuncia è ampia, e si ricollega a un quadro complessivo che la Corte di giustizia sta lentamente, ma minuziosamente, costruendo. Si costruiscono ponti e collegamenti tra sentenze, che non rilevano solo nel caso specifico, o sul versante

[127] Corte di giustizia dell'Unione europea, Grande sezione, Sent. 6 ottobre 2016, cit., par. 92.
[128] B. CAROTTI, *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa* in Giornale di diritto amministrativo 3/2016

tecnico, ma iniziano a delineare alcuni principî insopprimibili nella materia di Internet e del nuovo mondo digitale, con particolare riferimento al ruolo dei poteri pubblici, ai loro limiti e ai rapporti con i cittadini. Questo quadro complessivo, in costruzione, mira a rinsaldare il legame tra diritti fondamentali e nuove tecniche di comunicazione decentrata." [129] Nonostante il successivo intervento della Corte sul caso, occorre sottolineare l'importanza di tale pronuncia. Risulta sempre di maggiore importanza la tutela del diritto alla protezione dei dati personali e la necessità di un bilanciamento anche con le esigenze di sicurezza pubblica. "Se, dunque, i casi giunti all'attenzione delle Corti dimostrano che, in taluni casi, possa esistere un contrasto tra l'esigenza di proteggere i dati personali e l'esigenza di garantire la sicurezza, occorre però dire che tutti i giudizi delle Corti (a Strasburgo come a Lussemburgo) concorrono a smentire la semplificazione "*privacy* vs. sicurezza". Esse dimostrano, invece, che il bilanciamento o la contestuale tutela può (e deve) svolgersi in modo tale che nessuna delle due esigenze sia sacrificata e, nello specifico, preservando il nucleo essenziale del diritto individuale alla protezione dei dati personali."[130]

__4.3.1 Il recente annullamento del *Privacy Shield*

La pronuncia analizzata non rappresenta l'ultima tappa della vicenda che ha coinvolto l'avvocato Max Schrems. Dopo l'intervento della Corte di giustizia dell'UE, *Facebook Ireland* ha continuato a trasferire dati agli Stati Uniti sulla base della Decisione della Commissione 2010/87. Questa decisione si occupava delle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi. Dietro richiesta di Schrems, l'Autorità garante *privacy* irlandese si è quindi trovata a dover decidere sulla validità della Decisione 2010/87 e ha portato la questione di fronte alla *High Court*. Nel frattempo, la Decisione della Commissione 2016/1250, ha stabilito l'adeguatezza del sistema di trasferimento dati tra Unione Europea e Stati Uniti, il "*Privacy Shield*". Le questioni proposte alla Corte di giustizia[131] sono le seguenti: 1) Se il Regolamento 2016/679 sia applicabile ai

[129] B. Carotti, *La Corte di Giustizia costruisce un ponte tra riservatezza e comunicazioni elettroniche*, cit.
[130] M. Orofino, Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta opposizione in medialaws.eu
[131] Corte di giustizia dell'Unione Europea, Grande sezione, 16 luglio 2020, Data Protection Commissioner c. Facebook Ireland Ltd, C-311/18ECLI: EU: C: 2020: 559

trasferimenti di dati personali che avvengono sulla base di clausole contrattuali standard ai sensi della Decisione 2010/87; 2) Quale livello di protezione sia richiesto dal GDPR in relazione ai trasferimenti; 3) Quali siano i compiti delle Autorità garanti in queste circostanze; 4) Se le Decisioni 2010/87 e 2016/1250 siano valide. La Corte di Giustizia ha innanzitutto sottolineato che il GDPR si applica ai trasferimenti di dati verso un Paese terzo anche se questi dati potrebbero essere trattati dalle autorità del Paese terzo per fini di difesa o pubblica sicurezza. Il livello di protezione che deve essere assicurato ai dati così trasferiti deve essere sostanzialmente equivalente a quello garantito nell'Unione. Le Autorità garanti privacy se si rendono conto che non è assicurata la protezione dei dati dei cittadini europei, devono sospendere o proibire il trasferimento dei dati verso quel Paese. La Corte si è poi pronunciata sulla validità della Decisione 2010/87 della Commissione sulle clausole contrattuali standard. Questa decisione stabilisce dei meccanismi che, da un lato, rendono possibile assicurare nella pratica il livello di protezione richiesto dalla legislazione europea e, dall'altro, fanno sì che i trasferimenti di dati personali che si basano su tali clausole vengano sospesi o vietati nel caso in cui queste siano violate o sia impossibile rispettarle. Inoltre, la Decisione obbliga l'esportatore e l'importatore di dati di verificare che il livello di protezione dei dati garantito nell'UE venga mantenuto. L'importatore dei dati deve informare l'esportatore nel caso in cui fosse in alcun modo impossibilitato a rispettare le clausole contrattuali standard, così che il contratto tra i due possa essere terminato. Alla luce di queste considerazioni, la Corte di Giustizia è giunta alla conclusione che la Decisione in questione sia valida. La Corte ha, invece, dichiarato invalida la Decisione 2016/1250 della Commissione con la quale era stata decisa l'adeguatezza dell'accordo "*Privacy Shield*". La corte ha osservato che le leggi statunitensi sull'accesso e utilizzo di dati da parte delle autorità pubbliche limitavano la protezione dei dati personali e che i cittadini non erano garantiti dalla possibilità di presentare rimedi giurisdizionali. Gli obblighi previsti dal *Privacy Shield* coincidevano solo parzialmente con quelli del GDPR, il cui processo di adozione è avvenuto parallelamente con la negoziazione dell'accordo *Privacy Shield*. Questa mancata sovrapposizione è evidente con riferimento ai requisiti che il GDPR pone a carico del responsabile del trattamento dei dati. La Corte ha affermato che i programmi di sorveglianza delle autorità degli USA non sono limitati allo stretto necessario e, dunque, non rispettano il principio di proporzionalità. La sentenza del caso "Schrems II"

riapre la questione riguardante i trasferimenti di dati personali dall'Unione Europea agli Stati Uniti. "Ancora una volta le imprese si trovano a operare in assenza di una decisione di adeguatezza della Commissione, per cui molte saranno costrette a rivedere i propri sistemi di trasferimento di dati. Inoltre, il fatto che la Decisione 2010/87 resti in piedi non può significare un utilizzo indiscriminato delle clausole contrattuali standard per i trasferimenti di dati negli USA, dovendo valutare caso per caso se i requisiti richiesti dalla CGUE sono rispettati – un compito non facile, viste le critiche sollevate dalla Corte ai sistemi statunitensi di protezione della privacy degli individui"[132]. La Commissione europea ed il Dipartimento del Commercio statunitense hanno annunciato il 10/08/2020, in una dichiarazione congiunta del Commissario europeo per la Giustizia Didier Reynders e del Segretario del Commercio degli Stati Uniti Wilbur Ross, l'avvio delle discussioni per valutare un rafforzamento del Privacy Shield. L'Unione europea e gli Stati Uniti riconoscono l'importanza vitale della protezione dei dati e l'importanza dei trasferimenti transfrontalieri di dati e condividono l'impegno per la privacy e lo stato di diritto, e il rafforzamento delle reciproche relazioni economiche, per le quali hanno collaborato per diversi decenni.

4.4 Il caso Tele2: la compatibilità delle legislazioni interne con il diritto dell'Unione Europea

La sentenza che si occupa del caso Tele2[133] costituisce un ulteriore tassello nel cammino verso l'affermazione del c.d. "*Habeas Data*", il diritto al controllo dei propri dati. La sentenza tratta congiuntamente due cause, la C-203/15 e la C-698/15, al fine di verificare la compatibilità con il diritto dell'Unione europea delle legislazioni interne. Tale pronuncia si colloca temporalmente dopo la sentenza *Digital Rights* con la quale la corte aveva dichiarato invalida la direttiva 2006/24. Alcuni paesi, tuttavia, continuavano ad obbligare i fornitori di servizi di comunicazione elettronica alla conservazione, per un determinato periodo di tempo, di dati di traffico e di ubicazione degli utenti. Ancora una

[132] M. Martorana, *Fine del Privacy Shield: la Corte di Giustizia invalida la decisione di adeguatezza* in Altalex.com, 5 agosto 2020.

[133] Corte di giustizia dell'Unione Europea, Grande sezione, 21 dicembre 2016, Tele2 Sverige AB (C-203/15) c. Post- och telestyrelsen e Secretary of State for the Home Department (C-698/15) c. Tom Watson, Peter Brice, Geoffrey Lewis, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970.

volta sul piatto della bilancia troviamo, da un lato la tutela della *privacy* digitale e dall'altro la sicurezza pubblica. "Da una parte, la conservazione dei dati relativi alle comunicazioni consente «al governo di controllare i governati», mettendo a disposizione delle autorità competenti un mezzo di indagine che presenta un'utilità certa nel contrasto ai reati gravi, e in particolare nella lotta contro il terrorismo. Dall'altra, non può non porsi il problema dell'esigenza «di obbligare il governo a controllare sé stesso» per quanto riguarda sia la conservazione, sia l'accesso ai dati conservati, tenendo conto delle minacce per il diritto alla *privacy*, sempre più a "trazione costituzionale" in ambito europeo."[134] Nel caso di specie, ad essere oggetto di interpretazione è la direttiva 2002/58/CE, antecedente alla direttiva c.d. *Data Retention*. Per condurre il proprio ragionamento la corte si serve degli art.7 e 8 della Carta dei diritti fondamentali dell'Unione Europea[135], ma anche la sentenza *Digital Rights Ireland* vedremo costituirà un parametro di giudizio. La direttiva 2002/58/CE integra la direttiva 95/46/CE e si occupa del trattamento dei dati personali e della tutela della vita privata nel settore delle comunicazioni elettroniche. I fatti sono i seguenti. La Tele2 Sverige, fornitore di servizi di comunicazione elettronica con sede in Svezia, a seguito della invalidazione della direttiva 2006/24, aveva dichiarato che avrebbe cessato di conservare i dati relativi alle comunicazioni elettroniche e avrebbe provveduto alla soppressione dei dati conservati. Tale condotta, tuttavia, sembrava porsi in contrasto con la legislazione interna e le autorità svedesi avevano ordinato a Tele2 di provvedere alla conservazione dei dati relativi alle comunicazioni elettroniche. Il caso arrivò dinanzi ai giudici nazionali, i quali ritennero necessario disporre un rinvio pregiudiziale dinanzi alla Corte di giustizia. Con la prima questione la Corte d'appello amministrativa di Stoccolma chiede se l'art 15[136], paragrafo 1, della direttiva 2002/58/CE,

[134] M. Bassini e O. Pollicino, *La corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico in Diritto penale contemporaneo*, 9 gennaio 2017

[135] Diversamente da quanto accaduto nella sentenza Digital Rights, la Corte di giustizia torna a considerare come un binomio inscindibile gli artt.7 e 8 della Carta.

[136] Artt. 15 direttiva 2002/58/CE: 1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative, le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono

alla luce degli artt. 7, 8 e 52, paragrafo 1, possa essere di ostacolo ad una normativa nazionale, come quella oggetto di esame. La legislazione svedese prevedeva, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati ed utenti iscritti concernente tutti i mezzi di comunicazione elettronica. La disposizione di cui all'artt. 15 della direttiva 2002/58/CE consente agli Stati membri di derogare al principio di riservatezza per adottare misure necessarie, opportune e proporzionate per la salvaguardia di alcuni interessi come la sicurezza pubblica. Tale disposizione è in stretto collegamento con la direttiva c.d. Data Retention, "la quale era stata adottata, nel 2006, anche per uniformare l'atteggiamento degli Stati membri nel derogare al diritto alla privacy dei cittadini sulla base dell'art. 15. Evidente, infatti, era la preoccupazione che, in carenza di indicazioni univoche, ciascun ordinamento potesse modellare in modo assai differente l'ambito di interferenza legittimato dalla norma ora richiamata."[137] Nella seconda causa era contestato il potere del Ministro dell'Interno britannico di imporre ai fornitori di servizi di comunicazione elettronica la conservazione di dati per un periodo massimo di dodici mesi senza alcun preventivo scrutinio delle autorità competenti. In entrambi i casi si coglie l'incertezza circa le conseguenze della decisione *Digital Rights Ireland* e dell'annullamento della direttiva c.d. *Data Retention,* rispetto a misure formalmente estranee all'ambito di applicazione della direttiva ma mosse dalla medesima ratio. La corte di giustizia perviene alla seguente conclusione. La normativa adottata dagli Stati membri ai sensi dell'art.15 rientra nell'ambito di applicazione della direttiva 2002/58/CE, in quanto ha ad oggetto il trattamento di dati personali da parte dei fornitori di servizi di comunicazione elettronica. "Tuttavia, alla luce dell'economia generale della direttiva 2002/58, gli elementi rilevati al punto precedente della presente sentenza non consentono di concludere che le misure legislative contemplate dall'articolo 15, paragrafo

conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea. 2. Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa. 3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.

[137] Bassini M. e Pollicini O., *La corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, cit.

1, della direttiva 2002/58 siano escluse dall'ambito di applicazione di tale direttiva, a pena di privare detta disposizione di qualsiasi effetto utile. Infatti, il citato articolo 15, paragrafo 1, presuppone necessariamente che le misure nazionali da esso contemplate, come quelle relative alla conservazione di dati per finalità di lotta contro la criminalità, rientrino nell'ambito di applicazione di questa medesima direttiva, dato che quest'ultima autorizza espressamente gli Stati membri ad adottare le misure in questione unicamente a condizione di rispettare le condizioni da essa previste."[138] L'art. 15 deve essere oggetto di una interpretazione restrittiva, in quanto costituisce un'eccezione rispetto al divieto di memorizzare dati di traffico senza il consenso degli utenti da parte di qualsiasi soggetto. "Nondimeno, l'articolo 15, paragrafo 1, della direttiva 2002/58, consentendo agli Stati membri di limitare la portata dell'obbligo di principio di garantire la riservatezza delle comunicazioni e dei dati relativi al traffico a queste correlati, deve essere interpretato, conformemente alla consolidata giurisprudenza della Corte, in maniera restrittiva…In proposito, occorre rilevare come l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 stabilisca che le misure legislative che esso prevede e che derogano al principio della riservatezza delle comunicazioni e dei dati relativi al traffico ad esse correlati debbono avere come obiettivo «la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica», oppure devono perseguire uno degli altri obiettivi contemplati dall'articolo 13, paragrafo 1, della direttiva 95/46, cui l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 rinvia. Una siffatta elencazione di obiettivi presenta carattere esaustivo… Pertanto, gli Stati membri non possono adottare misure siffatte per finalità diverse da quelle elencate in quest'ultima disposizione"[139] In seguito la corte si occupa di esaminare i criteri che le possibili interferenze con i diritti fondamentali tutelati dalla Carta devono rispettare. La corte fa, in primo luogo riferimento all'art 52, paragrafo 1, della Carta, il quale dispone che le limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a

[138]Corte di giustizia dell'Unione Europea, Grande sezione, 21 dicembre 2016, cit., par. 73.
[139] Corte di giustizia dell'Unione Europea, Grande sezione, 21 dicembre 2016, cit., Paragrafi 89-90.

finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Bisogna verificare se la legislazione nazionale sia compatibile con questo primo criterio. La corte da un giudizio negativo a questo quesito. La normativa interna prevede una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica. Il legislatore, così facendo, obbliga i fornitori di servizi di comunicazione elettronica a conservare i dati in modo sistematico e continuo. Peraltro, i dati a cui si fa riferimento corrispondono a quelli la cui conservazione era prevista dalla direttiva 2006/24. Si tratta del nome e dell'indirizzo dell'abbonato, il numero di telefono del chiamante e il numero chiamato, nonché un indirizzo IP per i servizi Internet. Questi dati consentono di sapere quale sia la persona con la quale un abbonato o un utente iscritto ha comunicato e attraverso quale mezzo, di stabilire il tempo della comunicazione, nonché il luogo a partire dal quale quest'ultima ha avuto luogo. Inoltre, essi permettono di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente iscritto con talune persone durante un periodo determinato. Come possiamo dedurre e come la stessa corte denota all'interno della sentenza, presi nel loro insieme questi dati possono fornire notizie molto precise circa la vita privata degli individui. Si tratta di un'attività che comporta una ingerenza grave negli artt. 7 e 8 della carta. I giudici parlano di "sorveglianza continua". Sebbene una simile attività venga giustificata da esigenze legate alla sicurezza pubblica, la direttiva 2002/58 impone che la conservazione dei dati rappresenti l'eccezione, mentre nel caso di specie si tratta della regola. Infatti, non è prevista alcuna differenziazione, limitazione o eccezione in relazione all'obiettivo perseguito. La corte mette in evidenza come questa attività di profilazione venga svolta anche a danno di persone, il cui comportamento non può in alcun modo essere indiziario di violazioni penali gravi e non essendo previste eccezioni, vengono conservate comunicazioni persone sottoposte al segreto professionale. "Una normativa nazionale come quella in discussione nei procedimenti principali travalica dunque i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta."[140] La normativa nazionale dovrebbe, pertanto, prevedere regole chiare e precise che regolino la

[140] Corte di giustizia dell'Unione Europea, Grande sezione, 21 dicembre 2016, par. 107.

conservazione dei dati e disporre tutte le garanzie necessarie in modo da eliminare possibili abusi. Inoltre, la conservazione deve rispondere a criteri oggettivi, in base a un rapporto tra dati da conservare e obiettivo perseguito. La seconda questione pregiudiziale a cui risponde la corte è se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta, debba essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre tale accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione. Per quanto riguarda gli obiettivi idonei a giustificare una normativa nazionale che deroghi al principio della riservatezza delle comunicazioni elettroniche, la corte ricorda che l'elenco fornito dall'art. 15, paragrafo 1 è esaustivo. Per quanto attiene al rispetto del principio di proporzionalità, la normativa nazionale deve consentire l'accesso ai dati conservati alle autorità pubbliche soltanto entro i limiti dello stretto necessario e in presenza di presupposti precisi. Occorre, pertanto, che l'accesso delle autorità nazionali competenti sia subordinato ad un controllo da parte di un giudice o di altra entità amministrativa indipendente, che venga data notizia dell'accesso alle persone interessate, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità e in modo tale da consentire l'esercizio del diritto al ricorso. La corte fa, successivamente, riferimento alla necessità di garantire le misure necessarie per prevenire il rischio di abusi e accesso illecito. Infine, gli stati devono garantire il controllo, del rispetto del livello di protezione garantito dal diritto dell'Unione in materia di tutela delle persone fisiche riguardo al trattamento dei dati personali, secondo quanto previsto dall' art. 8 della Carta. Alla luce di quanto affermato, la Corte risponde alla seconda questione pregiudiziale affermando che l'art. 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli artt. 7, 8, 11, e 52, paragrafo 1, della Carta deve essere interpretato nel senso che una normativa nazionale, la quale disciplini l'accesso delle autorità nazionali competenti ai dati conservati, può essere legittima solo se rispetti le condizioni previste. La sentenza analizzata costituisce un importante tassello nel bilanciamento *privacy* digitale e sicurezza. Nella sentenza *Digital Rights*, la Corte

aveva annullato la direttiva che sacrificava la tutela dei dati personali in virtù di una maggiore sicurezza pubblica. Nella sentenza Schrems, la Corte era intervenuta nei rapporti tra Unione europea e Stati Uniti, pretendendo i medesimi standard di protezione garantiti nell' U.E. in caso di trasferimento dati. Infine, nella sentenza Tele2, i giudici, affermano, l'obbligo per gli Stati membri di garantire la tutela della Privacy secondo le condizioni previste dal diritto dell'Unione europea.

4.5 Il recente intervento della Corte di giustizia: *data retention* e lotta ai reati gravi

Il 5 aprile 2022, è stata emessa una importante sentenza della Corte di giustizia dell'UE, che va ad aggiungere un altro importante tassello nel quadro relativo alla protezione dei dati personali di cui ci occupiamo e che si pone in linea con la giurisprudenza da noi analizzata[141]. Questa volta, la Corte è stata chiamata a valutare la compatibilità della disciplina irlandese in tema di *data retention* con il diritto europeo e con i principi della Carta europea dei diritti fondamentali della UE.

I fatti alla base del rinvio pregiudiziale sono i seguenti. Un imputato per omicidio riteneva violati i propri diritti fondamentali in ragione di indagini fondate su dati ricavabili dalle comunicazioni elettroniche illegittimamente conservati in maniera indifferenziata e generalizzata. A seguito di una lunga storia processuale, la Corte suprema d'Irlanda decideva, quindi, di sollevare rinvio pregiudiziale. Il giudice del rinvio si chiedeva se l'art. 15, par.1, della direttiva 2002/58, letto alla luce degli articoli 7,8, 11 e dell'art. 52, par. I, della Carta, dovesse essere interpretato nel senso che esso osta a una normativa nazionale che preveda una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai fini di lotta alla criminalità grave.

[141] Corte di giustizia dell'Unione europea, Grande sezione, 5 aprile 2022, G.D. c. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General, C-140/20, ECLI:EU:C:2022:258

Nella sentenza, la Corte, riunita in grande sezione, conferma, in primo luogo, la propria costante giurisprudenza[142] secondo la quale il diritto[143] dell'Unione osta a misure legislative che prevedano, a titolo preventivo, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione afferenti alle comunicazioni elettroniche, per finalità di lotta ai reati gravi. Per quanto attiene al sistema introdotto dalla direttiva 2002/58 occorre ricordare che l'art. 5, par. 1 enuncia il principio di riservatezza sia delle comunicazioni sia dei dati relativi al traffico a queste correlate e il divieto della loro memorizzazione di tali dati da parte di terzi. L'art. 15, par. 1 della direttiva consente una deroga a tali principi purché tale misura sia "necessaria, opportuna e proporzionata all'interno di una società democratica". Inoltre, una simile limitazione è consentita solo per i fini indicati dalla norma in un elenco che deve essere considerato tassativo. La corte esclude che la criminalità anche grave possa essere equiparata alla minaccia per la sicurezza nazionale, per la quale, invece, è consentita una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, sulla base di statuizioni precedenti della Corte[144]. Per quanto attiene all'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, la Corte, tenendo conto della giurisprudenza precedente[145], afferma che l'art. 15, par. 1 della direttiva 2002/58/CE, deve essere interpretato nel senso che esso osta a misure legislative che prevedano, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e

[142] Digital Rights Ireland, C-293/12; Tele2 Sverige et Watson e a., C-203/15 e C-698/15; del 6 ottobre 2020, Privacy International, C-623/17, e La Quadrature du Net e a., C-511/18, C-512/18 ,Ordre des barreaux francophones et germanophone e.a., C-520/18 (v. comunicato stampa n. 123/20); e del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18 (v. comunicato stampa n. 29/21).

[143] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002, L 201, p. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, p. 11) (in prosieguo: la «direttiva relativa alla vita privata e alle comunicazioni elettroniche»), letta alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in proseguio la «Carta»).

[144] Corte di giustizia dell'Unione Europea, Grande sezione, 6 ottobre 2020, La Quadrature du Net (C-511/18 e C-512/18), French Data Network (C-511/18 e C-512/18), Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 e C-512/18), Igwan.net (C-511/18), c. Premier ministre (C-511/18 e C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 e C-512/18), Ministre de l'Intérieur (C-511/18), Ministre des Armées, C 511/18 e C512/18, ECLI:EU:C:2020:791 in curia.europa.eu

[145] Corte di giustizia dell'Ue, Grande sezione, 8 aprile 2014…, cit.; Corte di giustizia dell'UE, Grande sez., 6 ottobre 2020…, cit.

indifferenziata di dati relativi al traffico e dei dati relativi all'ubicazione. Il predetto articolo 15, par. 1, letto alla luce degli articoli 7, 8, 11 e 52, par. 1 della Carta, non osta, invece, a misure legislative che prevedano, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica:

– la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;

– la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;

– la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e

– il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono tali fornitori di servizi,

se tali misure garantiscono, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi[146].

Per ciascuna di tali categorie la Corte fornisce anche varie precisazioni.

Per quanto attiene alla conservazione mirata, gli elementi oggettivi che giustificano il ricorso a tale misura, possono variare. La conservazione può fondarsi sul criterio personale e riguardare persone precedentemente identificate come soggetti che costituiscono una minaccia per la sicurezza pubblica o nazionale; persone sottoposte ad indagine o altre misure di sorveglianza. La conservazione mirata può essere fondata anche sul criterio geografico, qualora vi siano zone caratterizzate da un rischio elevato di

[146] Corte di giustizia dell'Unione europea, Grande sezione, 5 aprile 2022…, cit., par. 101

preparazione o commissione di atti di criminalità grave. Inoltre, e soprattutto, una misura di conservazione mirata può riguardare luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone o luoghi strategici, quali aeroporti, stazioni, porti marittimi o zone di pedaggio. Questo consente alle autorità competenti di raccogliere dati relativi al traffico e, in particolare, dati relativi all'ubicazione di tutte le persone che utilizzano, in un determinato momento, un mezzo di comunicazione elettronica in uno di tali luoghi. La durata di questa conservazione mirata non può eccedere lo stretto necessario alla luce dell'obiettivo perseguito e delle circostanze che la giustificano, fatto salvo un eventuale rinnovo a motivo della persistenza della necessità di procedere a una siffatta conservazione. Possono essere, eventualmente, previsti criteri diversi da quello personale o geografico purché vi sia sempre un nesso, almeno indiretto, tra gli atti di criminalità grave e le persone i cui dati sono conservati. Per quanto, invece, concerne la conservazione rapida dei tabulati dei quali i fornitori dispongano a fini commerciali (tecnici o di fatturazione), la Corte ammette che la legislazione nazionale ne preveda la conservazione, per un periodo determinato, sulla base di un provvedimento dell'autorità competente "soggetto a un controllo giurisdizionale effettivo". In tal caso, l'ordine di conservazione può estendersi, pur nella misura della stretta necessità, ai tabulati relativi a persone diverse da quelle sospettate di avere progettato o commesso un reato grave o un attentato alla sicurezza nazionale, purché tali dati possano contribuire, sulla base di elementi oggettivi e non discriminatori, all'accertamento di un siffatto reato o attentato alla sicurezza nazionale, quali i dati della vittima o del suo ambiente sociale o professionale. Inoltre, l'ordine di conservazione rapida può riguardare anche zone geografiche determinate in connessione, a vario titolo, con il fatto di reato e può, in ogni caso, intervenire sin dall'avvio delle indagini.

In conclusione, la Corte di giustizia torna a dichiarare l'importanza della tutela della vita privata e della protezione dei dati personali, anche nel caso in cui l'obbiettivo da perseguire sia lotta a un crimine grave. Tale statuizione non potrà che avere pesanti ricadute in tema di indagini e prevenzione dei reati.

5. La lotta al *cybercrime*: gli strumenti normativi sovranazionali

5.1 L'emersione della categoria dei reati informatici

Quando si parla di tematiche che hanno a che fare con la rete, non esistono confini e il nemico è comune a tutti gli stati. Il tema della criminalità informatica deve, pertanto, necessariamente essere analizzato nella prospettiva sovranazionale. In particolare, attraverso gli strumenti normativi sovranazionale andremo alla scoperta del diritto penale dell'informatica, con particolare riguardo alla categoria dei reati a tutela della riservatezza informatica. Il primo lavoro organico in questo settore è stato compiuto da un gruppo di esperti riunito a Parigi ad opera del Comitato per la Politica dell'Informazione, dell'Informatica e delle Comunicazioni dell'Ocse. Il gruppo di esperti compilò tra il 1984 e il 1985, un ampio rapporto nel quale furono analizzati i principali orientamenti normativi dei paesi membri della suindicata organizzazione di fronte alla frode informatica e le soluzioni concrete adottate nell'ambito del diritto penale. A seguito di tale lavoro, il 13 settembre del 1989 il Comitato dei Ministri degli Stati membri dell'OCSE approvò la Raccomandazione n. R. (89) 9, relativa alla criminalità informatica. L'organismo europeo non era interessato a dare una definizione univoca al fenomeno. L'obiettivo era dettare alcune direttive ai legislatori degli Stati membri e lasciare, allo stesso tempo, a ciascuno di essi, la possibilità di adattare ai singoli sistemi giuridici nazionali ed alle loro tradizioni storiche e culturali le formulazioni proposte. Le indagini casistiche svolte negli anni'80 rivelarono che si trattava di fenomeni reali, che avrebbero potuto avere conseguenze devastanti sul piano dei rapporti economici e giuridici. Il legislatore doveva pertanto prendere seriamente in considerazione, non solo per prevenire i danni, ma anche, per offrire senza ritardo strumenti di tutela, che sopperissero alla vulnerabilità dei sistemi informatici. Il Comitato si trovò di fronte ad una serie di difficoltà. L'intervento penale avrebbe dovuto avere un alto valore general preventivo in vista di una crescita esponenziale di questo tipo di infrazioni. Tuttavia, non erano ancora chiare le modalità di accertamento di queste infrazioni e gli strumenti offerti dal diritto penale vigente erano inefficienti. Per tale motivo, il Consiglio d'Europa nel suo schema di lavoro si limitò ad indicare in termini frammentari l'ambito di estensione del diritto penale dell'informatica, raccomandando ai legislatori nazionali una "lista minima" di infrazioni, contenente quelle condotte che gli stati sono tenuti a reprimere con la pena ed una "lista facoltativa", contenente quelle condotte la cui repressione è lasciata alla valutazione dei singoli stati. Facevano parte della lista minima: la frode informatica, il falso in documenti informatici, il danneggiamento di dati o programmi , il sabotaggio

informatico, l'accesso non autorizzato ad un sistema informatico o ad una rete informatica violando delle misure di sicurezza, l'intercettazione non autorizzata con l'impiego di mezzi tecnici, di comunicazioni destinate a, provenienti da, o nell'ambito di, un sistema o una rete informatici, la riproduzione non autorizzata di un programma non protetto, la riproduzione non autorizzata di una topografia. La lista facoltativa ricomprendeva: l'alterazione di dati o di programmi informatici non autorizzata, lo spionaggio informatico, l'utilizzazione non autorizzata di un elaboratore, l'utilizzazione non autorizzata di un programma informatico. Tale atto costituisce, però, uno strumento di soft law. Esso non pone alcuno specifico obbligo in capo agli stati, lasciando libera azione e non prevedendo sanzioni in capo agli stati inadempienti. Questo testo, seppur rappresenta una svolta nella lotta al crimine informatico, non ha posto l'attenzione su un elemento fondamentale, su cui si tornerà presto, che è la cooperazione tra gli stati nella lotta contro la criminalità informatica. Qualche anno dopo la Raccomandazione del Consiglio d'Europa, l'Association Internationale de Droit Pénal (AIDP) è tornata sul tema della criminalità informatica nel suo XV congresso. L'AIDP ha prospettato la necessità di considerare unitaria la lista, ritenendo doveroso incriminare anche le condotte contenute nella lista facoltativa e ha introdotto ulteriori forme di abuso ritenute meritevoli di repressione.

5.2 La convenzione *cybercrime* di Budapest

Il 23 novembre del 2001, il Consiglio d'Europa approvò la "Convenzione di Budapest" che rappresenta una svolta decisiva nella lotta al *Cybercrime*. Tale convenzione costituisce la risposta dei membri del Consiglio d'Europa e di alcuni Stati non membri[147] ai cambiamenti di carattere tecnologico di cui abbiamo discusso in precedenza. Il lavoro è stato condotto da una commissione di esperti che ha collaborato con il G-8 e altri organismi internazionali ed è stato portato a termine in 4 anni. Essa costituisce il primo documento normativo disciplinante i reati commessi attraverso internet o reti elettroniche e tratta: le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Va subito precisato che la Convenzione si applica ai reati da essa stessa definiti "reati cibernetici in senso stretto", ma anche ai "reati

[147] La convenzione è stata origine firmata da 30 stati, 26 dei quali membri del consiglio d'Europa e 4 non membri (United States, Canada, Japan, South Africa)

cibernetici in senso improprio." Quest'ultima categoria comprende: i reati commessi mediante un sistema informatico e qualsiasi reato di cui si debbano o possano raccogliere "prove in forma elettronica". Il documento contiene una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. L'obiettivo principale, enunciato nel preambolo[148], è perseguire una politica penale comune per la protezione della società dalla *cyber*-criminalità, individuando uniformi definizioni e adeguate forme di investigazione per i crimini informatici, promuovendo, quindi, più in generale, una effettiva cooperazione giudiziaria, di polizia ed operativa internazionale. Abbiamo già sottolineato che nell'ambito del *cybercrime*, l'armonizzazione delle leggi dei diversi stati, risulta indispensabile. Il *cyberspace* valica i confini nazionali e se una condotta è punita in una nazione e non in un'altra potrebbe risultare difficile perseguire il colpevole[149]. Infatti, una delle questioni più interessanti da affrontare in materia di rati informatici riguarda il *locus commissi delicti*. In particolare, in un settore in cui le informazioni corrono velocemente, occorre agire velocemente e con metodi professionali, specie per quanto attiene alla conservazione delle prove. Si deve riconoscere che la convenzione presta particolare attenzione alla tutela dei diritti fondamentali, vengono richiamate a tal proposito, la Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e le libertà Fondamentali, la Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici e gli altri trattati applicabili in tema di diritti umani. Riguardo al rapporto tra diritti umani e indagini informatiche, si occupa della tutela di situazioni giuridiche fondamentali, quali il diritto alla riservatezza, che acquisisce la dignità di bene giuridico sui generis e viene espressamente indicato nel titolo 1 del Cap.2. La convenzione si compone di quattro capitoli: "Uso dei termini", "Provvedimenti da adottare a livello nazionale", "Cooperazione internazionale" e "Disposizioni finali". Nel primo capitolo, all'art.1[150],

[148] Il testo ufficiale della convenzione è reperibile sul portale del Consiglio d'Europa: www.coe.int

[149] È ciò che è, per esempio, accaduto con la diffusione di un celebre virus "I LOVE YOU". Una coordinazione internazionale avrebbe consentito di agire in modo più immediato ed efficiente.

[150] Art.1 Convenzione di Budapest. Ai sensi della presente Convenzione, s'intende per:
a. sistema informatico: qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più| delle quali effettuano l'elaborazione automatica di dati in base a un programma;
b. dati informatici: qualunque presentazione di fatti, informazioni o concetti in una forma che si presta a elaborazione informatica, inclusi i programmi che permettono a un sistema informatico di svolgere una funzione;

vengono individuate le definizioni di "computer system", "computer data", "service provider" e "traffic data". Tali definizioni sono particolarmente importanti poiché verranno utilizzati all'interno di questo documento, ma anche all'interno delle legislazioni nazionali dei singoli Stati che hanno ratificato la Convenzione. Al secondo capitolo vengono elencati una serie di obblighi a carico degli Stati parte della Convenzione. Sotto il profilo di nostro interesse, vengono in rilievo gli obblighi di penalizzazione a tutela del bene giuridico della riservatezza (titolo I, Reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici). "La qualificazione delle fattispecie ricalca in buona sostanza fattispecie penali già esistenti sul piano nazionale, ma ne focalizza il bene giuridico attraverso un richiamo di carattere internazionale, ora reso indispensabile dal contesto globale ed istantaneo delle comunicazioni informatiche[151]." Questa coincidenza risulta a tratti solo apparente, visto il rinnovato contesto e l'esigenza una particola "sensibilità tecnica[152]", motivo che spingerà il legislatore italiano ad intervenire nuovamente nel 2008. Tuttavia, sotto alcuni aspetti, il legislatore italiano si trova in anticipo con i tempi, avendo recepito, nel 1993, alcuni obblighi resi formalmente vincolanti dalla Convenzione di Budapest[153]. In particolare, con riguardo alla tutela della riservatezza, gli artt. 2[154] e 3[155] della Convenzione dispongono l'introduzione delle misure necessarie al fine di sanzionare

c. fornitore di servizi: i. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico, e ii. qualunque altra entità che elabora o memorizza dati informatici per conto di tale servizio di comunicazione o per gli utenti di questo servizio; d. dati relativi al traffico informatico: tutti i dati relativi a una comunicazione che passa attraverso un sistema informatico, prodotti da quest'ultimo in quanto elemento della catena di comunicazione e indicanti l'origine, la destinazione, il percorso, l'ora, la data, la dimensione e la durata della comunicazione o il tipo di servizio utilizzato per la comunicazione.

[151] G. CORASANITI, Cybercrime, responsabilità degli enti, prova digitale, CEDAM, 2009, pp.16.

[152] G. CORASANTI, Cybercrime…, cit., pp.17

[153] L.PICOTTI, La ratifica della convenzione cybercrime in Dir.pen. e processo, 2008.

[154] Art.2 Convenzione di Budapest: Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per sanzionare come reato in base alla propria legge nazionale l'accesso all'intero sistema informatico o a parte di esso senza autorizzazione.
Una Parte può richiedere che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico.

[155] Art 3 Convenzione di Budapest: Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici. Una Parte può richiedere che il reato venga commesso con intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico.

penalmente le condotte di accesso abusivo a un sistema informatico e di intercettazione abusiva di comunicazioni informatiche. Con riguardo alla fattispecie di intercettazione illegale (art. 3 Convenzione *Cybercrime*), essa si occupa di proteggere i dati informatici e dunque la riservatezza del loro contenuto, esigendo che essa si realizzi mediante "mezzi tecnici". Non viene qui in rilievo la riservatezza personale od epistolare in quanto tale, ma la riservatezza propriamente "informatica", come dimostra la destinazione o provenienza o presenza dei dati all'interno di un sistema informatico e la specifica modalità di condotta che deve prevedere l'utilizzo di "mezzi tecnici". L'art. 3 della Convenzione di Budapest conferma l'autonomia del "nuovo" bene giuridico e, allo stesso tempo, la vulnerabilità dei dati informatici, bisognosi di specifica protezione anche penale. La convenzione venne firmata, da numerosi stati, anche molto distanti dal punto di vista giuridico tra loro, alcuni dei quali avevano già adottato disposizioni nella materia in esame, con esiti anche molto differenti, in quanto alcuni applicavano definizioni ristrette, altri richiedevano determinate circostanze. L'obiettivo perseguito dalla Convenzione era proprio quello di armonizzare tali differenze. Da un punto di vista generale va sottolineato che tutte le fattispecie considerate dalla Convenzione (ad eccezione di quelle in materia di diritto d'autore) richiedono che la loro commissione, sul piano oggettivo, avvenga "senza diritto" e su quello soggettivo "intenzionalmente". La prima clausola, c.d. di illiceità o antigiuridicità speciale, conferisce elasticità alle incriminazioni, rimandando alla violazione di regole giuridiche extra-penali ovvero di condizioni desumibili dal contesto in cui opera l'agente. Facciamo riferimento all' assenza di cause di giustificazione (quali il consenso dell'avente diritto, la legittima difesa, lo stato di necessità), ma anche alla competenza del soggetto ad agire, ovvero ad altri principi stabiliti dal diritto interno. Da questo punto di vista, potrebbero esserci delle difformità in sede applicativa tra i diversi Stati. Sotto il profilo soggettivo, la locuzione "intenzionalmente" esige che il fatto sia sempre sorretto dal dolo, il cui contenuto va però necessariamente interpretato secondo il diritto interno. Per cui esso potrebbe implicare la consapevolezza dell'illiceità "speciale" del fatto mancando una definizione e disciplina comuni non solo dell'elemento soggettivo (che può perciò abbracciare, oltre al dolo intenzionale in senso stretto, le altre figure del dolo diretto semplice e del dolo eventuale), ma anche dell'errore sugli elementi normativi della fattispecie o sul precetto. Inoltre, in molte ipotesi è richiesta un'intenzione specifica, raffrontabile con il nostro concetto di

dolo specifico, che viene così a far parte integrante dell'incriminazione. L'armonizzazione non può dunque che essere parziale, lasciando difformità in sede applicativa fra Stato e Stato. Analoghe situazioni si potranno verificare, del resto, anche laddove la Convenzione ha stabilito altre regole di carattere generale. Ci riferiamo alla punibilità dei reati a titolo di complicità e di tentativo (art. 11), alla responsabilità (non necessariamente di natura penale) delle persone (art. 12), alla tipologia e alla misura delle sanzioni (che devono essere "effettive, proporzionate e dissuasive" e comprendere "pene privative della libertà personale"). L'armonizzazione operata e voluta dallo strumento convenzionale non può, dunque, significare "unificazione" del diritto penale dei diversi ordinamenti interessati, sia pur nello specifico settore. Essa rappresenta il presupposto necessario per favorire la cooperazione internazionale ed avviare un più lungo processo di integrazione fra Stati. Altra importante notazione riguarda l'introduzione della responsabilità e delle sanzioni a carico delle persone giuridiche agli art.12[156]e 13[157] della convenzione. Si tratta di un'importante novità, su cui il legislatore italiano non si era ancora soffermato e che avrà modo di introdurre nel 2008 con la ratifica della convenzione di Budapest. In conclusione, tale documento costituisce un importante tassello, non solo per gli Stati che hanno fino ad ora ratificato la convenzione, ma anche per gli Stati non aderenti. Seppur non esiste una lista definitiva; infatti, si ritiene che molti Stati si siano ispirati a tale documento. Non mancano alcune critiche mosse alla convenzione, come l'inadeguata rappresentanza dei paesi in via di sviluppo e

[156] Art 12 Convenzione di Budapest: 1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché le persone giuridiche possano essere ritenute responsabili di un reato in base a questa Convenzione commesso per loro conto da una persona fisica che agisca sia individualmente che come membro di un organo di una persona giuridica che eserciti un potere di direzione al suo interno, nei termini che seguono: a. un potere di rappresentanza della persona giuridica; b. un'autorità per assumere decisioni nel nome della persona giuridica; c. un'autorità per esercitare un controllo all'interno della persona giuridica. 2. In aggiunta ai casi già previsti nel paragrafo 1. di questo articolo, ogni Parte deve adottare le misure necessarie affinché una persona giuridica possa essere ritenuta responsabile se la mancanza di sorveglianza o controllo di una persona fisica di cui al paragrafo 1. ha reso possibile la commissione di reati previsti al paragrafo 1. per conto della persona giuridica da parte di una persona fisica che agisca sotto la sua autorità. 3. Secondo i principi giuridici della Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa. 4.Questa responsabilità è stabilita senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso il reato.

[157] Art 13 Budapest convention: 1.Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché i reati previsti in applicazione degli articoli da 2 a 11 possano essere puniti con sanzioni effettive, proporzionate e dissuasive, che includano la privazione della libertà. 2.Ogni parte deve assicurarsi che le persone giuridiche ritenute responsabili in base all'articolo 12 siano assoggettate a sanzioni penali o non penali effettive, proporzionate e dissuasive o ad altre misure, incluse sanzioni pecuniarie.

l'imposizione di condizioni stringenti, nonostante la ratifica sia aperta anche ai paesi non membri. Altra notazione da fare è che il *cybercrime* è in continua evoluzione, pertanto taluni crimini come il *phishing*, sviluppatosi successivamente alla convenzione, non sono stati previsti.

5.3 La decisione 2005/222/GAI sugli attacchi informatici

La competenza penale dell'Unione europea in materia penale risulta ancora oggi una questione controversa[158], fino all'entrata in vigore del Trattato di Lisbona si riteneva che l'UE non disponesse di competenze e fonti proprie in tale settore. Le fonti vincolanti del diritto comunitario in senso stretto (cd. Primo pilastro: regolamenti e direttive) non apparivano adeguate ad intervenire in un settore così delicato, motivo per cui si è fatto spesso ricorso, nell'ambito del diritto penale sostanziale, allo strumento della decisione quadro[159]. Sono state varie le decisioni che sono intervenute nel corso del tempo e che hanno avuto un ruolo fondamentale nella costruzione di un "Diritto penale dell'informatica". Ai fini della nostra indagine, è necessario soffermarsi sulla decisione 2005/222/GAI sugli attacchi informatici, che ha costituito anche uno dei primi interventi a livello europeo per combattere la criminalità informatica, seppure si tratta di una normativa superata. Il 24 febbraio del 2005, gli Stati membri dell'Unione Europea, firmarono questa Decisione pubblicata nella Gazzetta Ufficiale Comunitaria n. L069, in base alla quale ciascuno Stato assumeva l'impegno di armonizzare la propria normativa in materia penale, introducendo entro il 16 marzo 2007 delle leggi adeguate in tema di sicurezza delle reti e dei sistemi di informazione. Era oramai evidente che l'avvento della tecnologia e di internet e la possibilità di usufruire di programmi all'avanguardia con cui orientarsi nel *cyber-space*, avevano moltiplicato le possibilità di cagionare danni alle reti telematiche dei singoli. Questi problemi destavano ancora maggiore timore, se utilizzati nell'ambito della criminalità organizzata e del terrorismo internazionale. "Solo così, si è stabilito a Bruxelles, è possibile creare i presupposti per realizzare una Società

[158] Per un'analisi dettagliata della tematica: R. SICURELLA, *Il diritto penale dell'Unione Europea dopo Lisbona. Dall' "ossimoro polisenso" al diritto penale di un sistema di ordinamenti integrati. Ancora a metà del guado*., in Archivio Penale n.1, 2021.

[159] Per un'analisi del sistema delle fonti dell'UE ed in particolare dello strumento della decisone, si rinvia a titolo esemplificativo: G. ADINOLFI, Introduzione al diritto dell'Unione Europea, Editori Laterza, Bari, 2019, pp. 150 ss.

dell'Informazione sicura: oggi giorno, infatti, la libera circolazione e la protezione dei dati personali di individui, enti ed imprese costituisce uno degli elementi indispensabili per poter garantire uno spazio di progresso, libertà, sicurezza e giustizia per i popoli dell'Unione Europea[160] ". La decisione ha ripreso i contenuti delle Linee guida sulla sicurezza delle reti approvate dall'O.C.S.E. il 25 luglio del 2002. Si presentava come documento complementare rispetto alla Convenzione di Budapest, come si evinceva esplicitamente dal testo del documento, ma si concentrava solo su talune fattispecie. Infatti, in termini di dimensione, risultava ridotta. Essendo una decisione non ha richiesto la ratifica dei singoli Paesi per la produzione di vincoli giuridici, ma ha creato obblighi in capo agli Stati dell'Unione Europea *ex ante*, sulla base della loro adesione alla Comunità. Gli obiettivi sono stati delineati nel testo della decisione[161]. Il Consiglio auspicava il raggiungimento di quello che era già lo scopo principale delineato nella Convenzione di Budapest: avvicinare quanto più possibile le normative degli stati. Il Consiglio ha prestato, inoltre, particolare attenzione al fenomeno della criminalità organizzata, per la quale dovrebbero essere previste sanzioni più severe e ha mostrato i suoi timori riguardo possibili attacchi terroristici contro i sistemi informatici degli Stati membri. Per quanto attiene alle sanzioni ha preferito evitare un'eccessiva penalizzazione, specialmente per i casi di minore gravità, e ha escluso la penalizzazione degli aventi diritto e delle persone autorizzate. L'articolo 1 definiva i concetti di ‹‹Sistema di informazione››, ‹‹Dati informatici››, ‹‹Persona giuridica›› e l'espressione ‹‹Senza diritto››[162]. L'art. 2 della decisione si occupava delle condotte di "Accesso illecito a sistemi di informazione"[163] e

[160] S. FRATTALONE, *Decisione quadro 2005/222/GAI del consiglio dell'unione europea* in Frattaloneepartnerslawfirm.it

[161] Il testo della decisione 205/222/GAI è reperibile sul sito: eur-lex.europa.eu

[162] Articolo 1 Decisione 2005/222/GAI: Ai fini della presente decisione quadro, si applicano le seguenti definizioni: a)per «sistema di informazione» s'intende qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione; b)per «dati informatici» s'intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata da un sistema di informazione, compreso un programma atto a far svolgere una funzione ad un sistema di informazione; c)per «persona giuridica» s'intende qualsiasi entità che abbia tale qualifica ai sensi della legislazione applicabile, eccetto gli Stati o altri organismi pubblici nell'esercizio dell'autorità statale e le organizzazioni internazionali; d) l'espressione «senza diritto» significa l'accesso o l'interferenza non autorizzati da parte di chi ha il diritto di proprietà o altro diritto sul sistema o una sua parte, ovvero non consentiti ai sensi della legislazione nazionale.

[163] Articolo 2 Decisione 2005/222/GAI: 1. Ciascuno Stato membro adotta le misure necessarie affinché l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso sia punito

gli artt. 3[164]e 4[165] delle "interferenze illecite" sui sistemi informatici e sui "dati". Notiamo, pertanto, come la presente decisione è intervenuta su quelle fattispecie, di cui si era occupata la Convenzione di Budapest. Quello realizzato nel 2005 ha costituito un altro importante tassello nella materia oggetto della nostra analisi. Infine, anche in tale occasione non è mancato l'intervento in materia responsabilità delle persone giuridiche (Art. 8 Decisione 2005/222/GAI [166]), su cui avremo modo di soffermarci nel proseguimento della nostra indagine.

5.4 La direttiva 2013/40/UE

L'entrata in vigore nel 2009 del Trattato di Lisbona, composto dal Trattato sull'unione europea e dal Trattato sul funzionamento dell'Unione europea, ha introdotto novità significative. Esso ha ampliato i poteri del Parlamento europeo e ha di conseguenza inciso nel ruolo dell'Unione Europea nell'ambito del diritto penale. Come abbiamo accennato all'inizio del precedente paragrafo, l'UE si è servita in passato delle decisioni- quadro per intervenire e gran parte di queste sono state, successivamente, sostituite con le direttive.

---

come reato, almeno per i casi gravi. 2. Ciascuno Stato membro può decidere che i comportamenti di cui al paragrafo 1 siano punibili solo quando il reato è commesso violando una misura di sicurezza.

[164] Art.3 Decisione 2005/222/GAI: Ciascuno Stato membro adotta le misure necessarie affinché l'atto intenzionale di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili sia punito come reato se commesso senza diritto, almeno per i casi gravi.

[165] Art.4 Decisione 2005/222/GAI: Ciascuno Stato membro adotta le misure necessarie affinché l'atto intenzionale di cancellare, danneggiare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione sia punito come reato se commesso senza diritto, almeno per i casi gravi.

[166] Art 8 Decisione 2005/222/GAI: 1. Ciascuno Stato membro adotta le misure necessarie affinché le persone giuridiche possano essere ritenute responsabili dei reati di cui agli articoli 2, 3, 4 e 5 commessi a loro beneficio da qualsiasi soggetto, che agisca a titolo individuale o in quanto membro di un organo della persona giuridica, il quale detenga una posizione preminente in seno alla persona giuridica stessa, basata: a) sul potere di rappresentanza di detta persona giuridica; o b) sul potere di prendere decisioni per conto della persona giuridica; o c) sull'esercizio di poteri di controllo in seno a tale persona giuridica.
2. Oltre che nei casi di cui al paragrafo 1, gli Stati membri assicurano che le persone giuridiche possano essere ritenute responsabili qualora la mancata sorveglianza o il mancato controllo da parte di uno dei soggetti di cui al paragrafo 1 abbia reso possibile la commissione dei reati di cui agli articoli 2, 3, 4, e 5 a beneficio della persona giuridica da parte di una persona soggetta alla sua autorità.
3. La responsabilità delle persone giuridiche ai sensi dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali contro le persone fisiche che siano autori, istigatori o complici di uno dei comportamenti di cui agli articoli 2, 3, 4 e 5.

È ciò che accaduto alla decisione 2005/222/GAI sostituita con la direttiva 2013/40/UE[167]. Tale strumento mira ad avvicinare il diritto penale degli Stati membri e favorisce la cooperazione tra le autorità giudiziarie e di polizia. Ai sensi dell'art 83 del TFUE, l'Unione europea ha facoltà di stabilire, attraverso le direttive, norme minime relative alla definizione dei reati e delle sanzioni, in sfere della criminalità particolarmente gravi tra cui l'informatica. L'intervento della direttiva del 2013 si fonda sulla considerazione che il buon funzionamento e la sicurezza dei sistemi di informazione siano fondamentali per lo sviluppo del mercato interno e di un'economia competitiva e innovativa; tuttavia, minime sono le differenze riscontrabili tra la decisione quadro analizzata e la direttiva sostitutiva. Ci soffermeremo sulle novità che possono essere d'interesse ai fini della nostra analisi. L'art. 3 della direttiva si occupa della fattispecie di accesso abusivo a un sistema informatico. Il legislatore europeo è intervenuto, affermando la punibilità della condotta solo quando realizzata in violazione di una misura di sicurezza. Tuttavia, questa scelta di limitare la punibilità alle condotte più ostinate e aggressive non impedisce agli Stati di adottare un più alto *standard* di protezione dei sistemi informatici, considerando abusivo anche l'accesso che non violi alcuna misura di sicurezza. Le principali novità attengono all'introduzione degli artt. 6 "Intercettazione illecita"[168] e 7 "Strumenti utilizzati per commettere reati"[169] della direttiva, anche se per il legislatore italiano non rappresentano una novità. La direttiva fa un generico riferimento agli "strumenti" utilizzabili per commettere i reati da essa previsti, ma solo per tenere conto delle varie modalità con cui possono essere effettuati gli attacchi a causa della continua evoluzione degli *hardware* e dei *software*. "Pertanto, si richiede la verifica dell'intenzione di impiegarli al fine di commettere uno dei reati elencati proprio per evitare di criminalizzare

[167] Il testo della direttiva è disponibile sul sito: eur-lex.europa.eu

[168] Art 6 direttiva 2013/40/UE: Gli Stati membri adottano le misure necessarie affinché l'intercettazione, tramite strumenti tecnici, di trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche da un sistema di informazione che trasmette tali dati informatici, compiuta intenzionalmente e senza diritto, sia punibile come reato, almeno per i casi che non sono di minore gravità.

[169] Art 7 direttiva 2013/40/UE: Gli Stati membri adottano le misure necessarie affinché la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo intenzionali di uno dei seguenti strumenti, compiuti senza diritto e con l'intenzione di utilizzarli al fine di commettere uno dei reati di cui agli articoli da 3 a 6, siano punibili come reato, almeno per i casi che non sono di minore gravità: a) un programma per computer, destinato o modificato principalmente al fine di commettere uno dei reati di cui agli articoli da 3 a 6; b) una password di un computer, un codice d'accesso, o dati simili che permettono di accedere in tutto o in parte a un sistema di informazione.

la mera detenzione di strumenti solo potenzialmente idonei all'attacco informatico, laddove siano prodotti e commercializzati per scopi legittimi, come la verifica dell'affidabilità dei prodotti di tecnologia dell'informazione o la sicurezza dei sistemi di informazione[170]." Altra novità riguarda la punibilità a titolo di tentativo della sola fattispecie di "Interferenze illecite" e l'introduzione di alcune cause di non punibilità e circostanze aggravanti, nell'ottica di evitare la criminalizzazione per le ipotesi di minore gravità[171]. In conclusione, osserviamo come, limitatamente alle fattispecie considerate, le novità non appaiono rilevanti. La direttiva costituisce un tassello fondamentale nella lotta alla criminalità informatica, che non può prescindere dai numerosi sforzi a livello transnazionale, per le sue peculiari caratteristiche e modalità di attuazione. Come nota R.Flor "Appare evidente che, a livello europeo, i sistemi di informazione sono considerati un elemento chiave dell'interazione politica, sociale ed economica dell'Unione, nonché fondamentali per lo sviluppo del mercato interno e di un'economia competitiva e innovativa, proprio in quanto la società odierna è fortemente dipendente dalla tecnologia[172]." Risulta interessante, a tal proposito, prestare attenzione alla Relazione della Commissione al Parlamento europeo e al Consiglio del 13.9.2017, la quale valuta le misure adottate dagli Stati membri per conformarsi alla Dir. 2013/40/UE. La Relazione si apre con il riferimento alla valutazione della minaccia della criminalità organizzata su *Internet* (IOCTA 2016) svolta dall'Europol. Tra le gravi forme di attacchi menzionate si configurano l'uso di *softwares* maligni e dell'ingegneria sociale per infiltrarsi in un sistema di informazione e acquisirne il controllo o per intercettare le comunicazioni, ovvero attacchi alla rete su vasta scala, anche ai danni di infrastrutture critiche. La relazione evidenzia i progressi che la direttiva ha determinato nell'ambito della lotta agli attacchi informatici, facilitando la cooperazione transfrontaliera fra le autorità competenti. La Commissione riconosce, inoltre, gli sforzi compiuti dagli Stati membri per dare attuazione alla direttiva, tuttavia, anche se non ritiene necessario proporre modifiche, evidenzia nuovi possibili margini di intervento. Alcuni miglioramenti che gli Stati membri dovrebbero realizzare riguardano, *in primis*, l'uso delle definizioni (art. 2),

[170] S. CIVELLO CONIGLIARO, "*La tutela penale europea dei sistemi di informazione*" in Diritto penale contemporaneo

[171]Per un'analisi dettagliata delle altre novità introdotte dalla direttiva 2013/40/UE si rinvia a:S. CIVELLO CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione*, cit.

[172] R.Flor, "La Cybercriminality: le fonti internazionali ed europee" in OMNIA: Cybercrime diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, UTET, Milano, 2019, pp. 121.

che incide sull'entità dei reati definiti nel diritto nazionale; in secondo luogo, sono stati rilevati problemi nella formulazione dei reati di cui agli artt. 3-7 e 9. Altre problematiche sembrano riguardare l'attuazione delle disposizioni amministrative riguardanti i canali di comunicazione idonei (art. 13, par. 3) e il monitoraggio e le statistiche sui reati contemplati dalla direttiva (art. 14). La Commissione ha affermato di essere pronta a fornire sostegno agli Stati membri ai fini dell'attuazione della direttiva, rafforzando, se necessario, anche le disposizioni operative sullo scambio di informazioni (art. 13, par. 1 e 2), sui canali di comunicazione (art. 13, par. 3) e sul monitoraggio e sulle statistiche (art. 14).

6. Gli interventi in materia di *cybersecurity* per un'Unione europea più resiliente

6.1 La direttiva NIS

La questione legata alla *cybersecurity* è di estrema rilevanza ed è strettamente legata al tema dei reati informatici e del rapporto tra sicurezza e riservatezza di cui ci occupiamo. Ad oggi è sufficiente un minimo di conoscenza informatica per poter compiere attacchi ed essere pressoché invisibile. In tale contesto, il ruolo delle istituzioni è imprescindibile per poter garantire adeguati livelli di sicurezza. Infatti, due chiavi necessarie per combattere il fenomeno degli attacch1i informatici su internet sono: la cooperazione tra gli stati e la rapidità nell'azione. Il mondo digitale consente di espandere il concetto di territorialità e fisicità dei beni e dei documenti riuscendo a smaterializzarli. In particolare, il dato può essere attaccato anche simultaneamente da più aggressori. Per questa fragilità, la protezione dei dati rappresenta un'imponente sfida per aziende, enti pubblici e privati cittadini. Al fine di rafforzare le strategie sulla *cybersecurity*, il Parlamento europeo ha approvato la risoluzione del 12 settembre 2013 "sulla strategia dell'Unione europea per la *cybersecurity*: un ciberspazio aperto e sicuro", contenente un invito rivolto a tutti gli Stati membri ad adottare specifiche normative nazionali al fine di prevenire e rispondere agli attacchi che colpiscono i sistemi di telecomunicazione in Europa. "Con un approccio *top down*, l'Unione ricorda come un alto livello di sicurezza informatica sia necessario, non solo per mantenere i servizi essenziali e per il funzionamento della società e

dell'economia, ma anche per salvaguardare l'integrità fisica dei cittadini"[173]. Uno degli elementi di questa strategia è la Direttiva 2016/1148 del Parlamento Europeo e del Consiglio, nota come Direttiva Nis. Lo studio di questo documento risulta indispensabile nella nostra analisi, in quanto rappresenta il primo insieme di regole sulla sicurezza informatica univoco a livello dell'Unione Europea. Questo documento si inserisce perfettamente nella tematica da noi affrontata circa il rapporto tra sicurezza e riservatezza. Del resto, qualche paragrafo fa, abbiamo risolto il binomio costituito da riservatezza e sicurezza nel senso*: privacy* è sicurezza. E questo documento come del resto gli altri che andremo ad analizzare ne sono la perfetta dimostrazione. Una normativa che regoli sapientemente gli *standard* di sicurezza, specie con riguardo al mondo dei dati e al *cyberspace*, tenendo conto del corretto bilanciamento tra i diritti in gioco, è un elemento fondamentale per garantire la riservatezza degli individui. All'interno della direttiva, in particolare, viene sottolineato il ruolo vitale svolto da reti, sistemi e servizi informativi all'interno della società. Strumenti che è necessario siano affidabili e sicuri per lo svolgimento delle attività economiche. Tuttavia, vengono rilevate anche le carenze nell'attuale sistema di sicurezza e la necessità di cooperazione tra gli stati. "Le capacità esistenti non bastano a garantire un livello elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. I livelli di preparazione negli Stati membri sono molto diversi tra loro, il che ha comportato una frammentazione degli approcci nell'Unione. Ne deriva un livello disomogeneo di protezione dei consumatori e delle imprese che compromette il livello globale di sicurezza delle reti e dei sistemi informativi nell'Unione. La mancanza di obblighi comuni imposti agli operatori di servizi essenziali e ai fornitori di servizi digitali rende inoltre impossibile la creazione di un meccanismo globale ed efficace di cooperazione a livello dell'Unione"[174]. Questo ci permette di introdurre un altro profilo alla luce del quale osservare il rapporto tra sicurezza e riservatezza. Ci discostiamo dall'individuo per rivolgere la nostra attenzione agli enti. Anche questi ultimi si sono dovuti adattare al continuo evolversi delle tecnologie e hanno dovuto imparare da un lato a proteggersi dagli attacchi informatici e dall'altro ad adottare efficaci modelli organizzi per evitare di incorrere in responsabilità da reato. Adesso sono chiamati a fare la loro parte al fine di garantire uno spazio virtuale sicuro. La direttiva Nis, infatti, rappresenta

[173] R. Brighi e P. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea* in federalismi.it, 8 settembre 2021
[174] Il testo della direttiva è reperibile nella Gazzetta ufficiale dell'Unione europea.

un elemento cardine nella lotta contro la *cybercriminalità* che impone a tutti gli Stati membri dell'UE, alle aziende *Internet* e agli operatori di infrastrutture principali di garantire un ambiente digitale sicuro e affidabile. In particolare, essa si rivolge agli operatori di servizi essenziali (OES) stabiliti nell'Unione europea[175] e ai *digital service providers* (DPS).[176] "Un concetto importante che traspare in tutta la direttiva è quello della fiducia che è alla base delle transazioni commerciali ed anche degli scambi di informazioni e di dati per finalità connesse, ma anche non connesse, né direttamente né indirettamente con il commercio o con il profitto in generale, specialmente se eseguite a distanza."[177]

L'ambito della direttiva è delineato all'art.1. In particolare, il secondo comma dell'art.1 afferma che la presente direttiva: a) fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; b) istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi; c) crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace; d) stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali; e) fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.

L'art. 4 individua alcune importanti definizioni. In particolare, per "sicurezza delle rete e dei sistemi informativi" si intende la capacità di una rete e dei sistemi informativi di resistere a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi. Per "incidente" si intende: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi.

[175] Si tratta dei soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali;

[176] Si tratta delle persone giuridiche che forniscono servizi della società dell'informazione, delle persone giuridiche che forniscono servizi di *e-commerce, cloud computing* o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.

[177] A. Contaldo e D. Mula, *Cybersecurity law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pacini Giuridica, Pisa, 2020, pag. 44.

Per “rischio” si intende: ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi.

La strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi affronta in particolare i seguenti aspetti: 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. Ciascuno stato dovrà individuare una o più autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi e designare uno o più CSIRT. Il CSIRT (*Computer security incident response team*) è la struttura che ha la responsabilità di monitorare, intercettare, analizzare e rispondere alle minacce. Viene, inoltre, istituita una rete di CSIRT, composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE. La cooperazione rappresenta uno dei punti focali della direttiva.

Per tale motivo è stato istituito un gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione e dell’ENISA (*European Union for Network and Information Security Agency*), che faciliti i rapporti tra gli stati e aumenti la fiducia. Le quattro aree di lavoro del gruppo saranno: pianificazione, guida, segnalazione e condivisione. Ogni Stato membro designa un punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi («punto di contatto unico»). Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri con le autorità competenti negli altri Stati membri e con il gruppo di cooperazione di cui all'articolo 11 e la rete di CSIRT di cui all'articolo 12. Gli Stati membri provvedono affinché gli operatori di servizi essenziali si dotino di misure di sicurezza appropriate e notifichino senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi

essenziali prestati. Le notifiche includono le informazioni che consentono all'autorità competente o al CSIRT di determinare qualsiasi impatto transfrontaliero dell'incidente. L'obbligo di segnalazione mira a garantire lo scambio di informazioni tra il settore privato e quello pubblico[178]. Anche i fornitori di servizi digitali saranno tenuti ad attuare misure di sicurezza appropriate e notificare gli incidenti, ma la direttiva prevede alcuni elementi di specificità, come ad esempio la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio e i *test* e la conformità a norme internazionali. "Come si può intuire, la condivisione delle informazioni ha un'importanza strategica, preventiva e di gestione degli incidenti, dove la Direttiva ha inserito punti di obbligatorietà nei processi, anche se la trattativa tra i vari paesi membri ha portato verso un approccio più volontario di adesione: per gli operatori di servizi essenziali, gli ambiti obbligatori sono sicurezza e notifica; per i fornitori di servizi digitali si richiede di avere un approccio strutturato sulla sicurezza di sistemi della gestione degli incidenti, sulla continuità operativa e sulla gestione del rischio."[179]

Gli Stati membri dovranno definire sanzioni penali effettive, proporzionate e dissuasive. La scelta di disciplinare il settore con una direttiva è stata determinata dalla volontà di attuare una base comune per gli Stati membri, senza ingerenze nella sovranità di ciascuno Stato. Alcune criticità nell'attuazione della direttiva sono: la risposta ai gli attacchi informatici, la condotta degli OTT[180] e la difficoltà di ottenere informazioni rapide e complete. A questi problemi l'Unione ha cercato di porre soluzione, individuando un rappresentante, ovvero "la persona fisica o giuridica stabilita nell'Unione, espressamente designata ad agire per conto di un fornitore di servizi che non è stabilito nell'Unione a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del fornitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo." È facile prevedere che tale atto possa avere delle ricadute nella costituzione de Modello organizzativo 231 in materia di prevenzione dei reati informatici, poiché uno degli obiettivi della direttiva è individuare le potenziali aree di rischio. Di tali informazioni gli enti potrebbero servirsene al fine della

[178] Tale obbligo ricade su operatori di servizi essenziali e fornitori di servizi digitali come operatori di infrastrutture critiche in settori quali servizi finanziari, trasporti, energia e assistenza sanitaria, società di servizi IT, inclusi negozi online di applicazioni, piattaforme del commercio elettronico, portali di pagamento su Internet, piattaforme di cloud computing, motori di ricerca e reti sociali, pubbliche amministrazioni…

[179] A. Contaldo e D. Mula, Cybersecurity…, cit., pag.47.

[180] Per OTT si intendono gli *Over The Top* (Google, Facebook, Yahoo, Microsoft).

redazione del Modello dato che una delle fasi principiali è proprio il riconoscimento delle aeree all'interno della struttura aziendale sensibili ad eventuali attacchi informatici. Inoltre, la direttiva mira a individuare programmi di formazione, che sappiamo essere fondamentali per dimostrare l'efficacia del Modello 231. Infine, non possiamo sottovalutare il rapporto tra pubblico e privato che qui viene messo in evidenza e che potrebbe avere un ruolo nell'accertamento della responsabilità degli enti.

6.2 Il *Cybersecurity act*

Il *Cybersecurity Act* (Regolamento UE 2019/881)[181] fa parte del progetto di un'Unione Europea più resiliente alle minacce cibernetiche e rientra tra le proposte della Commissione al fine di colmare le lacune già esistenti e rafforzare la strategia del 2013. L'obiettivo è quello di uniformare la disciplina della *cybersecurity* a livello comunitario. Nel testo viene sottolineata l'importanza delle reti e dei sistemi informativi e le carenze a livello europeo. "Sebbene un numero crescente di dispositivi sia connesso a *Internet,* la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza." Il nucleo centrale della questione è che mentre gli attacchi informatici vengono realizzati attraverso le frontiere, le competenze in materia di cibersicurezza sono prevalentemente nazionali. Occorre pertanto attuare una risposta coordinata tra tutti gli stati membri. Il regolamento è entrato in vigore il 27 giugno del 2019 ed ha sostituito il precedente Regolamento del PE e del Consiglio 2013/526. Gli obiettivi principale sono: 1) la creazione di un sistema europeo certificativo della sicurezza informatica; 2) il consolidamento del ruolo dell'ENISA. L'art. 2 del regolamento contiene una serie di definizioni. La *cyber-security* viene definita come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[182]. Si tratta di una nozione più ampia delle precedenti che ricomprende un ampio perimetro di rischi. Nella prima parte del documento viene specificato e potenziato il ruolo dell'ENISA. L'ENISA, che ricopriva un ruolo di mera consulenza tecnica nei confronti degli Stati membri in caso di attacchi o incidenti informatici, adesso assume un ruolo operativo nella gestione di tali minacce. In questo modo la risposta agli attacchi informatici, che era un tempo

[181] Il testo del regolamento UE 2019/881 è reperibile sul sito eur-lex.europa.eu
[182] Il testo del regolamento è reperibile sul sito eur-lex.europa.eu

competenza degli Stati Membri, viene coordinata e supportata a livello sovranazionale. "L'ENISA svolge i compiti che le sono attribuiti ai sensi del presente regolamento allo scopo di conseguire un elevato livello comune di cibersicurezza in tutta l'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione nel miglioramento della cibersicurezza. L'ENISA funge da punto di riferimento per pareri e competenze in materia di cibersicurezza per le istituzioni, gli organi e gli organismi dell'Unione nonché per altri portatori di interessi pertinenti dell'Unione."[183] Gli obiettivi dell'ENISA vengono fissati nell'art.4: "1.L'ENISA opera come centro di competenze nel campo della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite, alle informazioni che mette a disposizione, alla trasparenza delle procedure, ai metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti. 2. L'ENISA assiste le istituzioni, gli organi e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche dell'Unione relative alla cibersicurezza, ivi comprese le politiche settoriali in materia di cibersicurezza. 3. L'ENISA sostiene lo sviluppo delle capacità e la preparazione nell'Unione, assistendo le istituzioni, gli organi e gli organismi dell'Unione, nonché gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo e nel miglioramento delle capacità di ciberresilienza e di risposta, nonché nello sviluppo di abilità e competenze nel campo della cibersicurezza. 4. L'ENISA promuove la cooperazione, inclusa la condivisione di informazioni, e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i portatori di interessi del settore pubblico e privato su questioni relative alla cibersicurezza. 5. L'ENISA contribuisce a rafforzare le capacità di cibersicurezza a livello di Unione per sostenere le azioni degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri. 6. L'ENISA promuove l'uso della certificazione europea della cibersicurezza, con l'obiettivo di evitare la frammentazione del mercato interno. L'ENISA contribuisce all'istituzione e al mantenimento di un apposito quadro europeo di certificazione della cibersicurezza, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dei prodotti TIC, dei servizi TIC e dei

[183] Art 3, comma 1, *Cyber-Act*.

processi TIC in termini di cibersicurezza, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività. 7. L'ENISA promuove un elevato livello di consapevolezza in materia di cibersicurezza, incluse l'igiene informatica e l'alfabetizzazione informatica, tra cittadini, organizzazioni e imprese". Come possiamo osservare vengono delineati in maniera specifica gli obiettivi affidati all'istituto, il quale fungerà da principale punto di riferimento in materia di *cybersecurity* e certificazione europea della sicurezza informatica. Accanto agli obiettivi, il documento fissa i compiti dell'ENISA all'art 5. Sono inoltre previste una serie di disposizioni che riguardano il ruolo di questo istituto nell'ambito della cooperazione a livello dell'Unione[184]. Per quanto attiene al sistema di certificazione UE, l'ENISA ha i seguenti compiti: 1) monitora gli sviluppi nei settori di normazione connessi e raccomanda adeguate specifiche tecniche ai fini dello sviluppo di sistemi europei di certificazione della cibersicurezza; 2) prepara proposte di sistemi europei di certificazione della cibersicurezza per prodotti TIC, servizi TIC e processi TIC conformemente all'articolo 49; 3) valuta i sistemi europei di certificazione della cibersicurezza adottati; 4) partecipa a valutazioni *inter pares* a norma dell'articolo 59, paragrafo 4; 5) assiste la Commissione nel provvedere alle funzioni di segretariato dell'ECCG a norma dell'articolo 62, paragrafo 5; 6) elabora e pubblica orientamenti e sviluppa buone pratiche in merito ai requisiti di cibersicurezza per i prodotti TIC, i servizi TIC e i processi TIC, in cooperazione con le autorità nazionali di certificazione della cibersicurezza e con il settore in modo formale, strutturato e trasparente; 7) contribuisce a uno sviluppo delle capacità relative ai processi di valutazione e certificazione mediante l'elaborazione e la pubblicazione di orientamenti, nonché fornendo sostegno agli Stati membri, su loro richiesta; 8) facilita la definizione e l'adozione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC; 9) redige, in collaborazione con gli Stati membri e con il settore, pareri e orientamenti riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali, nonché riguardanti le norme già esistenti, comprese le norme nazionali degli Stati membri, ai sensi dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;10) L'ENISA effettua regolarmente, diffondendone poi i risultati, analisi delle principali tendenze del mercato della cibersicurezza sul versante sia della domanda che dell'offerta,

[184] Art. 7 del *Cyber-act*.

al fine di promuovere tale mercato nell'Unione[185]. Il regolamento dedica, successivamente, una serie di articoli alla composizione dell'ENISA, su cui in questa sede non ci soffermiamo. Nella seconda parte, il Regolamento introduce la creazione di un quadro comune europeo per la certificazione della sicurezza informatica dei prodotti ICT e dei servizi digitali, con l'obiettivo di facilitarne lo scambio nella UE e di aumentare la fiducia dei consumatori. "Il quadro europeo di certificazione della cibersicurezza prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC valutati nel loro ambito siano conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita"[186]. Si evince, ancora una volta, da tale passaggio come la cibersicurezza sia strettamente connessa alla tutela dei dati e rafforzare la prima significa proteggere l'altra. Gli obiettivi di sicurezza dei sistemi di certificazione sono i seguenti: 1) proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC; 2) proteggere i dati conservati, trasmessi o altrimenti trattati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità durante l'intero ciclo di vita del prodotto TIC, del servizio TIC o del processo TIC; 3) le persone, i programmi o le macchine autorizzati devono poter accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso; 4) individuare e documentare le dipendenze e vulnerabilità note; 7.6.2019 Gazzetta ufficiale dell'Unione europea L 151/55 IT; 5) registrare a quali dati, servizi o funzioni è stato effettuato l'accesso e quali sono stati utilizzati o altrimenti trattati, in quale momento e da chi; 6) fare in modo che si possa verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso, che sono stati utilizzati o altrimenti trattati, in quale momento e da chi; 7) verificare che i prodotti TIC, i servizi TIC e i processi TIC non contengano vulnerabilità note; 8) ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico; 9) i prodotti TIC, i servizi TIC e i processi TIC

[185] Art.8 del *Cyber-act.*
[186] Art. 46, comma 2 del *Cyber-act*.

devono essere sicuri fin dalla progettazione e per impostazione predefinita; 10) il *software* e l'*hardware* dei prodotti TIC, dei servizi TIC e dei processi TIC devono essere aggiornati, non contenere vulnerabilità pubblicamente note e devono disporre di meccanismi per effettuare aggiornamenti protetti.[187] Il sistema individua tre livelli di affidabilità: "di base", "sostanziale" e "elevato". Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC o processo TIC, in termini di probabilità e impatto di un incidente. Il certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «di base» assicura che i prodotti TIC, i servizi TIC e i processi TIC rispettino i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e siano stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Il certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «sostanziale» assicura che i prodotti TIC, servizi TIC e processi TIC per i quali è rilasciato tale certificato, rispettino i corrispondenti requisiti di sicurezza e siano stati valutati a un livello inteso a ridurre al minimo i rischi connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici, causati da soggetti dotati di abilità e risorse limitate. Il certificato europeo di cibersicurezza che si riferisca al livello di affidabilità «elevato» assicura che i prodotti TIC, i servizi TIC e i processi TIC per i quali è rilasciato tale certificato rispettino i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e siano stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Il legislatore consente autovalutazioni della conformità per i prodotti TIC, servizi TIC e processi TIC che presentano un basso rischio corrispondenti al livello di affidabilità "di base". La certificazione della cibersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o degli Stati membri. La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza. L'art. 58, comma 1, prevede che ciascuno stato membro designi una o più autorità nazionali di certificazione della cibersicurezza nel suo territorio. Il comma 7 elenca, inoltre, gli obblighi specifici e i poteri delle autorità nazionali di certificazione. Al fine di ottenere norme equivalenti in tutta l'Unione relativamente ai certificati europei

[187] Art 51 del *Cyber-act*.

di cibersicurezza e alle dichiarazioni UE di conformità, le autorità nazionali di certificazione della cibersicurezza sono soggette a una valutazione *inter pares* e sono sottoposte ad una serie di obblighi di notifica alla Commissione europea. L'art. 62 istituisce il Gruppo per la certificazione della *cybersecurity*, il quale ha i seguenti compiti: 1) consigliare e coadiuvare la Commissione nelle sue attività volte a garantire un'attuazione e un'applicazione coerente delle disposizioni; 2) assistere, consigliare e collaborare con l'ENISA in relazione alla preparazione di una proposta di sistema ai sensi dell'articolo 49; 3) adottare un parere sulle proposte di sistemi preparate dall'ENISA ai sensi dell'articolo 49; 4) chiedere all'ENISA di preparare proposte di sistemi ai sensi dell'articolo 48, paragrafo 2; 5) adottare pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza; 6) esaminare gli sviluppi che presentano un interesse in materia di certificazione della cibersicurezza e scambio di informazioni e buone pratiche sui sistemi europei di certificazione della cibersicurezza; 7) agevolare la cooperazione tra le autorità nazionali di certificazione della cibersicurezza di cui al presente titolo attraverso lo sviluppo della capacità e lo scambio di informazioni; h) sostenere l'attuazione dei meccanismi di valutazione *inter pares* in conformità delle regole fissate da un sistema europeo di certificazione della cibersicurezza; 8) agevolare l'allineamento dei sistemi europei di certificazione della cibersicurezza alle norme riconosciute a livello internazionale, rivedendo i sistemi europei di certificazione della cibersicurezza esistenti e, ove opportuno, rivolgendo raccomandazioni all'ENISA affinché collabori con le pertinenti organizzazioni internazionali di normazione per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello internazionale. Infine, è di competenza degli Stati l'applicazione di sanzioni effettive, proporzionate e dissuasive. Anche questo documento può essere messo in relazione con la responsabilità da reato degli enti, infatti l'introduzione del sistema di certificazione europeo può avere un'importante ricaduta nella redazione del MOG. Facciamo sempre riferimento all'utilizzazione della *cybersecurity* al fine di prevenire quei reati informatici a cui abbiamo fatto cenno in virtù delle normative sovranazionali ma che avremo modo in seguito di approfondire. "Le organizzazioni, i fabbricanti o i fornitori coinvolti nella progettazione e nello sviluppo di prodotti TIC, servizi TIC e processi TIC dovrebbero essere incoraggiati ad attuare misure nelle prime fasi di progettazione e sviluppo per tutelare il più possibile sin dall'inizio la

sicurezza di tali prodotti, servizi e processi, in modo che si presuma il verificarsi di attacchi informatici e se ne anticipi e riduca al minimo l'impatto («sicurezza fin dalla progettazione»). La sicurezza dovrebbe essere assicurata in tutto il ciclo di vita del prodotto TIC, servizio TIC o processo TIC, con un'evoluzione costante dei processi di progettazione e sviluppo al fine di ridurre il rischio di danni derivanti da un utilizzo doloso"[188]. Il possesso di prodotti e servizi TIC certificati, costituirebbe una garanzia di affidabilità dei sistemi informatici presenti all'interno della struttura di cui si potrebbe tener conto in sede giudiziale. Inoltre, la possibilità di conservare i dati e tenere traccia degli eventuali accessi consentirebbe di individuare l'autore del reato ed escludere la responsabilità da reato degli enti. Del resto all'interno del Regolamento leggiamo "la cibersicurezza non costituisce soltanto una questione relativa alla tecnologia, ma anche una in cui il comportamento umano è di pari importanza. Di conseguenza, è opportuno promuovere energicamente l'«igiene informatica», vale a dire semplici misure di routine che, se attuate e svolte regolarmente da cittadini, organizzazioni e imprese, riducono al minimo la loro esposizione a rischi derivanti da minacce informatiche"[189]. Occorre inoltre sottolineare che l'ENISA oggi fornisce importanti strumenti alle imprese, consultabili anche sul loro sito www.enisa.europa.eu, che potrebbero sicuramente aiutare le imprese ad orientarsi nella prevenzione dei reati informatici, seppure non nascondiamo i timori della crescente potenza di questo istituto.

6.3 La strategia europea per il decennio digitale

Il 16 dicembre 2020, la Commissione Europea e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato la nuova Strategia Europea sulla *Cybersecurity*[190]. Questo documento costituisce un elemento coerente e integrato con il piano europeo di transizione digitale, il *Recovery Plan* e la Strategia Europea sulla Sicurezza di luglio 2020. La pandemia ha portato a cambiamenti degni di nota all'interno della società. Si calcola che il 40 % dei lavoratori all'interno dell'Unione è passato al telelavoro e anche il panorama industriale dell'UE è sempre più digitalizzato e connesso.

[188] Cyberact, par. 12
[189] Cyberact par. 8
[190] Il testo della strategia dell'UE in materia di cibersicurezza per il decennio digitale è reperibile sul sito eur-lex.europa.eu

Questo ha sicuramente incrementato la vulnerabilità agli attacchi informatici. I dati in materia di cybercriminalità sono molto preoccupanti. Circa i due quinti degli utenti UE hanno sperimentato problemi riguardanti la sicurezza[191] e un'impresa su otto è stata oggetto di attacchi informatici[192]. "Migliorare la cibersicurezza è pertanto di fondamentale importanza affinché le persone possano fidarsi, fare uso e beneficiare delle innovazioni, della connettività e dell'automazione, come pure per salvaguardare i diritti e le libertà fondamentali, compresi i diritti alla riservatezza e alla protezione dei dati personali nonché la libertà di espressione e di informazione[193]". La Commissione ha fissato come obiettivo la prevenzione, resilienza e capacità di risposta agli incidenti di enti pubblici e privati, delle autorità competenti e dell'Unione nel suo complesso. Questo ambizioso progetto ha dato luogo a due proposte legislative: la revisione della direttiva NIS, NIS 2.0 e una nuova Direttiva sulla resilienza delle Entità critiche. All'interno della strategia del 2020 il concetto di *cybersecurity* viene inteso da un lato come bene meritevole di tutela in sé e dall'altro come bene strumentale per la tutela e il godimento di diritti fondamentali. Da un lato si sottolinea la necessità della robustezza dei sistemi per creare fiducia o fare affidamento nell'ambiente digitale. Dall'altro lato, la *cyber-security* è lo strumento per garantire e promuovere diritti e libertà fondamentali, quali il diritto alla *privacy* e alla protezione dei dati personali, la libertà di espressione e di informazione. Le tre aree in cui la strategia interviene sono le seguenti: 1) resilienza, sovranità tecnologica e *leadership*; 2) Sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta; 3) Promozione di un ciberspazio globale e aperto. Nell'ambito della prima area di azione, l'obiettivo è quello della redistribuzione della responsabilità e della collaborazione tra pubblico e privato. Interessante è la proposta di una certificazione a norma del *Cyber Security Act* e lo sviluppo di uno *standard* europeo per la conformità alla *cyber-security* dei prodotti. Nelle intenzioni del legislatore europeo, l'istituzione di un sistema comune di certificazione dovrebbe favorire la cosiddetta "*security by design*", ovvero la presa in considerazione della sicurezza informatica fin dagli stadi iniziali della progettazione dei prodotti ICT, inclusi quei dispositivi di consumo connessi alla rete che costituiscono il cosiddetto "internet delle

[191] Indice di digitalizzazione dell'economia e della società 2020.
[192] Conferenza stampa di Eurostat, "*ICT security measures taken by vast majority of enterprises in the EU*", 6/2020 - 13 gennaio 2020.
[193] La strategia dell'UE in materia di cibersicurezza per il decennio digitale, cit., pag.4

cose" o "IoT". Il possesso di tali certificazioni consentirebbe alle imprese di aumentare la propria affidabilità all'interno del mercato europeo. Inoltre, la Commissione propone di creare una rete di centri operativi di sicurezza al fine di sostenere il miglioramento di quelli esistenti. Facciamo riferimento agli ISAC (condivisione e analisi delle informazioni), SOC (centri operativi di sicurezza) e i CSIRT. Questa rete costituirebbe un vero e proprio scudo di cibersicurezza per l'UE. Nell'ambito della seconda area di azione, la *Joint Cyber Unit* (unità congiunta per il *cyberspace*) sarebbe il primo strumento per la cooperazione tra le diverse comunità (civili, diplomatiche, delle forze dell'ordine, della difesa) europee di *cybersecurity*. Tale unità colmerebbe una ulteriore lacuna nella *governance* delle crisi informatiche a livello tecnico e operazionale e dovrebbe consentire agli Stati membri e alle istituzioni, agli organismi, alle agenzie dell'UE di utilizzare appieno le strutture, le risorse e le capacità esistenti, nonché promuovere il principio della necessità di condividere. Essa fornirebbe l'opportunità di rinforzare ulteriormente la cooperazione riguardo all'architettura del programma e di sfruttare i progressi compiuti. Gli obiettivi all'interno di questa terza area sono i seguenti: 1) Contrastare la criminalità informatica; 2) Un pacchetto di strumenti della diplomazia informatica dell'UE, tra cui figura l'istituzione di un gruppo di lavoro di *intelligence* informatica degli Stati membri all'interno del centro Ue di situazione e di *intelligence* (INTCEN); 3) Rivedere il quadro strategico e la capacità di cyberdifesa, facilitando lo sviluppo di una visione e strategie militari dell'UE sul cyberspazio come dominio operativo per le missioni e le operazioni militari della politica di sicurezza e di difesa comune (PSDC). Infine, nell'ambito della terza area, la Commissione propone di insistere sulla collaborazione e cooperazione con i *partner* internazionali, per promuovere un modello politico e una visione del ciberspazio fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici che generino sviluppo sociale, economico e politico a livello globale e contribuiscano a un'Unione della sicurezza. Questa strategia garantirebbe un decennio digitale sicuro dal punto di vista della cibersicurezza per l'UE, la realizzazione di un'Unione della sicurezza e il rafforzamento della posizione dell'UE a livello globale.

__6.3.1 La proposta di direttiva NIS 2.0

La commissione europea, nell'ambito della Strategia dell'UE in materia di cibersicurezza per il decennio digitale, ha proposto l'adozione di una direttiva NIS 2.0. L'Obiettivo è

quello di aumentare il livello di ciberresilienza di tutti i settori pertinenti, pubblici e privati che svolgono una funzione importante per l'economia e la società, mettendo in atto norme più specifiche. Secondo le stime fornite dalla Commissione europea, l'opzione strategica prescelta apporterebbe una riduzione, pari a 11,3 miliardi di euro dei costi degli incidenti di cibersicurezza. Questa proposta arriva in un momento delicato, a pochi giorni dall'attacco informatico contro l'Agenzia Europea del Farmaco (Ema), che ha causato l'esposizione di informazioni sensibili legate al vaccino anti Covid Pfizer-*BioNTech* e dal *cyber* attacco contro il colosso americano *SolarWinds*, il quale ha permesso l'introduzione di alcuni *hacker* statali all'interno di enti governativi e privati di tutto il mondo. Da un lato la proposta per la direttiva NIS 2.0 ha riconosciuto la capacità della direttiva NIS di migliorare la *cybersecurity* a livello nazionale e la cooperazione a livello dell'Unione. Dall'altro lato, la valutazione ha evidenziato significative criticità. "Nonostante i buoni risultati raggiunti, la direttiva NIS ha tuttavia evidenziato alcuni limiti, laddove la trasformazione digitale della società, intensificata dalla crisi di COVID-19, ha ampliato il panorama delle minacce accentuando la vulnerabilità delle nostre società, sempre più interdipendenti di fronte a rischi rilevanti e imprevisti. Sono emerse nuove sfide, che richiedono risposte adeguate e innovative. Le risultanze dell'ampia consultazione svolta con le parti interessate ha messo in luce l'insufficiente livello di cibersicurezza in capo alle imprese europee, l'applicazione incoerente delle regole da parte degli Stati nei vari settori e la carente comprensione delle principali minacce e sfide"[194]. In primo luogo, l'ambito della direttiva NIS è troppo limitato. Il maggior grado di connessione e digitalizzazione ha determinato l'esclusione di settori strategici e attori che forniscono servizi fondamentali nella società. Inoltre, la direttiva si è rivelata non sufficientemente chiara per quanto riguarda la portata degli operatori di servizi essenziali e la competenza nazionale sui fornitori di servizi digitali. Questo ha determinato una situazione in cui alcuni soggetti giuridici non sono stati identificati in tutti gli Stati membri e non sono stati tenuti a mettere in atto misure di sicurezza e a segnalare incidenti. Una ulteriore causa di incertezza è dovuta alla sovrapposizione di obblighi di notifica ai sensi della direttiva NIS con altri doveri di segnalazione di violazioni in materia di *cybersecurity* ai sensi di altre leggi dell'UE, ad esempio il GDPR. Inoltre, il regime di supervisione e di applicazione

[194] Parere del Comitato economico e sociale europeo, reperibile nella Gazzetta ufficiale dell'Unione Europea.

della direttiva si è rivelato inefficace, vista la reticenza degli Stati membri nell'applicazione delle sanzioni. Altre disparità tra Stati membri sono emerse nelle risorse finanziarie e umane da essi riservate per l'adempimento dei loro compiti. Ciò aggrava ulteriormente le differenze nella resilienza informatica tra gli Stati membri. Infine, è stato riconosciuto il fallimento nell'obiettivo della cooperazione strategica e dello scambio di informazioni, tra gli Stati membri, tra soggetti privati e tra soggetti pubblici e privati.

Alla luce di tali lacune, i principali obiettivi della revisione sono: 1) aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea; 2) ridurre le incongruenze in termini di resilienza del mercato interno nei settori già contemplati dalla direttiva vigente; 3) migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta. La proposta di direttiva è stata strutturata nel modo seguente. Il capo 1 contiene disposizioni di carattere generale. Nei capi 2 e 3 viene fatto obbligo agli Stati membri di adottare una strategia nazionale per la cibersicurezza (artt. da 5 a 11) e di designare autorità nazionali competenti, punti di contatto unici e *team* di risposta agli incidenti di sicurezza informatica - CSIRT (artt. da 12 a 16). La proposta stabilisce, inoltre, obblighi di gestione e segnalazione dei rischi di cibersicurezza per i soggetti indicati come "soggetti essenziali" all'allegato I e come "soggetti importanti" all'allegato II (artt. da 17 a 23). Prevede inoltre che alcuni tipi di soggetti (fornitori di servizi DNS, fornitori di servizi di *cloud computing*, fornitori di servizi di *data center* e fornitori di reti di distribuzione dei contenuti, nonché alcuni fornitori di servizi digitali) siano sottoposti alla giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) dovrà creare e mantenere un registro dei soggetti di quest'ultimo tipo (artt. 24 e 25). Il capo V stabilisce obblighi in materia di condivisione delle informazioni sulla cibersicurezza (artt. 26 e 27). Gli artt. da 28 a 34 definiscono infine gli aspetti relativi alla vigilanza e all'imposizione di sanzioni.

La nostra analisi si soffermerà adesso sugli aspetti di maggiore rilevanza e differenza rispetto all’attuale direttiva NIS. Per quanto attiene all’ambito di applicazione, vengono ampliati in modo significativo i settori cui si applica questa direttiva. La direttiva NIS si applica ai servizi sanitari, i trasporti, le istituzioni finanziarie, la produzione e distribuzione di energia, la fornitura di acqua, le infrastrutture digitali e i fornitori di servizi digitali. La nuova versione della direttiva comprende anche le aziende che si

occupano di trattamento e ricircolo dei rifiuti, i produttori di prodotti critici, come ad esempio le industrie farmaceutiche, le industrie alimentari, i servizi postali e spaziali, ed i fornitori di sistemi pubblici di comunicazioni, nonché l'amministrazione pubblica.

Inoltre, la direttiva NIS 2 ha sostituito la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali con una classificazione di soggetti, pubblici e privati, tra essenziali e importanti. Entrambe le categorie saranno soggette agli stessi obblighi in materia di gestione del rischio e di segnalazione delle violazioni, mentre il regime di vigilanza e sanzione sarà differente. Da una parte, agli operatori essenziali si applicherà un vero e proprio regime di vigilanza *ex ante*, mentre, le entità importanti saranno soggette solamente a uno schema più soft di vigilanza *ex post*, nel caso in cui si rilevi un'inottemperanza alle disposizioni. Un ulteriore fattore di ampliamento è determinato dalla eliminazione dell'esclusione di micro e piccole imprese, qualora integrino certi requisiti. "Ciò configura un'importante semplificazione rispetto al regime attuale, caratterizzato da un'applicazione disomogenea, da parte degli Stati membri, dei criteri di identificazione degli operatori che rientrano nel campo di applicazione della direttiva NIS. Ricordiamo infatti che uno dei motivi alla base della sua revisione è proprio quello di ridurre *"[the] inconsistencies across the internal market*" e sicuramente tale disposizione rappresenterà un indubbio progresso in termini di funzionalità della normativa[195]." La proposta, pertanto, dimostra di prendere sul serio la *cybersecurity*, non solo ampliando il novero delle imprese soggette alla direttiva e ai conseguenti obblighi, ma anche attraverso veri e propri sistemi di vigilanza, che spingerebbe le imprese a rafforza i sistemi di sicurezza informatica. Una importante novità è rappresentata dall'art.6 che si occupa della divulgazione della vulnerabilità. Ogni Stato membro dovrà designare uno dei propri CSIRT di cui all'articolo 9 come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato agirà da intermediario di fiducia agevolando, se necessario, l'interazione tra il soggetto che effettua la segnalazione e il fabbricante o fornitore di servizi TIC o prodotti TIC. L'ENISA ha il compito di elaborare e mantenere un registro europeo delle vulnerabilità. Il registro contiene le informazioni che illustrano la vulnerabilità, i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata,

[195] A. Valeriani, *NIS 2: verso una nuova strategia in ambito cybersecurity,* in Iusintinere.it, 28 dicembre 2021.

la disponibilità di relative *patch* e, qualora queste non fossero disponibili, orientamenti rivolti agli utenti dei prodotti e dei servizi vulnerabili sulle possibili modalità di attenuazione dei rischi derivanti dalle vulnerabilità divulgate.[196] "Osserviamo, dunque, come l'intenzione del legislatore europeo sia quella di favorire un approccio sempre più stretto di cooperazione tra i soggetti privati e pubblici, in ragione dei rischi e delle vulnerabilità aventi un impatto sulla società intera"[197].

Il progresso nella cooperazione a livello europeo, si fonda su una nuova organizzazione, chiamata *European Cyber Crises Liaison Organization Network* (EU-CyCLONe). Quest'ultima avrà l'incarico di gestire in modo coordinato attacchi informatici su larga scala e aumentare il livello di preparazione e consapevolezza per la gestione di crisi e incidenti. A tal fine è necessario aumentare lo scambio di informazioni fra i paesi membri e coordinare gli interventi sulle vulnerabilità, spesso individuate in un paese, ma non condivise con altri paesi. Vengono fissati requisiti di base in materia di misure tecniche, organizzative e di gestione del rischio, lasciando meno discrezionalità agli Stati membri[198]. È da accogliere favorevolmente la prevista possibilità di introdurre formati *standard* per la procedura di notifica, predisposti dalla Commissione. Infatti, l'esistenza di formati uniformi tra gli Stati Membri potrebbe essere un significativo aiuto per la predisposizione di procedure interne che tengano in considerazione, anticipatamente, le informazioni necessarie da raccogliere per adempiere all'obbligo di notifica, in caso di incidente. Così facendo si semplificherebbe il lavoro delle società, in momenti critici come quelli di gestione di un incidente di *cyber sicurezza*. La direttiva prevede, inoltre, nuovi obblighi per i soggetti rientranti nell'ambito di applicazione. I soggetti NIS devono tener conto delle vulnerabilità specifiche per ogni fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei propri fornitori e fornitori di servizi[199]. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi, sistemi o prodotti TIC[200]. Gli operatori di servizi

[196] Art 6, proposta direttiva NIS 2.
[197] R. Brighi e P. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, cit., pag. 38
[198] Art 18, comma 2, Proposta direttiva NIS 2.
[199] Art 18, comma 3, Proposta direttiva NIS 2.
[200] Art. 19, comma 1, Proposta direttiva NIS 2.

essenziali e fornitori di servizi digitali devono segnalare subito alle autorità nazionali incidenti significativi[201]. Sono introdotte disposizioni più dettagliate sulla procedura di segnalazione degli incidenti. Esiste ora una chiara definizione del concetto di incidente avente un impatto significativo sulla continuità e sulla fornitura dei servizi e sulle sue modalità di segnalazione. Un incidente è considerato significativo se ha causato o può potenzialmente causare notevoli turbative operative o perdite finanziarie per l'entità interessata o se ha colpito (o può potenzialmente colpire) altre persone fisiche o giuridiche causando considerevoli danni materiali o non materiali[202]. Si rileva, inoltre, l'introduzione di un rigido limite temporale per le notifiche. Una volta che l'operatore viene a conoscenza dell'avvenuto incidente, la notifica deve essere effettuata entro 24 ore alle autorità competenti o al *Computer Security Incident Response Team* (CSIRT). In aggiunta, a distanza di un mese, dovrà essere rilasciato un report finale comprendente almeno una descrizione dettagliata dell'incidente, della sua gravità e del suo impatto, il tipo di minaccia o la causa che lo ha probabilmente provocato e le misure di mitigazione previste[203]. Per la prima volta le persone fisiche possono essere ritenute responsabili della violazione dei loro obblighi nel garantire l'ottemperanza alle misure di sicurezza[204].

Gli enti, pertanto dovranno preoccuparsi di attuare quanto previsto dalla direttiva non solo per evitare di incorrere nella responsabilità da reato degli enti (la quale comunque non impone l'obbligatoria adozione di modelli organizzativi), ma anche per evitare le sanzioni espressamente ricollegate all'inadempimento degli obblighi. A tal proposito l'art. 18 afferma: "Per valutare l'adempimento degli obblighi di cui alla presente direttiva da parte dei soggetti individuati come soggetti critici ai sensi dell'articolo 5 dagli Stati membri, questi provvedono affinché le autorità competenti siano dotate dei poteri e dei mezzi per: (a)effettuare ispezioni in loco dei locali utilizzati dal soggetto critico per fornire i suoi servizi essenziali, e vigilare a distanza sulle misure adottate dai soggetti critici ai sensi dell'articolo 11; (b)svolgere o disporre *audit* nei confronti di tali soggetti. 2.Gli Stati membri provvedono affinché le autorità competenti abbiano i poteri e i mezzi per richiedere, qualora necessario per lo svolgimento dei loro compiti ai sensi della presente direttiva, che i soggetti da essi individuati come soggetti critici ai sensi dell'articolo 5

[201] Art 20, comma 2, Proposta direttiva NIS 2.
[202] Art 20, comma 3, Proposta direttiva NIS 2.
[203] Art 20, comma 4, Proposta direttiva NIS 2.
[204] Art. 17, Proposta direttiva NIS 2.

forniscano, entro un ragionevole periodo di tempo stabilito da dette autorità: (a)le informazioni necessarie per valutare se le misure adottate per garantire la resilienza soddisfino i requisiti di cui all'articolo 11; (b)la prova dell'effettiva attuazione di tali misure, inclusi i risultati di un *audit* svolto da un revisore indipendente e qualificato, selezionato da tale soggetto, ed effettuato a spese di questo. Quando richiede tali informazioni l'autorità competente indica lo scopo della richiesta specificando il tipo di informazioni da fornire. 3.Fatta salva la possibilità di infliggere sanzioni ai sensi dell'articolo 19, le autorità competenti possono esigere, a seguito delle azioni di vigilanza di cui al paragrafo 1 o della valutazione delle informazioni di cui al paragrafo 2, che i soggetti critici interessati adottino entro un ragionevole periodo di tempo da esse stabilito le misure necessarie e proporzionate per porre rimedio a qualsiasi violazione individuata della presente direttiva e forniscano loro informazioni sulle misure adottate. Tali provvedimenti tengono conto, in particolare, della gravità della violazione. 4.Gli Stati membri provvedono affinché i poteri di cui ai paragrafi 1, 2 e 3 possano essere esercitati solo fatte salve le opportune garanzie. Deve essere garantito, in particolare, che tali poteri vengano esercitati in modo obiettivo, trasparente e proporzionato e che i diritti e gli interessi legittimi dei soggetti critici interessati, inclusi il diritto al contraddittorio, i diritti della difesa e il diritto a un ricorso effettivo dinanzi a un giudice indipendente, siano debitamente tutelati. 5.Gli Stati membri provvedono affinché, quando un'autorità competente valuta il rispetto degli obblighi da parte di un soggetto critico ai sensi del presente articolo, essa informi le autorità competenti dello Stato membro interessato designate ai sensi della [direttiva NIS 2] e possa chiedere a tali autorità di valutare la cibersicurezza di tale soggetto, e cooperi e scambi informazioni a tal fine". Inoltre, l'art 19[205] richiede che gli stati membri adottivo sanzioni effettive, proporzionate e dissuasive in caso di violazione delle disposizioni nazionali adottate ai sensi della presente direttiva. Ci avviamo, pertanto, verso la ridefinizione di obblighi sempre più incisivi a carico degli enti, i quali dovranno prendere sempre più sul serio la sicurezza informatica per evitare sanzioni. Del resto, possiamo immaginare che di un provato inadempimento in merito a

[205] Art 19 proposta direttiva NIS 2: Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle disposizioni nazionali adottate ai sensi della presente direttiva e prendono tutte le misure necessarie per assicurarne l'attuazione. Le sanzioni previste sono effettive, proporzionate e dissuasive. Gli Stati membri notificano tali disposizioni alla Commissione al più tardi entro [due anni dall'entrata in vigore della presente direttiva], e provvedono poi a darle immediata notifica delle eventuali modifiche successive

tali obblighi si potrebbe tener conto nell'accertamento della colpa di organizzazione. Infatti, la direttiva consente agli Stati effettuare ispezioni per valutare le misure adottate nell'ottica di rafforzare la collaborazione tra pubblico e privato. Altro elemento d'interesse è lo scambio di informazioni fra i vari enti e paesi coinvolti rappresenta un aspetto fondamentale di intervento tempestivo, in caso di violazioni. Gli Stati membri devono provvedere affinché i soggetti essenziali e importanti possano scambiarsi pertinenti informazioni sulla cibersicurezza, comprese informazioni relative a minacce informatiche, vulnerabilità, indicatori di compromissione, tattiche, tecniche e procedure, allarmi di cibersicurezza e strumenti di configurazione.[206] Il legislatore subordina la condivisione di informazioni a due condizioni. L'informazione deve prevenire, rilevare o attenuare gli incidenti o aumentare il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento delle minacce, strategie di attenuazione o fasi di risposta e recupero[207]. Queste previsioni normative saranno essenziali per il settore privato per garantire la robustezza del sistema e imparare dai pari[208]. Viene inoltre prevista la possibilità per i soggetti che non rientrano nell'ambito di applicazione della direttiva, di poter trasmettere su base volontaria notifiche di incidenti significativi, minacce informatiche o quasi incidenti[209]. Al fine di tutelare gli interessi privati e di incentivare tali pratiche, lo scambio di informazioni dovrà avvenire "nell'ambito di comunità fidate di soggetti essenziali e importanti. Tale scambio è attuato mediante accordi di condivisione delle informazioni che tengono conto della natura potenzialmente sensibile delle informazioni condivise[210]".

Infine, nella proposta troviamo un incremento notevole delle sanzioni imposte in caso di violazione delle misure di gestione del rischio e degli obblighi di notifica.

La maggioranza delle autorità competenti e delle imprese si è mostrata favorevole a una revisione della direttiva NIS. Tuttavia, il CESE (Consiglio economico e sociale europeo) ha rilevato l'opportunità di operare attraverso lo strumento giuridico del regolamento e

[206] Art 26, comma 1, Proposta direttiva NIS 2.
[207] Art 26, comma 1, lettera A e B, Proposta direttiva NIS 2.
[208] R. Brighi e P. Chiara, *La cybersecurity…,* cit., pg.40.
[209] Art 27, comma 1, Proposta direttiva NIS 2.
[210] Art.26, comma 2, Proposta direttiva NIS 2.

non della direttiva e la necessità di specificare ulteriormente l'ambito di applicazione della medesima. Anche il Garante *privacy* europeo si è mostrato, in via generale, soddisfatto della proposta ma ha messo in rilievo alcuni aspetti. L'Autorità garante ricorda che il perseguimento di obiettivi di *cyber security* a livello europeo può talvolta portare all'attuazione di misure che, nel concreto, interferiscono con i diritti alla protezione dei dati e alla *privacy*. Ne consegue l'obbligo, per il legislatore, di elaborare previsioni che garantiscano che ogni potenziale limitazione del diritto alla protezione dei dati personali e della vita privata debba necessariamente soddisfare i requisiti contenuti all'art. 52 par. 1 della Carta dei Diritti Fondamentale dell'UE, ossia previsioni legislative che siano proporzionate, necessarie e rispettose dell'essenza del diritto. L'EDPS ritiene che sarebbe opportuno indicare in maniera esplicita che l'adozione della Direttiva NIS 2 lasci impregiudicata l'attuale normativa europea sulla protezione dei dati personali, e non alteri in alcun modo i compiti e i poteri da questa attribuititi alle autorità garanti della *privacy*. Attualmente, l'articolo 2 della proposta di Direttiva NIS 2 specifica che la stessa "si applica senza pregiudizio" di una serie di direttive europee, ma tra queste non menziona il GDPR e la Direttiva *ePrivacy*. L'EDPS si sofferma anche sul tema dell'intelligenza artificiale, ove utilizzata al fine di rilevare, analizzare, contenere e rispondere alle minacce e agli incidenti informatici. In particolare, evidenzia come sia necessario indicare espressamente, anche all'interno della Direttiva NIS 2, la necessità fare applicazione dei principi di *data protection by design* e *data protection by default*, ai sensi dell'art. 25 GDPR. Di tale proposta, si possono apprezzare i continui sforzi, fatti a livello europeo, anche alla luce degli stravolgimenti dovuti alla pandemia da COVID-19, tuttavia il testo della proposta potrebbe subire delle modifiche nel corso dell'iter legislativo.

Alla luce di quanto appena analizzato, questo documento ha un valore particolare nel responsabilizzare le imprese nel campo della *cybersecurity* e prevenire gli attacchi informatici. Le indicazioni fornite ma soprattutto il timore di possibili sanzioni potrebbe spingere le imprese a destinare sempre maggiori risorse sulla *cybersecurity*. In questa sede, sottolineiamo il rischio di attribuire un eccessivo peso agli operatori coinvolti nell'adempimento degli obblighi. Si dovrebbe piuttosto cercare di garantire un equilibrio tra le misure efficaci ad assicurare un adeguato livello di *cybersicurezza* anche nell'ottica di prevenire una eventuale responsabilità da reato degli enti e una opportuna flessibilità

per gli operatori dall'altro, al fine di guardare alla *compliance* come ad un'opportunità e non solo ad un costo.

Capitolo II: La tutela della riservatezza e sicurezza informatica nell'ordinamento italiano

1. Gli strumenti normativi nella lotta al *cybercrime*: il piano nazionale

Nel capitolo precedente abbiamo visto come la riservatezza abbia acquisito riconoscimento giuridico grazie anche al contributo di una serie di atti sovranazionali. In particolare, facciamo riferimento alla CEDU, adottata in senso al Consiglio d'Europa[1]. Abbiamo concentrato la nostra indagine sul volto assunto da questo interesse in una società governata dalla tecnologia. Ci riferiamo alla colossale massa di dati che viene giorno dopo giorno archiviata e memorizzata, grazie all'uso di *computer* e telefoni. Tuttavia, dal riconoscimento di un diritto non discende l'obbligo per l'ordinamento di assicurarne tutela mediante sanzioni penali. "Tanto la Costituzione quanto il diritto internazionale dei diritti umani lasciano, di regola, il legislatore libero di valutare se sia necessario apprestare tutela penale a un determinato diritto fondamentale o se invece il doveroso obiettivo di proteggere il diritto stesso dalle aggressioni provenienti dai terzi possa essere efficacemente assicurato mediante strumenti alternativi".[2] Il legislatore

[1] La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, concepita in seno al Consiglio d'Europa, è stata firmata a Roma il 4 novembre 1950 ed è entrata in vigore il 3 settembre 1953. Di essa fanno parte i 47 Stati membri del Consiglio d'Europa. In questa sede giova precisare che ai sensi dell'art. 6, par. 3 del Trattato di Lisbona: "I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali". Inoltre, l'art. 52 della Carta dei diritti fondamentali prevede che: 1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. 2. I diritti riconosciuti dalla presente Carta che trovano fondamento nei trattati comunitari o nel trattato sull'Unione europea si esercitano alle condizioni e nei limiti definiti dai trattati stessi. 3. Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa. Tali disposizioni sono utili per comprendere i rapporti tra CEDU e diritto dell'Unione Europea.

[2] Sent. Corte costituzionale, n. 37 del 23 gennaio 2019, in www. cortecostituzionale.it, pag. 8.

italiano ha fatto una precisa scelta politico-criminale, decidendo di intervenire anche attraverso strumenti di carattere penale al fine di tutelare i nuovi interessi divenuti rilevanti con il progressivo evolversi della tecnologia. A tal proposito, se fino ad ora abbiamo utilizzato i termini diritto e interesse, è ora giunta l'ora di fare più specifico riferimento alla nozione di bene giuridico[3], poiché in questo secondo capitolo andremo ad indagare gli strumenti penali introdotti per contrastare il *cybercrime*. In questa sede non ci soffermiamo, tuttavia, sulle etichettature dogmatiche[4], volendo piuttosto sottolineare la decisività della capacità selettiva del legislatore al momento di procedere alle concrete scelte di tutela. La decisione presa dal legislatore italiano si deve ritenere fondata su una concezione costituzionalmente orientata del bene giuridico. Infatti, proprio al fine di evitare il rischio di arbitrio la dottrina ha assunto la Costituzione come parametro di riferimento di ciò che può legittimamente assurgere a reato[5].

Del resto, ormai una fetta importante della nostra vita, relazioni sociali, istruzione e lavoro, si è trasferita in questo parallelo spazio virtuale, che abbiamo definito *cyberspace*. La tecnologia ci ha consentito di liberarci dallo spazio e di aumentare la nostra capacità di circolazione, ma ha anche in gran parte abolito la distinzione tra spazio privato e pubblico[6]. Di fatto lo sviluppo di una tracciabilità e geolocalizzazione sempre più incisive hanno reso quasi impossibile trovare un posto sicuro[7]. La despazializzazione ha indebolito le categorie e distinzioni fondamentali attraverso cui il diritto si presentava. Andremo a indagare, pertanto, la risposta del legislatore di fronte a queste incertezze occupandoci di quelle fattispecie penali appartenenti alla categoria dei reati informatici, poste a salvaguardia di nuovi beni giuridici strettamente connessi al mondo dell'informatica. Ci riferiamo alla riservatezza informatica, la sicurezza informatica e alla

[3] Questi ultimi sono comunemente definiti come beni socialmente rilevanti, considerati in ragione della loro importanza, meritevoli di protezione giuridico penale. Infatti, secondo una concezione ancora tutt'oggi dominante nella scienza penalistica, il diritto penale contribuisce tendenzialmente ad assicurare le condizioni essenziali della convivenza, predisponendo la sanzione più drastica a difesa dei beni giuridici (cfr. G. FIANDACA E. MUSCO, *Diritto penale: parte generale,* Bologna, Zanichelli, 2019, pag. 4.)

[4] Si rinvia esemplificativamente per la trattazione circa la definizione di bene giuridico a: G. FIANDACA E. MUSCO, *Diritto penale: parte generale*, Zanichelli, Bologna, 2019, pagg. 4- 18.

[5] G. FIANDACA E. MUSCO, *Diritto penale: parte generale*, Zanichelli, Bologna, 2019, pag. 12 ss.

[6] A. GARAPON, La despazializzazione della giustizia, Mimemis edizioni, Milano, 2021, pag. 50

[7] Ibidem

veridicità e genuinità delle comunicazioni informatiche e telematiche. Prima di entrare nel vivo della trattazione ci soffermiamo su alcuni aspetti di carattere terminologico.

Uno dei primi problemi che la dottrina penalistica si trovò ad affrontare all'inizio degli anni '70 con l'avvento del *computer* fu la definizione da dare al nuovo fenomeno dei reati commessi con l'ausilio di strumenti tecnologici. La dottrina italiana mutuò dalla dottrina americana e anglosassone il termine *computer's crimes*. Questa definizione indicava una molteplicità di fenomeni illeciti attinenti alle scienze ed alle attività informatiche. Si tratta, tuttavia, di una questione che secondo alcuni autori non riveste importanza, mentre per altri individuare una definizione soddisfacente è impossibile. A tal proposito C. Pecorella nota che "con l'adozione della Raccomandazione del 1989 da parte del comitato dei Ministri del Consiglio d'Europa, è diventata superflua la ricerca di una definizione unitaria della criminalità informatica, e superata ogni disquisizione circa i criteri da utilizzare per decidere della appartenenza o meno ad essa di una determinata condotta."[8]. Ancora G. Pica afferma "La nozione di *computer crimes* rappresenta quindi una categoria concettuale di ordine generale, ma non appare in grado di assumere un significato tecnico preciso sul piano giuridico"[9]. Estremamente arduo è stato, inoltre, individuare quali caratteristiche consentissero la caratterizzazione di questa nuova categoria di reati, tanto che c'è chi nota che "può anche risultare impossibile tracciare una sistematica dei fatti illeciti fondata sulla sola natura delle nuove tecnologie"[10]. Inoltre, queste tecnologie possono costituire al contempo oggetto di tutela e mezzo di commissione di reati e questa doppia natura rende ancora più complessa la situazione. Da taluni il minimo comune denominatore dei diversi tipi di abuso era stato ravvisato nella conoscenza della tecnologia informatica necessaria per poter eseguire, scoprire o perseguire l'illecito. Altra teoria aveva cercato di restringere la definizione di *computer crime* a quei reati nei quali il *computer* è il mezzo dell'azione[11]. Questa teoria, tuttavia non impediva che a quella nozione venissero ricondotte forme di aggressione alla componente materiale di un sistema informatico, non differenti da altre condotte riservate ad altri beni (ad esempio il

[8] C. PECORELLA, *Diritto penale dell'informatica*, Padova, Cedam, 2006
[9] G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, Utet, 1999, pag. 10.
[10] Ibidem
[11] In questo senso F. MUCCIARELLI, *I computer-crimes nel disegno di legge 1657/1984*, in *Rivista italiana di diritto e procedura penale*, 1986, pp. 785 ss.

danneggiamento o il furto del *monitor* o della stampante di un sistema informatico)[12]. Inoltre, "se l'utilizzazione del *computer* costituisce la modalità usuale, e spesso essenziale, di commissione dei c.d. illeciti informatici è incontestabile che in essi confluisce una moltitudine di comportamenti che necessitano di ben altri criteri di distinzione, dal momento che taluni appaiono non necessariamente rilevanti sul piano penale, e molti altri, invece, di assai maggiore gravità risultano lesivi di beni giuridici assai diversi"[13].

La dottrina più attenta ha pertanto rivolto la propria attenzione non tanto sul ruolo del *computer* come mezzo per commettere il reato, ma quale oggetto sul quale verte la condotta. "In tale prospettiva, alla definizione del *computer crime* come reato commesso con l'uso del *computer* si affianca, e talora si sostituisce, un nuovo criterio, incentrato sui dati, le informazioni e le operazioni di programma che identificano il bene informatico quale oggetto materiale delle condotte criminose".[14]

Negli anni '90, l'apertura di *internet* al pubblico ha avuto una influenza nel campo del diritto penale. Si assiste al passaggio dai *computer crimes* (reati informatici in senso stretto) ai *cybercrimes* (reati cibernetici). Ai primi faceva riferimento la Raccomandazione del 1989 che, come abbiamo visto nel capitolo precedente, prevedeva un limitato elenco di reati. Nel 2001, con la Convenzione *Cybercrime*, venne emanato un elenco ben più articolato. "Dunque, accanto a reati che si possono definire reati informatici in senso stretto, perché includono elementi tecnico-informatici (quali: "sistema informatico", "dato informatico", "trasmissione di dati informatici", "programma informatico", ecc.), senza cui non sarebbero concepibili, è emersa un'altra categoria di reati- che si può definire "aperta"- definibili informatici in senso ampio o, meglio, cibernetici, perché pur non presentando necessariamente le sopradette caratteristiche tecnico-informatiche fra gli elementi costitutivi della fattispecie legale, meritano un particolare rilievo giuridico e processuale".[15]

[12] C. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, pag. 6.
[13] G. PICA*, Diritto penale…*, cit., pag. 12.
[14] D. PETRINI, *La responsabilità penale per i reati via internet*, Casa editrice Jovene, Napoli, 2004, pag. 29
[15] L. PICOTTI, *Cybercrime e diritto penale* in "*Diritto penale dell'informatica: reati della rete e sulla rete" a cura* di C. PARODI e V. BELLAROLI, Giuffrè, 2020, pag. 709- 725.

Questa ultima categoria ricomprende tutti quei reati che costituiscono forme di aggressione di beni già tutelati da norme incriminatrici comuni[16]. Ci riferiamo ai delitti di diffamazione *online*, il *cyberstalking*, il *cyberbullismo*, il *revenge porn*, ma l'elenco potrebbe continuare.

Fatta questa premessa circa le difficoltà di definizione ci addentriamo nell'analisi della disciplina italiana. Il primo passo del legislatore italiano sul tema della criminalità informatica è avvenuto con la Legge n. 547 del 1993, con cui ha cercato di recepire le indicazioni del Consiglio d'Europa e dell'AIDP. Questo intervento ha chiuso la fase definita del *computer crime* classico ed ha aperto la fase attuale definita del *cyber crime.*[17] La presente legge, composta di dodici articoli, è intervenuta modificando e integrando il Codice penale, intervenendo su settori eterogenei, che possono essere raggruppati in quattro grandi macrocategorie: le frodi informatiche, le falsificazioni, la lesione dell'integrità dei dati e dei sistemi e violazione della riservatezza di dato e comunicazioni informatiche. L'ultima categoria, quella che relativa alle aggressioni alla riservatezza dei dati e delle comunicazioni informatiche, sarà oggetto della nostra indagine[18].

Facciamo riferimento a sei norme incriminatrici collocate in diverse sezioni del titolo XII, dedicato ai "delitti contro la persona" del libro II del Codice penale. In particolare, ci occuperemo dei reati di accesso abusivo a un sistema informatico (art 615-ter c.p.), di detenzione e diffusione abusiva di codici di accesso a sistemi informatici (art 615- quater c.p.), di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- quinquies c.p.) e delle disposizioni concernenti le intercettazioni di comunicazioni informatiche e telematiche di cui agli artt. 617-quater, 617-quinquies e art. 617-sexies.

Questa delimitazione dell'area di indagine è giustificata dal fatto che si tratta di fattispecie con cui il legislatore ha inteso tutelare la riservatezza e sicurezza dei dati e delle comunicazioni informatiche, una scelta che pertanto si basa sui beni giuridici tutelati e di

[16] C. PECORELLA*, Reati informatici*, in Enc. Dir., Annali X, 2017, pagg. 707 ss.
[17] Per un'ampia trattazione delle fattispecie che non sono in questa sede oggetto di indagine rimando, esemplificativamente a: C. PECORELLA, *Diritto penale*…, cit.
[18] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati* in "*Il diritto penale dell'informatica nell'epoca di internet*" a cura di L. PICOTTI, Padova, Cedam, 2004, pag. 28.

cui ci occuperemo nei paragrafi seguenti[19]. Seguiamo pertanto quel filo conduttore che nel precedente capitolo ci ha permesso di andare alla scoperta del rapporto tra riservatezza e sicurezza. L'indagine si concentrerà, quindi sull'ambito strettamente penale, individuando la tutela offerta dal legislatore ai beni giuridici precedentemente nominati della riservatezza informatica, sicurezza informatica e della veridicità e genuinità delle comunicazioni informatiche e telematiche.

La questione, tuttavia, è particolarmente complessa e non può essere risolta in maniera univoca. Per tale ragione, sarà necessario indagare per ogni singola fattispecie le problematiche connesse alle particolari declinazioni dei predetti beni giuridici.

La scelta legislativa del '93 si è discostata dall'operato di altri legislatori europei, come quello francese, e non ha previsto un apposito titolo all'interno del Codice dedicato a tale tipo di condotte, ma ha collocato le nuove disposizioni accanto ai reati già esistenti. Per quanto attiene alla tecnica legislativa, il legislatore è intervenuto sulle definizioni, sia introducendone di nuove, sia estendendo la portata di altre già esistenti. Il legislatore ha, infatti, ampliato la disposizione di cui all'art 621 c.p., ‹‹rivelazione del contenuto di documenti segreti››, ai documenti contenuti in un supporto informatico. Inoltre, ha esteso la nozione di corrispondenza contenuta nell'articolo 616 c.p. in modo da ricomprendervi anche quella informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza. Negli altri casi il legislatore ha fatto ricorso a fattispecie nuove ma ricalcate sulle fattispecie tradizionali. Questo *modus operandi* non sembra garantire sufficiente chiarezza "data la difficoltà di far rientrare fatti, condotte ed oggetti profondamenti diversi in schemi concepiti per realtà differenti"[20] e comporta il rischio di dilatazioni, sovrapposizioni e lacune. Il legislatore così facendo ha rinunciato a "cogliere le specificità della criminalità informatica, che incide sui beni giuridici, in tutto o in parte, nuovi, non avvedendosi delle significative ricadute che i reati informatici hanno sul piano dogmatico (in relazione al concetto di azione, di evento, al concorso di persone nel reato, al momento consumativo, al locus commissi delicti, ecc..).[21] Autorevole dottrina ha,

[19] Questa delimitazione sistematica si basa sul lavoro di I. SALVADORI, *I reati contro la riservatezza informatica* in "*Cybercrime"* a cura di A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, Utet giuridica, Milano, 2019, pag. 655- 724.

[20] L. PICOTTI, *Sistematica dei reati*…, cit., pag. 53

[21] I. SALVADORI, *"I reati contro la riservatezza informatica*" in Cybercrime a cura di A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, Utet giuridica, Milano, 2019, pag. 658

tuttavia, apprezzato gli sforzi fatti dal legislatore. "Certamente apprezzabile, ci sembra lo sforzo del legislatore del 1993 di collocare nel *corpus* del codice penale esistente le nuove fattispecie, evitando di affiancare ad esso l'ennesima legge speciale…per non contribuire ulteriormente al progressivo fenomeno della decodificazione che sta caratterizzando la più recente produzione giuridica: tra l'altro le modalità dell'innesto delle nuove fattispecie presentano anche il pregio di sottolineare che buona parte dei reati informatici attingono, sia pure con modalità commissive diverse, beni giuridici già contemplati e tutelati dall'ordinamento. Non può negarsi, tuttavia, che la strada seguita ha comportato anche alcune forzature, sia nell'uso della terminologia descrittiva delle fattispecie, e sia nella scelta della collocazione sistematica di queste"[22].

Il legislatore italiano tornerà sul tema con la legge N. 48/2008, che ha dato esecuzione alla Convenzione *Cybercrime* di Budapest. La riforma è stata, tuttavia, ritenuta frettolosa[23]. Essa ha apportato significative modifiche alla disciplina delle falsità informatiche e dei danneggiamenti informatici ed ha introdotto le nuove fattispecie di falsità al certificatore di firma elettronica (art. 495-bis c.p.) e di frode del certificatore (art. 640- quinquies c.p.), ma non ha interessato le fattispecie oggetto della nostra analisi, ad eccezione dell'art. 615-quinquies c.p. Alcuni spunti sono comunque di interesse: in primo luogo, curiosa appare la scelta di non ratificare interamente la Convenzione. Ad esempio, non viene recepita nel nostro ordinamento la definizione di "sistema informatico" offerta dal testo convenzionale, e in tal senso già i primi commentatori non vi hanno rilevato qui un caso di dimenticanza, quanto piuttosto una scelta di opportunità. In particolare, si è voluto evitare di incorrere nel limite rappresentato dal principio di tassatività, lasciando la definizione alla giurisprudenza[24]. Dall'altro lato, non si può negare che da questa scelta ne possa derivare minore certezza del diritto, poiché sarà il magistrato a decidere circa la presenza di un sistema informatico o telematico[25].

L'intervento legislativo del 2008 è, tuttavia, da ricordare per aver esteso a taluni reati informatici la disciplina di cui al d.lgs. 231/2001. In particolare, l'art. 24-bis del d.lgs.

[22] G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, Utet, 1999, pag. 21.
[23] L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* in "*Diritto penale e processo*", n.6/2008
[24] S. AETERNO., M. CUNIBERTI, G.B. GALLUS., F.P. MICOZZI, *Cybercrimine: prime note sulla legge di ratifica della Convenzione di Budapest* in altalex.com, 8 maggio 2008
[25] Ibidem.

231 ha introdotto nel decreto i reati di cui all'art. 615-ter c.p., 615-quater c.p., 615-quinquies c.p., 617- quater c.p. e 617- quinquies c.p. Risulta pertanto essere esclusa la fattispecie di cui all'art. 617-sexies c.p., della quale ci occupiamo in questo capitolo per avere la possibilità di trattare con completezza la questione relativa alla tutela della riservatezza dei dati e delle comunicazioni informatiche e telematiche. L'indagine delle fattispecie risulta essere necessaria per poter comprendere appieno le implicazioni dell'estensione della responsabilità da reato degli enti ai reati informatici, argomento di cui ci occuperemo nel capitolo seguente.

Il quadro normativo, così delineato dal legislatore italiano, non è stato tuttavia giudicato dalla Commissione europea idoneo e sufficiente per soddisfare le esigenze di tutela necessarie alla respressione della criminalità informatica e, per tale ragione, è stata aperta la procedura di infrazione n. 2019/2033 con cui è stato evidenziato che l'ordinamento italiano non ha recepito l'art. 7, l'art. 9, par. 2 e l'art. 12, par. 1 lett. B) della Direttiva 2013/40/UE. L'articolo 7, impone agli Stati membri di adottare le misure necessarie affinché la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo intenzionali di determinati strumenti (programmi per *computer* o *password* o codici d'accesso o simili), con l'intenzione di utilizzarli per commettere un reato di accesso illecito a sistemi di informazione, interferenza illecita in un sistema o a dati, intercettazione illecita, siano punibili come reato, almeno per i casi che non sono di minore gravità. L'articolo 9, paragrafo 2, impone agli Stati membri di prevedere, per i reati di cui agli articoli da 3 a 7 della direttiva (accesso illecito a sistemi di informazione; interferenza illecita relativamente ai sistemi; interferenza illecita relativamente ai dati; intercettazione illecita; messa a disposizione di strumenti utilizzati per commettere tali reati), una pena detentiva massima non inferiore a due anni, almeno per i casi che non sono di minore gravità. L'articolo 12, paragrafo 1, lettera b), impone agli Stati di affermare la propria giurisdizione relativamente ai reati di cui agli articoli da 3 a 8 della direttiva (accesso illecito a sistemi di informazione; interferenza illecita relativamente ai sistemi; interferenza illecita relativamente ai dati; intercettazione illecita; messa a disposizione di strumenti utilizzati per commettere tali reati e connesse ipotesi di istigazione, favoreggiamento, concorso e tentativo), quando il reato sia commesso da un loro cittadino anche all'estero. Recentemente è stata, pertanto, approvata la l. 238 del 23 dicembre 2021, pubblicata in Gazz, Uff, il 17 gennaio 2022 e

entrata in vigore il primo febbraio 2022, recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea- Legge europea 2019-2020", che ha risposto a varie procedure di infrazione con le quali la Commissione europea ha contestato all'Italia il mancato recepimento della normativa europea, tra cui quella a cui abbiamo fatto riferimento. Il testo si compone di 48 articoli che modificano o integrano disposizioni vigenti nell'ordinamento nazionale, riguardanti settori eterogenei, tra cui quello della criminalità informatica di cui ci occupiamo. Fondamentale ai fini della nostra indagine è l'art. 19, il quale introduce alcuni correttivi alle disposizioni del Codice penale al fine di adeguare la normativa italiana, relativa agli attacchi contro i sistemi informatici, alla direttiva 2013/40/UE. In particolare, la norma ha modificato, tra le fattispecie di nostro interesse, gli artt. 615- quater c.p., 615- quinquies c.p., art. 617-quater c.p., e art- 617- quinquies c.p. Tali modifiche sono di duplice tipologia. Da un lato, l'art. 19 ha rimodulato gli artt. 615 quater, 615 quinquies e 617 quinquies, ampliando i comportamenti integranti le condotte delittuose richieste dalle varie ipotesi di reato. Dall'altro con riferimento ai reati di cui agli artt. 615- quater e 617- quater ha innalzato i minimi e massimi edittali delle pene già previste. Le modifiche non hanno, tuttavia, prestato ossequio in tutte le disposizioni a quanto disposto a livello sanzionatorio dalla diretta 2013/40/UE, prevedendo sanzioni più calmierate. Tali problematiche richiedono, pertanto, una riflessione in materia di dosimetria sanzionatoria. I principi di uguaglianza e di rieducazione impongono che la reazione penale debba essere parametrata in modo proporzionato sia al disvalore d'evento, sia a quello d'azione. Si tratta di un tema su cui la Corte Costituzionale si è più volte pronunciata, anche di recente[26], sebbene con riferimento ad altri reati. I riferimenti normativi sono il principio d'uguaglianza, di cui all'art. 3, co. 1, Cost., il quale «esige che la pena sia proporzionata al disvalore del fatto illecito commesso» e solo l'ossequio a questo asserto permette al sistema sanzionatorio di adempiere sia la funzione di difesa sociale, sia quella di tutela degli individui; e l'art. 27, co. 3, Cost., in quanto la palese sproporzione del sacrificio della libertà personale provocata dalla previsione di una sanzione penale manifestamente eccessiva rispetto al disvalore dell'illecito, vanifica il fine rieducativo della pena. Si tratta di un principio enunciato anche nella Carta dei diritti fondamentali dell'Unione europea che, all'art. 49, co. 3, recita: «Le pene inflitte non devono essere sproporzionate rispetto al reato»; così

[26] Corte cost. n. 117/2021 in Cortecostituzionale.it

come all'art. 52, co. 1, sancisce che i diritti e le libertà riconosciuti dalla Carta possono sì essere limitati, però solo nel rispetto del principio di proporzionalità. La mancanza di proporzione tra pena e disvalore del reato potrebbe, pertanto, condurre a una dichiarazione di illegittimità delle norme incriminatrici, sebbene in verità la corte ha fino ad ora teso a salvare le disposizioni normative in virtù della discrezionalità del legislatore. Occorre quindi riflettere sul reale disvalore delle azioni che potrebbero integrare tali reati al fine di evitare sanzioni eccessive.

Le modifiche introdotto sono esclusivamente in *malam partem*, pertanto in virtù del principio di irretroattività della legge penale sfavorevole (art. 25, c.2, della Cost.[27] e art. 7 CEDU[28]), saranno applicabili solo ai reati commessi successivamente al primo febbraio 2022, data di entrata in vigore della legge. L'analisi delle fattispecie verrà condotta tenendo conto di queste recenti modifiche.

2. L'intricata questione relativa al bene giuridico

Le funzioni tradizionalmente assegnate al concetto di bene giuridico dalla teoria del reato[29] presentano nel campo del diritto penale dell'informatica delle peculiarità. Siamo consapevoli che quello, da noi analizzato, è un settore dell'ordinamento di recente formazione e al cui interno trovano spazio una serie eterogenea di norme. Inoltre, l'opera dell'interprete è complicata dal fatto che tale disciplina ha ad oggetto "atti e comportamenti mediati dagli strumenti informatici o addirittura realizzati per via telematica, ricadendo perlopiù su oggetti smaterializzati…senza contatto diretto o intervento fisico su di essi o sul soggetto passivo"[30]. Può essere utile, tenere in particolare considerazione, il parametro del bene giuridico tutelato, per cercare di dare ordine alla materia. La questione è, tuttavia, tutt'altro che semplice. Infatti, molto spesso le

[27] Art. 25, comma 2 Cost.: "Nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso".
[28] Art. 7 CEDU: "1. Nessuno può essere condannato per una azione o una omissione che, al momento in cui è stata commessa, non costituiva reato secondo il diritto interno o internazionale. Parimenti, non può essere inflitta una pena più grave di quella applicabile al momento in cui il reato è stato commesso. 2. Il presente articolo non ostacolerà il giudizio e la condanna di una persona colpevole di una azione o di una omissione che, al momento in cui è stata commessa, costituiva un crimine secondo i principi generali di diritto riconosciuti dalle nazioni civili".
[29] G. FIANDACA E. MUSCO, *Diritto penale: parte generale*, Torino, Zanichelli, 2019, pag. 4 ss.
[30] L. PICOTTI, *Sistematica dei reati*…, cit., pag. 89.

fattispecie in materia di criminalità informatica non contengono né direttamente né indirettamente un riferimento al bene giuridico tutelato. Per cercare di far emergere questo elemento bisognerà prendere in considerazione tutti gli elementi oggettivi che concorrono a descrivere l'offesa, ma anche i presupposti, la qualifica dell'agente, l'evento, il rapporto di causalità, l'oggetto materiale, il fine e il comportamento e il ruolo della persona offesa.[31] Abbiamo già accennato al dibattito sorto, in Italia, all'indomani della l. 547/1993, circa il bene giuridico tutelato dalle nuove fattispecie incriminatrici. La crescente attenzione dedicata dal legislatore alle nuove tecnologie ha indotto la dottrina a parlare di beni informatici, facendo riferimento all'oggetto delle nuove normative. Alcuni autori si sono riferiti al bene informatico per fare riferimento alla "sintesi di serie documentale e macchina, di *hardware* e *software*, contenuta nel sistema informatico"[32], mentre altri hanno fatto ricorso all'espressione per indicare nuovi beni giuridici meritevoli di tutela penale. In particolare, alcuni autori avevano individuato un unico bene giuridico posto a tutela di tutte le nuove fattispecie introdotte dalla legge del '93. Facciamo riferimento all'intangibilità informatica. Quest'ultima indicava la "multiforme esigenza di non alterare la relazione triadica fra dato della realtà, rispettiva informazione, e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi".[33] Questa teoria, tuttavia, non convinse poiché "coglieva solo un aspetto, generico, della *ratio* di tutela delle nuove tecnologie, mentre risultava inidoneo a racchiudere in sé l'intera valenza degli illeciti informatici, poiché tralasciava i profili patrimoniali e personali"[34]. Apparve presto chiaro che tutti i tentativi di delineare un bene giuridico unitario fossero destinati a fallire[35]. "C'è da chiedersi se il diritto penale abbia realmente bisogno di elaborare un nuovo, unitario bene giuridico che esprima ed isoli tutti i tratti della variegata e mutevole patologia dell'informazione automatica, ed indirizzi la cultura giuridica verso la costruzione di un sistema informativo dotato di forte autonomia"[36]. Altra teoria che

[31] I. SALVADORI, *L'Accesso abusivo a un sistema informatico o telematico: una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica* in *Tutela della persona e delle nuove tecnologie* a cura di L. Picotti, Padova, 2013, pag. 127-128.
[32] F. BERGHELLA, R. BLAIOTTA, "*Diritto penale dell'informatica e beni giuridici*" in *Cassazione Penale*, n.9/1995, pag. 2335.
[33] V. MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni,* in "*Rivista trimestrale di diritto penale dell'economia",* 1992.
[34] G. PICA, *Diritto penale…*, cit., pag. 34.
[35] G. PICA, *Diritto penale…,* cit., pag. 35.
[36] F. BERGHELLA R. BLAIOTTA, *Diritto penale…*, pag. 2336.

sembrerebbe essere quella accolta dallo stesso legislatore ritiene che le nuove fattispecie riguardino nuove aggressioni a beni giuridici già esistenti[37]. Questo spiegherebbe la collocazione delle nuove disposizioni all'interno del codice.

Altra parte della dottrina ha ritenuto forzata quest'ultima teoria, ritenendo che le analogie con i preesistenti beni siano solo presunte[38]. "Un ampio settore dottrinale e giurisprudenziale, attribuendo eccessiva importanza alla collocazione delle nuove norme incriminatrici all'interno del Codice penale, ha equiparato i beni giuridici da esse tutelati a quelli protetti dalle fattispecie tradizionali, alle quali sono stati affiancate. Si è così finito per riconoscere un valore assorbente alla loro collocazione topografica, ignorando però che quest'ultima è soltanto uno degli strumenti interpretativi per determinare l'effettivo interesse giuridico oggetto di tutela…Per una corretta individuazione dei beni giuridici protetti dai reati informatici, è dunque necessario muovere dall'analisi della formulazione delle fattispecie". Questo orientamento ritiene necessario fare ricorso a beni giuridici del tutto inediti[39]. Gli studiosi sostenitori di questa tesi sottolineano le peculiarità del nuovo oggetto della tutela penale che impedirebbe di fare riferimento ai tradizionali beni giuridici[40]. "Si rivela decisiva la teorica del bene giuridico perché resta l'unico strumento dogmatico e allo stesso tempo esegetico, in grado di rappresentare il minimo comune denominatore che fa da rimedio aggregante di fattispecie diverse nel Codice penale"[41]. Le due principali categorie di beni a cui sembrano riconducibili questi nuovi interessi, non privi di connessione tra loro, sono da un lato, quello dell'integrità e sicurezza informatica, dall'altro quella della riservatezza informatica. Si tratta dei beni giuridici tutelati dalle fattispecie di cui andremo ad occuparci.

2.1 La riservatezza informatica

L'incessante sviluppo delle nuove tecnologie dell'informazione e della comunicazione (TIC) ha comportato la creazione di nuovi spazi virtuali, dove si possono intrattenere relazioni interpersonali e svolgere attività di varia natura. Questi luoghi virtuali non

[37] Cfr. F. BERGHELLA R. BLAIOTTA*, Diritto penale…,* cit., pag. 2329 ss. e G. Pica, *Diritto penale*…, cit.
[38] I. SALVADORI, *I reati contro*…, cit., pag. 657
[39] Cfr. L. PICOTTI, *Sistematica dei reati informatici*…, cit.
[40] Ibidem
[41] P. TRONCONE, *La tutela penale della riservatezza e dei dati informatici*, Edizioni scientifiche, Napoli, 2020, pag. 68.

possono essere equiparati alla nozione di domicilio tradizionale, inteso quale spazio fisico di espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti essenziali agli articoli 614 e 615 del Codice penale. All'interno di questi spazi virtuali non bisogna necessariamente tutelare "il contenuto personale riservato segreto delle informazioni contenute in suddetti spazi ovvero dei messaggi e delle conversazioni trasmesse o ricevute da un sistema informatico. Si tratta piuttosto di garantire anche in questi casi il libero esclusivo e pacifico godimento di nuovi ambiti, spazi o dispositivi informatici in modo da permettere la piena estrinsecazione della persona che dipende anche dalla facoltà di poter comunicare in modo sicuro senza interferenze altrui"[42]. Non si tratta pertanto di tutelare né il luogo, materialmente inteso, così come avviene rispetto al comune delitto di violazione di domicilio di cui all'art. 614 c.p., né la riservatezza dei dati poiché potrebbero venire in rilievo informazioni già note o prive di rilevanza per il titolare. "Il valore o interesse da proteggere consiste piuttosto nell'assicurare a ciascuno l'utilizzo o godimento indisturbato ed esclusivo di questi spazi, anche solo virtuali, che possono permettere un pieno sviluppo ed una libera estrinsecazione della persona umana. La dimensione e rilevanza sociale - prima ancora che economica e giuridica- che queste nuove sfere di competenza e disponibilità hanno acquisito tra i consociati, ha elevato al rango di nuovo interesse meritevole di tutela (anche) penale nella moderna società degli informazione, la riservatezza informatica, espressamente richiamata a livello internazionale dalla Convenzione *Cyber Crime* del Consiglio d'Europa, il cui titolo uno della sezione uno del capitolo due è specificatamente dedicato alla confidenzialità dei dati e dei sistemi informatici"[43]. La riservatezza informatica si configura come interesse al godimento e controllo esclusivi dei prodotti e delle utilità delle nuove tecnologie[44]. Si tratta di un vero e proprio diritto di esclusione dei terzi non legittimati che non sarebbe stato sufficientemente garantito dai tradizionali mezzi di tutela della proprietà e del possesso delle cose materiali, né dalla protezione assicurata al segreto, alla riservatezza personale e domiciliare e ai beni immateriali tradizionali. La riservatezza informatica supera i tradizionali ambiti di tutela delle informazioni concernenti persone fisiche determinate, il domicilio come luogo in cui si svolge la vita privata e il segreto. Inoltre, questo nuovo

[42] I. SALVADORI, *I reati contro la riservatezza*…, cit., pag. 661.
[43] I. SALVADORI*, I reati contro la riservatezza*…, cit., pag. 663.
[44] L. PICOTTI, *Sistematica dei reati informatici…*, cit., pag. 78.

bene giuridico abbraccia un ambito di rapporti più ampio e diverso da quello in cui si collocano i peculiari diritti di esclusiva sui beni immateriali tradizionali (quali i diritti d'autore e i brevetti tradizionali). In particolare, vengono in rilievo tutte quelle informazioni oggetto di trattamento automatizzato. "Essa riguarda infatti il nuovo interesse all'esclusività (o possibilità autonoma di controllo e limitazione) dell'accesso, utilizzo, trattamento di dati e sistemi informatici in quanto tali, che si giustifica per la (ben maggiore) utilità così garantita al titolare, di fronte all'altrimenti "strutturale" accessibilità, facilità di circolazione ed ampiezza di diffusione- proprio attraverso le connessioni e procedure automatizzate- dei dati e delle informazioni, spesso (ma non necessariamente) di rilevante valore economico e patrimoniale, ovvero personale, politico, ideologico, militare, ecc."[45]. Le misure di tutela di natura tecnica, organizzativa, amministrativa o di altre specie volte a contrastare le continue intrusioni, intercettazioni, riproduzioni e sottrazioni abusive da parte di soggetti non legittimati si sono rivelate insufficienti. Il legislatore ha, pertanto, deciso di fare ricorso allo strumento penale. "Non è però un'esclusione di terzi né, del resto, una tutela personale che abbiano caratteri di assolutezza, presentandosi piuttosto come strutturalmente circoscritte ad ambiti, mezzi e procedimenti determinati, sempre soggette al bilanciamento con contrapposti beni ed interessi di sicura rilevanza per la persona e la collettività, ed in specie per lo sviluppo delle relazioni sociali e del mercato"[46]. Nel caso di specie la contrapposta esigenza da tutelare è la libertà della circolazione delle informazioni, di diffusione, accessibilità o trasparenza dei dati e relativi trattamenti[47].

Occorre, per chiarezza espositiva, sottolineare la differenza tra l'ambito della riservatezza informatica e quello della *privacy*. Quest'ultima viene in rilievo rispetto ai trattamenti di dati effettuati anche senza l'ausilio di strumenti elettronici, andando quindi oltre la dimensione informatica. Inoltre, la *privacy* nella sua accezione moderna come diritto alla protezione dei dati personali va oltre i confini della tutela della vita privata per abbracciare complesse discipline volte ad assicurare a chiunque la possibilità di esercitare un controllo sui dati personali che lo riguardano, garantendo al contempo l'esigenza della loro corretta circolazione ed accessibilità da parte di terzi[48]. Si tratta di quella complessa questione

[45] Ibidem
[46] L. PICOTTI, *Sistematica dei reati informatici…*, cit., pag. 79.
[47] Ibidem
[48] I. SALVADORI, *I reati informatici…*, cit., pag. 663.

connessa all'autonomia tra gli artt. 7 e 8 della Carta dei diritti fondamentali affrontata nel corso del primo capitolo. Da un lato l'art. 7, il quale tutela il tradizionale diritto al rispetto della propria vita privata e familiare, dall'altro l'art. 8 che individua il nuovo e autonomo diritto alla protezione dei dati personali. In particolare, in quest'ultimo diritto si coglie il punto di arrivo di quel percorso da noi precedente analizzato che ha finito per intendere la *privacy* come diritto di mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata. Adesso viene in rilievo il bene giuridico della riservatezza informatica che, invece, concerne l'interesse all'esclusività e sicurezza della fruizione e dell'accesso ad uno o più spazi virtuali, anche se questi sono vuoti o contengono soltanto dati, informazioni o programmi di pubblico dominio. Il diritto alla riservatezza e alla tutela della *privacy* prende in questo ambito un'accezione di riservatezza informatica, termine con il quale si intendono "quelle nuove aree virtuali ove i soggetti titolari memorizzano ed elaborano con una certa facilità e velocità un'ampia quantità di informazioni e di dati, con conseguente libera valorizzazione della personalità individuale e svolgimento di qualsiasi attività di natura economica, libero-professionale, sociale, culturale…L'ambito di tutela di tale bene giuridico è rappresentato dall'esigenza di salvaguardare il pieno diritto di godimento di tali confini virtuali da parte del legittimo titolare, e ciò si proietta non solo sul contestuale sviluppo della personalità umana, ma prefigura anche la possibilità di escludere soggetti terzi dall'illimitata possibilità di intrusione nel sistema informatico altrui"[49]. In definitiva, la riservatezza informatica assurge a diritto fondamentale dell'uomo, quale manifestazione del diritto generale di personalità, che si fonda sull'art. 2 Cost., e, più specificamente, sull'art. 8 CEDU e sugli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Interesse che è stato ritenuto meritevole di tutela dal legislatore penale per garantire all'individuo la disponibilità esclusiva e libera dei nuovi mezzi tecnologici o ambiti virtuali da illegittime interferenze. Non può, inoltre, essere ignorata l'importanza sistematica di questo nuovo bene giuridico, il quale darebbe vita ad uno "Statuto personale della riservatezza digitale"[50]. "Si può dire che viene fornito un

[49] M. CASELLATO, A. DI MAIO, D. LA MUSCATELLA, *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali* in Cassazione Penale, fasc.7, 1° luglio 2019

[50] P. TRONCONE, *La tutela penale della riservatezza e dei dati personali*, Edizioni scientifiche, Napoli, 2020, pag. 60.

contributo importante per individuare un nuovo bene giuridico di categoria, con l'intesa che questo possa dettare le coordinate per un ordine sistematico e, sul piano della esegesi, possa consentire la tutela più aderente ai propositi legislativi nel rispetto dei principi di garanzia".[51] Abbiamo, così facendo delineato il profilo di questo nuovo bene giuridico, nell'analisi delle disposizioni penali poste a sua tutela potremo analizzare le peculiarità connesse alle singole fattispecie.

2.2 La sicurezza informatica

La protezione della riservatezza informatica dipende anche dal raggiungimento di un elevato livello di sicurezza dei mezzi e dei sistemi informatici. Riservatezza e sicurezza informatica finiscono, così per intersecarsi e sovrapporsi. Questo si evince dai numerosi atti analizzati nel precedente capitolo volti a garantire la riservatezza e la sicurezza nella rete. Ci riferiamo alla Convenzione *Cybercrime,* il cui titolo 1 è dedicato ai comportamenti contro la riservatezza, l'integrità o la sicurezza dei dati e dei sistemi informatici. Questa relazione risulta ancora più manifesta nella direttiva Nis che ha l'obiettivo di individuare misure volte a garantire un livello di comune di sicurezza dei reati e dei sistemi informatici all'interno dell'UE. All'art. 4, n. 2, infatti, sottolinea come la sicurezza informatica dipenda dalla disponibilità, dall'autenticità, dall'integrità e dalla riservatezza dei dati conservati, trasmessi o trattati da un sistema. Mentre la riservatezza informatica viene in evidenza quale bene giuridico disponibile, poiché fa parte dei diritti della personalità, la sicurezza informatica in quanto interesse super individuale e collettivo alla integrità e disponibilità dei dati, dei programmi e dei sistemi di informazione, assume una peculiare rilevanza pubblica[52]. Pertanto, la sicurezza informatica deve essere tutelata nell'interesse della collettività al fine di garantire un livello elevato di protezione ai dispositivi e sistemi informatici da cui dipendono numerosi servizi offerti nella società moderna[53].

Un orientamento dottrinale ha precisato che l'ambito di operatività di tale concetto ha natura prodromica rispetto all'effettiva lesione dell'integrità e dell'utilizzabilità dei documenti e dei programmi telematici, in quanto lo scopo del legislatore è stato quello di

[51] Ibidem
[52] L. PICOTTI, *Sistematica*…, cit., pag. 74.
[53] I. SALVADORI*, I reati informatici*…, cit., pag. 665.

intervenire anticipatamente nei confronti di quelle condotte che sono in grado di causare non soltanto il malfunzionamento delle reti *Internet* e delle piattaforme digitali, ma anche la produzione di gravi costi economici alla collettività[54]. Come può osservarsi, la regolarità del flusso di dati *online*, la corretta erogazione dei servizi nel quadro del *cyberspazio*, la veridicità dei dati, e l'adozione di buone prassi comportamentali tra gli internauti, ha determinato l'evidente diminuzione degli episodi criminosi commessi in rete, e la contestuale realizzazione del libero accesso e della circolazione dei dati e delle informazioni nei settori digitali.

Varie sono le fattispecie che il nostro legislatore ha introdotto a protezione della riservatezza e della sicurezza informatica, quali autonomi e nuovi interessi giuridici fra loro correlati. In particolare, tra quelle di nostro interesse rileva la fattispecie di accesso abusivo ad un sistema informatico telematico di cui all'articolo 615- ter c.p.[55]. Tramite questa disposizione, il legislatore ha voluto tutelare in maniera diretta la riservatezza informatica e indirettamente la disponibilità ed integrità dello stesso sistema, ovvero dei programmi in esso contenuti, come si evince dalla circostanza aggravante di cui all'articolo 615 ter, comma 2, numero 3 c.p., il quale prevede la pena della reclusione da uno a cinque anni "se il colpevole per commettere il fatto usa violenza sulle cose o sulle persone, ovvero se è palesemente armato". Pertanto, la disposizione penale prevista dall'art. 615-ter c.p. non mira soltanto alla mera tutela del domicilio informatico dell'avente diritto, ma acquisisce anche una dimensione sovra-individuale, nella misura in cui incide su un gruppo indeterminato di individui e promuove il corretto funzionamento dei dati e dei sistemi telematici. Lo stesso si può dire in relazione al delitto previsto dall'articolo 617 sexies[56], che oltre a proteggere la libertà e la discrezione delle comunicazioni informatiche o telematiche, salvaguarda la disponibilità e l'integrità dei dati informatici, nel contenuto trasmesso con le comunicazioni stesse. In particolare, l'interesse collettivo della sicurezza in informatica viene minacciato dalle condotte di accesso abusivo a sistemi informatici di interesse pubblico e che gestiscono le cosiddette infrastrutture critiche, ma numerosi sono divenuti gli attacchi ai sistemi informatici

[54] M. CASELLATO, A. DI MAIO, A. LA MUSCATELLA, *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali* in Cassazione Penale, fasc.7, 1° luglio 2019

[55] Rinvio al paragrafo 3. 1 per una completa trattazione della fattispecie.

[56] Rinvio al par. 3.4.3 per una completa trattazione della norma in esame.

privati. Infatti, gli utenti svolgono sempre più spesso, attraverso i *computer*, attività socialmente, economicamente e giuridicamente rilevanti, basti pensare allo *smart-working*, che ha consentito a molti lavoratori, durante la pandemia, di spostare la sede di lavoro dagli uffici alle proprie case o alla didattica a distanza (DAD).

Tutti questi sistemi connessi a rete private o pubbliche, contengono importanti informazioni commerciali e professionali, dati personali e sensibili che possono riguardare anche soggetti terzi o che comunque vengono impiegati per fornire importanti servizi. La sicurezza dei dati e dei programmi contenuti nei sistemi informatici e, più in generale nelle esperienze virtuali, non sono più un esclusivo interesse privato, ma acquistano una nuova dimensione super individuale facente capo ad una schiera indeterminata di soggetti. Non è sufficiente tutelare la riservatezza informatica, il solo *jus excludendi* del titolare del sistema, ma occorre indirettamente proteggere l'interesse collettivo a regolare il funzionamento all'integrità e alla disponibilità dei sistemi: la sicurezza informatica. Bene, quest'ultimo, che il legislatore ha inteso proteggere in modo diretto mediante l'articolo 615-quinquies c.p.[57] e le disposizioni in materia di danneggiamenti informatici e, in via indiretta, con la previsione dei reati contro la riservatezza informatica.[58]

3. Analisi di alcune fattispecie: tutela dei nuovi beni giuridici e reati presupposto della responsabilità amministrativa da reato degli enti

3.1 L' accesso abusivo a un sistema informatico

Tra i fenomeni a cui la rivoluzione tecnologica ha dato vita, vi è quello dei cosiddetti *hackers*[59]. Il legislatore italiano aveva cercato di offrire tutela penale ai casi di accesso non autorizzato ricorrendo a fattispecie già esistenti nel Codice penale, tra queste: il reato di violazioni di domicilio, i reati di falsità personale e l'intercettazione abusiva di

[57] Rinvio al par. 3.3 per una completa trattazione della fattispecie.
[58] I. SALVADORI, *I reati informatici*…, cit., pag. 666.
[59] Questa espressione designa nel campo informatico quei soggetti in possesso di particolari conoscenze e capacità inerenti alle tecnologie informatiche che si introducono nei sistemi informatici altrui attraverso le reti telematiche, aggirando le protezioni elettroniche create dai proprietari di tali sistemi per tutelarsi dagli accessi indesiderati (Cfr. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, pag. 39.)

comunicazioni telefoniche e telegrafiche. Una tale operazione, tuttavia, si scontrava con i principi di legalità e tassatività rispetto ai nuovi fatti da punire, travalicando i limiti dell'interpretazione estensiva per tracimare nel procedimento analogico. Nel 1993 è stata introdotta nel Codice penale, tra le nuove disposizioni sulla criminalità informatica una nuova fattispecie che vieta l'accesso non autorizzato ad un sistema informatico. Il reato si colloca tra i delitti contro la inviolabilità di domicilio, subito dopo i reati di violazioni di domicilio (art. 614-615 c.p.) e di interferenze illecite nella vita privata (art. 615-bis). Questo dimostrerebbe di voler attribuire rilievo e tutela giuridica al domicilio informatico[60]. Quest'ultima posizione non è tuttavia unanimemente accolta e solo al termine dell'analisi della fattispecie potremo trarre le nostre conclusioni.

L' art. 615-ter c.p., al comma 1, prevede che : " 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 disposizione prevede, inoltre, una serie di circostanze aggravanti. La formulazione ricalca quella del delitto di violazione di domicilio, "riproducendo nella tipizzazione della condotta- figurativamente riferita al diverso contesto virtuale- l'alternativa dell'introduzione abusiva" ovvero del "mantenimento contro la volontà" del titolare dello *jus excludendi*"[61]. La norma sanziona due ipotesi alternative di condotta. Da un lato quella attiva di chi abusivamente si introduce in un sistema informatico o telematico, dall'altro lato, quella omissiva di chi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo[62]. Diversa soluzione propone G. Pica, il quale ritiene che l'ipotesi di abusivo mantenimento rappresenti una condotta commissiva poiché il mantenimento nel

[60]G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, pag. 40.
[61] L. PICOTTI, *Sistematica dei reati informatici…*, cit., pag. 52.
[62] La giurisprudenza nella sent. Tribunale Bari sez. uff. indagini prel., 11/12/2009 in banca dati De Jure ha affermato che per sistema informatico deve intendersi quel complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime sono caratterizzate 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) numerici ("codice"), in combinazioni diverse; tali "dati", elaborati automaticamente dalla macchina, generano le "informazioni" costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente. Nel caso di specie, era stato ritenuto "sistema informatico" il c.d. Re.Ge., il sistema che, attraverso tecnologie informatiche, raccoglie un insieme di dati per poi organizzarli al fine di fornirli agli uffici giudiziari autorizzati. Cfr. Tribunale Milano sez. III, 19/03/2007 in banca dati De Jure.

sistema è una condotta che perdura consapevolmente[63]. "La struttura della norma, non è infatti incentrata sulla sanzione dell'omesso abbandono del sistema, ma sul volontario mantenimento dell'accesso, nonostante il divieto espresso o tacito del titolare".[64] Per quanto attiene alla prima ipotesi, l'intrusione penalmente rilevante non consiste in un contatto con il sistema informatico o telematico. Questa interpretazione porterebbe, paradossalmente, alla conseguenza di configurare il reato anche nell'ipotesi di mero contatto fisico con un elaboratore. L' intrusione sarà penalmente rilevante nel caso in cui si configuri una sorta di dialogo logico o automatizzato con la parte *software* del sistema informatico[65]. Si tratta, pertanto, di una introduzione elettronica, poiché se anche l'agente compia inizialmente atti fisici di avvicinamento, dovrà servirsi della tecnologia per compiere l'azione finale[66]. "L'introduzione in un sistema informatico ai sensi dell'art. 615 ter c.p. consiste nell'ottenere l'accesso alla memoria interna del sistema, mettendosi così nella condizione di poter richiamare i dati e i programmi che vi sono registrati o che sono eventualmente contenuti su supporti esterni collegati con il sistema stesso, senza che sia a tal fine necessario superare ulteriori barriere logiche o fisiche"[67]. Solo a partire da questo momento si concretizza il rischio di pericolo per la riservatezza dei dati e dei programmi in vario modo presenti[68]. Possiamo pensare, ad esempio, all'accesso ad una rete Wi-Fi o

[63] G. PICA, *Diritto penale…*, cit., pag. 41-42.
[64] Ibidem.
[65] I. SALVADORI, *L'Accesso abusivo a un sistema informatico o telematico: una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica* in *Tutela della persona e delle nuove tecnologie* a cura di L. PICOTTI, Padova, 2013, pag. 135. Cfr. Cassazione penale sez. V, 08/07/2008, n.37322 in banca dati De Jure in cui la corte rileva che il termine accesso deve essere interpretato non tanto come collegamento fisico, ma quanto logico. Pertanto, per accesso deve intendersi non l'accensione dello schermo, ma il superamento della barriera di protezione del sistema che rende possibile il dialogo con il medesimo in modo che l'agente viene a trovarsi nella condizione di conoscere dati, informazioni e programmi.
[66] G. PICA, *Diritto penale…*, cit., pag. 41.
[67] C. PECORELLA, *Diritto penale…*, cit. pag.335.
[68] Ibidem.

ad un *account* di posta elettronica[69], ma anche nel profilo dell'utente di un *social network*[70].

La fattispecie assume pertanto i caratteri di un reato di pericolo astratto[71]. L'accesso può avvenire da vicino quando il soggetto accende il sistema e inizia a dialogare con il *computer*, ma potrebbe avvenire anche da lontano, collegandosi con il proprio *computer* al sistema da remoto tramite rete telematica. Occorre escludere, invece, sulla base del tenore letterale della norma, che la fattispecie si configuri esclusivamente nel caso in cui l'agente prenda conoscenza dei dati e dei programmi memorizzati nel sistema[72]. Il reato potrà pertanto dirsi consumato allorché l'agente sia riuscito ad eludere la protezione e ad accedere ai dati contenuti del sistema, indipendentemente dal fatto che ne abbia avuto effettiva conoscenza[73]. Concorda in tal senso anche la giurisprudenza[74]. In una recente sentenza la Corte ha rilevato che l'articolo 615-ter del Codice penale descrive un reato di mera condotta che si perfeziona con la violazione del domicilio informatico, mediante l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, a nulla rilevando che si verifichi un'effettiva lesione della riservatezza degli utenti. Nel caso di specie, il Tribunale ha condannato per il reato *de quo* l'imputato che, dopo essersi procurato la *password*, si era introdotto abusivamente

[69] Cassazione penale sez. V, 28/10/2015, n.13057 in banca dati De Jure. In questa sentenza la corte ha precisato che La casella di posta elettronica rappresenta un "sistema informatico", essendo uno spazio di memoria destinato alla memorizzazione di messaggi, o informazioni di altra natura (immagini, video), di un soggetto identificato da un account registrato presso un provider del servizio: pertanto, allorché questa "porzione di memoria" sia protetta mediante l'apposizione di una password, in modo tale da rivelare la chiara volontà dell'utente di farne uno spazio a sé riservato, ogni accesso abusivo concreta l'elemento materiale del reato di cui all'art. 615 ter c.p.

[70] Cassazione penale sez. V, 02/10/2018, n.2905 in banca dati De Jure; Cassazione penale sez. V, 23/03/2018, n.20485 in banca dati De Jure: In questo caso la corte rileva che nel caso di accesso abusivo a un profilo Facebook, l'indirizzo IP consente di individuare il colpevole.

[71] Si rimanda per un chiarimento su tale concetto a G. FIANDACA e E. MUSCO, *Diritto penale: parte generale,* Bologna, 2019, pag. 211 ss.

[72] C. PECORELLA, cit., pag. 336.

[73] G. PICA, cit., pag. 57.; In giurisprudenza: Tribunale Salerno sez. I, 17/01/2020, n.166 in banca dati De Jure Cassazione Penale, Sez. I, 27 settembre 2013 n. 40303 in penale.it; Corte di appello di Bologna, 30 gennaio 2008, in Guida al diritto, 48/2008; Corte appello Bologna sez. II, 27/03/2008 in banca dati DeJure; Cassazione penale sez. V, 06/02/2007, n.11689 in banca dati De Jure, Tribunale Bologna, 21/07/2005, n.1823 in banca dati De Jure; Cassazione penale sez. VI, 04/10/1999, n.3067 in banca dati De Jure. Una dottrina minoritaria: Mantovani, *Diritto penale parte speciale: delitti contro la persona*, CEDAM, Vicenza, 2019, pag. 571 ss. ritiene necessario che il soggetto prenda conoscenza dei dati. In tale ipotesi ci troveremmo al cospetto di un reato di danno.

[74] Tribunale Salerno sez. I, 17/01/2020, n.166 in banca dati De Jure.

nella casella di posta elettronica utilizzata dalla moglie, al fine di stampare delle *e-mail* da utilizzare nel giudizio di separazione personale.

La norma richiede, inoltre, che la condotta di intrusione sia attuata abusivamente. Questo significa che il soggetto attivo deve essersi introdotto nel sistema, nonostante il dissenso espresso o tacito di chi ha il diritto di escluderlo. Secondo parte della dottrina il richiamo all'avverbio abusivamente sarebbe pleonastico, poiché avrebbe la sola funzione di mettere in evidenza il momento dell'antigiuridicità del fatto[75]. Si tratterebbe di una clausola di illiceità espressa. Il giudice dovrebbe limitarsi ad accertare che l'introduzione non venga attuata con il consenso del titolare dell'*jus excludendi* o in presenza di altre scriminanti. Tale tesi, tuttavia, non sembra convincere. Il termine abusivamente, invece, rappresenta un elemento costitutivo del reato che contribuisce a descrivere il fatto tipico e a, delimitare l'ambito di applicazione, poiché in sua assenza la previsione avrebbe scarso significato. Infatti, le condotte di introduzione e di permanenza in un sistema informatico o telematico sono di per sé prive di autonoma carica offensiva[76]. Inoltre, la disposizione richiede la necessaria presenza di misure di sicurezza. Questa espressione non risulta particolarmente felice, poiché restringe eccessivamente l'ambito di applicazione del reato. Possiamo pensare al caso di un sistema informatico protetto da misure di sicurezza esterne ma non interne. Chi tenta l'accesso abusivo da vicino forzando le barriere fisiche sarà punibile, mentre chi tenti di introdursi nel sistema da lontano e non aggiri nessuna misura di protezione non sarà incriminabile. Altre ipotesi è quella di chi accede ad un sistema informatico non protetto, nonostante l'espresso divieto del proprietario. Dalla generale mancanza di misure di protezione non sembra potersi desumere la volontà del proprietario di lasciare a terzi il libero accesso al proprio sistema informatico. Infatti, secondo autorevole dottrina il fulcro dell'accesso abusivo non dovrebbe essere costituito dalla protezione del sistema, ma andrebbe ravvisato nell'elemento psicologico di chi agisce. Dovrebbe, pertanto essere sufficiente l'altruità del sistema (come lo è per l'altruità del domicilio) a rendere abusivo l'accesso che avvenga contro la volontà del proprietario.[77] Allo stato attuale, tuttavia, la norma richiede tale condizione.

[75] G. PICA, *Diritto penale…,* cit., pag. 38 ss.
[76] I. SALVADORI*, I reati informatici*…, cit., pag. 669.
[77] G. PICA, *Diritto penale*…, cit., pag. 48.

Fondamentale è stato l'intervento di dottrina e giurisprudenza nell'interpretazione di questo passaggio. In assenza di una definizione legale del requisito delle misure di sicurezza (che peraltro, specie, in ambito penalistico potrebbe creare non poca confusione), si ritiene che il reato si possa perfezionare se il soggetto si introduce, senza esservi autorizzato, nel sistema protetto da misure di sicurezza, indipendentemente dalla natura e dall'efficacia di quest'ultima, potendosi trattare di meccanismi di selezione anche solo di natura organizzativa[78]. Mentre un tempo si riteneva che l'apposizione di una semplice *password* non fosse sufficiente, ben presto, si è arrivati ad una conclusione differente[79]. La prima sentenza di merito che si è occupata della questione così affermava: " la normativa di cui all'art. 615 ter c.p.…ha inteso reprimere qualsiasi introduzione in un sistema informatico che avvenga contro la precisa volontà dell'avente diritto, e per rendere penalmente apprezzabile una simile contraria volontà è da ritenersi sufficiente qualsiasi mezzo di protezione, anche se facilmente aggirabile da persona mediamente esperta, ma che abbia comunque la caratteristica di rendere palese tale contraria volontà"[80]. In un'altra sentenza, la corte afferma che assume rilievo qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso, indipendentemente dalla sua capacità ed idoneità ad assicurare la protezione effettiva del sistema cui esso è apposto[81]. Peraltro, nel caso di accesso da vicino, non si può escludere che il concetto di misure di sicurezza possa essere riferito alle barriere e mezzi posti a protezione dell'ambiente fisico in cui si trova il sistema, come porte blindate o personale di vigilanza[82].

Il legislatore italiano, diversamente da altri (come quello spagnolo e tedesco) non ha però previsto espressamente, come elemento tipico della fattispecie, la violazione delle misure di sicurezza. Si è limitato a richiedere che il sistema sia protetto. Ciò significa che il reato si configura anche nel caso in cui l'accesso avviene quando la misura di sicurezza è momentaneamente disattivata, purché il soggetto sia a conoscenza della sua esistenza[83].

---

[78] Cfr. R. FLOR, *Art 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico* in "*Diritto penale e processo*" n.1/2008, pag. 106-112

[79] In dottrina, cfr. G. PICA, *Diritto penale…*, cit. pag. 53. In giurisprudenza, cfr. Cassazione penale sez. V, 08/07/2008, n.37322; Tribunale Milano sez. II, 28/09/2007 in banca dati De jure

[80] Sent. Tribunale di Torino, sez. IV, 7 febbraio 1998, consultabile sul sito www.penale.it

[81] Cass. Pen., Sez. V, 7 novembre 2000, n. 12732, Zara, pubblicata nella rivista Cassazione Penale, n.3/2002, pag. 1015 ss.

[82] G. PICA, *Diritto penale…*, cit. pag. 52. Cfr. Cassazione penale sez. V, 07/11/2000 in banca dati De Jure

[83] I. SALVADORI, *Quando un insider accede abusivamente a un sistema informatico o telematico? Le sezioni unite precisano l'ambito di applicazione dell'art. 615- ter c.p.*, in "*Rivista semestrale di diritto*

In una sentenza la Corte di Cassazione ha ritenuto sussistente il reato in esame nel caso in cui l'imputato dopo aver acceduto al profilo "*Facebook*" della ex moglie avvalendosi delle credenziali a lui note, aveva preso conoscenza delle conversazioni riservate della donna e aveva poi cambiato la "*password*" al fine di impedirle di accedere al *social network*[84]. Pertanto, per la corte, non rileva neppure la circostanza che le chiavi di accesso al sistema informatico protetto siano state comunicate all'autore del reato, in epoca antecedente rispetto all'accesso abusivo, dallo stesso titolare delle credenziali, qualora la condotta incriminata abbia portato ad un risultato certamente in contrasto con la volontà della persona offesa ed esorbitante l'eventuale ambito autorizzatorio. Tuttavia, questo tema richiede un approfondimento, che verrà affrontato nel paragrafo successivo.

Oltre all' ipotesi di introduzione abusiva, l'articolo 615-ter c.p. sanziona la condotta omissiva del mantenersi in un sistema contro la volontà espressa o tacita di chi ha il diritto di escluderlo. L'ipotesi è quella in cui il soggetto, dopo essersi introdotto in maniera casuale o autorizzata all'interno del sistema si trattiene nel sistema contro la volontà del titolare del diritto di escluderlo. Un esempio tipico è quello del tecnico informatico che viene autorizzato ad accedere a un sistema per verificarne il corretto funzionamento ma vi si trattenga consapevolmente dopo aver terminato il lavoro, con il rischio che possa svolgere delle attività contrarie a quelle per le quali era stato autorizzato[85]. La permanenza non deve intendersi in senso fisico, bensì come mantenimento della connessione inizialmente ottenuta in modo autorizzato o fortuito al sistema informatico o telematico[86]. Anche in queste ipotesi la permanenza deve avere ad oggetto un sistema protetto da misure di sicurezza[87]. Per tale motivo, nel caso in cui l'agente non sia a conoscenza del carattere protetto del sistema, "la sua condotta seppur meritevole di rimprovero penale, non potrebbe essere facilmente sussunta nella fattispecie di accesso abusivo, non integrandosi, tutti gli elementi soggettivi richiesti dal tipo (coscienza e volontà di mantenersi all'interno di un sistema protetto da misure di sicurezza)"[88]. L'agente deve essere consapevole di trovarsi in uno spazio protetto del sistema informatico all'interno

penale dell'economia", 2012, n. 1-2, pag. 384. In giurisprudenza, cfr. Cassazione penale sez. V, 07/11/2000, n.12732 in banca dati De Jure.

[84] Cassazione penale sez. V, 02/10/2018, n.2905 in banca dati De Jure

[85] C. PECORELLA, *Il diritto penale…*, cit., pag. 351

[86] I. SALVADORI, *L'accesso abusivo a un sistema informatico…*, cit., pag. 138.

[87] C. PECORELLA, *Il diritto penale…*, cit., pag. 349-350.

[88] I. SALVADORI, *L'accesso…*, cit., pag. 140.

del quale non è autorizzato a trattenersi. Non è richiesto, invece, che il soggetto superi le misure di protezione, essendo quest'ultima condotta sussumibile nell'ipotesi attiva dell'introduzione abusiva[89]. Il reato si consuma con la scadenza del termine fissato per uscirne. Questo termine viene individuato in base alle norme *extra* penali che disciplinano l'attività del soggetto agente che opera nel sistema informatico (ad esempio un contratto di lavoro) o sulla base dell'autorizzazione espressa o tacita concessa dal titolare. Mentre la condotta dell'introduzione deve essere realizzata abusivamente, la permanenza deve realizzarsi contro la volontà espressa o tacita di chi ha diritto di escludere. L'impiego di tale ultima formula, in luogo di quella del l'abusività, tuttavia, sembra soddisfare mere esigenze di stile[90]. Sicuramente sarebbe stata sufficiente un'unica qualifica di illiceità speciale per connotare entrambe le condotte. L' inciso "contro la volontà espressa o tacita di chi ha il diritto di escluderlo", per entrambe le condotte, secondo autorevole dottrina sarebbe stata più adeguata, poiché esplicitamente esprime l'esigenza di rispetto del diritto del titolare di disporre dei contenuti informatici, mentre l'avverbio abusivamente risulta più generico[91]. Non sembra configurabile il concorso materiale tra l'ipotesi di introduzione abusiva e quella del mantenimento abusivo, poiché quest'ultimo presuppone un'introduzione lecita nel sistema[92]. Dalla giurisprudenza, la scelta di incriminare la permanenza nel sistema è stata accolta positivamente poiché consentirebbe la repressione delle condotte illecite poste in essere da impiegati disonesti o *insider*, che si trattengono in un sistema informatico per finalità diverse da quelle consentite. Tuttavia, parte della dottrina non è dello stesso avviso. "Più corretta sembrerebbe piuttosto l'incriminazione, oltre all'ipotesi di accesso non autorizzato o abusivo ad un sistema informatico o ad una parte dello stesso, di quello commesso eccedendo i limiti dell'autorizzazione, come previsto ad esempio negli Stati Uniti, a livello tanto federale quanto statale"[93]. Questa formulazione sarebbe in linea con le prescrizioni degli organismi internazionali. In particolare, facciamo riferimento alla Convenzione *Cybercrime* del Consiglio d'Europa. Questa scelta consentirebbe di sanzionare, sia le intrusioni non autorizzate realizzate da *insider* e *outsider*, ma anche la permanenza contro la volontà del titolare dello *ius*

[89] I. SALVADORI, *Quando un insider…*, cit., pag. 380.
[90] I. SALVADORI, *I reati informatici…*, cit., pag. 670.
[91] G. PICA, *Diritto penale…*, cit., pag. 51.
[92] G. PICA, *Diritto penale…,* cit., pag. 42.
[93] I. SALVADORI*, L'accesso abusivo…*, cit., pag.143.

excludendi. Del resto, la permanenza in un *computer* consiste nel continuare ad accedere o restare connesso con il sistema oltre i limiti e termini dell'autorizzazione[94].

Occorre, infine, soffermarci sull'elemento psicologico che caratterizza tale reato. Non vi è dubbio che il delitto sia di natura dolosa, essendo necessario che la condotta sia supportata dall'intenzionalità. Si tratta tuttavia di dolo generico, visto che la fattispecie prescinde dalle finalità soggettive dell'agente. Non si può, tuttavia, escludere che la condotta venga realizzata in assenza di dolo ed eventualmente con colpa. Possiamo pensare ad un soggetto che abbia a disposizione un *computer* altrui ed accidentalmente attivi un programma automatico esistente in quel computer per l'accesso a banche dati remote. Il legislatore ha tuttavia ritenuto di non criminalizzare l'accesso abusivo che non sia doloso e non è quindi configurabile una responsabilità colposa.

___3.1.2 Alcune questioni giurisprudenziali riguardanti l'accesso abusivo a un sistema informatico

a) La minaccia dell'*insider*

Dottrina e giurisprudenza hanno dovuto affrontare la questione relativa alla configurabilità o meno del delitto previsto dall'art. 615- ter c.p., nel caso in cui il soggetto agente sia formalmente abilitato ad accedere ad un sistema informatico o telematico, ma vi si introduca o si mantenga al suo interno per uno scopo diverso da quello consentito. Nonostante il reato di accesso abusivo venga generalmente realizzato dagli *hacker*, che si introducono in un sistema, servendosi di un altro *computer* (c.d. accesso da lontano), sempre più diffusi sono in casi nei quali il soggetto agente è una persona legittimata ad avere accesso al sistema (c.d. accesso da vicino). Quest'ultimo tipo di accesso viene in genere realizzato da dipendenti (c.d. *insiders*), che possono facilmente aggirare le misure di sicurezza presenti. L'ipotesi più frequente è quella del soggetto che sia provvisto di autorizzazione delimitata alla consultazione o impiego di solo alcuni dei dati presenti, ma oltrepassi le condizioni previste. Tale questione ha dato luogo all'avvicendarsi di pronunce diverse tra loro. Un primo orientamento riteneva possibile configurare il reato

[94] I. SALVADORI, *Quando un insider…*, cit., pag. 395.

nell'ipotesi in esame[95]. A tal proposito citiamo la sentenza n. 12732 del 7.11.2000, Zara[96], ove era stato argomentato che "l'analogia con la fattispecie della violazione di domicilio deve indurre a concludere che integri la fattispecie criminosa (prevista dall'art. 615 ter c.p.) anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva". L'orientamento opposto ritiene che l'art. 615 ter c.p. si applichi soltanto agli *outsiders*, vale a dire ai soggetti non autorizzati ad introdursi nell'elaboratore[97]. Il reato non si configurerebbe nel caso degli *insiders* che, in quanto legittimati ad accedere al sistema informatico, non vi si potrebbero introdurre abusivamente. Questi ultimi risponderebbero soltanto per le autonome condotte illecite poste in essere a seguito dell'accesso autorizzato al sistema. Tale orientamento si basa sul fatto che la sussistenza della volontà contraria del titolare debba essere verificata con riferimento al momento dell'accesso del soggetto e non già con riferimento alle condotte successive[98]. Le Sezioni Unite hanno risolto il contrasto giurisprudenziale in favore del primo orientamento[99]. Il caso in esame riguardava un Maresciallo dell'Arma dei Carabinieri che si era introdotto abusivamente nel sistema informatico S.D.I (Sistema di Indagine), in dotazione alle forze di polizia e protetto da misure di sicurezza. Il soggetto si era introdotto nel sistema con abuso di poteri e in violazione dei doveri inerenti alla funzione di ufficiale di p.g. e delle direttive concernenti l'accesso al sistema. Le Sezioni Unite hanno ritenuto che non dovesse essere posta l'attenzione sulle finalità perseguite dal soggetto al momento in cui accede al sistema o vi si mantiene al suo interno. La

[95] In dottrina citiamo C. Pecorella, *Diritto penale…*, cit., pag. 349 ss. Cfr. Cass. n. 12732 del 7.11.2000 in Cass. pen. n. 3/2002; Tribunale Nola, 11/12/2007 in banca dati De Jure; Cassazione penale sez. V, 10/12/2009, n.2987 in banca dati De Jure; Cassazione penale sez. V, 13/02/2009, n.18006 in banca dati De Jure; Cassazione penale sez. un., 27/10/2011, n.4694 in banca dati De Jure; Cassazione penale sez. IV, 18/01/2011, n.24583 in banca dati De Jure; Cassazione penale sez. V, 08/07/2008, n.37322 in banca dati De Jure; Tribunale Milano sez. II, 28/09/2007 in banca dati De Jure ; Tribunale Viterbo, 05/07/2005 in banca dati De Jure.

[96] La sentenza è consultabile nella rivista "Cassazione Penale", n.3/2002, pag.1015 ss.

[97] Cfr. Cassazione penale sez. VI, 13/10/2010, n.38667 in banca dati De Jure; Cassazione penale sez. VI, 08/10/2008, n.39290 in banca dati De Jure; Cassazione penale sez. V, 29/05/2008, n.26797 in banca dati De Jure; Tribunale Nola sez. uff. indagini prel., 14/12/2007, n.488 in banca dati De Jure; Tribunale Viterbo, 05/07/2005 in banca dati De Jure.

[98] Cass., sez. V, 20.12.2007, n. 2534 in banca dati De Jure

[99] Cass. Sez. un., 7 febbraio 2012 n. 4694, consultabile sul sito www.dirittopenalecontemporaneo.it

disposizione per affermarne la responsabilità ai sensi dell'articolo 615 ter c.p. richiede di verificare la contraria volontà da parte del titolare dello *ius excludendi*, indipendentemente dalle finalità dell'agente. La Corte, pertanto, ritiene che l'indagine debba concentrarsi sul profilo oggettivo dell'accesso e del trattenimento nel sistema informatico, per verificare se il soggetto possa ritenersi autorizzato ad accedervi e permanervi. La verifica deve concentrarsi sulla sussistenza o meno della violazione da parte dell'agente delle prescrizioni impartite dal *dominus* circa l'uso del sistema. La condotta di accesso abusivo si deve ritenere integrata "allorquando il soggetto violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito". La chiave di volta della fattispecie penale viene individuata dalla corte, nella "violazione" dello *ius excludendi* del titolare del sistema informatico. "Tale violazione, secondo i Giudici, esprime il disvalore essenziale del fatto, indipendentemente dai motivi o dai propositi perseguiti dall'agente, dall'accesso reale a dati o informazioni e dalla loro natura, nonché dal loro successivo utilizzo, trovando il reato consumazione nella realizzazione delle condotte tipiche e, con riferimento a quella di permanenza *invito domino*, nella violazione delle disposizioni del titolare"[100]. La Corte è giunta a queste affermazioni sulla base di un'interpretazione estensiva dell'avverbio "abusivamente". Tale termine indicherebbe non solo l'accesso senza autorizzazione ad un sistema, ma anche quello realizzato eccedendo i limiti dell'autorizzazione. Il fatto è pertanto rilevante penalmente in sé, indipendentemente da condotte ulteriori commesse dal soggetto di cui eventualmente dovrà rispondere. Per poter stabilire quando un soggetto abilitato abbia ecceduto i limiti dell'autorizzazione, sarà necessario che le prescrizioni impartite dal titolare prevedano in modo chiaro i limiti dell'accesso e della permanenza in un sistema. Nei casi in cui manchino tali disposizioni o siano comunque troppo generiche ed equivoche, al punto da rendere arduo al soggetto abilitato stabilire se la sua condotta si ponga in contrasto con gli interessi del titolare, il giudice dovrà escludere l'applicabilità dell'articolo 615 ter c.p. In conclusione, in base all'orientamento espresso dalle Sezioni Unite, l'agente potrà solo effettuare accessi o operazioni per le quali sia stato espressamente autorizzato e nei limiti

[100] FLOR R., *La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere* in Diritto penale e processo n.4/2018

di essi. Qualora il soggetto oltrepassi tali limiti sarà chiamato a rispondere del reato di accesso abusivo a sistema informatico o telematico.

b) L'accesso abusivo realizzato dal pubblico ufficiale o dall'incaricato di pubblico servizio

Gli orientamenti giurisprudenziali immediatamente successivi alla decisione delle Sezioni Unite Casani hanno evidenziato alcune discordanze in merito all'applicazione del criterio "oggettivo", relativo alla "violazione delle disposizioni del titolare", ai pubblici ufficiali ed agli incaricati di pubblico servizio, manifestando l'esigenza di ulteriori specificazioni. Nella sentenza Carnevale, la corte aveva ritenuto che nel caso in cui l'agente sia un pubblico dipendente "non può non trovare applicazione il principio di cui alla L. 7 agosto 1990 n. 241, art. 1, in base al quale l'attività amministrativa persegue fini determinati dalla legge ed è retta da criteri di economicità, efficacia, imparzialità, pubblicità, trasparenza, secondo le modalità previste dalla presente legge e dalle disposizioni che disciplinano singoli procedimenti, nonché dai principi dell'ordinamento comunitario" [101]. Ne deriva la ontologica incompatibilità dell'accesso al sistema informatico senza il rispetto di tali principi, in quanto fuoriuscente dalla *ratio* del conferimento del relativo potere. La condotta del pubblico ufficiale che accede al sistema per scopi diversi da quelli istituzionali deve considerarsi "abusiva" in base ai principi generali che governano l'azione amministrativa ed è pertanto applicabile l'art. 615-ter, comma 2, n.1. Viceversa, la sentenza Mecca affermava fosse necessario, anche in relazione ai pubblici ufficiali, dimostrare che l'agente avesse violato specifiche prescrizioni impartite dal titolare del sistema[102]. Il richiamo ai principi generali di cui all'art. 1, l. 7 agosto 1990, n. 241 avrebbe infatti svuotato nella sostanza il riferimento a parametri di natura oggettiva operato dalla sentenza Casani.

Nel 2017 le Sezioni Unite sono intervenute per dirimere il contrasto nella nota sentenza Savarese[103]. Il caso è originato dal fatto commesso da un funzionario di cancelleria, il quale, sebbene legittimato ad accedere al Registro informatizzato delle notizie di reato - c.d. Re.Ge. - conformemente alle disposizioni organizzative della Procura della

[101] Cass. pen., Sez. V., 24 aprile 2013, n. 22024, Carnevale, in sites.les.univr.it
[102] Cass. pen., Sez. V., 20 giugno 2014, n. 44390, Mecca in sites.les.univr.it
[103] Cass., sez. unite, sent. 18 maggio 2017 n. 41210, in diritto penale contemporaneo, fasc. 10/2017

Repubblica presso cui prestava servizio, aveva preso visione dei dati relativi ad un procedimento penale per ragioni estranee allo svolgimento delle proprie funzioni. La questione di diritto sottoposta alle Sezioni unite è stata la seguente: "Se il delitto previsto dall'art. 615-ter c.p., comma 2, n. 1, sia integrato anche nella ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio, formalmente autorizzato all'accesso ad un sistema informatico o telematico, ponga in essere una condotta che concreti uno sviamento di potere, in quanto mirante al raggiungimento di un fine non istituzionale, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative". La corte, in via preliminare, decide di delimitare il campo di indagine al secondo comma, n.1 dell'art. 615-ter. Il collegio rileva che si tratta di una circostanza aggravante esclusivamente soggettiva, nel senso che descrive la condotta punibile in quanto posta in essere da determinati soggetti. Il pubblico ufficiale, l'incaricato di pubblico servizio, l'investigatore privato e l'operatore del sistema possono rispondere del reato solo in forza di questa previsione e per tali soggetti il reato è sempre aggravato. La *ratio* sottesa all'aggravante è facilmente rintracciabile nel rapporto di agevolazione o nel maggiore stigma che lega la qualifica ricoperta alla commissione del fatto tipico[104]. In primo luogo, le Sezioni Unite si soffermano sulla nozione di c.d. sviamento di potere. Tale nozione rappresenta una delle tipiche manifestazioni della più generale categoria del vizio di "eccesso di potere" e ricorre quando l'atto amministrativo non persegue un interesse pubblico, ma un interesse privato. In particolare, incorre nello sviamento di potere il pubblico funzionario che nella sua attività concreta "persegua una finalità diversa da quella che gli assegna in astratto la legge sul procedimento amministrativo"[105]. La Corte passa poi in rassegna le principali norme che delineano lo *status* della persona dotata di funzioni pubbliche. Vengono in rilievo, anzitutto, alcune disposizioni del Testo Unico sul pubblico impiego e del Codice di comportamento dei pubblici dipendenti, che specificano i principi già enunciati dalla legge sul procedimento amministrativo. Inoltre, i giudici fanno riferimento agli articoli 54, 97 e 98 della Costituzione, che richiedono al dipendente l'adesione ai "principi di etica pubblica". Tali previsioni normative, insieme ad altre

[104] R. BERTOLESI, *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere* in diritto penale contemporaneo, fasc. 10/2017; R. FLOR*, La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere* in Diritto penale e processo n.4/2018.
[105] Art. 1, L. 241/1990

disposizioni settoriali (come, ad esempio, quelle relative all'utilizzo dei registri informatizzati da parte dell'amministrazione della giustizia) rendono evidente che i pubblici dipendenti e gli incaricati di pubblico servizio sono tenuti ad agire per il perseguimento delle finalità istituzionali in vista delle quali il rapporto funzionale è instaurato. Venendo più nello specifico al tema controverso, le Sezioni Unite sottolineano come la giurisprudenza di legittimità si sia da tempo orientata verso la riconducibilità dello sviamento di potere all'interno delle nozioni di *abusività* della condotta e di fatto commesso con violazione dei doveri di ufficio. Ciò emerge con particolare evidenza nella giurisprudenza sul reato di abuso di ufficio. Si legge infatti nella sentenza a Sezioni Unite Rossi che: "ai fini della configurabilità del reato di abuso d'ufficio, sussiste il requisito della violazione di legge non solo quando la condotta del pubblico ufficiale sia svolta in contrasto con le norme che regolano l'esercizio del potere, ma anche quando la stessa risulti orientata alla sola realizzazione di un interesse collidente con quello per il quale il potere è attribuito, realizzandosi in tale ipotesi il vizio dello sviamento di potere, che integra la violazione di legge poiché lo stesso non viene esercitato secondo lo schema normativo che ne legittima l'attribuzione"[106]. Alla luce di queste essenziali considerazioni, la Corte osserva che l'accesso ad un sistema informatico per ragioni estranee a quelle di ufficio si traduce per il pubblico ufficiale in una condotta abusiva, ponendosi in un rapporto di "*ontologica incompatibilità*" con la funzione svolta. Da ultimo, la Corte ha cura di precisare che l'art. 615-*ter* co. 2 n. 1 c.p. non si applica al pubblico dipendente che agisce al di fuori della qualifica di pubblico ufficiale o di incaricato di pubblico servizio. In tale ultimo caso, tornerà pertanto ad applicarsi l'ipotesi base di reato di cui al primo comma dell'art. 615 *ter* c.p.

c) Critiche e prospettive di riforma dopo la sentenza Savarese

La pronuncia non è andata esente da critiche. In particolare, autorevole dottrina rileva che sostenere che, in mancanza di prescrizioni del titolare possano valere i principi generali che governano l'attività della pubblica amministrazione sposta la tutela da una dimensione prevalentemente privatistica ad una pubblicista, tipica dei reati contro la

[106] Cass. SS. UU., 29 settembre 2011, in *Banca dati Dejure.*

pubblica amministrazione[107]. In questo modo viene tradita la *ratio* del delitto ex art. 615-ter c.p. e della scelta di prevedere la presenza delle misure di sicurezza, tra gli elementi costituti del reato. Se applicassimo tali rilievi al caso affrontato dalle Sez. Unite, si giungerebbe a una conclusione diversa da quella prospettata. In altri termini, il pubblico ufficiale che accede con le proprie credenziali di autenticazione al sistema, mantenendosi all'interno di questo in difetto di una regolamentazione interna, anche solo su base consuetudinaria, che delimiti oggettivamente l'ambito del mantenimento non commetterebbe il reato di accesso abusivo, poiché non sarebbe rintracciabile la violazione della *voluntas domini*. Le stesse "operazioni di natura ontologicamente diversa", ferma restando l'indeterminatezza di tale locuzione, devono essere valutate in relazione all'ambito di operatività discrezionalmente delimitato o meno dal titolare e al rapporto funzionale di cui il soggetto è investito nei confronti del sistema. Se a fini organizzativi, il cancelliere è autorizzato ad accedere a tutti i dati archiviati in un data-base, si dovrebbe desumere che il titolare del sistema non ha inteso apportare limitazioni. Pertanto, se il cancelliere prende visione dei fascicoli che, in quel momento, non ha in carico, non sta realizzando "operazioni di natura ontologicamente diversa", in quanto rientrano nel suo ambito di operatività legittimamente conferito dal titolare del sistema, a prescindere dai motivi che reggono la condotta del pubblico ufficiale. Questo ultimo potrebbe eventualmente incorrere nella commissione di altri reati, fra cui l'abuso d'ufficio o la rivelazione di segreti d'ufficio, ovvero la corruzione per l'esercizio della funzione, ricorrendone i requisiti. Quindi, l'abuso del pubblico ufficiale (o la violazione dei doveri inerenti alla funzione), dovrebbe essere tenuta distinta dall'abusività dell'accesso o del mantenimento senza autorizzazione nel sistema informatico. Il pubblico ufficiale o l'incaricato di pubblico servizio, ad esempio, potrebbe abusare della propria qualifica o posizione, senza violare le regole relative all'accesso o al mantenimento in un sistema informatico e, viceversa, potrebbe violare queste ultime senza di per sé abusare dei poteri o violare i doveri inerenti alla loro funzione o servizio. L'accoglimento della

[107] Si veda R. FLOR*, La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere* in Diritto penale e processo n.4/2018 e ancora M. CASELLATO, A. DI MAIO, A. LA MUSCATELLA, *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali* in Cassazione Penale, fasc.7, 1° luglio 2019.

interpretazione ermeneutica prospettata nel caso Sevarese ha comportato l'emersione di un parametro estraneo alla struttura obiettiva della norma incriminatrice, e l'adozione in *malam partem* dell'ambito applicativo di questa disposizione penale, con (presunta) violazione del principio di legalità[108]. "Dunque, la condotta dell'imputata, che si è esplicata nella mancata osservanza delle disposizioni previste dal Registro delle notizie di reato (Re.Ge.), nella misura in cui ha prodotto un legittimo accesso informatico ed ha visualizzato determinati contenuti per scopi estranei alla sua funzione, sebbene sia certamente idonea ad integrare i criteri specializzanti di cui all'art. 615-ter, secondo comma, n. 1, c.p., sembrerebbe non sufficiente per includere i requisiti della fattispecie penale-base"[109]. Inoltre, il ragionamento logico-giuridico espresso dalla Corte di cassazione sembra confliggere anche con il principio di offensività, che subordina l'attuazione della disposizione penale all'effettiva lesione o messa in pericolo del bene giuridico protetto dal legislatore, e delimita così l'ambito di punibilità della fattispecie[110]. Nel caso di specie, l'azione compiuta dal dipendente pubblico non presenterebbe i tratti dell'abusività poiché l'ingresso e la permanenza nello spazio digitale sono avvenuti nell'integrale rispetto dei parametri oggettivi di abilitazione. In tal modo, risulterebbe assente l'offesa all'interesse tutelato, che opera nelle ipotesi in cui gli atti commessi dall'agente siano obiettivamente incompatibili con il titolo di accesso, e non in base a criteri teleologici, la cui inosservanza acquisirebbe, al massimo, rilievo sotto il profilo esclusivamente deontologico[111].

Le perplessità suscitate da questa sentenza possono costituire terreno fertile per pensare una riforma dell'illecito penale[112]. Una possibile soluzione potrebbe essere rappresentata da una selezione degli atti criminosi che integrano il reato previsto dall'art. 615-ter c.p. In tal senso, la soluzione prospettata da molti legislatori nazionali (ad esempio, quello

[108] CASELLATO M., DI MAIO A., LA MUSCATELLA A., *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali* in Cassazione Penale, fasc.7, 1° luglio 2019

[109] Ibidem

[110] CASELLATO M., DI MAIO A., LA MUSCATELLA A., *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali* in Cassazione Penale, fasc.7, 1° luglio 2019

[111] Ibidem

[112] Facciamo riferimento alle riflessioni di: CASELLATO M., DI MAIO A., LA MUSCATELLA A., *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali* in Cassazione Penale, fasc.7, 1° luglio 2019

spagnolo, austriaco) ha circoscritto i profili di rilevanza penale ai casi di accesso non autorizzato ai programmi ed ai sistemi informatici attraverso la diretta elusione delle misure di sicurezza. Questa formulazione consentirebbe una maggiore comprensione del rapporto di conflittualità intersoggettiva da parte dell'agente nel momento in cui, privo di autorizzazione, elude le misure di protezione e penetra in maniera abusiva nello spazio digitale altrui. Questa diversa ricostruzione dell'illecito penale condurrebbe all'esclusione del ricorso al diritto penale non solo nel caso in cui il soggetto attivo si trattenga nello spazio digitale in seguito ad un'intrusione fortuita od inizialmente consentita, ma anche qualora il dipendente od *insider*, munito di proprie credenziali di autenticazione, ecceda i limiti previsti dalla legge o da regolamenti e si insinui in settori informatici non protetti per consultare informazioni e dati altrui. Sotto tale profilo, una possibile prospettiva di riforma potrebbe consistere nella riformulazione di tale norma attraverso la delimitazione dei confini penalmente rilevanti alle sole ipotesi in cui il trasgressore effettui l'accesso abusivo nel sistema informatico con il preciso scopo di procurarsi in maniera illecita dati informatici, secondo quanto stabilito dall'art. 2, par. 2, della Convenzione *Cybercrime* o dal Codice penale austriaco. Invero, il fatto tipico verrebbe integrato dal soggetto attivo qualora penetri abusivamente nella sfera digitale altrui, giustificando così l'obiettivo interesse all'esclusione di terzi.

d) Le Sezioni Unite escludono l'*overruling*

Aldilà delle prospettive di riforma ipotizzabili, la sentenza Savarese apre una ulteriore questione, ossia quella dell'applicazione retroattiva di un *overruling* sfavorevole. Infatti, le Sezioni unite sembrano essersi rimangiate il precedente principio di diritto secondo cui ‘‘integra la fattispecie (...) la condotta di accesso (...) posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo (...) gli scopi e le finalità che soggettivamente hanno motivato l'ingresso", espresso nella sentenza Casani.

In estrema sintesi, il quadro intertemporale della vicenda può essere riassunto in tre momenti cronologicamente susseguenti: quello in cui si assiste al contrasto sincronico in seno alla Corte di cassazione; quello di vigenza della prima pronuncia delle Sezioni unite:

la sentenza Casani; infine, quello del possibile *overruling* sfavorevole determinato dalla seconda pronuncia delle stesse Sezioni unite. La condotta della ricorrente, nel caso Sevarese, si colloca tra il secondo ed il terzo momento; più precisamente, due mesi dopo la pronuncia delle Sezioni unite Casani nel senso della rilevanza del solo c.d. abuso oggettivo del titolo di legittimazione e cinque anni prima che le Sezioni unite attribuissero rilievo anche alle finalità perseguite dall'agente. La giurisprudenza della Corte di Strasburgo richiede, affinché´ vi sia una legittima base legale per l'incriminazione e quindi affinché´ si possa escludere la violazione dell'art. 7 della Convenzione EDU, che la condanna del soggetto fosse (anche) ragionevolmente prevedibile. Il mutamento giurisprudenziale sfavorevole e imprevedibile determina la violazione dell'art. 7 della Convenzione.

Sul presunto *overruling* sfavorevole si è espressa la Cassazione penale, sez. V nella sentenza n. 37857/2018 in un caso similare[113]. La corte rileva che la ragionevole prevedibilità di una interpretazione giurisprudenziale rappresenta il discrimine fra condotte che possono essere punite anche in ragione di una interpretazione che si è affermata in epoca successiva al loro compimento e condotte che debbono andare, invece, esenti da pena. Nel caso di specie, le argomentazioni delle Sez. Unite non costituivano un'innovazione giurisprudenziale. Bensì dopo aver operato una ricognizione degli indirizzi giurisprudenziali contrapposti, i giudici hanno optato per l'interpretazione più estensiva, già oggetto di numerose pronunce. La non prevedibilità di una decisione giudiziale che ne preclude l'applicazione retroattiva deve certamente escludersi in una situazione di contrasto giurisprudenziale, in cui l'esito interpretativo, seppur controverso, è comunque presente. Secondo l'opinione della Corte, pertanto, nessuna rilevanza assume la circostanza che l'orientamento adottato dalle Sezioni Unite sia quello minoritario, atteso che l'unico aspetto rilevante è che al momento in cui ha posto in essere la propria condotta, l'imputato potesse ragionevolmente prefigurare l'astratta integrazione degli estremi della fattispecie criminosa, nel caso di specie quelli di cui all'art. 615-ter c.p. Un'altra recente sentenza ci offre lo spunto per ulteriori riflessioni, si tratta della sentenza cass. penale, sez. V n. 47510/2018[114]. La corta si pronuncia in merito al possibile *overruling* operato dalla sentenza Savarese, vista la precedente pronuncia delle sez. unite

[113] Cassazione penale sez. V - 24/04/2018, n. 37857 in banca dati DeJure
[114] Cassazione penale sez. V, 09/07/2018, n. 47510 in banca dati DeJure

nel caso Casani. I giudici rilevano che dalla motivazione della sentenza Savarese emerge chiaramente che la giurisprudenza formatasi in epoca successiva alla sentenza Casani aveva manifestato l'esigenza di ulteriori precisazioni e specificazioni, in funzione estensiva, della portata del principio di diritto espresso. Le Sezioni Unite Savarese hanno puntualizzato ed approfondito l'analisi della precedente sentenza Casani, senza affatto ribaltarne l'impostazione ermeneutica, come espressamente affermato[115].

In particolare, con la sentenza Savarese è stato approfondito e specificato il concetto di "operazioni ontologicamente estranee" a quelle consentite, qualora la condotta criminosa sia posta in essere da un pubblico ufficiale o da un incaricato di pubblico servizio. I giudici pertanto escludono che si possa configurare un'ipotesi di *overruling* sia perché l'orientamento da ultimo espresso dalle Sezioni Unite con la sentenza Savarese si è inserito nella fisiologica evoluzione dell'approfondimento ermeneutico di un profilo non specificamente analizzato dalla precedente sentenza Casani, sia perché non si era mai formato, neanche dopo la sentenza Casani, alcun univoco orientamento, da parte delle Sezioni semplici della Corte. L'esclusione dell'*overruling* è stata poi ribadita successivamente in altre sentenze. Infatti, quella dei pubblici ufficiali o incaricati di pubblico servizio che hanno realizzato condotte ascrivibili all'ambito dell'art. 615-ter dopo la sentenza Casani e prima della sentenza Savarese e che lamentano una lesione dell'art. 7 per l'applicazione del mutato orientamento sfavorevole della giurisprudenza è tutt'altro che infrequente. Nei casi, fino ad oggi sottoposti alle corti, i giudici, tuttavia, hanno escluso l'ipotesi dell'*overruling*[116].

___3.1.3 La problematica individuazione del bene giuridico tutelato: una fattispecie paradigma

Abbiamo affrontato in linea generale la questione relativa al bene giuridico in particolare, tutelato dalle fattispecie oggetto della nostra indagine[117], è interessante soffermarci, in particolare, ad indagare la questione con riferimento all'accesso abusivo ad un sistema

[115] pag. 5 della motivazione: "Ritiene il Collegio che lo spunto fornito dalla vicenda processuale debba indurre a puntualizzare alcuni dei passaggi della precedente decisione delle Sezioni Unite C".
[116] Cass. penale, sez. VI, 23/11/2021 n. 5541 in banca dati DeJure; Cassazione penale sez. V, 30/04/2021, (ud. 30/04/2021, dep. 06/07/2021), n.25683 in banca dati DeJure; Cassazione penale sez. I, 27/04/2021, (ud. 27/04/2021, dep. 18/06/2021), n.24095 in banca dati DeJure
[117] Rinvio ai paragrafi 2, 2.1 e 2.2 per una trattazione generale del bene giuridico.

informatico, norma paradigma nella lotta alla criminalità. In questo paragrafo delineeremo le varie teorie elaborate in ordine al bene giuridico tutelato per cercare di pervenire ad una conclusione. Una prima tesi, partendo dalla collocazione della fattispecie tra i delitti contro l'inviolabilità del domicilio, ha ritenuto che il bene giuridico tutelato dalla norma dovesse essere individuato nel domicilio informatico[118]. Un appoggio a tale orientamento è stato rintracciato nella relazione ministeriale, dove si legge: "I sistemi informatici e telematici costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del Codice penale". La stessa circostanza che la tutela sia accordata solo ai sistemi informatici o telematici "protetti da misure di sicurezza" indicherebbe la volontà di assimilare il sistema informatico o telematico a un luogo chiuso e riservato, così come accade per il domicilio tradizionale[119]. Questa tesi ha trovato appoggio anche in giurisprudenza[120] ma dottrina prevalente respinge questa teoria in quanto i sistemi informatici non possono in alcun modo essere assimilati ai luoghi privati menzionati nell'art 614 c.p. Il concetto di domicilio, infatti, "trasuda fisicità e spazialità", mentre la criminalità informatica si caratterizza per "l'assenza di fisicità"[121]. In particolare, una simile teoria impedirebbe una tutela penale a sistemi informatici, quali quelli industriali o commerciali, i cui dati vengono trattati solo per finalità di tipo scientifico o culturale o per fornire determinati servizi agli utenti, e quindi privi di un contenuto personalistico e privatistico[122]. Inoltre, se accogliessimo questa teoria, non sarebbe comprensibile il requisito prescritto dal legislatore circa la presenza di misure di sicurezza, dovendo essere sufficiente il dissenso all'accesso mostrato in qualunque modo[123]. Altra parte della dottrina ha sostenuto che il reato di accesso abusivo a un sistema informatico tutelerebbe l'interesse giuridico

[118] In dottrina G. PICA, *Diritto penale*…cit., pag. 31 ss.; In giurisprudenza Cass., sez. V, 8 luglio 2008, in Diritto penale e processo, 2009, p. 720.
[119] C. PIERGALLINI*, I delitti contro la riservatezza informatica* in *Trattato di diritto penale parte speciale* a cura di G. MARINUCCI e E. DOLCINI, CEDAM, Vicenza, 2015, pag. 771
[120] Cfr. Cassazione penale sez. V, 19/02/2020, n.17360 in banca dati De Jure; Cassazione penale sez. II, 29/05/2019, n.26604 in banca dati De Jure; Cassazione penale sez. II, 14/01/2019, n.21987 in banca dati De Jure; Cassazione penale sez. V, 30/09/2008, n.1727 in banca dati De Jure; Corte appello Bologna sez. II, 27/03/2008 in banca dati De Jure; Tribunale Trapani, 22/12/2005 in banca dati De Jure; Cass. 7 novembre 2000, in Cassazione penale, 2002, 1015; Cassazione penale sez. VI, 04/10/1999, n.3065 in banca dati De Jure.
[121] C. PIERGALLINI, *I delitti*…, cit., pag. 772
[122] C.PECORELLA*, Il diritto penale dell'informatica*, CEDAM, Padova, 2006, pp. 315 ss.
[123] C. PECORELLA, *Il diritto*…, cit., pag. 317

dell'integrità dei dati e dei programmi informatici[124]. Se venisse così interpretata, la *ratio* della disposizione sarebbe quella di prevenire un danno al sistema informatico, che risulta avere un rilievo secondario poiché chi accede ad un sistema in maniera illecita è mosso principalmente dall'intenzione di carpire informazioni[125]. Inoltre, la critica mossa a tale teoria è che se il bene giuridico tutelato fosse quello dell'integrità dei sistemi sorgerebbero problemi di concorso di norme tra il delitto di accesso abusivo a un sistema informatico, quale forma tentata di lesione del bene giuridico dell'integrità, ed i reati in materia di danneggiamento informatico, che tutelano la sicurezza informatica. Infine, risulterebbe incomprensibile la scelta di delimitare l'ambito della tutela penale ai soli dati e programmi contenuti in sistemi protetti da misure di sicurezza[126]. Pertanto, neanche questa teoria può convincerci. Altra teoria ha invece individuato il bene giuridico nell'interessa alla indisturbata fruizione del sistema da parte del gestore, sulla base di un parallelismo con l'art. 637 c.p., che reprime l'accesso abusivo nel fondo altrui[127]. Questa tesi non convince poiché non sempre l'accesso o la permanenza non autorizzata danno luogo ad un pregiudizio alla possibilità di utilizzare il sistema in tutte le sue molteplici funzioni da parte del gestore[128]. Una quarta teoria individua il bene giuridico protetto nella riservatezza dei dati e dei programmi contenuti in un sistema informatico[129]. Quello che non convince è il fatto che una simile interpretazione escluderebbe il reato ex art. 615 ter c.p. nei casi di intrusione in un sistema informatico che, pur essendo protetto da misure di sicurezza, non contenga alcun dato o informazione personale o riservata. Infatti, in tal senso la protezione verrebbe trasferita dal sistema informatico o telematico ai suoi contenuti, ma una simile interpretazione sembra tradire la lettera della norma. Inoltre, si deve aggiungere che il bene giuridico della riservatezza nella moderna società dell'informazione travalica i confini della sua originaria dimensione personalistica e si collega strettamente a quello di natura collettiva della sicurezza informatica. In conclusione, ci sembra corretto sostenere la tesi secondo cui il nuovo bene giuridico, sia

[124] Questa teoria è esposta da M. MANTOVANI nel suo scritto *Brevi note a proposito della nuova legge sulla criminalità informatica* in *Critica del diritto*, n. 4/1994, pag. 17 ss. L'autore trova, in particolare, un sostegno alla sua teoria nel Codice penale francese e nella dottrina francese.
[125] C. PECORELLA*, Il diritto*…, cit., pag. 321.
[126] In tal senso: C. PECORELLA, Il diritto…, cit. pag. 321 e I. SALVADORI, I reati informatici…, cit., pag. 691
[127] BERGHELLA- BLAIOTTA, *Diritto penale dell'informatica e beni giuridici tradizionali* in *Cassazione penale*, 1995, pag. 2333.
[128] C. PIERGALLINI, *I delitti*…, cit., pag. 773.
[129] C. PECORELLA*, Il diritto*…, cit., pag. 322 ss.

quello della riservatezza informatica[130], da intendersi come "una sfera speciale di protezione, che ha ad oggetto l'interesse all'esclusività dell'accesso ad uno o più spazi informatici, a prescindere dalla natura dei dati e delle informazioni ivi archiviati, nonché alla loro disponibilità rispetto ad illegittime interferenze da parte di terzi soggetti"[131]. In questo senso l'articolo 615 ter si configura come delitto di pericolo astratto.

3.2 Detenzione, diffusione e installazione abusiva di apparecchiature, codici, e altri mezzi atti all' accesso a sistemi informatici o telematici

L'articolo 615-quater del Codice penale prevede il reato di detenzione, diffusione e installazione abusiva di apparecchiature, codici, e altri mezzi atti all' accesso a sistemi informatici o telematici. Nella formulazione precedente alla legge 238 del 2021 era previsto, invece, il più limitato reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. Tali correttivi sono stati introdotti, ricordiamo, al fine di adeguare la normativa italiana, relativa agli attacchi contro i sistemi informatici, alla direttiva 2013/40 /UE. Oltre a modificare la rubrica, l'art. 19 della 238 del 2021 ha esteso il campo di applicazione e modificato il regime sanzionatorio del reato. La norma, nel testo previgente, disponeva che:" Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a euro 5.164". A seguito della novella, è stato ampliato il novero di condotte idonee a integrare la fattispecie di reato e aggiunti nuovi oggetti materiali. Il testo prevede che: "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164". Possiamo notare come siano

[130] I. SALVADORI*, I reati informatici…*, cit. pag. 692
[131] R. FLOR, "*Riservatezza informatica*" in Enciclopedia treccani.it, 2017

state aggiunte alle condotte sanzionabili anche la "detenzione, la produzione, l'importazione e la messa a disposizione di altri in altro modo, l'installazione" oltre che di codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico anche di "apparati, strumenti, parti di apparati o parti di strumenti". L'oggetto materiale della condotta è stato esteso, quindi, anche ad apparati e strumenti, ossia quelle apparecchiature che servono per accedere al sistema informatico. La pena della reclusione, prima prevista fino ad un anno, è stata elevata sino a due anni ed è stato modificato anche l'ultimo comma dell'articolo, che ora prevede un aggravamento di pena da uno a tre anni nel caso in cui ricorrano le circostanze previste dall'art. 617 quater, comma quarto, cod. pen. Un tempo invece era previsto l'aggravamento di pena da uno a due anni nel caso in cui ricorrevano le circostanze aggravanti previste nell'art. 617 quater, comma quarto, n. 1 e 2. Questa modifica, si ritiene sia stata introdotta al fine di rendere omogenea la disciplina dell'art. 615- quater a quella di cui agli artt. 615- ter, comma 2, n. 1 e 617- quater cod. pen. La norma offre una tutela anticipata al bene giuridico della riservatezza informatica[132] e, in modo indiretto, al bene della sicurezza informatica, incriminando condotte prodromiche alla realizzazione di più gravi reati informatici (accesso abusivo ad un sistema informatico, danneggiamenti informatici, intercettazioni, frodi). Le condotte illecite tipizzate dalla norma sono le seguenti. Il soggetto potrebbe procurarsi abusivamente i codici o altre informazioni similari idonei a consentire l'accesso ad un sistema informatico o telematico protetto da misure di sicurezza. Altra ipotesi consiste nella diffusione, comunicazione o consegna a terzi dei codici o altre informazioni similari[133]. Altra condotta tipizzata consiste nel fornire indicazioni o istruzioni idonee a consentire l'accesso ad un sistema informatico altrui protetto da misure di sicurezza. Queste condotte consistono, pertanto, nel procurare a sé o ad altri la disponibilità dei mezzi di accesso necessari per superare le barriere protettive di cui un sistema informatico può essere dotato[134]. Non assume rilievo la circostanza che il codice

[132] Cfr. Tribunale Torino, 30/09/2002 in banca dati De Jure

[133] La Corte di appello di Milano ha chiarito che l'art. 615 quater punisce anche il riprodurre codici di accesso a un sistema informatico o telematico: l'inserimento di tali dati nella memoria di un apparato telefonico è una riproduzione che connota d'illiceità la provenienza dell'apparecchio che, per effetto di tale delitto, viene a contenere dentro di sè il codice così illecitamente riprodotto. Nel momento in cui le risultanze processuali fanno propendere non per una diretta clonazione dell'apparecchio da parte degli imputati, ma per la ricezione da parte loro dello stesso già clonato, deve essere affermata la penale responsabilità per il delitto di ricettazione (Corte appello Milano, 15/06/2001 in banca dati DeJure)

[134] C. PECORELLA, *Il diritto penale...*, cit., pag. 358

di accesso al sistema informatico altrui, oggetto della cessione, sia stato o meno ottenuto illecitamente dall'agente che poi lo abbia trasmesso. La norma oggi punisce, inoltre, la mera detenzione, che un tempo avrebbe potuto costituire, tutt'al più, prova difficilmente confutabile di una precedente condotta del soggetto volta a procurarsi la disponibilità di tali codici. Essa deve intendersi come "qualsiasi rapporto che implichi un potere di fatto (e non giuridico) sulle *res* immateriali e materiali qui tipizzate, al di là della qualificazione civilistica dell'*animus detinendi*. Si è coniata, *in parte qua*, un'ipotesi di reato di mero possesso, ancorata sulla intrinseca pericolosità delle *res* possedute"[135]. Inoltre, viene punita anche la produzione, da intendersi come diretta realizzazione ovvero come mera elaborazione o autonoma progettazione delle chiavi di accesso o degli strumenti o altri apparati idonei all'accesso abusivo ai sistemi informatici o telematici. Con l'aggiunta di questa condotta, prodromica rispetto alle altre condotte punite, il Parlamento ha anticipato ancor di più la soglia di tutela penale della norma incriminatrice in esame. L'importazione deve intendersi come introduzione in Italia dall'estero, anche mediante acquisto *online*, delle chiavi meccaniche, elettroniche, degli apparati o degli strumenti (o parti di essi) prodotti da terzi al di fuori del territorio nazionale. La messa a disposizione in altro modo consiste in un'ipotesi residuale, presente nell'articolo 7 della Direttiva, e volta a estendere nella massima ampiezza l'ambito applicativo della norma sì da riferirsi a qualunque condotta che offra a terzi o dia ad altri la possibilità di utilizzare le *res* immateriali e materiali qui tipizzate. Infine, l'installazione deve essere intesa come messa in opera dei codici, *software* maligni o degli strumenti o apparati informatici (*hardware)*, a prescindere dal loro effettivo utilizzo o operatività.

La giurisprudenza in realtà non ci offre molte applicazioni di tale norma; tuttavia, citiamo alcune sentenze per dare rilievo pratico alla fattispecie. Nella sentenza, cass. penale sez. II, 03/10/2013, n.47021, la corte rileva che integra il reato di detenzione e diffusione abusiva di codici di accesso a servizi informatici e telematici (art. 615 quater c.p.) e non quello di ricettazione la condotta di chi riceve i codici di carte di credito abusivamente scaricati dal sistema informatico, ad opera di terzi e li inserisce in carte di credito clonate poi utilizzate per il prelievo di denaro contante attraverso il sistema bancomat[136]. In

[135] A. NATALINI, *"Giro di vite" sui reati informatici, spettro applicativo ad ampio raggio* in Guida al diritto, n. 7, 26 febbraio 2022

[136] Cassazione penale sez. II, 03/10/2013, n.47021 in banca dati DeJure; in senso conforme: Cassazione penale sez. II, 17/01/2003, n.36288 in banca dati DeJure

un'altra sentenza, i giudici hanno individuato il reato nella condotta di colui che si procuri abusivamente il numero seriale di un apparecchio telefonico cellulare appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cosiddetta clonazione) è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce un sistema telematico protetto, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche[137].

La fattispecie in esame è stata ritenuta applicabile in un caso di illecita acquisizione di codici di accesso a conti correnti bancari e postali *online* per effettuare prelievi e bonifici non autorizzati (c.d. *phishing*)[138]. Le condotte previste nell'articolo 615 quater c.p. hanno rilevanza solo in quanto realizzate abusivamente da parte di chi non sia autorizzato dal titolare del sistema. L'avverbio abusivamente costituisce un presupposto della condotta. La previsione non mira a constatare l'assenza di cause di giustificazione. Il legislatore, tramite questa clausola di antigiuridicità speciale, ha inteso rinviare a regole extra-penali o comunque desumibili dal contesto nel quale il soggetto opera[139].

La previsione in esame dà luogo, tuttavia, ad alcune incertezza. Essendo il reato di accesso abusivo, un reato di pericolo, la fattispecie di cui all'articolo 615 quater c.p. dà luogo ad un'ipotesi di reato di pericolo indiretto[140], poiché dal concretizzarsi di questa condotta deriva il pericolo del configurarsi della fattispecie di accesso a un sistema informatico altrui. La norma, in base a questo orientamento sarebbe in contrasto con il principio di proporzione in base al quale viene valutata la legittimità costituzionale dei reati di pericolo indiretto, trattandosi di reati che in via del tutto eccezionale incriminano atti meramente preparatori di altri fatti delittuosi. In base a questo principio, la legittimità del ricorso alla pena può essere affermata solo in presenza di un ragionevole rapporto tra la gravità dell'offesa che si reprime e il rango del bene protetto. Nell'ipotesi di specie, non sembra che la tutela della riservatezza di un sistema informatico possa giustificare l'arretramento della soglia di intervento penale ad uno stadio nel quale il pericolo cui tale bene viene sposto è solamente indiretto, in quanto pericolo di un pericolo di lesione[141].

[137] Cassazione penale sez. II, 17/12/2004, n.5688 in banca dati DeJure
[138] Tribunale di Milano, 28 luglio 2006, in Dir. Internet, 2007, pag. 62.
[139] I. SALVADORI, *I reati informatici*…, cit., pag. 697.
[140] C. PECORELLA, *Diritto penale*…, cit., pag. 360.
[141] C. PECORELLA, *Diritto penale*…, cit., pag. 361.

L'oggetto materiale del reato è costituito da codici, parole chiave o mezzi idonei ad accedere ad un sistema informatico o telematico ovvero da indicazioni o istruzioni idonee al già menzionato scopo, ma anche da apparati, strumenti, parti di apparati o parti di strumenti. Per codice o parola chiave deve intendersi qualsiasi sequenza alfanumerica idonea a consentire a chi ne ha la disponibilità di accedere ad un sistema informatico protetto da misure di sicurezza[142]. La locuzione "altrimenti idonei" costituisce una clausola di chiusura particolarmente elastica, capace di ricomprendere anche gli strumenti tecnologici non ancora scoperti. In tal modo "il legislatore ha inteso sanzionare non solo i *software* multifunzionali o multiscopo che consentono di aggirare le misure di sicurezza poste a protezione di un sistema informatico e di accedere a dati e dai programmi in esso contenuti, ma anche qualsiasi dispositivo o mezzo fisico che permetta di introdursi in un sistema"[143]. Dovranno invece essere escluse da tale nozione le schede informatiche che consentono di vedere in chiaro programmi televisivi o le schede telefoniche o il rispettivo codice di identificazione poiché il loro utilizzo indebito permette soltanto di usufruire gratuitamente delle prestazioni di un apparecchio telefonico[144].

La modifica del 2021, che ha ampliato l'oggetto materiale del reato risulta, criticabile, poiché, l'introduzione di tali termini è avvenuta per adeguare la norma all'art. 7 della Direttiva in cui, tuttavia, si chiarisce che con il termine strumenti si intende "programma per *computer*", "*password*", "codici di accesso" o "dati simili", elementi che erano già presenti nella precedente versione dell'art. 615 quater. In ogni caso, il legislatore ha aggiunto, al fine di adeguare la norma a ogni potenzialità offensiva offerte dalla scienza e dalle nuove tecnologie, i riferimenti agli "apparati, strumenti, parti di apparati o di strumenti", sicché rileveranno d'ora in poi tutte quelle possibili *res materiali* (*hardware)* organizzate tecnologicamente per mezzo di speciali programmi (*software*) idonei all'accesso a sistemi informatici o telematici protetti da misure di sicurezza[145]. Con indicazioni o istruzioni idonee al predetto scopo si intendono le informazioni che consentono aggirare o eludere le misure di sicurezza poste a protezione del sistema

[142] C. PECORELLA, *Diritto penale*…, cit., pag.365.
[143] I. SALVADORI*, I reati informatici*…, cit., pag. 697.
[144] C. PECORELLA, *Diritto penale*…, cit., pag. 366. Cfr. Tribunale Trapani, 22/12/2005, n.892 in banca dati De Jure
[145] A. NATALINI, "*Giro di vite" sui reati informatici, spettro applicativo ad ampio raggio* in Guida al diritto, n. 7, 26 febbraio 2022

informatico. Ad esempio, potrebbe rilevare un *tutorial* disponibile sul *web* che spiega come introdursi illecitamente in un sistema protetto[146]. Un elemento caratterizzante è la previsione del dolo specifico. La condotta si realizza solo nel caso in cui il soggetto agente è mosso dall'intenzione di procurare a sé o ad altri un profitto o arrecare ad altri un danno[147]. Questo elemento psicologico è rimasto invariato, anche a seguito della novella, nonostante l'art 7 della Direttiva 2013/40/UE faccia riferimento ad un elemento psicologico più ampio poiché fa riferimento a condotte intenzionali compiute senza diritto con l'intenzione di utilizzare (i predetti strumenti) al fine di commettere uno dei reati di cui agli artt. da 3 a 6 della direttiva stessa. In una sentenza si legge "perché sussista il dolo specifico richiesto dalla norma dell'art. 615 quater è sufficiente che il responsabile possegga personali conoscenze informatiche per l'attività professionale dallo stesso esercitata"[148]. Questo impedisce di applicare la norma a chiunque, per motivi leciti, comunichi ad altri una *password* di accesso ad un sistema informatico[149]. La fattispecie si configura, nonostante le critiche di parte della dottrina, come reato di pericolo indiretto[150]. Possiamo pensare al fatto di chi al fine ottenerne un profitto si procuri un *software* con l'obiettivo di accedere abusivamente ad un sistema informatico altrui protetto da misure di sicurezza. La condotta consistente nel procurarsi il *software* rappresenta il pericolo del pericolo di una lesione per il bene giuridico della riservatezza e sicurezza informatica[151]. Altra tesi poco convincente ritiene che oggetto di tutela della norma in esame sia la riservatezza delle chiavi di accesso. Questi ultimi sarebbero considerati dal legislatore alla stregua di qualità personali riservate, in quanto identificatrici della persona che consentono di fruire di ogni genere di servizio informatico[152].

---

[146] I. SALVADORI, *I reati informatici…*, cit., pag. 398.
[147] Tribunale Milano sez. II, 28/09/2007 in banca dati DeJure
[148] Tribunale Torino, 08/04/2002 in banca dati DeJure
[149] G. PICA, *Diritto penale…*, cit., pag. 80.
[150] C. PECORELLA, *Diritto penale…*, cit., pag. 615; I. SALVADORI, *I reati informatici…*, cit., pag. 700. In giurisprudenza: Tribunale Milano 10/10/2000 in banca dati DeJure: "La struttura dell'art. 615 quater c.p. - con l'attribuzione di rilevanza penale a comportamenti che, in sé, non sono atti a ledere i beni giuridici tutelati- evidenzia la volontà del legislatore di anticipare la soglia della punibilità rispetto al momento dell'effettivo conseguimento di un profitto, concependo la fattispecie quale reato di pericolo e non già quale illecito di danno. Ne consegue che la condotta con la quale - già venuto ad esistenza il pericolo di ledere l'interesse tutelato - lo si pregiudica, rappresenta un "post factum" non punibile".
[151] I. SALVADORI, *Diritto penale…*, cit., pag. 701.
[152] G. PICA, *Diritto penale…*, cit., pag.81

Una questione da affrontare riguarda il rapporto con il reato di accesso abusivo a un sistema informatico. Secondo un orientamento sembra potersi configurare un'ipotesi di concorso tra le due fattispecie tanto per la diversità strutturale, quanto per la diversità dell'oggetto di tutela[153]. Sul piano dell'oggetto della tutela l'art. 615-ter tutelerebbe il bene della riservatezza del domicilio informatico, mentre l'art. 615-quater c.p. la riservatezza dei codici di accesso. Tale teoria sottolinea, inoltre, che mentre la condotta di cui all'articolo 615 ter c.p. co. 1 è punibile a querela, la condotta di cui all'articolo 615 quater c.p. è punibile d'ufficio. Questa differenza ci farebbe comprendere la diversa rilevanza dei due fatti nell'ottica del legislatore. La riservatezza delle chiavi di accesso sarebbe un interesse pubblico (indisponibile), mentre del domicilio informatico è titolare esclusivo il singolo proprietario del domicilio e il legislatore ha riconosciuto a questi la scelta se chiedere o meno la punizione dell'intrusore. Un esempio è quello dell'*hacker* che utilizza la stessa tecnologia informatica per tentare di aggirare le protezioni di un sistema e in questo modo si procuri illecitamente un codice di accesso al fine di introdursi abusivamente al sistema altrui. Tuttavia, diverso orientamento, recentemente accolto dalla cassazione, esclude l'ipotesi del concorso di reati. I giudici rilevano che le due fattispecie incriminatrici sarebbero poste a presidio del medesimo bene giuridico, individuato, dalla corte nel c.d. domicilio informatico. Tra le due ricorrerebbe una stretta connessione, poiché nel tutelare lo stesso bene giuridico, sono punite condotte meno invasive (detenzione e diffusione) e più invasive (accesso abusivo), laddove le prime presuppongono le seconde. Pertanto, si assisterebbe ad una forma di antefatto non punibile, sussistendo quindi un concorso apparente di norme per assorbimento[154]. Secondo la Corte di Cassazione, "In generale, l'antefatto non punibile ricorre nei casi in cui la commissione di un reato meno grave costituisce ordinariamente strumento per la commissione di un reato più grave. Esso (come la progressione criminosa ed il postfatto non punibile) non costituisce fattispecie autonomamente disciplinata, poiché rientra tra i casi di concorso apparente di norme da risolvere ai sensi dell'art. 15 c.p., attraverso una operazione interpretativa che impone la considerazione "congiunta" di due fattispecie tipiche, resa oggettivamente evidente dal fatto che per una di esse, destinata ad essere assorbita nell'altra, sia prevista una sanzione più lieve"[155]. Sulla base di tali argomenti, la

[153] G. PICA, *Diritto penale*…, cit., pag. 83 ss.
[154] Cassazione penale, 14 gennaio 2019, n.21987, sez. II in banca dati DeJure
[155] Cassazione penale, 14 gennaio 2019, n.21987, sez. II in banca dati DeJure

Corte ha dunque affermato che il meno grave delitto di cui all'art. 615-quater, c.p. non possa concorrere con quello, più grave, di cui all'art. 615-ter, c.p., del quale costituisce naturalisticamente un antecedente necessario, sempre che quest'ultimo sia contestato, procedibile e integrato nel medesimo contesto spazio-temporale in cui fu perpetrato l'antefatto ed in danno della medesima persona fisica (i.e. il titolare del bene protetto)[156]. La sentenza richiama anche l'opposto orientamento giurisprudenziale emerso nella sentenza cass., sez. 2 n. 36721/2008. In proposito, si è osservato che, "dal momento che il delitto di accesso abusivo è strutturato come reato di pericolo, la norma di cui all'art. 615-quater delinea una fattispecie di pericolo necessariamente indiretto: dalla condotta diretta a procurare a sé o ad altri il codice di accesso al sistema informatico altrui deriva, infatti, il pericolo sia di una successiva, immediata introduzione abusiva nel sistema stesso (che è situazione di per sé pericolosa per la riservatezza dei dati e/o dei programmi che vi sono contenuti), sia di una ulteriore condotta di diffusione del codice (in favore di soggetti) che potranno, a loro volta, servirsene per realizzare un accesso abusivo oppure cederlo a terzi"[157]. Tuttavia, il collegio ritiene che i due reati non possano concorrere per le motivazioni esposte sopra.

3.3 Detenzione, diffusione e installazione abusiva di apparecchiature dirette a danneggiare un sistema informatico

L'art. 615 quinquies c.p. è stato introdotto dal legislatore nel 1993, in una formulazione diversa da quella attuale, anticipando le scelte politiche sovranazionali ed in particolare la Convenzione *Cybercrime* (art. 6). Si trattava di una fattispecie innovativa, introdotta con lo scopo di contrastare i nuovi fenomeni dei programmi *virus*. Nonostante l'intervento del legislatore fosse stato lungimirante, la disposizione presentava e presenta ancora, nonostante l'intervenuta modifica, alcune criticità. Un primo problema attiene alla collocazione. La disposizione, infatti, si trova, ancora oggi, nell'ambito dei delitti contro l'inviolabilità del domicilio, nonostante si tratti di un delitto prodromico al danneggiamento. In merito alla precedente formulazione, Picotti afferma: "era criticabile

[156] A. UBALDI, *Accesso abusivo e detenzione/diffusione di codici di accesso: concorso apparente di reati* in Diritto & Giustizia, fasc. 91/2019

[157] Cass. pen., Sez. II, 21 febbraio 2008, n. 36721 in banca dati DeJure

la formulazione alquanto complessa e, nel contempo, insufficiente a delimitare con precisione i contenuti dell'illiceità penale del fatto"[158].

Nella sua versione originaria, l'art. 615- quinquies c.p. puniva il fatto di diffondere, comunicare o consegnare un programma informatico avente per scopo o per effetto il danneggiamento di dati o sistemi informatici. Il legislatore, così facendo, puniva "le condotte volte a far entrare i c.d. *malware* nella sfera altrui", mentre escludeva dall'ambito di applicazione della norma "i comportamenti finalizzati a ottenere la disponibilità di tali programmi"[159]. Questa scelta non appariva una ponderata decisione politico-criminale, bensì una svista del legislatore, in contraddizione con la volontà di creare un reato-ostacolo[160]. Discutibile era, inoltre, la scelta di delimitare l'oggetto della tutale ai programmi che hanno per scopo od effetto il danneggiamento di dati e sistemi informatici. Questa disposizione, così formulata non riusciva a fissare precisi limiti tra lecito e illecito penale[161]. Di fatto, sarebbero potuti ricadere nell'ambito di applicazione della disposizione in esame anche quei programmi utilizzati per aggredire sistemi da cui partono gli attacchi informatici. Il legislatore è intervenuto, una prima volta, modificando la norma con la legge 48/2008. In questa seconda versione la norma disponeva che: "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". La disposizione è stata estesa dal punto di vista oggettivo. Sono state inserite le condotte di chi "si procura, produce, riproduce, importa". Oggetto materiale della norma sono ora "apparecchiature, dispositivi o programmi informatici". Il fine o scopo di danneggiare è stato trasferito dal programma alla condotta dell'agente. Il delitto è, pertanto, divenuto punibile a titolo di dolo specifico. Infatti, il reato si consuma nel momento in cui il soggetto entra nella disponibilità di apparecchiature, dispositivi o programmi informatici ovvero li mette a

[158] L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* in "*Diritto penale e processo*", n.6/2008, pag. 708.
[159] I. SALVADORI, *I reati contro la riservatezza*…, cit., pag. 702
[160] L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*…, cit., pag. 708.
[161] Ibidem

disposizione di terzi. Con riferimento all'elemento soggettivo la giurisprudenza ha chiarito che "si ritiene sufficiente che vi sia l'accertata volontà dell'agente di diffondere il programma con la consapevolezza dei suoi effetti non esigendo la norma che il fine dell'azione sia la distruzione o il danneggiamento del sistema informatico"[162]. Una sentenza recente che si è occupata di questo reato ha approfondito il concetto di sistema informatico[163]. Un soggetto si era abusivamente procurato un congegno elettronico, atto a danneggiare ed alterare il sistema di protezione delle macchine cambiamonete, con la finalità di impadronirsi delle somme ivi contenute. La corte individua il sistema informatico "nell'attitudine della macchina (*hardware*) ad organizzare ed elaborare dati, in base ad un programma (*software)*, per il perseguimento di finalità eterogenee. Nella definizione che qui interessa, dunque, alla funzione di registrazione e di memorizzazione dei dati, anche elettronica, si affianca l'attività di elaborazione e di organizzazione dei dati medesimi"[164]. In particolare, i giudici escludono che il cambiamonete possa essere considerato un sistema informatico poiché "nelle sentenze di merito, non viene spiegato congruamente e logicamente, come la macchina cambiamonete sia qualificabile sistema informatico. Alcun accenno, infatti, si rinviene in merito all'attitudine dell'apparecchio cambiamonete ad organizzare ed elaborare i dati, sulla base di un programma, posto che l'apparecchio non viene descritto, né il funzionamento del predetto viene illustrato dai giudici di merito, che limitano la descrizione, al congegno trovato in possesso

[162] Tribunale Bologna sez. I, 22/12/2005, n.1823 in banca dati DeJure. Nel caso in esame soggetto è stato condannato ex artt. 615 ter e 615 quinquies c.p. per aver creato un cosiddetto "*virus*", cioè un programma dall'unica funzione di introdursi e danneggiare sistemi informatici, "Vierika", che era stato trasmesso in via informatica al *provider* "Tiscali"; attraverso questo il *virus* si era introdotto nei sistemi di circa 900 utenti, acquisendo dati riservati nei relativi *personal computers*, danneggiandone i programmi e pregiudicandone il corretto funzionamento. Per quanto attiene al reato ex art. 615 quinquies C.p., Vierika, inizialmente inviato dall'imputato ad alcuni indirizzi di posta elettronica reperiti sulla bacheca virtuale del sito www.sexualcyber.com alterava la funzionalità telematica del sistema infettato, per effetto della alterazione dei parametri di protezione del *browser,* all'oscuro dell'utente, e dell'invio automatico e massiccio di *e-mail*, con ciò integrandosi anche detta fattispecie.

[163] Cassazione penale sez. V, 16/04/2018, (ud. 16/04/2018, dep. 12/09/2018), n.40470 in banca dati DeJure

[164] Cassazione penale sez. V, 16/04/2018, (ud. 16/04/2018, dep. 12/09/2018), n.40470 in banca dati DeJure. In altra sentenza meno recente si legge: "Deve ritenersi "sistema informatico", secondo la ricorrente espressione utilizzata nella l. 23 dicembre 1993 n. 547, un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati" (Tribunale La Spezia, 23/09/2004 in banca dati De Jure)

dell'imputato, indicato come capace di incidere sul funzionamento della macchina cambiamonete".

L'art. 19 della l. n. 238 del 2021 ha modificato l'art. 615- quinquies, nuovamente, intervenendo, sia sul novero delle condotte incriminate, sia sulla rubrica che prima faceva riferimento alla sola "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico", mentre ora fa riferimento alla "Detenzione, diffusione e installazione abusiva…". Il testo attuale prevede che: " 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri, installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329". La modifica ha disposto la sanzione delle condotte di detenzione, installazione e messa a disposizione di altri delle apparecchiature e dei dispositivi o programmi informatici diretti a danneggiare irrimediabilmente i programmi installati i dati immagazzinati e i sistemi operativi, in aggiunta a quelle già previste. La condotta di detenzione è stata espressamente introdotta, mentre in precedenza veniva ritenuta implicita nelle condotte di diffusione e consegna. Con l'introduzione della condotta di installazione viene sanzionata la condotta tipica di chi si occupa di programmi informatici, che tuttavia si sarebbe potuta ritenere ricompresa nella diffusione o nella messa a disposizione. Il legislatore opportunatamente ha inserito, con riferimento alla messa a disposizione, l'espressione in altro modo poiché così si consente l'incriminazione di comportamenti non ancora descrivibili nel loro contenuto, ma resi possibili dalla rapida evoluzione tecnologica. La novella ha, inoltre, inserito nella norma l'avverbio abusivamente per indicare che i vari contenuti tenuti dall'agente, per essere penalmente rilevanti, devono essere eseguiti *contra ius,* in linea con le disposizioni ex artt. 615- ter e 615- quater c.p. "Tale elemento include così nella struttura della fattispecie un aspetto di antigiuridicità speciale, volto a dare esplicito rilievo (analogamente all'articolo 617-quater del Cp, ove però compare l'avverbio «fraudolentemente») a ogni modalità illegittima, *sine titulo* di messa in circolazione, contro la volontà dell'utilizzatore, di

apparecchiature “maligne” o programmi informatici virali in grado di infettare il sistema informatico”[165].

L’aggiunta di tale elemento non appare superflua poiché evita l’eccessiva dilatazione della sfera di applicabilità della disposizione in esame[166].

L’art 615- quinquies c.p., tuttavia, integra un’ipotesi di reato di pericolo indiretto anticipando, in tal modo, notevolmente la tutela del bene giuridico della sicurezza e della riservatezza informatica[167].

La punibilità prescinde dal danneggiamento contemplato nell’art. 635- bis c.p. L’agente, che abbia lo scopo o l’intenzione di danneggiare un sistema informatico altrui, incorre nel reato anche se non è in grado di arrecare alcun tipo di danno perché il *virus* è inidoneo o perché l’agente decida di non utilizzarlo. La sussistenza del dolo specifico consente, tuttavia, di delimitare l’ambito di applicazione. Dubbi permangono circa la configurabilità del tentativo che già prima veniva esclusa poiché avrebbe comportato l’arretramento eccessivo della soglia di rilevanza penale e la punibilità della mera ideazione di oggetti pericolosi[168].

3.4 La tutela della corrispondenza e delle comunicazioni telematiche

Le novità in campo tecnologico hanno riguardato anche la corrispondenza e le telecomunicazioni che oggi si realizzano attraverso supporti informatici. La l. 547/1993 ha cercato di soddisfare le nuove esigenze, estendendo la tutela penale a queste nuove forme di comunicazione. In realtà già prima di questo intervento normativo, la dottrina

[165] NATALINI A., *“Giro di vite” sui reati informatici, spettro applicativo ad ampio raggio* in Guida al diritto, n. 7, 26 febbraio 2022

[166] Cass., Ufficio del Massimario e del Ruolo, relazione alla legge 23 dicembre 2021, n. 238, 21 marzo 2022 in sistemapenale.it

[167] I. SALVADORI, I reati contro…, cit., pag. 704; In giurisprudenza si veda Cassazione penale sez. V, 16/04/2018, (ud. 16/04/2018, dep. 12/09/2018), n.40470 in banca dati DeJure:” Si tratta, diversamente da quanto sostenuto nel ricorso, di reato di pericolo, che in questo caso si è ritenuto integrato dalla condotta dell'imputato, il quale, è stato trovato in possesso di un apparecchio, secondo la ricostruzione dei giudici di merito, in grado di alterare il funzionamento delle macchine cambiamonete, con l'evidente finalità di impossessarsi delle somme in essere contenute. I giudici di merito, infatti, hanno esposto che, una volta inserito l'apparecchio reperito, nell'alloggiamento1 ove va posizionata la carta moneta, questo avrebbe provocato l'erogazione continua di danaro, creando un campo magnetico capace di interferire sulla funzione della macchina”.

[168] Cfr. I. SALVADORI, I reati…, cit.; F. MANTOVANI, Diritto penale…, cit.; Contra G. PICA, Diritto penale…, cit.

era certa di poter garantire una copertura costituzionale ex art. 15 cost. Il legislatore ha, tuttavia, deciso, modificando il quarto comma dell'articolo 616 del Codice penale, di estendere la nozione di corrispondenza alle comunicazioni informatiche o telematiche, ovvero effettuate con ogni altra forma di comunicazione a distanza. Con l'articolo 623 bis è stata estesa la punibilità delle condotte previste a tutela dei segreti (sez. V del Codice penale), anche ad ogni altra forma di trasmissione a distanza di suoni, immagini o di altri dati. Sono stati, inoltre, introdotti gli articoli 617 quater, 617 quinquies e 617 sexies del Codice penale, con la funzione di estendere la tutela già prevista dall'articolo 617 alle comunicazioni informatiche o telematiche. Queste disposizioni ricalcano il modello delle preesistenti fattispecie poste a tutela della riservatezza delle comunicazioni e delle conversazioni telefoniche o telegrafiche tra persone. Nonostante l'apparente completezza della materia, l'interprete si trova di fronte a molteplici problemi, dovuti alla eccessiva dilatazione delle previsioni penali[169]. Prima di procedere all'analisi delle fattispecie di cui agli artt. 617- quater; -quinquies e -sexies c.p. è bene soffermarci sul bene giuridico tutelato da tali disposizioni, poiché fermo quanto abbiamo detto in via generale nei paragrafi dedicati alla riservatezza informatica e sicurezza informatica, occorre fare alcune precisazioni. Parte della dottrina ritiene che le disposizioni introdotte con gli articoli 617 quater c.p., e 617 quinquies c.p. tutelino i beni della genuinità e riservatezza delle comunicazioni[170]. "La genuinità esprime l'esigenza di autenticità del contenuto e di inviolabilità *ab externo* della tecnologia; la riservatezza, benché sia un termine non nuovo esprime la perdurante ed innegabile esigenza che, anche per le comunicazioni telematiche, sia tutelata la *privacy* dei contenuti, i quali sono pur sempre al di là della veste tecnologica che li recepisce e li trasmette, espressione di idee, emozioni, pensieri, volontà, delle persone che li formano e gli affidano alle tecnologie"[171]. Secondo tale orientamento la disposizione di cui all'art. 617 quater c.p. configura un reato di danno poiché le condotte cagionerebbero una lesione dell'interesse tutelato. Altro orientamento ritiene che le disposizioni in esame non prestino tutela alla riservatezza personale, vista l'eliminazione del riferimento alla comunicazione tra persone. Ad essere protetta sarebbe, invece, la sicurezza del sistema informatico o telematico. Si tratta della "capacità tecnica ed attitudine del sistema a diffondere e veicolare comunicazioni tra più soggetti, non solo

[169] G. PICA*, Diritto penale…*, cit., pag. 170.
[170] G. Pica, *Diritto penale…*, cit., pag. 178.
[171] Ibidem.

in condizioni di effettiva affidabilità e di sostanziale fedeltà quanto ai contenuti e alla destinazione dei messaggi, ma anche in modo tale da precludere che il circuito liberamente attivato e controllato dai soggetti che di tale sistema informatico e telematico si avvalgano possa essere in qualche modo alterato, violando il rapporto fiduciario con il gestore della rete o stravolgendo i criteri prescelti circa l'accesso alle informazioni"[172]. La tesi più accreditata, ritiene che ad essere tutelati siano i nuovi beni giuridici della riservatezza e sicurezza informatica, quale diritto di comunicare in modo libero e sicuro[173]. "La norma incriminatrice non protegge pertanto il diritto alla riservatezza delle persone coinvolte nelle comunicazioni informatiche o telematiche, bensì l'integrità del mezzo di comunicazione a svolgere la sua funzione in modo libero e pacifico, quale presupposto per garantire la possibilità di scambiare dati ed informazioni tra soggetti". Come per l'art. 617- quater c.p., la norma tutela, in via ulteriormente anticipata, la riservatezza e sicurezza informatica.[174] Per quanto attiene, invece alla fattispecie di cui all'art. 617- sexies c.p., il bene giuridico tutelato viene identificato nell'integrità, autenticità e genuinità del contenuto di dati costitutivi di comunicazioni informatiche o telematiche[175].

Occorre, adesso, soffermarci sull'articolo 616 ed in particolare sull'ultimo comma introdotto nel 1993 per chiarire alcuni concetti utili. L'articolo 616 del Codice penale dispone che: "1. Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516. 2. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. 3. Il delitto è punibile a querela della persona offesa. 4. Agli effetti delle disposizioni di questa sezione, per

[172] R. BORRUSO, G. BUONOMO, G. CORASANITI, G. D'AIETTI, *Profili penali dell'informatica*, Milano, Giuffrè, 1994, pag. 120

[173] I. SALVADORI, *I reati informatici*…, cit., pag. 712; C. PIERGALLINI, I delitti contro la riservatezza e la libertà delle…, cit., pag. 838.

[174] Ibidem

[175] I. SALVADORI, *I reati contro la riservatezza*…, cit., pag. 718.

"corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza". Il legislatore ha adeguato l'ordinamento alla nuova realtà facendo semplicemente riferimento ad ogni altra forma di comunicazione a distanza. A questo nuovo tipo di comunicazioni, la legge del 1993 ha esteso la tutela penale di cui godevano le altre forme di comunicazione personale. "Una tutela ad ampio raggio che ne abbraccia sia il profilo statico, ossia la materializzazione in un idoneo supporto del contenuto del pensiero da comunicare, sia il profilo dinamico consistente nella trasmissione vera e propria del messaggio"[176]. Questa scelta è stata aspramente contestata in dottrina a causa della sua indeterminatezza, ma anche il riferimento alla comunicazione telematica appare poco preciso[177]. Di diverso orientamento altra parte della dottrina che ha ritenuto chiaro il riferimento alla corrispondenza informatica e telematica, mentre l'utilizzo della formula in chiusura sembra voler preservare la norma da un invecchiamento precoce[178].

Occorre precisare che per corrispondenza deve intendersi lo scambio di informazioni e messaggi tra persone determinate, mentre è esclusa la tutela penale per i messaggi rivolti ad un pubblico indeterminato. Si definisce informatica quella corrispondenza destinata ad essere inoltrata e/o ricevuta per mezzo di un sistema informatico e il cui oggetto, codificato in un linguaggio comprensibile dall' elaboratore è fissato su un supporto di memoria in attesa di essere trasmesso al destinatario oppure in attesa che quest'ultimo ne prenda conoscenza. La disposizione si applica principalmente a quelle comunicazioni effettuate tramite posta elettronica[179]. Facciamo quindi riferimento a messaggi registrati in supporti di memoria interni al sistema informatico, ma può costituire corrispondenze informatica anche il messaggio che venga modificato e memorizzato su un supporto esterno all' elaboratore, come un disco o un nastro magnetico, per essere inviato al destinatario, il quale lo potrà leggere attraverso il proprio computer. Analizzando le diverse fasi della trasmissione di un messaggio elettronico, possiamo definire corrispondenza informatica: "Il messaggio registrato nella memoria del *computer* del mittente, in attesa di essere trasmesso all'elaboratore del fornitore del servizio di posta

[176] Ibidem.
[177] G. Pica, *Diritto penale…*, cit. pag. 172.
[178] C. Pecorella, *Diritto penale…*, cit., pag. 292.
[179] Cfr. Cassazione penale sez. V, 25/03/2019, n.18284 in banca dati De Jure; Cassazione penale sez. V, 02/02/2017, n.12603 in banca dati De Jure

elettronica utilizzato dal mittente stesso; il messaggio proveniente dall'utente e registrato nella memoria del *computer* del *provider,* in attesa di essere trasmesso all'elaboratore del provider utilizzato dal destinatario; il messaggio trasmesso dal *provider* e del mittente registrato nella memoria del *server* del *provider* del destinatario in attesa di essere ricevuto da quest'ultimo in occasione del primo collegamento alla sua casella di posta; il messaggio finalmente giunto a destinazione, in quanto scaricato dal destinatario sulla memoria del proprio *computer* e qui registrato in attesa di essere letto"[180]. Occorre fare questa precisazione poiché a partire dal momento in cui viene letto, il messaggio riceve tutela dall'ordinamento in quanto tale e non più per la libertà e la riservatezza che doveva essere assicurata alla comunicazione. Ad esempio, se un messaggio già letto e conservato nell'apposito archivio venga cancellato o manomesso, non verrà applicato l'art. 616 c.p. bensì la norma sul danneggiamento informatico (art. 635-bis c.p.). Inoltre, risulta importante sottolineare la distinzione tra corrispondenza aperta e chiusa, poiché è solo riguardo a quest'ultima viene punita anche l'abusiva presa di cognizione. Possiamo pensare, ad esempio, al gestore del servizio di posta elettronica che prenda visione della corrispondenza giacente nella memoria del suo *computer* e destinata ad un suo determinato cliente. Viene invece considerata aperta la corrispondenza inviata e ricevuta nell'ambito delle cosiddette conferenze o gruppi di discussione nelle quali lo scambio di messaggi (*post*) tra i partecipanti non avviene in tempo reale, ma attraverso l'affissione di essi ad una sorta di bacheca elettronica. Il terzo estraneo che sia riuscito ad inserirsi nella sala conferenze virtuale non risponderà penalmente per l'eventuale presa di cognizione dei messaggi altrui, potendo tutt'al più incorrere in una sanzione penale nell'ipotesi in cui compia sui messaggi stessi una delle diverse condotte previste dall'articolo 616 c.p. In una sentenza con riferimento al tema della violazione dell'art. 616 c.p. la Corte ha precisato che per contenuto di corrispondenza deve intendersi non soltanto ciò che è manifestato mediante espressioni grafiche, ma tutto ciò che, affidato alla protezione della busta, è destinato a significare al destinatario un pensiero o un'azione del mittente, ogni cosa (danaro o fotografie), concernente i rapporti personali fra persone lontane[181]. Pertanto, il prender conoscenza del contenuto di una corrispondenza non implica necessariamente la lettura di una missiva. Nel caso in esame l'imputato aveva aperto la

[180] C. PECORELLA, *Il diritto penale…*, cit., pag. 295. Cfr. Cassazione penale sez. V, 29/09/2020, n.30735 in banca dati De Jure

[181] Cassazione penale sez. V, 04/06/2015, n.34993 in banca dati De Jure

busta di una raccomandata indirizzata all'ex convivente, asserendo di non averne letto il contenuto. Con riferimento a questa norma, è interessante citare un'altra sentenza della Corte di legittimità[182]. La Corte di cassazione ha ritenuto di escludere la ravvisabilità del reato di cui all'art. 616 c.p. nella condotta del superiore gerarchico che prenda cognizione della posta elettronica contenuta nel *computer* del dipendente, assente dal lavoro, dopo avere a tal fine utilizzato la *password* in precedenza comunicatagli in conformità al protocollo aziendale[183]. Infatti, ha argomentato la Corte, tale corrispondenza può essere qualificata come "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di invio o di ricezione dei singoli messaggi e ciò perché, diversamente da quanto avviene per la corrispondenza cartacea, di regola accessibile solo al destinatario, è appunto la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle informazioni in esso custodite sicché tale legittimazione può dipendere non solo dalla proprietà, ma soprattutto dalle norme che regolano l'uso degli impianti. In particolare, quando il sistema telematico sia protetto da una *password*, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano della chiave informatica di accesso. Anche nel caso in cui la legittimazione all'accesso sia condizionata, l'eventuale violazione di tali condizioni può rilevare sotto altri profili, ma non può valere a qualificare la corrispondenza come "chiusa" anche nei confronti di chi sin dall'origine abbia un ordinario titolo di accesso. Nel caso di specie, era emerso che le *passwords* poste a protezione dei *computers* e della corrispondenza di ciascun dipendente dovevano essere a conoscenza anche dell'organizzazione aziendale, essendone prescritta la comunicazione, sia pure in busta chiusa, al superiore gerarchico, legittimato ad utilizzarla per accedere al *computer* anche per la mera assenza dell'utilizzatore abituale. L'imputato, pertanto, del tutto lecitamente aveva preso cognizione della corrispondenza informatica aziendale del dipendente, utilizzando la chiave di accesso di cui legittimamente disponeva, come noto allo stesso dipendente. La soluzione è senz'altro convincente, anche considerando che, secondo le prescrizioni del provvedimento del Garante per la protezione dei dati personali n. 13 del 1° marzo 2007, i dirigenti dell'azienda possono accedere legittimamente ai *computers* in dotazione ai propri dipendenti quando delle

[182] Cass., Sez. V, 11 dicembre 2007 in Cass. pen., 2008, p. 4669

[183] Cfr. Tribunale Milano, 10/05/2002 in banca dati De Jure; Tribunale Torino, 20/06/2006 in banca dati De Jure

condizioni di tale accesso sia stata loro data piena informazione. Resta solo da aggiungere che, laddove fosse stata accertata l'abusività dell'intrusione, per non avere il titolare legittimo accesso agli apparecchi in uso nell'azienda, si sarebbe potuto addirittura porre un problema di possibile contestabilità del reato di cui all'art. 615-ter c.p., unitamente a violazioni del codice della *privacy* e dell'art. 4 dello Statuto dei lavoratori in tema di divieto di controllo dell'attività del lavoratore.

Importante ai fini della nostra indagine è anche l'art. 623-bis c.p. "Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati". Si tratta della norma di chiusura della sezione V del codice, introdotta nella sua formulazione originaria nel 1974 per contrastare le intrusioni nella riservatezza delle "comunicazioni e conversazioni telegrafiche e telefoniche", estendendo ad esse l'applicazione di tutte le disposizioni contenute nella sezione predetta. Nel 1993 ha compreso anche le comunicazioni e conversazioni "informatiche e telematiche" e ha stabilito che tutte le disposizioni si applichino anche a "qualsiasi altra trasmissione a distanza di suoni, immagini o altri dati". Anche tale norma è stata aspramente criticata perché risulta difficile delimitare i caratteri identificativi della categoria, come accaduto per la simile clausola che chiude la definizione di corrispondenza. Inoltre, fino ad oggi, tale clausola ha avuto scarsa operatività, mentre paradossalmente quella aggiunta nel 1974 aveva fatto emergere lacune di tutela in relazione all'intercettazione di comunicazioni radio riservate fra le forze di polizia, perché non avrebbe consentito di ricomprendervi quelle mediante c.d. "onte guidate". "In altri termini, si dimostra che *l'horror vacui* non può essere un criterio razionale di guida per il legislatore nella formulazione della disciplina penale diretta a contrastare i fenomeni criminosi nascenti dall'utilizzo delle nuove tecnologie, occorrendo piuttosto che vi sia sempre, alla base delle scelte di politica criminale e delle correlate formulazioni normative, un'attenta analisi e conoscenza, degli stessi fenomeni, sia sul piano criminologico, sia su quello più specificamente tecnico"[184].

[184] L. Picotti, Reati informatici, riservatezza, identità digitale in www. aidp.it

___3.4.1 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

L'aggiornamento della disciplina sulle comunicazioni ha richiesto un intervento articolato. Nel 1963 sono state introdotte nuove figure di reato, sul modello di quelle poste a tutela delle comunicazioni tradizionali. Facciamo riferimento alle disposizioni agli artt. 617 quater ss. Tali norme presentano alcune peculiarità riguardo la formulazione e la previsione di circostanze aggravanti, mentre non vi sono differenze in merito al regime di perseguibilità e al trattamento sanzionatorio. La disposizione è stata, inoltre, oggetto di modifica a seguito del recente intervento del legislatore nel 2021, il quale si è limitato ad innalzare le pene previste.

L'art. 617 quater c.p., ora dispone che: "Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a quattro anni". La stessa pena è prevista per "chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma". Questa norma ha lo scopo di proteggere le comunicazioni informatiche in fase di trasmissione da ogni disturbo e interferenza[185]. In una recente sentenza la Cassazione è intervenuta sul punto[186]. Ai fini della nostra analisi è interessante notare come la Corte sottolinei che gli artt. 616 e 617- quater c.p. abbiano ambiti operativi diversi. "Mentre nell'ambito dell'art. 617-quater c.p. il termine corrispondenza non comprende ogni forma di comunicazione, ma assume un significato più ristretto, riferibile alla comunicazione nel suo momento "dinamico" ossia in fase di trasmissione - come si ricava anche dai termini impiegati per definire la condotte alternative a quella di intercettazione, ossia "impedisce" e "interrompe" -, nell'art. 616 c.p., il termine "corrispondenza" risulta invece funzionale ad individuare la comunicazione umana nel suo profilo "statico" e cioè il pensiero già comunicato o da comunicare fissato su supporto fisico o altrimenti rappresentato in forma materiale, come si ricava anche in questo caso dai termini impiegati per descrivere le altre condotte tipizzate alternativamente a quella

[185] C. PECORELLA, *Diritto penale*…, cit., pag. 303.
[186] Cassazione penale sez. V, 29/09/2020, (ud. 29/09/2020, dep. 04/11/2020), n.30735 in banca dati De Jure

di illecita cognizione"[187]. Nel caso di specie, secondo la ricostruzione del fatto operata dai giudici del merito, l'agente ha intercettato le *e-mail* che venivano inviate alla moglie, nel momento in cui la loro trasmissione era in corso, cosicché, in applicazione del principio sopra esposto, non risulta applicabile l'art. 616, comma 1, c.p., né il comma 4 della medesima disposizione, che si riferisce alla divulgazione della corrispondenza "statica". Il legislatore ha, fin dall'utilizzo dei termini, mostrato tutte le sue difficoltà ad affrontare il tema della tecnologia, nella presente fattispecie[188]. Il titolo della disposizione utilizza l'espressione comunicazioni informatiche o telematiche. Tuttavia, occorre sottolineare che le comunicazioni che avvengono mediante tecnologie informatiche possono definirsi solo telematiche. L'informatica è la tecnologia che gestisce la comunicazione e quest'ultima si denomina telematica. Successivamente, nel testo, invece, il legislatore modifica il suo linguaggio e fa riferimento alle comunicazioni relative ad un sistema informatico o telematico, ma neanche tale formula può convincere. Infatti, la tecnologia è pur sempre a servizio dell'uomo e guidata ed utilizzata da questi, mentre l'attenzione viene in questo caso concentrata sul momento della comunicazione tra tecnologie. Possiamo, tuttavia, cercare di chiarire la disposizione in esame, grazie all'intervento della dottrina[189]. Con l'espressione "comunicazioni relative ad un sistema informatico", si fa riferimento a comunicazioni tra due apparecchi, uno dei quali soltanto è costituito da un sistema informatico, dal quale le comunicazioni provengono e al quale sono dirette (possiamo fare riferimento all'invio di un *fax* ad un *computer* che sia in grado di riceverlo e riprodurne il contenuto). Con l'espressione "comunicazioni informatiche tra più sistemi "si fa riferimento a comunicazioni tra sistemi informatici, ad esempio l'invio di un messaggio di posta elettronica. Questa disposizione tutela anche quelle particolari forme di conversazioni rese possibili dalle c.d. *chat line*. In questo tipo di comunicazioni, un utente può intervenire, inviando il proprio messaggio attraverso la tastiera del *computer* e altri utenti potranno replicare al dibattito in tempo reale. Poiché lo scambio di messaggi avviene in diretta, sfruttando il *computer* di un *server* che funziona come centralina telefonica, dei messaggi non rimane alcuna traccia nella memoria del *computer*. Le condotte incriminate nel primo comma sono l'intercettazione,

[187] Cassazione penale sez. V, 29/09/2020, (ud. 29/09/2020, dep. 04/11/2020), n.30735 in banca dati De Jure
[188] G. PICA*, Diritto penale*…, cit., pag. 177
[189] C. PECORELLA, *Diritto penale*…, cit.

l'impedimento o l'interruzione delle comunicazioni telematiche. Si tratta di condotte alternative. Nel caso del compimento di più condotte, non si configurerà concorso di reati, ma il soggetto sarà punibile per un unico reato, a meno che le azioni non abbiano ad oggetto delle comunicazioni telematiche distinte. Per intercettazione parte della dottrina intende la presa di coscienza, in parte o in tutto della comunicazione[190]. Altra parte della dottrina ritiene, invece, che per configurarsi l'intercettazione sia sufficiente che l'agente riesca a procurarsi i *dati* o i *file* che costituiscono l'oggetto delle comunicazioni in fase di trasmissione fra sistemi informatici e che per diventare intellegibili all'uomo devono essere successivamente trattati da un programma informatico[191]. Quest'ultima tesi sembra quella più convincente poiché, appoggiando la tesi opposta, la disposizione apparirebbe superflua. Infatti, lo scopo di punire il prendere conoscenza del contenuto delle comunicazioni informatiche è già perseguito dall'art. 616 c.p. Inoltre, il fatto che il legislatore non abbia voluto punire la presa di conoscenza del contenuto delle comunicazioni si deduce dall'art 617-quater, comma 2, che fa, invece, espresso riferimento al contenuto delle comunicazioni[192]. L'interruzione o l'impedimento della comunicazione si configura nel caso in cui l'attività di intercettazione porti a distogliere parzialmente o totalmente la comunicazione dal suo destinatario naturale e questi non la riceva o la riceva in ritardo o solo in parte. La caratteristica principale di questa condotta è la fraudolenza. Questo concetto deve intendersi in senso oggettivo, ossia come modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che trasmette la comunicazione. Sul punto è intervenuta una recente sentenza della Cassazione[193], la quale ha escluso la sussistenza dell' elemento della fraudolenza richiesto dal reato ex art. 617-quater c.p. poiché l'installazione del programma che consentiva l'intercettazione delle attività di navigazione in *internet* era conosciuta alla moglie, in quanto era stata attuata di comune accordo molti anni prima allo scopo di controllare la navigazione su *internet* della figlia minore per impedire che la stessa potesse utilizzare il *computer* per accedere a contenuti inappropriati. Nella sentenza precedente della Corte di appello che si era occupa del medesimo caso, la Corte aveva invece ritenuto sussistente l'elemento della

[190] In dottrina: G. PICA, Diritto penale…, cit., pag. 177; C. Piergallini, *I delitti contro la riservatezza della corrispondenza e delle comunicazioni*…, cit., pag. 839.
[191] I. SALVADORI, *I reati contro*…, cit., pag. 707.
[192] Ibidem
[193] Cassazione penale sez. V, 29/09/2020, (ud. 29/09/2020, dep. 04/11/2020), n.30735 in banca dati De Jure

fraudolenza poiché il soggetto aveva agito con l'intento di intercettare la corrispondenza della moglie e in alcun modo tale condotta poteva essere giustificata dall'intento di controllare l'attività informatica della figlia minore. Però anche la Corte d'appello aveva contraddittoriamente sottolineato che non era possibile stabilire quando il programma fosse stato installato e quando fosse iniziata l'attività di intercettazione. Circostanza che sembra confliggere con il dolo richiesto dai delitti di cui agli artt. 617- bis c.p. e 617-quater c.p.

A tal proposito, autorevole dottrina ritiene che solo in relazione alla intercettazione occorre che l'agente abbia agito fraudolentemente[194]. L'interruzione e l'impedimento si qualificano, secondo questa tesi, come condotte a forma libera, potendo essere eseguite con qualsiasi mezzo e nei confronti di qualsiasi interlocutore[195]. Anche parte della giurisprudenza ha accolto questa tesi. Pertanto ai fini della configurabilità del reato di interruzione di comunicazioni informatiche (art. 617 quater, comma primo, seconda parte), non sarebbe necessario l'uso di mezzi fraudolenti, essendo tale requisito riferibile esclusivamente alla condotta di intercettazione, prevista dalla prima parte dell'art. 617 quater, comma primo, cod. pen., che tutela la riservatezza delle comunicazioni dalle intromissioni abusive, attuate con captazioni fraudolente, cioè con strumenti idonei a celare ai comunicanti l'illecita intromissione dei soggetti agenti. Con riferimento all'art. 617, quater, comma primo, seconda parte, parte della giurisprudenza afferma che esso tutela la libertà delle comunicazioni, che può essere impedita con qualsiasi mezzo diretto o indiretto, anche non fraudolento[196]. Vale la pena di segnalare, tuttavia, un orientamento dottrinale, secondo il quale il requisito della fraudolenza del mezzo attraverso cui si realizza l'illecito, andrebbe esteso anche ai casi di interruzione ed impedimento delle comunicazioni[197].

Il secondo comma dell'articolo 617 quater c.p. stabilisce che "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

[194] In tal senso C. PECORELLA, cit., pag. 305.; G. Pica, cit., pag. 177; C. PIERGALLINI*, I delitti contro la riservatezza della corrispondenza…*, cit., pag. 840.
[195] C. PIERGALLINI, *I delitti contro la riservatezza della corrispondenza…*, cit., pag. 841.
[196] Cassazione penale sez. V, 30/01/2015, n.29091 in banca dati De Jure
[197] D. FONDAROLI, *La tutela penale dei "beni informatici"* in Diritto dell'informazione e dell'informatica, 1996, pag. 316

primo comma". La disposizione fa riferimento a qualunque strumento di divulgazione, ivi compresa la stessa via telematica e quindi la diffusione della comunicazione via *internet* o attraverso qualsiasi altra rete. In una sentenza si legge: "La previsione di cui all'art. 617-quater comma 2 c.p. - nel sanzionare la condotta di chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte il contenuto delle comunicazioni di cui al comma 1 - non richiede quale presupposto del reato l'intercettazione fraudolenta delle comunicazioni (sanzionata dall'art. 617-quater comma 1), in quanto la *ratio* della tutela penale è quella di evitare che siano divulgate con qualsiasi mezzo di informazione al pubblico comunicazioni cosiddette "chiuse", destinate a rimanere segrete, delle quali l'agente sia comunque venuto a conoscenza[198]. Tale orientamento è condiviso da parte della dottrina[199], sebbene occorra rilevare una tesi contraria[200]. In un caso la Cassazione ha escluso la sussistenza del reato ex art. 617- quater c.p., comma 2 poiché è necessario che la divulgazione del contenuto della comunicazione intercettata avvenga mediante qualsiasi mezzo d'informazione al pubblico, mentre nel caso di specie la divulgazione era avvenuta mediante la produzione delle *e-mail* in un giudizio di separazione personale dei coniugi pendente tra l'imputato e la persona offesa, modalità che è inidonea a rivelare il contenuto della comunicazione alla generalità dei terzi[201]. L'oggetto materiale dell'illecito resta una comunicazione interindividuale "conclusa, in atto o in procinto di essere allacciata"[202]. Non occorre che la captazione, l'interruzione o l'impedimento comportino l'effrazione di misure di protezione. La formula è ampliata tramite il disposto di cui all'articolo 623 bis c.p. del Codice penale, il quale prevede che le disposizioni contenute nella presente sezione relativa alle comunicazioni, conversazioni telegrafiche, telefoniche, informatiche o telematiche si applicano a qualunque altra trasmissione a distanza di suoni, immagini, altri dati, le quali peraltro non risultano protette da particolari dispositivi. Ne deriva che l'illecito va applicato a quelle comunicazioni c.d. chiuse, destinate a rimanere segrete[203].

[198] Cassazione penale sez. V, 19/05/2005, n.4011 in banca dati De Jure
[199] F. MANTOVANI, *Diritto penale: delitti contro la persona*, Milano, Cedam, 2019, pag. 637
[200] F. ANTOLISEI, Manuale di diritto penale, Milano, Giuffrè, 2016, pag. 249
[201] Cassazione penale sez. V, 29/09/2020, (ud. 29/09/2020, dep. 04/11/2020), n.30735 in banca dati De Jure
[202] C. PIERGALLINI, *I delitti…,* cit., pag. 842
[203] C. PIERGALLINI, *I delitti…*, cit., pag. 842

Il reato è punibile a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da tre a otto 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. La fattispecie è punibile a titolo di dolo generico, inteso, con riguardo ai casi di cui al primo comma, come volontà da parte dell'agente di inserirsi abusivamente in una comunicazione e di venire a conoscenza del contenuto oppure di interrompere od impedire *ab initio* la trasmissione; con riguardo al reato, di cui al secondo comma, quale volontà di rivelare al pubblico informazioni e dati, malgrado la consapevolezza della loro natura riservata.

___3.4.2 Installazione, detenzione, diffusione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

L'art. 617- quinquies c.p. tutela le stesse comunicazioni informatiche di cui si occupa l'art. 617- quater c.p., ma con riguardo a una serie di condotta prodromiche a quelle trattate nella disposizione antecedente. Prima dell'intervento del legislatore con la l. 238/2021, l'art. 617- quinquies c.p. disponeva che: "Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito 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 c.p.". Mentre oggi è previsto che: " Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito 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".

Il legislatore, nel 2021, ha ampliato il novero delle condotte punibili e conseguentemente la rubrica della norma che, oltre all'ipotesi già prevista di "installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni telematiche o informatiche", prevede anche quella di "detenzione e diffusione". Inoltre, il legislatore ha specificato nella rubrica che tali condotte devono essere abusive. Oltre all'installazione, precedentemente contemplata, viene sanzionata anche la condotta di chi "si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi".

Viene, altresì, introdotto il dolo specifico dato dal "fine di intercettare comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, ovvero impedirle o interromperle".

Sul versante sanzionatorio, il legislatore del 2021 non è intervenuto sull' art. 617-quinquies c.p., di cui ha confermato i limiti edittali vigenti.

La norma ricalca l'art. 617- bis c.p. e parte della dottrina ritiene che le scarse differenze tra le disposizioni non giustifichino l'introduzione della nuova fattispecie. "L'assoluta identità strutturale della fattispecie prevista dall'articolo 617-quinquies c.p. rispetto a quella già prevista, per le intercettazioni di comunicazioni o conversazioni telefoniche o telegrafiche, dall'articolo 617-bis c.p., con la mera diversificazione delle tipologie delle comunicazioni intercettate, o intercettande, lascia dedurre la inutilità dell'inserimento della nuova norma, che ben avrebbe potuto essere racchiusa in un nuovo comma del preesistente articolo 617-bis c.p., evitando l'ulteriore proliferazione della fattispecie."[204].

Il reato sussiste se il fatto avviene "fuori dai casi consentiti dalla legge". Questo significa che non saranno penalmente sanzionati gli atti di installazione realizzati da soggetti autorizzati a norma delle disposizioni del codice di procedura penale o di altre norme specifiche di legge e purché restino nei limiti previsti dalla legge. Tale clausola è stata mutuata dalla fattispecie dall'art. 617-bis. In quel contesto, la locuzione mirava ad

[204] G. PICA, *Diritto penale*…, cit., pag. 181.

escludere la punibilità delle intercettazioni di comunicazioni telegrafiche autorizzate dall'autorità giudiziaria. Questa interpretazione dovrebbe valere anche per la disposizione in esame, ma rischia di allargare eccessivamente l'ambito del reato, incriminando condotte prive di disvalore penale. Possiamo pensare all'installazione di un programma di tipo *spyware* per monitorare il corretto funzionamento di una rete aziendale da parte di un *system administrator*. Più adeguatamente, il legislatore avrebbe dovuto seguire le scelte sovranazionali e prevedere che il fatto fosse commesso senza autorizzazione o abusivamente[205]. In merito alle condotte, per i concetti di detenzione, produzione, importazione e messa in altro modo a disposizione di altri, rinvio a quanto rilevato a proposito delle analoghe aggiunte operate in seno all'articolo 615-quater del Codice penale. Per le altre aggiunte, il legislatore del 2021 ha qui inteso dare rilievo a ogni possibile condotta di attacco informatico che abbia a oggetto apparati o strumenti (o parti di apparati o di strumenti) "idonei a intercettare, impedire o interrompere comunicazioni informatiche o telematiche". Il procacciamento è commissibile da chiunque acquista in qualunque modo la disponibilità delle *res incriminate*; la riproduzione, deve intendersi come effettuazione di una copia in uno o più esemplari; la diffusione, deve intendersi come comunicazione, divulgazione, propagazione o consegna a terzi; la comunicazione, deve intendersi come sinonimo della condotta precedente. Oggetto dell'installazione sono le apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico telematico, ovvero intercorrenti tra più sistemi. Si pensi ad apparecchi e programmi informatici di tipo s*pyware* che consentono di ottenere l'accesso da remoto e di intercettare le comunicazioni[206].

Possiamo fare riferimento all'istallazione di una fotocamera digitale nel *postamat* di un ufficio postale[207]. Mentre si esclude il reato nel caso di utilizzo del cosiddetto *skimmer*, ovvero quel particolare apparecchio che, collegato abusivamente agli sportelli bancari automatici, permette di copiare all'insaputa degli utenti i dati contenuti nella banda magnetica di schede *bancomat* e carte di credito. Ciò in quanto tale apparecchio non è

[205] I. SALVADORI*, I reati informatici…*, cit., pag. 713
[206] Ibidem
[207] Cassazione penale sez. V, 22/11/2019, (ud. 22/11/2019, dep. 27/01/2020), n.3236 in banca dati De Jure

idoneo a riprendere i codici Pin dei clienti[208]. Infatti, affinché sussista il reato è necessario accertare l'idoneità dell'apparecchiatura installata a consentire la raccolta o la memorizzazione di dati[209]. Il reato, un tempo, punito a titolo di dolo generico "inteso come coscienza e volontà di installare illecitamente un dispositivo oggettivamente idoneo per intercettare, interrompere o impedire le comunicazioni relative ad un sistema informatico o intercorrenti tra più sistemi"[210], adesso è esplicitamente punito, come abbiamo detto, a titolo specifico. Tuttavia, anche prima della modifica del 2021, un orientamento riteneva che il reato fosse punibile a titolo di dolo specifico, poiché l'agente avrebbe dovuto essere mosso anche dalla volontà di intercettare, interrompere o impedire una comunicazione in corso di svolgimento[211]. Questa tesi, tuttavia non convinceva, poiché in contrasto con la precedente lettera della norma (che differisce dalla formulazione dell'art. 617 bis c.p.), la quale non richiedeva che il fine della condotta fosse quello di intercettare o impedire comunicazioni tra sistemi informatici (come nell'ipotesi prevista dall'art. 617 bis) [212]. Secondo parte della dottrina si tratterebbe di un'ipotesi di reato di pericolo indiretto, perciò il tentativo non sarebbe ammissibile[213]. Altro orientamento ritiene che la norma integri una fattispecie di pericolo concreto. "La norma, infatti, richiede espressamente che gli apparecchi siano volti ad intercettare comunicazioni. Si tratta quindi di un reato di pericolo concreto. Il giudice dovrà accertare di volta in volta che l'apparecchiatura installata sia idonea a produrre l'evento lesivo, cioè ad intercettare, impedire o interrompere comunicazioni informatiche"[214]. Tale orientamento è seguito anche in giurisprudenza[215]. Secondo la corte l'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies cod. pen.) è un reato di pericolo concreto, per la cui configurazione è necessario accertare la idoneità dell'apparecchiatura installata a consentire la raccolta o memorizzazione dei dati e non che tali operazioni siano state

[208] Cassazione penale sez. V, 22/11/2019, (ud. 22/11/2019, dep. 27/01/2020), n.3236 in banca dati De Jure
[209] Cassazione penale sez. V, 22/11/2019, (ud. 22/11/2019, dep. 27/01/2020), n.3236 in banca dati De Jure
[210] I. SALVADORI, *I reati informatici…*, cit., pag. 714.
[211] C. PECORELLA, *Diritto penale…*, cit., pag. 305.
[212] I. SALVADORI, *I reati informatici…*, cit., pag. 714.
[213] Ibidem
[214] C. PECORELLA, *Il diritto penale…*, cit., pag. 305.
[215] Cassazione penale sez. V, 22/11/2019, (ud. 22/11/2019, dep. 27/01/2020), n.3236 in banca dati De Jure

effettivamente eseguite. Infine, quanto al rapporto con altre figure criminose, se l'apparecchiatura è funzionante e viene materialmente utilizzata da colui che l'ha installata, si avrà un concorso materiale tra la fattispecie in parola ed il reato di cui all'art. 617- quater c.p.[216]. In giurisprudenza emerge un orientamento diverso, secondo cui il reato di installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies cod. pen.) è assorbito dal reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, ex art. 617, quater cod. pen.. Tale tesi si basa sul fatto che l'attività di fraudolenta intercettazione di comunicazioni informatiche presuppone necessariamente la previa installazione delle apparecchiature atte a realizzare tale intercettazione, configurandosi un'ipotesi di progressione criminosa. "Il legislatore, in altri termini, ha certamente voluto reprimere autonomamente anche la "semplice" opera di predisposizione delle apparecchiature atte a intercettare, anticipando la soglia di punibilità…, ma non si può ipotizzare che, in presenza di una effettiva attività di abusiva intercettazione, abbia voluto frazionare la condotta, ancorando la punibilità a due (distinte, ma conseguenti) azioni: la (necessitata) predisposizione e la (conseguente) intercettazione, trattandosi viceversa di un riconoscibile caso di progressione criminosa"[217].

___3.4.3 Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

L'articolo 617- sexies c.p. punisce "chiunque al fine di procurare a sé o ad altri un vantaggio o di recare 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". Questa norma ricalca la fattispecie di cui all'articolo 617- ter. Nella formulazione del reato di cui all'art. 617-sexies c.p., diversamente che in quella del reato preesistente, non si fa riferimento alla falsificazione, alterazione o soppressione del "testo" delle comunicazioni, ma del loro "contenuto". Questo ha fatto dubitare della natura

[216] C. PIERGALLINI, *I delitti*…, cit., pag. 846
[217] Cassazione penale sez. V, 18/12/2015, (ud. 18/12/2015, dep. 29/01/2016), n.4059 in Banca dati De Jure

di falso documentale (materiale) del delitto di cui trattasi. Tuttavia, si tratterebbe di un delitto di falso materiale in documento informatico privato, ai sensi del quale, la comunicazione falsamente formata è quella che non proviene dall'autore apparente[218]. In tale delitto il riferimento al testo presente nell'art 617- ter c.p. è stato sostituito con quello al contenuto, poiché, se le comunicazioni telefoniche e telegrafiche possono avere solo contenuto verbale (e quindi testuale), quelle informatiche e telematiche hanno sempre per oggetto dati che, tuttavia, possono essere rappresentativi di qualsiasi cosa: suoni, figure, filmati, ecc.[219]. Le condotte illecite punite sono la falsa formazione, l'alterazione o la soppressione della comunicazione e il successivo utilizzo da parte del soggetto agente o di un terzo. Tali condotte presuppongono la previa intercettazione, anche occasionale, del contenuto delle comunicazioni informatiche o telematiche. Irrilevanti, invece, sono le modalità con le quali l'agente è entrato nella disponibilità del contenuto dei dati informatici in fase di trasmissione tra i sistemi. In un caso[220], i giudici hanno escluso il reato di falsificazione nel caso di alterazione di pagina *Facebook* raffigurante una conversazione tra due persone. In particolare, erano state attribuite a uno dei soggetti affermazioni razziste e la conversazione alterata era stata diffusa a più persone. Nel caso la corte ha ritenuto che potesse configurarsi esclusivamente il reato di diffamazione. Questa soluzione deriva dal fatto che la falsa formazione deve riguardare il contenuto di una comunicazione intercettata nel corso della trasmissione tra sistemi informatici[221]. In un altro caso la Corte di cassazione ha, invece, ravvisato la sussistenza del reato di cui ci occupiamo nel caso della falsificazione della notifica di avvenuta lettura di una *e-mail* di convocazione per una procedura concorsuale indetta da un ente locale[222]. In altra recentissima sentenza i giudici hanno confermato la condanna ex. art. 617 sexies c.p., poiché per procurare a sé o ad altri un vantaggio, il soggetto agente aveva formato falsamente il contenuto di comunicazioni relative a sistemi informatici di diverse società, quali istituti di credito o anche PayPal, MasterCard, Visa, Carta Si, che erano state rinvenute nei *computer* e dispositivi in uso allo stesso imputato, sequestrati presso il suo domicilio. Dopo aver assunto simboli e loghi che riproducevano i siti ufficiali degli istituti

[218] V. PLANTAMURA, *La tutela penale delle comunicazioni informatiche e telematiche* in "*Diritto dell'informatica*", n.6/2006, pag. 847 ss.
[219] Ibidem
[220] Tribunale Milano sez. IV, 01/10/2018, n.8862 in banca dati "De Jure".
[221] I. SALVADORI, I reati contro la riservatezza…, cit., pag. 717.
[222] Cass. penale sez. V, 29/05/2017, n.397 in Banca dati "*De jure*"

di credito o altre società, l'imputato faceva comunicazioni ai singoli clienti, all'apparenza riferibili al medesimo istituto di credito, inducendo i clienti medesimi a fornire i propri dati, con modalità truffaldine o agiva attraverso la creazione di portali in cui invitava gli utenti ad inserire i propri dati personali[223]. Il fatto che l'articolo 617- sexies c.p. considera i dati nel momento dinamico in cui integrano il contenuto di una comunicazione, lo distingue dal reato di danneggiamento. Il reato si consuma nel momento in cui i dati contraffatti, modificati o eliminati vengono impiegati dallo stesso autore delle condotte illecite o da un terzo a cui venga concesso l'utilizzo. Il tentativo è astrattamente configurabile, anche se di difficile verificazione. La disposizione richiede il dolo specifico. Infatti, oltre alla coscienza e volontà di formare falsamente, alterare o sopprimere il contenuto di comunicazioni informatiche e di farne uso o acconsentire che terzi ne facciano uso, occorre il fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno. Il bene giuridico tutelato consiste nell'integrità, autenticità e genuinità del contenuto di dati costitutivi di comunicazioni informatiche o telematiche[224].

4. Il *locus commissi delicti* nel *cyberspace*

Ogni ordinamento giuridico deve istituire dei limiti di efficacia alla propria sovranità a livello territoriale, in modo tale da individuare la fattispecie criminosa nello spazio e nel tempo. Nei reati informatici, tuttavia, le condotte prescindono o si distanziano dalla fisicità dei comportamenti o dei fatti esteriori capaci di incorporare l'accadimento materiale[225]. Questo comporta un duplice problema, sul piano nazionale con riguardo all'attribuzione della competenza, su quello transnazionale, in relazione alla sussistenza della giurisdizione e all'eventuale violazione del *nes bis in idem*.

Il *cyberspace* consente la detemporalizzazione delle attività che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente senza necessità di un collegamento fra persona e sistema informatico. Altra peculiarità è la deterritorializzazione dell'utente, il quale può svolgere un'operazione complessa essendo presente virtualmente in più luoghi- spazi informatici anche nello stesso momento. Queste

[223] Cassazione penale sez. V, 21/01/2021 n.24211 in Banca dati "De Jure"
[224] I. SALVADORI*, I reati contro la riservatezza*…, cit., pag. 718.
[225] R. FLOR, "*La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*" in *Cybercrime* a cura di Cadoppi A, Canestrari S., Manna A., Papa M., Utet giuridica, Milano, 2019, pag. 141.

constatazioni possono facilmente mettere in crisi il diritto penale, poiché *Internet* ignora i confini territoriali, mentre gli ordinamenti necessitano di uno spazio sul quale esercitare la propria sovranità esclusiva[226]. La connessione tra diritto e spazio è tanto essenziale quanto instabile. Essa è funzionale sul territorio nazionale, ma diventa problematica quando ci si sposa in uno spazio più vasto[227]. Appare pertanto interessante la questione relativa al *locus commissi delicti* nel *cyberspace*. A tal proposito, si parla di *cyberspace,* proprio per indicare "il mondo virtuale, delocalizzato, privo di frontiere nazionali, globalizzato, nel quale è difficile, se non impossibile, calare le tradizionali categorie spaziali"[228]. Superata la teoria secondo cui la rete sarebbe uno spazio sottratto ad ogni giurisdizione[229], ci si è accorti che la difficoltà di localizzare i reati commessi nel *web* ha prodotto l'effetto contrario: ogni ordinamento potrebbe ritenere applicabile la propria legislazione e questo potrebbe portare ad una pluralità di giudicati in contrasto tra loro[230].

Per individuare una possibile soluzione alla questione relativa al *locus commissi delicti* possiamo dare uno sguardo alle teorie elaborate in ambito civilistico, in particolare nell'*e-commerce*, al fine di individuare il luogo di conclusione del contratto. La dottrina ha fatto riferimento al luogo di *up loading*, alla residenza del consumatore virtuale e al luogo nel quale l'acquirente manifesta la propria volontà con un'operazione del *mouse*. Queste soluzioni, tuttavia, ci aiutano in misura modesta a risolvere la questione del *locus commissi delicti*, poiché da un lato il sistema penale deve fare i conti con un soggetto che tende a non farsi identificare, rendendo spesso difficoltosa l'individuazione del luogo nel quale si è tenuta la condotta. Inoltre, come è quasi banale sottolineare, non è possibile ricorrere a precostituzioni consensuali di competenza penale, mentre in ambito commerciale spesso si ricorre a clausole contrattuali o precontrattuali che evitano l'insorgere di incertezze[231]. Non possiamo, pertanto che cogliere la novità della questione

[226] S. SEMINARA, *Locus commissi delicti, giurisdizione e competenza nel cyberspace* in flamminiiminuto-chiocci.it
[227] A. GARAPON, *La despazializzazione della giustizia*, Mimemis edizioni, Milano, 2021, pag. 36.
[228] D. PETRINI, *La responsabilità penale per i reati via internet,* Casa editrice Jovene, Napoli, 2001, pag. 211.
[229] BUONOMO, *Le responsabilità penali* in *I problemi giuridici di Internet* a cura di Tosi, Milano, 1999, pag. 301.
[230] C. SARZANA DI S. IPPOLITI, *I profili giuridici del commercio via internet*, Milano, 1999, pag. 172
[231] D. PETRINI, *La responsabilità*…, cit., pag. 213.

del *locus commissi delicti* e provare ad individuare una soluzione grazie al supporto di dottrina e giurisprudenza.

La nostra analisi non può prescindere dai principi tradizionalmente accolti nel nostro ordinamento in tema di *locus commissi delicti*. L'art. 6 comma 1 c.p. afferma che è punito secondo la legge italiana chiunque commette un reato nel territorio dello Stato. Inoltre, il reato si considera commesso nel territorio italiano, quando l'azione od omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione (art.6 c.p.). Dalla norma si evince l'applicazione nel nostro ordinamento del principio di territorialità, secondo il quale la legge nazionale si applica a tutti i soggetti che delinquono nel territorio dello Stato. Inoltre, il legislatore, definisce il concetto di *locus commissi delicti*, alla luce del criterio di ubiquità. In particolare, la locuzione "azione o omissione…avvenuta …in parte in Italia" ha aperto un dibattito tra gli studiosi. Ci si è chiesti se la parte di azione o omissione compiuta nel territorio dello Stato dovesse assumere gli estremi del tentativo punibile. Sembra da preferire la tesi negativa poiché l'art. 56 c.p. presuppone che "l'azione non si compia o l'evento non si verifichi", mentre l'art. 6 comma 2 c.p. prevede ipotesi delittuose che pervengono allo stadio di reati consumati[232]. Pertanto, secondo la tesi prevalente, è sufficiente accertare, sulla base di un giudizio a posteriori in concreto, che la parte o frazione di azione compiuta rappresenti un anello essenziale della condotta conforme al modello criminoso[233]. Il codice, inoltre, stabilisce cosa si intende per territorio. Questo chiarimento viene fornito dall'art. 4 del c.p.: "agli effetti della legge penale è territorio dello Stato il territorio della Repubblica e ogni altro luogo soggetto alla sovranità dello Stato". Secondo parte della dottrina il principio di territorialità costituisce, dunque il criterio principale che presiede alla disciplina relativa alla validità della legge penale nello spazio. Questo principio viene, tuttavia temperato dal contemporaneo ricorso ad altri criteri, ravvisati nel principio di personalità, universalità e difesa (artt. 7- 10 c.p.). Inoltre, come abbiamo potuto ravvisare nel precedente capitolo, la cooperazione è stata uno dei principali obiettivi a livello europeo, questo ha determinato un progressivo superamento della propensione ad utilizzare il principio di territorialità anche per "l'emersione di beni,

[232] G. FIANDACA E. MUSCO, *Diritto penale parte generale*, Zanichelli, Torino, 2019, pag. 142
[233] Ibidem.

di carattere non meramente interno o nazionale, che porta ad una trasmutazione della connessione territorio-beni nazionali da tutelare"[234].

Il d.lgs. n. 29/2016 ha dato attuazione alla decisione quadro 2009/948/GAI sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione dei procedimenti penale. La decisione ha fissato come obiettivo il miglioramento della cooperazione giudiziaria all'interno dell'Unione Europea, in modo da evitare procedimenti paralleli riguardanti gli stessi fatti e la stessa persona. Il legislatore europeo ha scelto di non fissare criteri rigidi in ordine alla risoluzione dei conflitti di giurisdizione, consentendo agli Stati di pervenire ad un accordo. Nella legislazione europea, vediamo alternativamente prospettati i criteri della territorialità, della personalità attiva e, relativamente alle persone giuridiche, del destinatario del profitto. In particolare, la Convenzione *Cybercrime* adotta il criterio della territorialità o, nel caso in cui il reato sia punibile nel luogo in cui è stato commesso ovvero non rientri nella competenza territoriale di nessuno Stato, il principio della personalità attiva[235].

Per chiarezza espositiva, occorre accennare alle disposizioni presenti all'interno del codice di procedura penale in materia di attribuzione della competenza. L'art 8 c.p.p. prevede le regole generali per l'attribuzione della competenza, secondo cui la competenza per territorio è determinata dal luogo in cui il reato è consumato. Se si tratta di reato permanente, è competente il giudice del luogo in cui ha avuto inizio la consumazione, anche se dal fatto è derivata la morte di una o più persone. Se si tratta di delitto tentato, è competente il giudice del luogo in cui è stato compiuto l'ultimo atto diretto a commettere il delitto. L'art. 9 c.p.p., stabilisce, inoltre, una serie di regole suppletive nel caso in cui la competenza non possa essere determinata ai sensi dell'art. 8 c.p.p. L'attuale assetto prevede, pertanto, in sintesi: la giurisdizione esclusiva per i fatti commessi nel territorio dello Stato, una definizione molto ampia di reato commesso nel territorio dello Stato, possibilità di applicare la legge penale italiana per fatti commessi interamente all'estero, tramite la previsione di criteri di collegamento tra fatto e ordinamento penale molto estesi.

[234] R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologia e difficoltà applicative* in *Cybercrime* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M*., Utet giuridica, Milano, 2019, pag. 145.
[235] S. SEMINARA, *Locus commissi delicti, giurisdizione e competenza nel cyberspace* in flamminiiminuto-chiocci.it

Un sistema come quello attuale, basato sul principio di ubiquità non si presta, però, a disciplinare i reati informatici, poiché sono di difficile collocazione nello spazio. "Il luogo dell'azione, rilevante ai sensi dell'articolo 6 comma 2 c.p. è pertanto parcellizzato in una infinità di spazi fisici, compreso quello in cui avviene la memorizzazione, la duplicazione, la trasmissione dei dati immessi ad altri *servers*, *computers* o snodi di rete…Il che equivale a dire che il principio di ubiquità in rete crea un forte rischio di sovrapposizione di ordinamenti giuridici diversi in ordine ai medesimi fatti"[236]. Nell'ambito della criminalità informatica è difficile individuare il luogo fisico nel quale si trova il soggetto che tiene la condotta. Questo rende difficile l'applicazione del principio di territorialità nella sua attuale dimensione. Il soggetto, infatti, potrebbe falsificare il proprio indirizzo IP oppure recarsi con un *personal computer* portatile provvisto di *modem* in una qualsiasi parte del mondo. In entrambi i casi il luogo fisico nel quale si è tenuta la condotta non sarebbe identificabile. Tuttavia, esisterebbe una dimensione spaziale certa. Si tratta del luogo nel quale è situato il *server* del *provider* che concede l'accesso ad *Internet* insieme agli altri servizi contrattualmente collegati, nonché il luogo fisico del *server* utilizzato dal *provider* per mettere in rete un sito[237].

Alla luce di tali considerazioni, occorre in primo luogo escludere le posizioni estreme, che da un lato vedono in *Internet* una realtà priva di ogni forma di localizzazione, dall'altro negano la particolarità dei reati commessi *online* dal punto di vista spaziale, ritenendo di poter semplicemente applicare i tradizionali criteri di definizione del *locus commissi delicti*. Occorre piuttosto assumere una posizione mediana. "Il principio di territorialità non può essere definitivamente abbandonato, ma deve essere rivisto"[238]. Anche parte della giurisprudenza accoglie questa tesi. In una sentenza la Corte, partendo dal principio di ubiquità, ha ritenuto che sia da considerarsi commessa nel territorio dello Stato ai sensi dell'articolo 6, comma due, l'offesa che, pur commessa all'estero, sia stata percepita in Italia dal destinatario[239]. Possiamo osservare che per affrontare la questione il principio di territorialità deve essere ripensato tenendo conto delle peculiarità che

[236] D. PETRINI, *La responsabilità*…, cit., pag. 238.
[237] Ibidem
[238] D. PETRINI, *La responsabilità*…, cit., pag. 239.
[239] Cass. Pen., Sez. V, 27/12/2000 reperibile sul sito privacy.it

caratterizzano la rete, nonché dell'attuale assetto dei rapporti con gli ordinamenti giuridici stranieri.

La soluzione ideale per risolvere il problema sarebbe, indubbiamente, quella di adottare un provvedimento sovranazionale, che impegni il maggior numero possibile di ordinamenti giuridici[240]. A livello europeo, tuttavia, sono stati fatti degli sforzi per raggiungere un simile obbiettivo. Fondamentale il ruolo di *Eurojust*, l'agenzia dell'Unione europea per la cooperazione giudiziaria penale. Questa agenzia, istituita nel 2002, sostiene il coordinamento e la collaborazione giudiziaria tra le amministrazioni nazionali nelle attività di contrasto del terrorismo e delle forme gravi di criminalità organizzata che interessano più di un paese dell'UE, compresa la criminalità informatica[241]. In particolare, coordina le indagini e i procedimenti giudiziari che interessano almeno 2 paesi, contribuisce a risolvere conflitti di giurisdizione, agevola la definizione e attuazione di strumenti giuridici dell'UE, come il mandato d'arresto europeo o i provvedimenti di confisca e congelamento[242].

Inoltre, facciamo riferimento alla previsione di cui all'articolo 22, paragrafo 5, della Convenzione di Budapest, la quale dispone che quando più parti rivendicano il proprio diritto a perseguire un'infrazione disciplinata dalla Convenzione, debbano consultarsi al fine di stabilire la competenza più appropriata per esercitare l'azione penale. Accanto ad essa si annoverano ulteriori fonti europee, emanate nella prospettiva di regolare le procedure inerenti a illeciti informatici, nella prospettiva di sanare le divergenze tra Stati che possono solo ostacolare la lotta contro codesta forma di criminalità. Si fa riferimento alla Direttiva europea 2013/40/UE, concernente gli attacchi contro i sistemi di informazione, che all'art. 12 dispone che "1. Gli Stati membri stabiliscono la propria competenza giurisdizionale relativamente ai reati di cui agli articoli da 3 a 8 quando il

[240] S. SEMINARA, *La responsabilità*…, cit., pag. 240.

[241] Nell'ultima relazione annuale del membro italiano presso Eurojust si sottolinea come, dalla complessiva operatività dell'agenzia, emerga chiaramente lo stretto connubio fra criminalità organizzata e tecnologie digitali, derivante dalla capacità delle predette organizzazioni di piegare ai propri scopi gli strumenti forniti dal web e dal deep web (soprattutto app e sistemi di pagamento on-line, che rendono le comunicazioni anonime e le transazioni di denaro difficilmente rintracciabili). Cfr. L. PRESSACO, *La relazione annuale del membro nazionale italiano presso Eurojust (2020)* in Cassazione Penale, fasc.6, 1° GIUGNO 2021, pag. 2199

[242] Con riguardo al divieto di *bis in idem* a livello transnazionale, cfr. art. 54 CAAS (Convenzione di applicazione dell'Accordo di Schengen) e art. 50 Carta dei diritti fondamentali dell'Unione europea.

reato sia stato commesso: a) in tutto o in parte sul loro territorio; o b) da un loro cittadino, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso. 2. Nello stabilire la propria competenza giurisdizionale conformemente al paragrafo 1, lettera a), uno Stato membro assicura di avere competenza giurisdizionale qualora: a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato. 3. Uno Stato membro informa la Commissione ove decida di stabilire la competenza giurisdizionale per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora: a) l'autore del reato risieda abitualmente nel suo territorio; o b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio"[243]. Tuttavia, autorevole dottrina ritiene che prima ancora di approntare misure sovranazionali riguardanti i conflitti di giurisdizione, bisognerebbe introdurre disposizioni penali omogenee in modo da consentire la respressione dei reati informatici ovunque essi siano realizzati[244]. Tale obiettivo non appare impossibile da raggiungere poiché l'opportunità di reprimere i fatti di cui ci occupiamo è ampiamente condivisa e numerosi sforzi sono stati compiuti dagli organismi europei. In particolare, il più importante tentativo di armonizzazione è stato compiuto dalla Convenzione di Budapest.

Altra dottrina propone una interessante soluzione[245]. Il fatto si considera commesso sia nel luogo nel quale l'agente ha operato in rete, sia nel territorio nel quale è situato il *server* del *provider* che concede l'accesso in rete, cioè che offre il servizio di posta elettronica, gestisce il BBS o le *chat lines* e soprattutto ha immesso in rete il sito incriminato. Questa soluzione eviterebbe anche possibili duplicazioni di giurisdizione, poiché nella maggior parte dei casi i due luoghi appartengono allo stesso ordinamento. Nel caso in cui, tuttavia, i luoghi, fossero diversi il secondo criterio dovrebbe divenire sussidiario al primo. In tal modo si esclude la rilevanza dei *server*, che hanno solamente memorizzato, duplicato o consentito il transito ai *bit* che contengono le informazioni illecite. Il criterio proposto

[243] La norma fa riferimento agli articoli da 3 a 8 della direttiva.
[244] S. Seminara, *La responsabilità penale degli operatori su internet* in *juseinternet.it*, 19 gennaio 2000
[245] D. Petrini, *La responsabilità*…, cit., pag. 246.

andrebbe poi integrato dal principio di difesa passiva, in base al quale, anche se commessi fuori dallo Stato, sarebbero punibili ai sensi della legge nazionale i fatti che pregiudicano gli interessi di un cittadino o dello Stato. Ancora si potrebbe immaginare una rilevanza sussidiaria del criterio di personalità attiva, quando si tratti di fatti di gravità tale da imporre all'ordinamento penale di perseguire i propri cittadini indipendentemente dal luogo nel quale i fatti si sono verificati. In tal modo, per quanto concerne il luogo, ove è situato il *server* del *provider* che garantisce l'accesso alla rete, si tratterebbe di un criterio sicuro. Inoltre, la combinazione dei criteri di territorialità e difesa passiva, intende affermare il principio che le eccezioni all'applicazione della legge penale per fatti commessi nel proprio territorio debbano trovare giustificazione in un significativo interesse dello Stato a perseguire i colpevoli. Interesse che viene individuato nell'esigenza di tutela delle vittime. Infine, radicare la giurisdizione per i fatti *online* che offendono l'onore, la *privacy* e il domicilio informatico nell'ordinamento dello Stato del quale la vittima è un cittadino costituisce una sorta di criterio naturale che giustifica la previsione di eccezioni alle regole generali. È quanto sostenuto anche dalla Corte costituzionale nella nota sentenza 42/96, sulla competenza per territorio[246]. Questa rappresenta una delle prospettive da cui guardare la questione.

4.1 Il caso emblematico dell'accesso abusivo a un sistema informatico: ipotesi di una soluzione

Nello sviluppo della problematica da noi tratta, risulta emblematico il caso di accesso abusivo a un sistema informatico su cui i giudici hanno avuto modo di intervenire per risolvere la questione dell'attribuzione della competenza. In giurisprudenza si sono tradizionalmente contrapposte due teorie. La prima tesi ritiene che il *locus commissi delicti* coincide con il luogo nel quale si trova il soggetto che si introduce nel sistema, la seconda si riferisce al luogo in cui è fisicamente collocata la banca dati oggetto dell'intrusione.

Nel 2015 le Sez. Unite sono intervenute per dirimere il contrasto sorto intorno al *locus commissi delicti* nell'accesso abusivo a un sistema informatico[247]. Il caso ha origine da

[246] Corte costituzionale sent. n. 42/1996 reperibile sul sito cortecostituzionale.it
[247] Sent. Cass., sez. un., 26 marzo 2015, n. 17325 reperibile sul sito eius.it

un accesso abusivo a un sistema informatico realizzato in concorso da una impiegata della Motorizzazione civile di Napoli e un amministratore di una agenzia di pratiche automobilistiche. I due soggetti si erano introdotti abusivamente e ripetutamente nel sistema informatico del Ministro delle Infrastrutture e dei Trasporti per effettuare visure elettroniche che esulavano dalle mansioni dell'impiegata e che interessavano l'amministratore dell'agenzia di pratiche. Nel 2013 il Giudice della udienza preliminare del Tribunale di Napoli aveva dichiarato la propria incompetenza per territorio ritenendo competente il Giudice del tribunale di Roma poiché riteneva che si dovesse fare riferimento al luogo in cui si trovava la banca dati che era stata violata. Il giudice dell'udienza preliminare del Tribunale di Roma, tuttavia, aveva sollevato, a sua volta conflitto negativo di competenza per territorio poiché riteneva che il luogo di consumazione del reato di accesso abusivo ad un sistema informatico dovesse radicarsi ove agiva l'operatore remoto e pertanto a Napoli. La Prima Sezione Penale a cui nel 2014 era stato rimesso il ricorso, rilevando il contrasto giurisprudenziale, aveva rimesso gli atti alle Sezioni Unite. Il quesito sottoposto alla corte è il seguente: "Se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615 ter. c.p., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il *server* che elabora e controlla le credenziali di autenticazione fornite dall'agente". Una sola sentenza della Cassazione[248] aveva approfondito il tema nel 2013 individuando il luogo di consumazione del reato nel luogo dove è materialmente collocata la banca dati violata. Secondo la tesi appoggiata dai giudici, la fattispecie risulta perfezionata nel momento in cui il soggetto entra nel sistema altrui, o vi permane, in violazione del domicilio informatico. Ne deriva che l'effettivo ingresso si realizza nel luogo in cui viene effettivamente superata la protezione informatica e si verifica la introduzione nel sistema e quindi dove è materialmente collocato il *server*, mentre la procedura di accesso deve ritenersi atto prodromico alla introduzione nel sistema. Questa tesi si basava sulla constatazione che ritenere che la condotta sia già perfezionata quando inizia il dialogo con il sistema, attraverso l'invio delle proprie credenziali di accesso,

[248] Cass. Sez. 1, n. 40303 del 27/05 2013; Con riferimento al reato di frode informatica altra sentenza (Cass., sez. 3, n. 23798 del 24/05/2012), pur senza approfondire, aveva individuato la competenza territoriale nel luogo in cui si trova il server all'interno del quale sono archiviati i dati oggetto di abusivo trattamento. In dottrina C. Piergallini, *I delitti*…, cit., pag. 781.

significa attribuire rilievo ad un momento che sarà pure quello nel quale la volontà delittuosa si realizza in modo inequivocabile ed irreversibile, ma non necessariamente è anche quello nel quale risulta offeso l'interesse protetto dalla norma incriminatrice. "La corte ha quindi in origine preferito articolare la competenza giurisdizionale secondo gli abituali schemi concettuali del mondo materiale, adottando quel criterio di fisicità che però è incompatibile con la circolazione dei dati in una rete di comunicazione telematica che ne permette la contemporanea consultazione da parte di una pluralità di utenti spazialmente diffusi sul territorio"[249]. Tale tesi, come ricordano le stesse Sezioni Unite nel 2015, era stata già criticata in dottrina e in giurisprudenza poiché l'intera architettura di un sistema per la gestione e lo scambio di dati (*server*, *client*, terminali e rete di trasporto delle informazioni) corrisponde, in realtà, ad una sola unità di elaborazione, definita sistema telematico[250]. Pertanto, il terminale mediante il quale l'operatore materialmente inserisce *username* e *password* è ricompreso, quale elemento strutturale ed essenziale, nell'intera rete di trattamento e di elaborazione dei dati, assumendo rilevanza il luogo di ubicazione della postazione con cui l'utente accede o si introduce nel sistema che contiene l'archivio informatico. Inoltre, l'adozione di questa soluzione avrebbe comportato l'allontanamento dell'autorità inquirente dal sistema utilizzato per accedere abusivamente al sistema e avrebbe reso più difficoltoso l'accertamento del reato[251].

Nel 2015 le Sezioni Unite dopo essersi soffermate sulla struttura della fattispecie ex art. 615 ter c.p., affermano di preferire la tesi che privilegia le modalità di funzionamento dei sistemi informatici e telematici, piuttosto che il luogo ove è fisicamente collocato il *server*. Infatti, il sistema informatico deve essere inteso come un complesso inscindibile nel quale le postazioni remote non costituiscono soltanto strumenti passivi di accesso o di interrogazione, ma essi stessi fanno parte integrante di un complesso meccanismo, che è strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del *client*. Alla luce di tali considerazioni la corte rileva che l'accesso inizia con l'unica condotta umana di natura materiale, consistente nella digitazione da remoto delle

[249] M.L. SCIUBA, *Osservazioni a Cass. Pen., 26 marzo 2015, sez. UU, N. 17325* in "*Cassazione Penale*" n.10/2015, pag. 3507
[250] Cass., sez. 1, n. 34165 del 15/06/2014
[251] C. PECORELLA, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico* in *Diritto penale contemporaneo*, 11 ottobre 2013.

credenziali di autenticazione da parte dell'utente, mentre tutti gli eventi successivi assumono i connotati di comportamenti comunicativi tra il *client* e il *server*. "L'ingresso o l'introduzione abusiva, allora, vengono ad essere integrati nel luogo in cui l'operatore materialmente digita la *password* di accesso o esegue la procedura di *login*, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca dati". Tale tesi è consona al concetto di giudice naturale, radicato al *locus commissi delicti* di cui all'art. 25 cost.[252]. In particolare, il principio del giudice naturale risponde all'esigenza di vedere giudicato il fatto da chi, essendo il più vicino all'ambiente nel quale esso si è verificato, risulta maggiormente legittimato a pronunciare il relativo giudizio[253]. Inoltre, che il *locus commissi delicti* sia collocato nel luogo in cui si trova l'autore del delitto si desume anche dal modo in cui risultano strutturate le circostanze aggravanti previste dal secondo comma dell'art. 615- ter c.p., poiché è sempre il luogo in cui si trova ed opera l'agente ad essere quello che meglio individua il fatto. Anche nel caso in cui il soggetto sia legittimato a introdursi nel sistema ma vi si intrattiene contro la volontà del titolare, eccedendo i limiti della autorizzazione, rileva il luogo della sua postazione periferica presso la quale vengono trasferiti i dati con la conseguenza che è irrilevante il luogo in cui è collocato il *server*. Inoltre, i giudici affermano che nelle ipotesi nelle quali non è individuabile la postazione da cui agisce il *client*, per la mobilità degli utenti e per la flessibilità di uso dei dispositivi portatili, la competenza sarà fissata in base alle regole suppletive (art. 9 cod. proc. pen.).

Tale sentenza, tuttavia, non è andata esente da critiche poiché la condotta potrebbe realizzarsi "attraverso *softwares* di controllo remoto che svolgono operazioni automatizzate e pianificate tramite la rete telematica, le quali possono essere delocalizzate rispetto alla collocazione fisica del terminale "*client*", od a quella del sistema o dello spazio informatico violati"[254]. In queste ipotesi la teoria formulata dalla Corte non offrirebbe valido supporto. Criticata, in particolare, è anche quella parte della sentenza, in cui la corte, a supporto della proprio tesi fa riferimento alle circostanze aggravanti previste dal secondo comma dell'art. 615 ter c.p., che danno rilievo alla condotta

[252] Cfr. S. BRASCHI, *La consumazione del reato,* Cedam, Milano, 2020, pag. 13.

[253] V. BELLACOSA*, Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in Diritto penale contemporaneo, 2 febbraio 2015

[254] R. FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle sezioni unite* in *Diritto penale e processo* n. 10/2015, pag. 1301.

dell'agente o alla qualifica posseduta. In questo caso i giudici legano la questione sulla competenza alle scelte di politica criminale del legislatore storico, ma in questo modo, dimostrano un approccio culturale alle problematiche poste dalle nuove tecnologie e dalla rete non adatto all'attuale contesto della società di *Internet.* Negli anni '90, il fenomeno di *internet* non era ancora esploso, pertanto, il legislatore aveva inserito delle ipotesi aggravate caratterizzate da accessi abusivi a sistemi informatici "da vicino" o, comunque, da un contatto "fisico" fra soggetto agente e terminale o spazio informatico oggetto di intrusione. "Oggi, invece, si assiste ad una continua evoluzione-rivoluzione dei sistemi e delle reti. *Cloud computing*, accessi da remoto o tramite VPN (*virtual private network*), utilizzo di *devices* mobili smaterializzano il rapporto utente - macchina. In altri termini, per accedere ad un sistema informatico non è necessario utilizzare un terminale "autorizzato", ma è possibile fruire di un proprio *device* o di postazioni pubbliche che consentano di usare le credenziali di autenticazione per accedere a spazi informatici, non sempre fisicamente e territorialmente individuabili"[255]. In questi casi la relazione uomo-macchina è evanescente. L'operatore remoto si relaziona e "colloquia" con il sistema dalla sua postazione periferica, ma tale "colloquio" avviene tramite processi di automazione delocalizzati e, nel caso di mantenimento non autorizzato, rileva penalmente con la prima violazione delle regole predisposte dal titolare dopo l'autenticazione o il dialogo con il sistema informatico di destinazione, a nulla rilevando le intenzioni dell'autore o i fini perseguiti. Per trovare una soluzione ermeneutica al quesito relativo alla competenza nella società di *Internet* è necessario ricorrere ad un approccio culturale slegato dalla nozione di territorialità "tradizionale" e più adatto al nuovo contesto tecnologico. Se accogliessimo l'impostazione della Corte, inoltre, l'agente potrebbe scegliere il luogo da cui far partire l'attacco, e con esso il luogo dove instaurare il capolinea della tracciabilità del percorso telematico.

Autorevole dottrina propone una soluzione legata al bene giuridico tutelato individuato nella riservatezza informatica, a prescindere dal luogo in cui si trova il terminale dell'agente o da quello in cui si trova il *server*. L'*iter* logico parte dall'assunto ex art. 8 c.p.p., secondo cui "la competenza per territorio è determinata dal luogo in cui il reato è stato consumato". La fattispecie penale di cui all'art. 615 ter c.p. si consuma, in caso di

[255] R. FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle sezioni unite* in *Diritto penale e processo* n. 10/2015, pag. 1302

accesso non autorizzato, con l'instaurazione del dialogo logico con il sistema informatico o telematico del titolare e, in caso di mantenimento abusivo, con la violazione delle disposizioni del titolare. L'azione umana penalmente rilevante si manifesta, pertanto, esteriormente non tanto con la digitazione di comandi sulla tastiera, bensì dopo la mediazione di processi logici di automazione e di "intermediari" tecnici che consentono la produzione degli effetti di quella attività. Perché possa instaurarsi il dialogo logico è necessaria l'"accettazione" da parte del sistema destinatario della richiesta. Inoltre, occorre osservare che la prima attività volta ad accertare l'esistenza di una violazione avviene proprio sul sistema di destinazione che si presume violato e solo dopo è possibile cercare di individuare la fonte dell'attacco o dell'abuso. Dovrebbe, pertanto, trovare applicazione una norma flessibile ed evolutiva che si basi sul legame tra il titolare dello "spazio informatico" e il bene giuridico tutelato. Nel caso in cui lo spazio informatico sia localizzabile, dovrebbe valere la regola che individua il *locus commissi delicti* nel luogo in cui si trova fisicamente lo spazio informatico o il *server* violato. Si pensi, ad esempio, all'accesso illecito alla banca dati del Ministero di un ministero che, tramite la collocazione delle relative infrastrutture logiche e fisiche è territorialmente individuabile. Nell'ipotesi in cui, invece, il reato si consumi con la violazione dell'area informatica di pertinenza del titolare la quale, però, non sia fisicamente o territorialmente individuabile o non sia circoscritta in un solo "luogo" (si pensi ai sistemi di *cloud computing* o ad architetture basate su *virtual private servers*), assume rilevanza il legame fra persona offesa, spazio informatico e bene giuridico protetto, ossia la riservatezza informatica. Ne consegue che il giudice competente dovrebbe essere quello del "luogo" in cui è "avvenuta una parte dell'azione o dell'omissione" (ex comma 1, art. 9 c.p.p.), ossia quello in cui "si trova" l'area informatica violata che, se non è territorialmente definibile, deve essere individuata tramite il legame con il suo titolare. Di conseguenza la competenza dovrebbe essere riconosciuta al giudice del luogo in cui la vittima possiede il proprio centro di interessi (domicilio, sede dell'azienda ecc., a seconda dello "spazio informatico" violato, ossia "privato", "aziendale" ecc.), in quanto riconducibile a quell'area virtuale di espressione della sua intera personalità umana[256].

[256] FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle sezioni unite* in *Diritto penale e processo* n. 10/2015, pag. 1307

Questa soluzione sarebbe in linea con il principio di universalità, o di tendenziale universalità, accolto dal nostro codice penale, anche nel caso di accessi provenienti dall'estero poiché parte della condotta abusiva (l'azione o l'omissione) si proietta sul sistema (o meglio su un'area di pertinenza esclusiva di un soggetto) situato (fisicamente o virtualmente) in Italia, con la conseguenza che il reato si può considerare comunque commesso nel "territorio" dello Stato italiano (ex comma 2, art. 6 c.p.). Dall'altro lato si adatta alla complessità tecnica di infrastrutture o architetture logiche che potrebbe determinare l'impossibilità di conoscere con esattezza l'ubicazione dell'"area informatica" e dei dati nel *cloud*, ovvero di sapere se e quando questi ultimi vengono inviati da una struttura logica ad un'altra. È bene precisare che il criterio ermeneutico che si intende proporre è "costruito" sul principio di territorialità, ma opera in forma modulare e flessibile valorizzando il legame sopra citato fra persona offesa, "spazio informatico" di sua pertinenza e bene giuridico protetto dall'art. 615 ter c.p. Questo approccio consentirebbe di evitare le innumerevoli difficoltà tecniche di localizzazione dei dati e, in ogni caso, di individuazione della "sorgente" dell'attacco, che potrebbe essere programmata *ad hoc* per beneficiare di legislazioni più permissive, se non di veri e propri "paradisi cibernetici". In secondo luogo, potrebbe spingere il titolare del sistema a concentrare i propri interessi nei luoghi o, meglio, in quei Paesi che offrono maggiori garanzie sia sul piano giuridico che su quello tecnico informatico e di *cybersecurity*, incentivando un'armonizzazione verso l'alto delle legislazioni nazionali. Tale soluzione, inoltre, supererebbe la consueta obiezione, sollevata nei casi di diffamazione *online* o di disseminazione di contenuti illeciti tramite la rete, ossia quella relativa alla questione dell'ignoranza della legge penale del luogo, quando l'agente non sia a conoscenza dell'incriminazione in quanto ritenga il fatto lecito ovvero in quanto gli assegni una rilevanza extra-penale. Tale teoria troverebbe sostegno nelle fonti europee, in particolare, l'art. 12, comma 2 della direttiva 2013/40/UE del 12 agosto 2013 e l'art. 22 della Convenzione del Consiglio d'Europa sulla criminalità informatica del 2014. Viste le difficoltà nella trattazione del tema, sarebbe, sicuramente opportuno un intervento legislativo nazionale che consideri le peculiari caratteristiche dei *cybercrimes.* In attesa di un intervento legislativo, tuttavia l'interpretazione evolutiva del principio di territorialità analizzata appare essere una soluzione adeguata.

5. Una proposta di riforma

In conclusione, facciamo riferimento a una proposta di ricollocazione sistematica delle fattispecie di cui ci siamo occupati, emessa a seguito del lavoro svolto nel 2020 dai gruppi di lavoro dell'Associazione italiana professori di diritto penale. Questa indagine risulta interessante poiché offre degli spunti di riflessione, che tuttavia il legislatore della l. 238 del 2021 ha mancato di cogliere.

Alla presente proposta hanno lavorato gli studiosi L. Picotti, R. Flor e I. Salvadori[257]. In particolare, il lavoro prevede una nuova e autonoma "Sezione VI" da aggiungere all'interno del capo III («Delitti contro la libertà individuale») del Titolo XII («Delitti contro la persona») del Libro II del Codice penale, denominata: "Dei delitti contro la riservatezza e la sicurezza informatiche". La collocazione nel Titolo XII, ed in specie nel Capo III dedicato alla "Libertà morale" si giustifica con il fatto che si tratta di delitti che offendono beni riferibili comunque alla persona, sebbene in senso lato. D'altronde dietro le comunicazioni ed i trattamenti informatici c'è sempre una persona umana od un ente. L'esigenza di autonomia anche sistematica, oltre che strutturale, delle nuove fattispecie risulta necessaria poiché i beni tutelati sono strettamente connessi con le esigenze di tutela delle reti e dei sistemi informatici.

In questa nuova Sezione VI verrebbero inserite le diverse fattispecie, in parte da riformulare, in parte da aggiungere, poste a presidio della "confidenzialità, integrità e disponibilità" (CIA) dei dati, dei sistemi informatici e delle relative comunicazioni, oltre che della "autenticità" dei trattamenti automatizzati, essendo ormai chiaramente emersa, a partire dalle fonti sovranazionali, l'esigenza di una loro specifica protezione penale. In questa nuova Sezione VI si potrebbero distinguere tre gruppi fondamentali di delitti. Un primo gruppo dovrebbe riguardare la "riservatezza informatica" intesa quale "confidenzialità" (non segretezza in senso stretto) e "disponibilità" dei dati, dei sistemi e delle stesse reti (in sintesi: di "spazi" informatici, ovunque si trovino, anche nel c.d. *cloud*), di pertinenza non solo di una persona fisica, ma anche di un ente o di una persona giuridica. Vi si devono quindi comprendere: a) il delitto di "accesso non autorizzato" ad un sistema informatico (attuale art. 615-ter c.p. che subirebbe delle modifiche); b) quello

[257] Il lavoro svolto e il testo del progetto di riforma sono reperibili sul sito aipdp.it

prodromico di “produzione e diffusione” di codici di accesso (attuale art. 615-quater c.p., parimenti da emendare); c) le “interferenze nelle comunicazioni informatiche” , compresa la corrispondenza elettronica (attuale art. 616, ultimo comma, c.p., da scorporare dall’equiparazione alla corrispondenza tradizionale, anche per quanto riguarda la tipologia delle condotte punibili), nonché altre forme di comunicazioni a distanza, cui già si richiama la disposizione estensiva di cui all’art. 623-bis c.p., che ne verrebbe assorbita; d) le “intercettazioni informatiche e telematiche” strettamente intese (attuale artt. 617-quater c.p., da emendare e semplificare), da ricondurre alle ipotesi di “interferenza” nelle menzionate comunicazioni informatiche; e) il delitto prodromico di “installazione di dispositivi atti ad intercettare, impedire od interrompere comunicazioni informatiche e telematiche” (attuale art. 617-quinquies c.p., parimenti da emendare).

Un secondo gruppo di delitti dovrebbe riguardare la “sicurezza informatica” più strettamente intesa, quale integrità ed autenticità dei dati, oltre che dei sistemi e dei trattamenti anche in rete, e comprendere: a) i vari delitti di “danneggiamento informatico” (attuali artt. 635-bis, 635-ter, 635- quater, 635-quinquies c.p.); b) il delitto prodromico di “produzione e diffusione di dispositivi idonei a danneggiare” (attuale art. 615-quinquies c.p., da emendare); c) la norma definitoria della c.d. “violenza informatica”, da rinominare più opportunamente come “interferenze non autorizzate in ambito informatico”.

Infine, in chiusura della nuova Sezione VI dovrebbe essere previsto il nuovo delitto di “violazione dell’identità digitale”. Nel presente paragrafo andremo ad analizzare le modifiche proposte alle fattispecie di cui ci siamo occupati. Secondo la proposta di riforma, il comma 1 dell’art. 615 ter prevederebbe che: “Chiunque accede senza autorizzazione o eccedendone i limiti ad un sistema informatico o ad una sua parte è punito, a querela della persona offesa, con la reclusione fino a tre anni”. Tale disposizione sarebbe in linea con quanto previsto dalle fonti sovranazionali. Attraverso la nuova formulazione, la relazione conflittuale tra i portatori di interessi contrapposti sarebbe, nel contesto virtuale, più facilmente percepibile dal soggetto agente. “Nel momento in cui l'utente “senza autorizzazione” viola una misura di sicurezza posta a protezione di un sistema informatico altrui, eccede consapevolmente i limiti della libertà di accesso e di

navigazione nel *Cyberspace*"[258]. Il riferimento all' accesso in assenza di autorizzazione viene preferito rispetto all'attuale introduzione in violazione delle misure di sicurezza poste a protezione del sistema, poiché, in tal modo verrebbe risolta la questione della rilevanza penale delle condotte dei c.d. *insider*. Tali condotte verrebbero punite poiché tali soggetti spingendosi oltre i limiti dell'autorizzazione, accedono di fatto "senza autorizzazione" a parti o spazi riservati, che sarebbero loro preclusi dal titolare o dall'ambito delle loro competenze. Il carattere abusivo o, meglio, "non autorizzato dell'intrusione" in un sistema informatico da parte dell'*insider*, verrebbe stabilito sulla base della violazione di specifici regolamenti interni, norme o disposizioni aziendali anche di natura contrattuale o comunque norme extra-penali. La mancanza di autorizzazione costituirebbe una clausola di illiceità speciale, che contribuisce alla tipizzazione oggettiva del fatto di reato. In questo modo si eviterebbero gli errori emersi da alcuni giudici, che hanno dato rilevanza alle finalità personali o soggettive dell'*insider*. Inoltre, verrebbe eliminato il riferimento al "mantenimento" nel sistema informatico, viste le difficoltà interpretative ed ermeneutiche a cui ha dato luogo. La norma prosegue, al secondo comma, nel seguente modo: "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 amministratore od operatore di sistema ; 2) se il colpevole per commettere il fatto usa violenza sulle cose o pone in essere interferenze non autorizzate in ambito informatico". Nella prima circostanza aggravante prevista dal secondo comma, si fa riferimento oltre ai soggetti già indicati all'"amministratore di sistema" che indica quei soggetti qualificati anche sul piano tecnico-informatico, che avendo il controllo delle fasi del processo di elaborazione e trattamento di dati informatici, possono disporre l'accesso con maggiore facilità ai sistemi informatici sui quali hanno competenza. Nella seconda aggravante è eliminato il riferimento al fatto che il soggetto sia palesemente armato e sostituito con il fatto che il soggetto pone in essere interferenze non autorizzate in ambito informatico. L'aggravante, nella formulazione oggi vigente, nella parte in cui contempla l'ipotesi del soggetto che accede abusivamente ad un sistema informatico «con

[258] L. PICOTTI, R. FLOR, I. SALVADORI, Reati contro la riservatezza e la sicurezza informatiche, nonché l'identità digitale in aipdp.it, 2020

violenza alle persone» ovvero di intrusione da parte di un soggetto «palesemente armato», possiede, come dimostra la sua scarsa (se non inesistente) applicazione giurisprudenziale, un ruolo del tutto marginale. Tale circostanza aggravante aveva un senso nell'epoca in cui, non essendo ancora diffusa l'interconnessione tra i *computer*, gli attacchi informatici presupponevano un contatto fisico con l'elaboratore. Con la progressiva e capillare diffusione delle reti telematiche, ed in specie di *Internet,* non è più necessario ed è anzi eccezionale che per introdursi abusivamente in un *computer* vi sia un contatto fisico con l'elaboratore attaccato o con le persone eventualmente addette alla sua sorveglianza. I criminali informatici (in specie *hacker* e *cracker)* invero sfruttano la rete per accedervi da remoto. Abrogata la terza ipotesi aggravante prevista, attualmente, al secondo comma. Infine, la norma prevederebbe, secondo il progetto di riforma che: "Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici di pubblica utilità o di una infrastruttura critica, 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". Per quanto attiene all'ipotesi ex art. 615- quater, la proposta di riforma prevede che: "Fuori dai casi previsti dall'articolo precedente , chiunque, al fine di procurare a sé o ad altri un ingiusto profitto o di arrecare ad altri un danno, abusivamente produce, procura per sé o per altri, riproduce, diffonde, comunica o consegna codici, *password* , dati informatici o altri mezzi idonei all'accesso non autorizzato ad un sistema informatico, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329 . La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 15.492 se ricorre taluna delle circostanze di cui al secondo, terzo e quarto comma dell'art. 615-ter c.p.". Importante è sottolineare la clausola di riserva iniziale, che ha lo scopo di evitare che il menzionato delitto preparatorio possa concorrere con quello più grave di accesso abusivo a un sistema informatico ex art. 615- ter c.p. Inoltre, l'impiego del concetto di "*password*", in luogo del meno appropriato «parole chiave», oltre ad essere più adeguata sul piano tecnico-informatico, è in linea con le prescrizioni di fonte sovranazionale. Infine, secondo gli studiosi sarebbe opportuno sopprimere la condotta, ulteriormente prodromica, del "fornire indicazioni o istruzioni idonee ad accedere ad un sistema informatico o telematico", dal momento che, in violazione del principio di offensività, porta ad una eccessiva anticipazione della tutela penale rispetto al bene giuridico della riservatezza informatica e, indirettamente, della

sicurezza informatica, punendo il "pericolo di un pericolo", vale a dire il pericolo di procurarsi o di produrre un codice di accesso, la cui disponibilità fa sorgere il pericolo di un accesso abusivo ad un sistema informatico. Le pene vengono peraltro allineate a quelle previste dall'attuale art. 615-quinquies non essendo il pericolo di offesa al bene giuridico della riservatezza informatica da considerare meno grave del pericolo di offesa a quello della sicurezza informatica, del resto strettamente collegato all'altro. Nel progetto di riforma, si prevede inoltre una revisione più profonda e incisiva delle comunicazioni informatiche e telematiche, in considerazione dei recenti sviluppi tecnologici, pensiamo all'intelligenza artificiale o ai *social network*. Previa abrogazione dell'ultima parte del comma 2 dell'art. 616 c.p., la riforma prevede l'introduzione all'interno della nuova "Sezione VI" del capo III del Titolo XII del Libro II del Codice penale, del seguente nuovo delitto: "Violazione della riservatezza, disponibilità ed integrità delle comunicazioni informatiche". "Chiunque senza autorizzazione intercetta, si procura, rende indisponibile ai legittimi destinatari od altera comunicazioni informatiche a lui non dirette o comunque a lui non rese disponibili da chi ha diritto di disporne, che abbiano un contenuto riservato, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni. Chiunque senza autorizzazione rivela, diffonde o rende comunque accessibile a terzi, anche mediante condivisione, riproduzione, messa a disposizione in rete, in tutto od in parte il contenuto delle comunicazioni informatiche di cui al primo comma, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a quattro anni. Agli effetti della legge penale, per "comunicazioni informatiche" si intendono quelle effettuate con ogni mezzo o tecnica di trasmissione a distanza, compresa la condivisione, riproduzione o messa a disposizione di dati informatici, che rappresentino scritti, voci, suoni, immagini anche in movimento o altri contenuti che abbiano rilevanza per la comunicazione fra persone fisiche, giuridiche, enti e sistemi informatici. Il delitto è punibile a querela della persona offesa". La fattispecie semplifica e riorganizza l'ambito delle incriminazioni concernenti le comunicazioni informatiche aventi contenuto riservato, estrapolandole dai vigenti artt. 616 e 617-ter e seguenti c.p., ed in particolare assorbendo gli artt. 617-quater, 617- quinquies e 617-sexies c.p. La fattispecie di cui all'attuale art. 615-quinquies c.p., pur da mantenere, dovrebbe essere significativamente riformulata in conformità alle prescrizioni di fonte sovranazionale (ed in specie della direttiva 2013/40/UE) e ricollocata tra i reati contro la "sicurezza

informatica", piuttosto che tra quelli contro la riservatezza informatica strettamente intesa: quindi subito dopo le fattispecie di danneggiamento di dati e di sistemi informatici (attuali artt. 635-bis, 635-ter, 635-quater, 635- quinquies c.p., da emendare e semplificare), in quanto è volta a punire comportamenti prodromici e preparatori rispetto alla consumazione di detti reati, anziché dell'accesso abusivo a sistemi informatici. La norma dovrebbe prevedere che "Salvo che il fatto costituisca più grave reato, chiunque, allo scopo di danneggiare senza autorizzazione dati o sistemi informatici, abusivamente produce, procura per sé o per altri, riproduce, importa, diffonde, comunica, consegna o mette a disposizione di altri dispositivi, programmi informatici o altri mezzi idonei a danneggiarli, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.". La previsione della clausola di riserva iniziale ha lo scopo di evitare che il delitto prodromico e preparatorio in esame possa concorrere con le più gravi fattispecie in materia di danneggiamento di dati e di sistemi informatici. Inoltre, per ragioni di economia legislativa, sembra opportuno semplificare la formulazione della fattispecie, sopprimendo il richiamo ai concetti di «informazioni» e di «programmi informatici», in quanto rientrano già in quello più ampio di «dati informatici» e limitando l'oggetto del dolo specifico al "danneggiamento" illecito di sistemi informatici o dei dati in essi contenuti, che abbraccia anche le ipotesi "speciali" di danneggiamento, che si sostanziano in una interruzione o alterazione del funzionamento di un sistema informatico. La vigente formulazione dell'art. 615-quinquies c.p. non richiede, sul piano oggettivo, l'intrinseca dannosità o pericolosità dei dispositivi che devono essere oggetto delle condotte di per sé neutre di procurarsi, produrre, diffondere, importare, distribuire o cedere suddetti oggetti materiali. Di conseguenza, il disvalore della norma incriminatrice viene a poggiare esclusivamente sul fine illecito che deve sorreggere il fatto-base. Onde evitare che vengano punite condotte prive di offensività oggettiva (ad es. chi consegna un programma informatico di per sé lecito al fine di commettere un danneggiamento di dati o di sistemi informatici) pare corretto richiedere, sul piano oggettivo, l'idoneità dei dispositivi a danneggiare dati o sistemi informatici, conservando però anche l'elemento finalistico, che serve a distinguere – nel caso di programmi e dispositivi c.d. *double use* – l'utilizzazione illecita da quella lecita (ad es. da parte di operatori di sistema che debbano testarne la sicurezza).

Capitolo III: *Cybercrime* e profili di responsabilità da reato degli enti

1. I reati informatici entrano a far parte del d.lgs. 231/2001

Nell'ambito del *cybercrime* il legislatore ha dimostrato di poter garantire una pronta risposta legislativa all'evolversi degli strumenti di offesa e dei beni oggetto di tutela[1] e nel corso dei precedenti capitoli abbiamo avuto modo di analizzare anche le più recenti novità in tema di criminalità informatica. Adesso proveremo ad incrociare tali tematiche con un'altra importante riforma all'interno del diritto penale: la responsabilità da reato degli enti. Del resto, nell'attuale società informatizzata, le imprese, indipendentemente dal settore in cui operano, fanno sempre più uso della tecnologia e raccolgono grandi masse di dati. Il rischio che vengano commessi reati informatici nel contesto aziendale ed in particolare quelli di cui ci siamo occupati nel precedente capitolo, è, quindi, sempre più alto. Ma la tecnologia non costituisce solo il mezzo per il compimento dei reati, essa vedremo incide anche sulle tecniche di prevenzione e se ne potrebbe servire, nel futuro, il giudice per compiere le proprie decisioni.

La tutela dei dati, pertanto, interessa non solo l'individuo ma anche e soprattutto le organizzazioni plurisoggettive "che, sono tenute, in un modo o nell'altro, a garantire la piena salvaguardia di tali informazioni attraverso una precipua serie di controlli e procedure atte ad evitare ogni possibile condotta finalizzata a distrarle per fini diversi ed ulteriori rispetto a quelli per cui sono state concesse"[2]. Nasce, pertanto, l'esigenza di proteggere non solo l'organizzazione e il patrimonio informatico, dal punto di vista della sicurezza, delle aggressioni esterne, ma anche di difendere la collettività dalla commissione di reati "provenienti" dall'interno della società[3]. Pertanto, *Cybercrime* e

[1] H. BELLUTA, *Cybercrime e responsabilità degli enti* in *Sistema penale e criminalità informatica* a cura di Luparia L., Milano, Giuffrè, 2009, pag. 83.
[2] P. AMODIO, *Digital compliance: spunti di riflessione e di riforma sui controlli di prevenzione e protezione dell'O.D.V*. in *Filodiritto*, 7 giugno 2021.
[3] D. FONDAROLI, *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001* in *Cybercrime* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M*., Utet giuridica, Milano, 2019, pag. 201.

responsabilità degli enti sono strettamente connessi tra loro. In particolare, "in questi settori, apparentemente così lontani, si percepiscono…la ruvidità delle prime applicazioni giurisprudenziali e i grandi spazi che l'inesperienza rimette all'opera esegetica e alla novellazione normativa"[4].

Uno dei principali problemi da affrontare è quello della immaterialità, infatti, ci troviamo ad operare con fattispecie delittuose "al limite dell'immaterialità`, quasi eteree, altamente volatili sia in fase di realizzazione sia nella successiva ricostruzione investigativa e probatoria, da un lato, e autori altrettanto immateriali, la cui struttura giuridica si avvicina al *no soul to damn, no body to kick*, dall'altro"[5]. L'estensione della responsabilità da reato degli enti a una serie di reati informatici è avvenuta in Italia, grazie alla spinta propulsiva degli obblighi assunti in sede di firma di talune Convenzioni internazionali. In particolare, ci riferiamo all'art. 7 della legge 18 marzo 2008 n. 48 che ha dato attuazione all'art. 12 della Convenzione di Budapest[6], la quale vincolava le parti firmatarie a prevedere, attraverso l'adozione di misure compatibili con i principi dell'ordinamento giuridico interno, una forma di responsabilità per le persone giuridiche nell'interesse o a vantaggio delle quali fossero stati commessi i reati informatici. La Convenzione, tuttavia, non indicava in maniera esplicita la natura della responsabilità e dunque lasciava i singoli Stati liberi di introdurre forme soltanto civili o amministrative indipendenti dal modello del decreto numero 231. Altra normativa sovranazionale che era intervenuta sul tema era la decisione quadro 2005/222/GAI sugli attacchi informatici all'art. 8[7]. Questo nuovo

[4] H. BELLUTA, Cybercrime…, cit., pag. 84.
[5] H. BELLUTA, Cybercrime…, cit., pag. 85.
[6] Art. 12 Convenzione cybercrime: 1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché le persone giuridiche possano essere ritenute responsabili di un reato in base a questa Convenzione commesso per loro conto da una persona fisica che agisca sia individualmente che come membro di un organo di una persona giuridica che eserciti un potere di direzione al suo interno, nei termini che seguono: a. un potere di rappresentanza della persona giuridica; b. un'autorità per assumere decisioni nel nome della persona giuridica; c. un'autorità per esercitare un controllo all'interno della persona giuridica. 2. In aggiunta ai casi già previsti nel paragrafo 1. di questo articolo, ogni Parte deve adottare le misure necessarie affinché una persona giuridica possa essere ritenuta responsabile se la mancanza di sorveglianza o controllo di una persona fisica di cui al paragrafo 1. ha reso possibile la commissione di reati previsti al paragrafo 1. per conto della persona giuridica da parte di una persona fisica che agisca sotto la sua autorità. 3. Secondo i principi giuridici della Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa. 4.Questa responsabilità è stabilita senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso il reato.
[7] Art. 8 decisione 2005/222/GAI: 1. Ciascuno Stato membro adotta le misure necessarie affinché le persone giuridiche possano essere ritenute responsabili dei reati di cui agli articoli 2, 3, 4 e 5 commessi a loro beneficio da qualsiasi soggetto, che agisca a titolo individuale o in quanto membro di un organo

intervento era stato giustificato dai numerosi attacchi della criminalità organizzata, che aumentavano le preoccupazioni circa la possibilità di attacchi terroristici contro i sistemi di informazione che fanno parte delle infrastrutture critiche degli Stati membri. In entrambe le normative vediamo come l'accento è posto sul ruolo assunto dalla persona che commette il reato e sulla responsabilità nel caso di mancata sorveglianza o mancato controllo. In particolare, quest'ultimo atto , "Potrebbe …offrire l'occasione per meglio adeguare le norme penali vigenti in Italia alla diversità concreta dei fatti a cui abbiamo fatto riferimento: adeguamento non nel senso ovviamente di eliminare previsioni di reato che sono pressoché tutte essenziali e devono restare nel nostro ordinamento, ma nel senso di introdurre previsioni attenuate e casi di esclusione per meglio mirarle agli obbiettivi da colpire, e diversificare o escludere il trattamento sanzionatorio nei casi di effettiva minima entità"[8]. La decisione quadro 2005/222/GAI è stata sostituita con la direttiva 2013/40/UE, che tuttavia non ha introdotto rilevanti novità. Sebbene la direttiva sia successiva all'intervento del legislatore del 2008 con cui ha esteso la responsabilità delle persone giuridiche ai reati informatici, occorre qui rilevare che l'art. 8 della decisione quadro e l'art. 10 della direttiva sono di fatto sovrapponibili. L'art. 10 prevede che: "1. Gli Stati membri adottano le misure necessarie ad assicurare che le persone giuridiche possano essere ritenute responsabili dei reati di cui agli articoli da 3 a 8, commessi a loro vantaggio da qualsiasi persona, che agisca a titolo individuale o in quanto membro di un organismo della persona giuridica, e che detenga una posizione dominante in seno alla persona giuridica basata: a) sul potere di rappresentanza della persona giuridica; b) sul potere di prendere decisioni per conto della persona giuridica; c) sul potere di esercitare il controllo in seno alla persona giuridica. 2. Gli Stati membri adottano le misure necessarie ad assicurare che le persone giuridiche possano essere ritenute responsabili qualora la

della persona giuridica, il quale detenga una posizione preminente in seno alla persona giuridica stessa, basata:

a) sul potere di rappresentanza di detta persona giuridica; o
b) sul potere di prendere decisioni per conto della persona giuridica; o
c) sull'esercizio di poteri di controllo in seno a tale persona giuridica.

2. Oltre che nei casi di cui al paragrafo 1, gli Stati membri assicurano che le persone giuridiche possano essere ritenute responsabili qualora la mancata sorveglianza o il mancato controllo da parte di uno dei soggetti di cui al paragrafo 1 abbia reso possibile la commissione dei reati di cui agli articoli 2, 3, 4, e 5 a beneficio della persona giuridica da parte di una persona soggetta alla sua autorità.

3. La responsabilità delle persone giuridiche ai sensi dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali contro le persone fisiche che siano autori, istigatori o complici di uno dei comportamenti di cui agli articoli 2, 3, 4 e 5.

[8] M. LANZIERI, *I nuovi reati informatici*, Altalex editore, Milano, 2010

mancata sorveglianza o il mancato controllo da parte di una persona di cui al paragrafo 1 abbia permesso la commissione, da parte di una persona sotto la sua autorità, di uno dei reati di cui agli articoli da 3 a 8 a vantaggio di tale persona giuridica. 3. La responsabilità delle persone giuridiche a norma dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali contro le persone fisiche che siano autori o istigatori o abbiano concorso in uno dei reati di cui agli articoli da 3 a 8". Nel corso del primo capitolo abbiamo anche analizzato gli interventi in materia di *cybersecurity*, che si sono rivolti proprio agli enti di cui ora ci occupiamo. Facciamo riferimento alla direttiva NIS, alla proposta di direttiva NIS 2.0 e al *Cybersecurity act*. Sebbene tali atti non facciano espresso riferimento alla responsabilità da reato degli enti, introducono una serie di obblighi e sanzioni in materia di sicurezza informatica che dovrebbe spingere le aziende a prendere sul serio tale tema e così prevenire anche i reati informatici che potrebbero essere commessi al loro interno.

Non mancano tuttavia di rilevare anche le ragioni economiche sottese alla introduzione di questa normativa. Va infatti riferito che, qualche giorno prima dell'entrata in vigore della legge 48/2008, il Consiglio d'Europa aveva indetto una conferenza destinata alla riunione di diversi esperti provenienti da tutto il mondo e di rappresentanti di governo, della polizia e dell'industria di *Internet*, tra cui *Microsoft*, *EBay*, *Symantec* e *McAfee*, al fine di migliorare la cooperazione internazionale in materia di crimini informatici. L'interesse economico è rilevante se si considera che è stata proprio la *Microsoft* a finanziare il progetto sulla criminalità informatica emesso nel settembre del 2006 e volto a promuovere lo sviluppo di leggi nazionali conformi alle disposizioni della Convenzione. Inoltre, nell'ottica della responsabilità para penale degli enti, non si può trascurare il profilo della tutela della concorrenza che, con l'introduzione della normativa, risulta essere più protetto. Infatti, si rileva come oggi i sistemi informatici e telematici siano un importante strumento di attuazione della concorrenza sleale tra le imprese. "La previsione di una responsabilità aziendale in caso di commissione di reati informatici potrebbe costituire sicuramente un efficace deterrente all'attività di spionaggio industriale ed economico o al semplice danneggiamento dei dati e dei sistemi informatici di una società ad evidenti fini anticoncorrenziali"[9]. Il legislatore italiano è intervenuto, come abbiamo prima accennato con l'art. 7 della legge 48/2008, attraverso l'introduzione dell'art. 24-

[9] G. CORRIAS LUCENTE, *Commento sub Art. 7 alla legge 48/2008* in *Cybercrime, Responsabilità degli enti e prova digitale* a cura di CORASANITI G. e CORRIAS LUCENTE G., Cedam, Padova, 2009, pag. 184.

bis nel corpo del d.lgs. 8 giugno 2001, n. 231, rubricato "Delitti informatici e trattamento illecito di dati". Il d.lgs. 231 del 2001 si è ormai "trasformato in un contenitore altamente elastico di una congerie eterogenea di figure criminose"[10]. Si viene così formando progressivamente un *corpus* autonomo. Il legislatore abbandona il precedente approccio *low profile* alla materia, seppur non arriva ad adottare il *modus operandi* di altri ordinamenti che hanno esteso questo tipo di responsabilità a qualsivoglia reato. La disciplina, tuttavia, suscita talune perplessità dal punto di vista sistematico poiché il legislatore aveva già affrontato il tema in precedenza. Infatti, ai sensi dell'art 24, l'ente è chiamato a rispondere del delitto di frode informatica (art. 640- ter c.p.), commessa in danno dello Stato o di altro ente pubblico. Inoltre, ai sensi dell'art. 25- quinquies, l'ente è responsabile in relazione alla commissione del delitto ex art. 600- quater c.p. in materia di pornografia virtuale. L'art. 24- bis c.p. tenendo conto degli elementi che accomunano i reati, prevede tre livelli di risposta sanzionatoria calibrati su altrettanti gruppi di fattispecie delittuose. Con il comma 1 annovera le figure di accesso abusivo ad un sistema informatico o telematico (art. 615- ter c.p.), l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617- quinquies c.p.), il danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.), il danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.), il danneggiamento di informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635- ter c.p.), il danneggiamento di sistemi informatici o telematici (art. 635- quater c.p.) e il danneggiamento di analoghi sistemi di pubblica utilità. Il profilo comune dei reati inseriti in questo primo comma è stato, talora identificato con il danneggiamento informatico. "Come tale deve intendersi ogni modifica dell'*hardware*, cioè sulla componente fisica, o sul *software*, vale a dire la componente logica del *computer*, che sia tale da impedire il relativo regolare funzionamento, sebbene solo parzialmente"[11]. Tale classificazione suscita talune perplessità poiché mentre non vi sono dubbi circa il fatto che il danneggiamento rappresenti l'elemento tipico delle fattispecie di cui al citato art. 635-bis e seguenti c.p. e 617-quater c.p., lo stesso non si può dire in ordine agli art. 615-ter e 617-quinquies c.p. Queste ultime due ipotesi di reato non sono di per sé in grado di danneggiare un sistema informatico. Pertanto, se il danno

[10] H. BELLUTA, *Cybercrime*…, cit., pag. 87.
[11] S. AETERNO, *Le fattispecie di danneggiamento informatico* in *Sistema penale e criminalità informatica* a cura di L. Luparia, Milano, Giuffrè, 2009, pag. 35 ss.

vuole essere assunto ad elemento tipico di siffatte ipotesi di reato deve necessariamente esserne assunta una concezione "potenziale". L'accesso abusivo e la detenzione di apparecchiature atte ad intercettare non producono alcun danno; tuttavia, si tratta di condotte che consentono ed agevolano l'alterazione o la distruzione di informazioni, programmi, dati ovvero sistemi informatici o telematici[12]. Il comma 2 contempla le due fattispecie della detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615- quater c.p.) e della diffusione di apparecchiature, dispositivi e programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- quinquies c.p.). Questi reati sono accomunati dal fatto di essere figure accessorie a quelle indicate al primo comma, "a mezzo delle quali il danneggiamento si realizza nel momento in cui i codici o i programmi vengono utilizzati per porre in essere accessi abusivi, intercettazioni, impedimenti o interruzioni di comunicazioni informatiche o telematiche"[13]. Vediamo, pertanto, che sono state inserite quelle fattispecie di cui ci siamo occupati nel capitolo precedente, ad eccezione dell'art. 617-sexies c.p., anche se in tale mancanza parte della dottrina rivela una lacuna[14]. Per completezza, citiamo il terzo comma all'interno del quale sono inseriti i reati di falso in documento informatico (art. 491-bis c.p.) e di frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.). In questo caso l'elemento comune consiste nell'essere reati che si compiono attraverso l'uso di sistemi informatici, e non su di essi, come nei casi dei commi 1 e 2 sopra descritti[15]. Per ciascun gruppo è prevista una diversa risposta sanzionatoria per l'ente al cui interno si sia realizzato il reato, e che ne abbia tratto un beneficio in termini di interesse o vantaggio. Per i reati richiamati al primo comma, sono previste la sanzione pecuniaria da cento a cinquecento quote e le sanzioni interdittive rappresentate dall'interdizione dall'esercizio dell'attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e dal divieto di pubblicizzare beni o servizi (art. 9, comma 2, lett. A, b, e d.lgs. 232 del 2001). Per il secondo gruppo di figure, invece, oltre alla sanzione pecuniaria sino a trecento quote, è previsto un possibile corredo

[12] Ibidem
[13] H. BELLUTA, *Cybercrime*…, cit., pag. 94.
[14] L. PICOTTI, *I delitti informatici previsti dal d.lgs. 231/2001* in Cybercrime e responsabilità da reato degli enti a cura di A. MONTI, Lavis, Giuffrè, 2022
[15] G. DEZZANI, *Una nuova ipotesi di reato…,* cit., pag. 77.

interdittivo costituito dalla sospensione o revoca delle autorizzazioni, licenze o concessioni, e dal divieto di pubblicizzare beni o servizi. Il meccanismo sanzionatorio è pertanto quello tipico per gli illeciti amministrativi dipendenti da reato. È prevista, infatti la pena pecuniaria a cui si aggiunge, nei casi previsti la sanzione interdittiva. La quantità della sanzione pecuniaria viene determinata dal giudice in due tappe. In primo luogo, occorre determinare il numero delle quote "tenendo conto della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti" (art. 11 comma 1 d.lgs. 231 del 2001). In secondo luogo, il giudice dovrà fissare l'importo della quota "sulla base delle condizioni economiche e patrimoniali dell'ente" (art. 11 comma 2 d.lgs. 231 del 2001). Quello che si evince è che il legislatore metta l'accento sul disvalore di un'atmosfera di illegalità ammessa dall'ente come costo della massimizzazione di profitti e/o del contenimento delle perdite[16]. Il gravoso apparato sanzionatorio conferma la gravità dei reati informatici. Infatti, le sanzioni interdittive possono essere predisposte anche in via cautelare (art. 45 d.lgs. 231 del 2001), quando sussistono gravi indizi per ritenere che l'ente sia responsabile dell'illecito derivante dal reato e vi siano fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede. All'interno di questa parte dell'elaborato, si cercherà di analizzare il problematico rapporto che intercorre fra le fattispecie analizzate nel secondo capitolo e la responsabilità penale delle persone giuridiche.

2. Responsabilità da reato degli enti e reati informatici

L'introduzione dei reati informatici nel d.lgs. 231/2001 ha una notevole importanza pratica poiché qualsiasi realtà aziendale si avvale della tecnologia per svolgere la propria attività e per custodire i dati. Nella casistica troviamo ipotesi di accesso non autorizzato finalizzato a ottenere dati sensibili di un'impresa (come la lista dei clienti) oppure forme di captazione abusiva di flussi di comunicazione impiegati poi a vantaggio dell'ente di appartenenza[17]. Si tratta di ipotesi affrontate già dalla giurisprudenza con riguardo alla

[16] H. BELLUTA, *Cybercrime*…, cit., pag. 95.
[17] In relazione alla responsabilità delle persone fisiche: Sent. Cass., 8 luglio 2008, n. 37322, in www.penale.it; Sent. Cass. 7 novembre 2000 n. 12732 Zara in "Cassazione Penale", n.3/2002, pag.1015 ss.

responsabilità delle persone fisiche ma che potrebbero essere ipotizzate anche con riguardo alla responsabilità da reato degli enti sussistendone i presupposti. Anche in questi casi si applicherà la normativa di cui al decreto 231. La trattazione non può perciò prescindere dall'analisi della disciplina ex D.lgs. n. 231/2001, seppure non possiamo essere in questa sede esaustivi cercheremo di soffermarci su alcuni punti chiave per delineare le conseguenze derivanti dall'estensione della responsabilità amministrativa degli enti ai reati informatici posti a tutela della riservatezza informatica e inseriti con la l. 48 del 2008 nel presente decreto. Il legislatore italiano ha introdotto il d. lgs. 231 del 2001 sotto la spinta di talune Convenzioni internazionali, ci riferiamo al II Protocollo alla Convenzione PIF 1997 del 1995, alla Convenzione UE per la lotta alla corruzione del 1997 ed alla Convenzione OCSE del 1997. In particolare, è con l'art. 2 della Convenzione OCSE, che si incontra il concetto di *Responsibility of Legal Persons*. Alla pressione esercitata a livello sovranazionale si aggiungeva, tuttavia, l'ormai evidente inefficacia degli strumenti repressivi predisposti per gli individui nel caso di reati commessi nell'ambito di specifiche politiche aziendali o che, comunque trovassero la propria matrice nella colpa organizzativa della società. "Il legislatore ha voluto così introdurre una disciplina destinata ad imporre, mediante il deterrente delle sanzioni (interdittive e pecuniarie e di condizioni esimenti la responsabilità), una maggiore eticità dell'azione imprenditoriale, attraverso l'imposizione di idonei apparati organizzativi destinati ad arginare il pericolo di commissione di reati"[18]. L'introduzione di una colpa di organizzazione a carico dell'ente svolge un'importante funzione preventiva. Infatti, ancorare il rimprovero dell'ente alla mancata ed efficace attuazione del modello organizzativo significa motivare l'ente stesso ad osservare le regole imposte.

La colpa d'organizzazione, tuttavia, è il criterio minimale sul quale si fonda la responsabilità dell'ente, nel senso che basta la colpa[19]. Il reato potrebbe anche configurarsi come espressione della politica d'impresa finalizzata alla commissione del reato: in tal caso la responsabilità troverà il proprio fondamento in una sorta di dolo dell'ente. In questa ipotesi, bisogna cercare di rendere chiara la linea di confine tra "illeciti di enti" e gli "enti illeciti". Con la prima espressione facciamo riferimento a quelle entità

[18] G. CORRIAS LUCENTE, *Commento sub Art. 7 alla legge 48/2008* in *Cybercrime, Responsabilità degli enti e prova digitale* a cura di CORASANITI G. e CORRIAS LUCENTE G., Cedam, Padova, 2009, pag. 160
[19] E. DOLCINI G.L. GATTA G. MARINUCCI, *Diritto penale parte generale*, Giuffrè, Milano, 2021, pag. 915

collettive lecite, occasionalmente coinvolte, proprio per quella "colpa di organizzazione" a cui abbiamo fatto prima cenno, nelle violazioni penali dalle quali discende la responsabilità amministrativa di cui al d.lgs. n.231/2001. In questo caso si applicano i criteri di imputazione oggettivi e soggettivi previsti dagli artt. 5, 6 e 7 e si applica il regime sanzionatorio previsto dagli artt. 9 ss. Diverso è il caso degli enti intrinsecamente illeciti, vere e proprie imprese criminali. In questo caso la strumentalizzazione dell'ente non è episodica ma strutturale, per cui l'ente è utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati. Questi non hanno un proprio specifico statuto nel d.lgs. n. 231/2001, poiché sarebbe particolarmente arduo addebitare una "colpa di organizzazione" ad una entità giuridica intrinsecamente dolosa e ben organizzata per la commissione dei reati. Per supplire a questo ostacolo, occorre fare riferimento alla previsione di cui all'art. 16 comma 3, d.lgs. n. 231/2001. La norma dispone che "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". Inoltre, disposizioni "speciali" di identico tenore sono previste dall'art. 24-ter c.p. comma 4, rispetto ai delitti di criminalità organizzata; dall'art. 25-quater comma 3, rispetto ai delitti con finalità di terrorismo o eversione dell'ordine democratico; dall'art. 25- quater, comma 2, con riferimento alle pratiche di mutilazione degli organi genitali femminili; dall'art. 25- quinquies comma 3, rispetto ai delitti contro la personalità individuale; dall'art. 25-undecies comma 8, con riferimento ad alcuni reati ambientali; dall'art. 10 comma 4 l. 146/2006 con riferimento ai reati transnazionali indicati da comma 2 dello stesso articolo. Poiché negli enti intrinsecamente illeciti è difficile individuare l'interesse che lega l'ente all'autore del reato in quanto l'ente è strumentalizzato alla commissione dell'illecito penale, si prescinde dall'indagine sull'interesse o vantaggio di cui all'art. 5, d.lgs. 231/2001 e si procede all'applicazione della sanzione interdittiva perpetua[20].

Per quanto attiene alla natura di questa forma di responsabilità da reato a carico degli enti, il dibattito è stato particolarmente acceso. In particolare, ci si è chiesti se questo tipo di responsabilità fosse di natura penale, amministrativa o se incarnasse un terzo modello.

[20] D. BADODI, Commento sub art 24-ter d.lgs 231/2001 in *Enti e responsabilità da reato a cura* di CADOPPI A. GARUTI G. VENEZIANI P, Torino, Utet giuridica, 2010

Sebbene il legislatore abbia utilizzato l'espressione "responsabilità amministrativa" anziché "penale", abbiamo ragione di credere che si tratta di una scelta di carattere simbolico volta ad alleviare le preoccupazioni sorte in ambito imprenditoriale[21]. Parte della dottrina nota che: "La responsabilità dell'ente è, infatti, strettamente agganciata alla commissione di un fatto di reato, e la sede in cui viene accertata è pur sempre il processo penale"[22]. Questo pensiero è confermato anche in giurisprudenza. La Cassazione, chiamata a pronunciarsi per la prima volta sul tema, ha affermato: "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.)" [23]. Infine, la corte arriva a formulare la tesi del *tertium genus* secondo cui la responsabilità ascrivibile all'ente sarebbe una sintesi tra materia penale e materia amministrativa. Tuttavia, non manca neppure chi sostiene si tratti un'autentica responsabilità amministrativa[24].

Per quanto attiene ai soggetti destinatari, la disciplina si applica non solo agli enti forniti di personalità giuridica, ma anche alle società e associazioni che ne sono prive, mentre non si applica allo Stato, agli enti pubblici territoriali, agli enti pubblici non economici, nonché agli enti che svolgono funzioni di rilievo Costituzionale. (Art. 1 D. lgs. 231/2001[25]).

---

[21] Citiamo, senza alcuna pretesa esaustiva, alcuni degli autori che appoggiano questa tesi: G. FIANDACA e E. MUSCO, *Diritto penale: parte generale*, Zanichelli, Bologna, 2017, pag. 175; A. LA MANNA, *La c.d. responsabilità amministrativa delle persone giuridiche: il punto di vista del penalista*, in Cass. pen., 2003, p. 1103 s. e 1109; E. MUSCO*, Le imprese a scuola di responsabilità tra pene pecuniarie e misure interdittive*, in Dir. e giust., 2001, n. 23, p. 8; C.E. PALIERO, Il d.lgs. 8 giugno 2001, n. 231: da ora in poi, societas delinquere (et puniri) potest, in Corr. giur., 2001, p. 845; ID., I criteri di imputazione e i modelli di organizzazione, in latribuna.corriere.it., p. 1; C. PIERGALLINI, Societas delinquere et puniri non potest: la fine tardiva di un dogma, in Riv. trim. dir. pen. econ., 2002a, p. 598

[22] G. FIANDACA e E. MUSCO, *Diritto penale: parte generale*, Zanichelli, Bologna, 2017, pag. 175.

[23] Facciamo riferimento alla sentenza della Corte di Cassazione, sez. II penale, n. 3615 del 30 gennaio 2006. Il testo è reperibile sul sito altalex.com

[24] G. MARINUCCI, "*Societas puniri potest": uno sguardo sui fenomeni e sulle discipline contemporanee,* in Riv. it. dir. proc. pen., 2002, p. 1201 ss.;

[25] Art. 1 d.lgs. 231/2001: 1. Il presente decreto legislativo disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.
2. Le disposizioni in esso previste si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica.
3. Non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale.

La sussistenza della responsabilità di cui ci occupiamo è subordinata alla commissione da parte di una persona fisica di uno dei reati previsti dal decreto 231 o da altra norma che richiami tale decreto e deve essere stato commesso, in forma consumata o tentata da uno dei soggetti indicati dall'art. 5. Abbiamo già avuto modo di analizzare quali tra i reati informatici sono stati inseriti all'interno della disciplina nel non lontano 2008. È necessario, inoltre, un rapporto qualificato tra l'autore del reato e l'ente. L'agente deve assumere una posizione apicale nella società, definibile in termini di rappresentanza, amministrazione, direzione, ovvero gestione o controllo di fatto, anche di unità organizzativa dotata di autonomia finanziaria e funzionale (art. 5, comma 1, lett. A d. lgs. 231/2001[26]); ovvero un rapporto di dipendenza del soggetto autore del reato da persone in posizione apicale (Art. 5, comma 1, lett. B d. lgs. 231/2001)[27].

Del resto, all'interno dell'ente o dell'azienda, uno dei fattori principali di rischio è la *Insider Threat*, cioè la minaccia proveniente da persone interne all' organizzazione e quindi dagli individui a cui fa riferimento il decreto 231[28]. Come riportato dall'ENISA *Threat Landscape* 2020- *Insider Threat*, il costo medio annuale sostenuto per singola organizzazione per riparare i danni causati da attacchi di tipo *insider* è di oltre 11. 45 milioni di euro. A mero titolo di esempio, citiamo il caso di cronaca che ha visto la Leonardo S.P.A. subire un accesso abusivo da parte di due *insiders*. Risolto, nel capitolo precedente, il dubbio circa la possibilità di realizzare un accesso abusivo da parte di un *insider*, occorrerà, sempre verificare la sussistenza degli ulteriori requisiti previsti dal d.lgs. 231/2001 per configurare una responsabilità da reato degli enti.

Essenziali, dal punto di vista dell'elemento "soggettivo" dell'illecito dell'ente, i documenti che consentono di individuare "chi deve fare cosa", poiché ai soggetti

[26] Art. 5 d.lgs. 231/2001: 1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:
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 persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi.

[27] Per una trattazione esaustiva circa l'individuazione degli apicali e dei subordinati rinvio a: BARTOLI R., Il criterio di imputazione oggettiva in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.-SEVERINO P., Giappichelli editore, Lavis, 2020

[28] L. V. MANCINI G. PAGNOTTA, *Cyberattack: tecniche di prevenzione, rilevazione e mitigazione* in *Cybercrime e responsabilità da reato degli enti* a cura di A. MONTI, Lavis, Giuffrè, 2022, pag. 1

formalmente investiti delle funzioni indicate dalla norma sono equiparati coloro che di fatto esercitano tali poteri o facoltà[29]. Facciamo riferimento all'organigramma, i mansionari e/o i funzionigrammi, il sistema delle procure e delle deleghe di funzione. La mancanza di queste ultime "è fatto che di per sé prova la mancanza di un efficace Modello organizzativo adeguato a prevenire la consumazione del reato da parte dei vertici societari"[30]. Inoltre, preme fin da subito sottolineare che poiché l'utilizzo della tecnologia è trasversale a tutti i dirigenti, titolari di funzioni e dipendenti dell'ente ovvero terzi che comunque hanno contatto con esso, risulta particolarmente complesso garantire una chiara divisione di compiti e poteri in questo ambito.

Fondamentale, affinché l'ente risulti responsabile è che il reato sia stato commesso nel suo interesse o a suo vantaggio.

Infine, non devono sussistere provvedimenti di amnistia per il reato da cui dipende l'illecito amministrativo.

Questi sono, in sintesi, i presupposti necessari, richiesti dal legislatore. Occorre ora soffermarci su alcuni punti fondamentali della disciplina.

2.1 I criteri oggettivi di imputazione

Bisogna innanzitutto chiarire il concetto di reato commesso nell'interesse o a vantaggio dell'ente, il quale rappresenta il criterio oggettivo di imputazione[31]. Con questa richiesta, secondo parte della dottrina, il legislatore ha inteso assicurare il rispetto del principio di

[29] D. FONDAROLI, *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001* in *Cybercrime* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M*., Utet giuridica, Milano, 2019, pag. 195.

[30] Cass., sez. III pen., 24/02/2017 n. 9132 in informaimpresa.it

[31] In dottrina, inoltre c'è chi ha sostenuto che la commissione del reato nell'interesse o a vantaggio dell'ente rappresenti un criterio di imputazione dell'illecito penale all'ente non soltanto sul piano oggettivo ma anche sul piano soggettivo: "il perseguimento di un vantaggio per l'ente di appartenenza, da parte del soggetto in posizione apicale, può promuovere una sorta di *translatio* del dolo di questi in capo alla *societas*; per converso, la condotta di agevolazione colposa del vertice rispetto al reato del sottoposto- pur non determinando in atto, come sopra visto, una responsabilità penale a tal titolo in capo alla persona fisica- può legittimamente suggerire il fondamento di una colpa in senso stretto riferibile all'ente come tale". Cfr. G. DE VERO, *Struttura giuridica e natura giuridica dell'illecito di ente collettivo dipendente da reato: luci e ombre nell'attuazione della delega legislativa* in Riv. it. dir. e proc. pen., fasc.4, 2001, pag. 1156

personalità, nella sua misura minima, che vieta forme di responsabilità per fatto altrui[32]. Per quanto attiene alla formula "nel suo interesse o a suo vantaggio", si registrano differenti orientamenti. Parte della dottrina ha interpretato la formula come un'endiadi, che sottende un criterio unitario incentrato su un interesse dell'ente in senso oggettivo, a prescindere da soggettive rappresentazioni o intenzioni del soggetto agente[33]. La relazione al decreto legislativo ci offre, invece, la seguente spiegazione. L'interesse caratterizzerebbe la condotta della persona fisica in senso marcatamente soggettivo, per cui sarebbe sufficiente una verifica *ex ante*[34]. Esso indica il fine in vista del quale il soggetto ha commesso il reato. Il vantaggio potrebbe essere ricavato anche quando la persona fisica non agisca per un interesse proprio occorrendo in proposito, sempre una verifica *ex post*. Pertanto, il vantaggio si connota in maniera oggettiva, facendo riferimento all'acquisizione di un profitto da parte dell'ente. La Corte di Cassazione ha già avuto modo di esprimersi sul punto. Essa ha sottolineato che l'espressione "interesse o vantaggio" si riferisce a concetti diversi sotto il profilo giuridico. "Non sembra quindi da condividere la definizione di endiadi attribuita da parte della dottrina alla locuzione: che diluirebbe, così, in più parole un concetto unitario. A prescindere dalla sottigliezza grammaticale che tale figura retorica richiederebbe la congiunzione copulativa "e" tra le parole interesse e vantaggio; e non la congiunzione disgiuntiva "o" presente invece nella norma, non può sfuggire che i due vocaboli esprimono concetti giuridicamente diversi: potendosi distinguere un interesse "a monte" della società ad una locupletazione - prefigurata, pur se di fatto, eventualmente, non più realizzata - in conseguenza dell'illecito, rispetto ad un vantaggio obbiettivamente conseguito all'esito del reato, perfino se non espressamente divisato "*ex ante*" dall'agente"[35]. Ad oggi, l'orientamento

[32] Non essendo in questa sede possibile soffermarci sulla questione rinvio, in via esemplificativa, per la trattazione del tema del rapporto tra l'art. 5 e il principio della responsabilità penale di cui all'art 27 comma 1 cost a: BARTOLI R., *Il criterio di imputazione oggettiva* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Giappichelli editore, Lavis, 2020.

[33] D. PULITANÒ, *La responsabilità da reato degli enti: i criteri di imputazione* in Riv. it. dir. e proc. pen., fasc.2, 2002, pag. 425

[34] A tal proposito segnaliamo una recente pronuncia della Cassazione in cui si rileva che pur essendo la nozione di "interesse dell'ente" caratterizzata (a differenza della nozione di vantaggio) da una prevalente connotazione soggettiva, non può prescindersi – specie se il reato è stato commesso nel prevalente interesse del singolo o di terzi – da un confronto con un parametro oggettivo, non rimesso esclusivamente ad imperscrutabili intendimenti dell'agente. (cfr. Cassazione penale sez. VI, 25/09/2018, n.54640 in banca dati De Jure)

[35] Corte di Cassazione, sez. II penale, n. 3615 del 30 gennaio 2006. Il testo è reperibile sul sito altalex.com. In senso conforme Cass. sez. II, 9 dicembre 2016, n. 52316: «In tema di responsabilità

maggioritario tiene, pertanto, i due concetti distinti. Tuttavia, si fa strada la tesi, non unanimemente accolta, della concezione oggettiva dell'interesse. Parte della giurisprudenza ha osservato che "la legge non richiede necessariamente che l'autore del reato abbia voluto perseguire l'interesse dell'ente perché sia configurabile da quest'ultimo, né è richiesto che lo stesso sia stato anche solo consapevole di realizzare tale interesse attraverso la propria condotta… la stessa previsione contenuta nell'art. 8, lett. A) del decreto (…) e l'introduzione negli ultimi anni di ipotesi di responsabilità dell'ente per reati di natura colposa, sembrano negare una prospettiva di tal genere"[36]. Si osserva, tuttavia, che l'accoglimento di quest'ultima teoria rende scarsamente visibile il confine tra interesse e vantaggio[37]. "Nella sostanza, ai fini dell'imputazione di un reato all'ente sembra essere necessario un nesso di strumentale utilità tra il reato e l'ente. E proprio perché interesse e vantaggio sono riferibili alla stessa utilità, la loro distinzione si basa sull'idea che mentre l'interesse deve essere valutato in termini potenziali rispetto alla condotta e al momento della sua realizzazione e quindi in una prospettiva *ex ante*, il

amministrativa degli enti, l'articolo 5 del decreto legislativo 8 giugno 2001 n. 231, che ne individua il presupposto nella commissione dei reati "nel suo interesse o a suo vantaggio", non contiene un'endiadi, perché i predetti termini hanno riguardo a concetti giuridicamente diversi, ed evocano criteri concorrenti, ma alternativi: il richiamo all'interesse dell'ente valorizza una prospettiva soggettiva della condotta delittuosa posta in essere dalla persona fisica da apprezzare ex ante, per effetto di un indebito arricchimento prefigurato, ma non necessariamente realizzato, in conseguenza dell'illecito; il riferimento al vantaggio valorizza, invece, un dato oggettivo che richiede sempre una verifica ex post quanto all'obbiettivo conseguimento di esso a seguito della commissione dell'illecito presupposto, pur in difetto della sua prospettazione ex ante. Da ciò deriva che i due presupposti si trovano in concorso reale, cosicché, ricorrendo entrambi, l'ente si troverebbe a dover rispondere di una pluralità di illeciti (situazione disciplinata dall'articolo 21 del decreto legislativo n. 231 del 2001)». Recentemente Cass. Sez. II pen., 9/1/2018 n. 295 in dpei.it: "Il criterio dell'interesse esprime una valutazione teleologica del reato apprezzabile *ex ante,* al momento della Commissione del fatto e secondo un metro di giudizio soggettivo in relazione all'elemento psicologico della specifica persona fisica autore dell'illecito; il criterio del vantaggio, ha, invece una connotazione essenzialmente oggettiva, come tale, valutabile *ex post* sulla base degli effetti concretamente derivati dalla realizzazione degli illecito e indipendentemente dalla finalizzazione originaria del reato. In altri ter mini, ai fini della configurabilità del reato dell'ente, è sufficiente che venga provato che lo stesso abbia ricavato dal reato un vantaggio anche quando non è stato possibile determinare l'effettivo interesse vantato *ex ante* alla commissione dell'illecito". E ancora la Cassazione rileva in tema di responsabilità da reato degli enti, i criteri di imputazione riferiti all'interesse e al vantaggio sono giuridicamente distinti giacché, mentre il primo è criterio soggettivo, da valutare ex ante, e consistente nella proiezione finalistica volta a far conseguire all'ente un profitto indipendentemente dall'effettiva realizzazione dello stesso, il secondo è criterio oggettivo, accertabile "ex post" e consistente nel concreto vantaggio derivato all'ente dal reato(Cfr. Cassazione penale sez. IV, 23/05/2018, n.38363 in banca dati DeJure).

[36] Cass., 28 novembre 2013, n. 10265 in www. studiolegaletosello.it; Cass. 27 novembre 2019, n. 49775 in sistemapenale.it

[37] R. BARTOLI, *Il criterio di imputazione oggettiva* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020, pag. 191

vantaggio costituisce invece un evento effettivo da accertare *ex post*, da riferire comunque alla condotta"[38]. Altro punto fondamentale è la nozione di utilità sottesa ai concetti di interesse e vantaggio. Essa non può essere considerata come una generica convenienza, ma pacifica è la teoria che abbia carattere patrimoniale economicamente quantificabile[39]. Se pensiamo al reato *ex* art. 615 quater c.p., potremmo fare l'esempio dell'acquisizione abusiva da parte di una società commerciale di codici di identificazione personale relativi al servizio Bancomat. Questa condotta assume estrema rilevanza, ai fini applicativi, se letta alla luce dell'orientamento della Suprema Corte che, seppur a proposito di una truffa ai danni dello Stato per la percezione di prestazioni indebite di finanziamenti e contributi ha ritenuto realizzato il profitto di rilevante entità già con il mero accredito delle somme erogate, reputando irrilevante, ai fini della elisione del dato storico del profitto, la condotta *post delictum* dell'immediato storno delle somme su conti personali dell'autore del delitto[40].

In riferimento a tale condotta è importante valutare se la persona ha agito nell'esclusivo interesse proprio o di terzi poiché in questo caso, ai sensi dell'art. 5 comma 2 d.lgs. 231/2001, è esclusa la responsabilità dell'ente. Inoltre, ai sensi dell'art. 12 comma 1 e dell'art. 13 comma 3, la sanzione pecuniaria è ridotta della metà e non può essere superiore a 103.291 euro e la sanzione interdittiva non può essere applicata nel caso in cui 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. Secondo l'interpretazione della Relazione ministeriale, che intende l'interesse di cui al primo comma in termini soggettivi, se la persona fisica ha agito per esclusiva finalità propria non può aver agito anche nell'interesse dell'ente, ne consegue che la finalità della persona fisica ad esclusivo vantaggio proprio esclude di per sé l'interesse per l'ente. Inoltre, in tale situazione il reato non si impunta all'ente anche se sussiste un vantaggio. Dall'altro lato l'art 12 fa riferimento all'ipotesi in cui l'agente abbia agito nell'interesse sia proprio che dell'ente. In questo caso si può distinguere a seconda che l'interesse proprio sia prevalente o meno. La situazione, tuttavia, si complica nel caso in cui si interpreta l'interesse in senso oggettivo, come abbiamo visto ha fatto parte della giurisprudenza.

[38] Ibidem
[39] Ibidem
[40] Cass., Sez. II pen., 20 dicembre 2005 n. 3615

Infatti, anche nel caso in cui il soggetto abbia agito nel proprio esclusivo interesse, è possibile che permanga un interesse oggettivo e che quindi la condotta sia idonea a generare una utilità per l'ente, destinata poi eventualmente a concretizzarsi in un vero e proprio vantaggio[41]. A questo punto, sono possibili due interpretazioni. Secondo la prima nel caso in cui il soggetto abbia agito per esclusivo interesse proprio, il reato non è mai imputato all'ente, anche se la condotta è oggettivamente a favore dell'ente ed anche se il reato ha prodotto un vantaggio. In base a una seconda interpretazione, nel caso in cui l'agente abbia agito per esclusivo interesse proprio bisogna distinguere due ipotesi. Se manca anche l'interesse oggettivamente inteso, la responsabilità dovrebbe essere esclusa anche se poi si verifica un vantaggio. Se, invece, sussiste anche l'interesse oggettivamente inteso, la responsabilità sussiste anche se manca il vantaggio, trovando applicazione l'art. 12. La seconda interpretazione è da preferire, secondo parte della dottrina, poiché è coerente con il rapporto utilitaristico oggettivo tra il reato e l'ente[42]. Anche la giurisprudenza sembra aderire a questo orientamento, ritenendo che se anche la persona fisica ha agito nell'esclusivo interesse proprio, la responsabilità sussiste allorché la condotta avvantaggi oggettivamente l'ente[43]. Diverso è il caso in cui l'agente commetta reati ai danni dell'ente e poi realizza ulteriori reati che possono avvantaggiare l'ente ma compiuti al solo fine di occultare i precedenti. In questo caso può essere esclusa la responsabilità dell'ente poiché i reati commessi a vantaggio dell'ente sono teleologicamente connessi con reati realizzati per danneggiare l'ente[44]. Infine, occorre precisare che il secondo comma dell'art. 5 è applicabile soltanto alle ipotesi dolose e non anche a quelle colpose poiché essendo una finalità soggettiva, l'interesse esclusivo proprio risulta compatibile soltanto con i delitti dolosi[45]. Per quanto attiene al delitto di intercettazione abusiva previsto dall'art. 617 quater e di installazione di apparecchiature atte ad intercettare ex art. 617 quinquies l'interesse sotteso a queste condotte potrebbe essere quello di carpire informazioni a fini di concorrenza sleale o altri scopi illeciti. Proprio con riferimento all'interesse o vantaggio, la giurisprudenza, seppure in materia di

[41] R. BARTOLI, *Il criterio di imputazione oggettiva* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020, pag. 195
[42] Ibidem
[43] Cass., 4 marzo 2014, n. 10265; Cass. 5 giugno 2013, n. 24559
[44] Cass., 15 novembre 2013, n. 45969 in banca dati De Jure
[45] R. BARTOLI, *Il criterio di imputazione oggettiva* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020, pag. 196

reati colposi, dovuti alla violazione di norme in materia di salute e sicurezza nei luoghi di lavoro, ha stabilito che "i criteri di imputazione oggettiva dell'interesse o vantaggio dell'ente sono riferibili alla condotta e non all'evento, in caso di reato colposi di evento", da ciò consegue che "è ravvisabile l'interesse dell'ente nel caso in cui l'omessa predisposizione dei sistemi di sicurezza, o l'inadeguatezza dell'attività di formazione e informazione dei lavoratori, determini un risparmio di spesa"[46].

Nonostante i reati presupposto di cui ci occupiamo siano dolosi, parte della dottrina non esclude una interpretazione estensiva di detto criterio nel caso in cui l'interesse dell'ente si concretizzi nel risparmio di spesa in ordine alla predisposizione di sistemi di sicurezza informatica di minore efficacia, che si dimostrino insufficienti o addirittura inesistenti, stante il considerevole impegno in termini di costi che comporta l'alta tecnologia[47]. Non si possono, tuttavia, in questa sede, nascondere le perplessità che sorgono dall'affermazione di un simile orientamento. Del resto per i reati dolosi di cui ci occupiamo, non sussistono le stesse problematiche che hanno animato il dibattito riguardo l'individuazione dell'interesse o vantaggio nel caso di reati colposi.

2.2 I criteri soggettivi di imputazione

Il decreto individua anche i criteri di carattere soggettivo. "È stato normativamente configurato un modello di colpevolezza *sui generis*, ritagliato sulle caratteristiche strutturali dell'ente, che a sua volta si ispira in larga misura al sistema dei *compliance programs* di origine nordamericana"[48]. La colpevolezza si fonda sempre sulla responsabilità soggettiva, strettamente connessa al fatto[49]. Nella relazione al decreto legislativo leggiamo: "Il reato dovrà costituire anche espressione della politica aziendale o quantomeno derivare da una colpa di organizzazione. All'ente viene in pratica richiesta l'adozione di modelli comportamentali specificamente calibrati sul rischio-reato, e cioè volti ad impedire, attraverso la fissazione di regole di condotta, la commissione di

[46] Di recente cfr. Cass., sez. IV pen., 23/11/2017, n. 53285
[47] D. FONDAROLI, *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001* in *Cybercrime* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M*., Utet giuridica, Milano, 2019, pag. 205; G. MINUCUCCI, *Reati informatici e responsabilità degli enti: vecchi e nuovi scenari* in disCrimen, 29 aprile 2022.
[48] G. FIANDACA e E. MUSCO, *Diritto penale: parte generale*, cit., pag. 178.
[49] Ibidem

determinati reati. Requisito indispensabile perché dall'adozione del modello derivi l'esenzione da responsabilità dell'ente è che esso venga efficacemente attuato". Pertanto, la colpevolezza dell'ente si configura quando il reato viene commesso da un organo, un sottoposto nell'ambito di una decisione imprenditoriale, quando il reato è conseguenza del fatto che l'ente medesimo non si è dotato di un modello di organizzazione idoneo a prevenire i reati del tipo di quello verificatosi, o altresì, quando vi è stata al riguardo omessa o insufficiente vigilanza da parte degli organismi dotati di potere di controllo[50]. Si parla di colpa o colpevolezza in organizzazione[51]. I criteri di imputazione soggettiva del reato all'ente vengono differenziati a seconda che il reato sia commesso da soggetti

[50] G. FIANDACA e E. MUSCO, Diritto penale: parte generale, cit., pag. 178
[51] Cfr. C. PIERGALLINI, Voce "Colpa" in Enciclopedia del diritto, Annali X, 2017

in posizione apicale (art. 6[52]) ovvero da persone sottoposte all'altrui direzione (art. 7[53]). Nel primo caso il legislatore è partito dal presupposto che i soggetti apicali agiscano

[52] Art. 6 d.lgs. 231/2001: 1. Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che:
a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).
2. In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle 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.
2-bis. I modelli di cui alla lettera a) del comma 1 prevedono:
(comma introdotto dall'art. 2 della legge n. 179 del 2017)
a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.
2-ter. L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.
(comma introdotto dall'art. 2 della legge n. 179 del 2017)
2-quater. Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del Codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.
(comma introdotto dall'art. 2 della legge n. 179 del 2017)
3. I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti,

secondo la volontà dell'impresa ed ha previsto pertanto un'inversione dell'onere della prova. Si tratta del "principio di identificazione", in base a cui l'ente si identifica nel soggetto in posizione apicale[54]. In questo caso sarà l'ente che per esimersi dalla responsabilità dovrà dimostrare che a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) gli apicali medesimi abbiamo commesso il reato eludendo fraudolentemente il modello di organizzazione e gestione[55]; d) che non vi è stata omessa o insufficiente sorveglianza da parte dell'organismo di vigilanza dell'ente dotato di autonomi poteri di iniziative e di controllo. Si configura una responsabilità per omessa adozione delle misure preventive idonee, sicché si tratta di una forma di violazione delle norme cautelari.

---

comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati.
4. Negli enti di piccole dimensioni i compiti indicati nella lettera b), del comma 1, possono essere svolti direttamente dall'organo dirigente.
4-bis. Nelle società di capitali il collegio sindacale, il consiglio di sorveglianza e il comitato per il controllo della gestione possono svolgere le funzioni dell'organismo di vigilanza di cui al comma 1, lettera b). *(comma introdotto dall'art. 14, comma 12, legge n. 183 del 2011)*
5. È comunque disposta la confisca del profitto che l'ente ha tratto dal reato, anche nella forma per equivalente.

[53] Art. 7 d.lgs. 231/2001: 1. Nel caso previsto dall'articolo 5, comma 1, lettera b), l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.
2. In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.
3. Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.
4. L'efficace attuazione del modello richiede:
a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

[54] P. VENEZIANI, *Art. 5 del d.lgs 231/2001* in Enti e responsabilità da reato a cura di CADOPPI A. GARUTI G. VENEZIANI P, Utet giuridica, Torino, 2010, pag. 111.

[55] Ne deriva che l'onere probatorio che grava sulla persona giuridica è quanto mai arduo tanto da far pensare ad una *probatio diabolica*: viene infatti posto a carico dell'ente il dubbio sulla dimostrazione degli inganni e dei raggiri messi in opera dai soggetti in posizione apicale per commettere un reato nell'interesse o a vantaggio della societas (CERQUA F., *Commento sub art. 6 del d.lgs 231/2001* in Enti e responsabilità da reato a cura di CADOPPI A. GARUTI G. VENEZIANI P, Utet giuridica, Torino, 2010, pag. 137). Tale prova, potrebbe risulta particolarmente difficile proprio per quanto attiene ai reati informatici, nei quali è più facile per un esperto occultare le prove.

Per quanto attiene invece al reato commesso dai sottoposti, sembra delinearsi una vera e propria fattispecie colposa (a prescindere dalla natura dolosa o colposa del reato-presupposto commesso dalla persona fisica), con una differente caratterizzazione della responsabilità per "colpa di organizzazione" dell'ente[56]. Ai sensi dell'art. 7 d.lgs. 231 l'ente è responsabile solo se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. L'inosservanza di tali obblighi è esclusa se l'ente prima della commissione del reato ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello che si è verificato.

2.3 I modelli di organizzazione e gestione

Da quanto appena analizzato si osserva pertanto l'importanza della previsione di un modello organizzativo. Il modello di organizzazione e gestione viene definito come il documento che l'ente deve predisporre con un contenuto minimo predeterminato dalla legge, in cui vengono fissati gli esiti dell'analisi del rischio e delle contromisure delle procedure di controllo e di aggiornamento individuati per la prevenzione dei reati[57]. Alcuni autori fanno discendere dal difforme tenore degli artt. 6 e 7 la necessità della predisposizione di due diversi modelli, articolati sulla differente posizione dei soggetti apicali rispetto ai subordinati. Dall'altro lato, vi è chi attribuisce le differenze terminologiche ad una mera svista del legislatore, infatti il modello di cui all'art. 6 è anche un modello di controllo, in considerazione degli obblighi di informazione all'organismo di vigilanza espressamente previsti[58]. La tesi dualistica non è accolta nella prassi aziendale, che spesso ricorre a clausole *ad hoc* incentrate sugli obblighi di controllo degli apicali[59].

---

[56] P. VENEZIANI, *Art. 5 del d.lgs. 231/2001* in Enti e responsabilità da reato a cura di CADOPPI A. GARUTI G. VENEZIANI P, Utet giuridica, Torino, 2010, pag. 112

[57] Cfr. F. CERQUA, *Commento sub art. 6 del d.lgs. 231/2001* in Enti e responsabilità da reato a cura di CADOPPI A. GARUTI G. VENEZIANI P, Utet giuridica, Torino, 2010; PIERGALLINI C., *I modelli organizzativi* in Reati *e responsabilità degli enti. Guida al d.lgs. 8 giugno 2021, n. 231*, Milano, Giuffrè editore, 2010; GULLO A., *I modelli organizzativi* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020.

[58] G. LASCO, Commento sub art. 7 d.lgs. 231/2001 in *Enti e responsabilità da reato* a cura di LASCO G., LORI V., MORGANTE M., Giappichelli Editore, Trofarello, 2017, pag. 119.

[59] R. BARTOLI, Il criterio di imputazione oggettiva in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Giappichelli editore, Lavis, 2020, pag. 213

Uno dei primi quesiti interpretativi su cui occorre soffermarsi attiene all'obbligatorietà dell'adozione del modello organizzativo. Autorevole dottrina ha risposto a tale quesito, affermando che la sua mancata adozione sarebbe sufficiente a fondare la rimproverabilità dell'ente[60]. Anche parte della giurisprudenza si è allineata a questa linea di pensiero. Secondo la Cassazione nel concetto di rimproverabilità dell'ente rientrerebbe "una nuova forma di colpevolezza per omissione organizzativa e gestionale, avendo il legislatore ragionevolmente tratto dalle concrete vicende occorse in questi decenni, in ambito economico e imprenditoriale, la legittima e fondata convinzione della necessità che qualsiasi complesso organizzativo costituente un ente ai sensi del d.lgs. art. 1, comma 2, adotti modelli organizzativi e gestionali idonei a prevenire la commissione di determinati reati, che l'esperienza ha dimostrato funzionali a interessi strutturati consistenti, giacché le principali e più pericolose manifestazione di reato sono poste in essere da soggetti a struttura organizzativa complessa"[61]. Ne deriva, dunque, che secondo l'orientamento della giurisprudenza di legittimità, dagli artt. 5 e 6 scaturisce il principio di diritto per cui l'ente che abbia omesso di adottare e attuare il modello organizzativo non risponde per il reato presupposto imputato, commesso dal suo esponente in posizione apicale, soltanto nell'ipotesi in cui l'autore persona fisica abbia agito nel proprio interesse o in quello di terzi[62]. La dottrina maggioritaria, ritiene invece che l'adozione di un modello organizzativo non costituisca un obbligo giuridico, trattandosi invece di un onere che comporta determinati benefici[63]. Una posizione mediana ritiene, invece, che l'adozione dei modelli sia obbligatoria per i reati dei sottoposti ma non per quelli dei soggetti apicali[64].

Nell'ambito dei reati informatici, di cui ci occupiamo, sembra di andare in direzione dell'obbligatorietà di tali modelli, alla luce delle sanzioni, del potere sempre maggiore in capo all'ENISA e dei numerosi atti nazionali e sovranazionali intervenuti in materia di *cybersecurity*, di cui ci siamo occupati nel capitolo 1 e che hanno imposto obblighi sempre

[60] C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale*, part. 1, in Cass. pen., fasc.1, 2013
[61] Cass. pen., 9/7/2009, n. 36083, pag. 382 ss.
[62] Cass. pen., 9/7/2009, n. 36083
[63] Cfr. F. CERQUA, *Commento sub art. 6 del d.lgs. 231/2001* in Enti e responsabilità da reato a cura di CADOPPI A. GARUTI G. VENEZIANI P, Utet giuridica, Torino, 2010; BARTOLI R., Il criterio di imputazione oggettiva in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Giappichelli editore, Lavis, 2020, pag. 215; In giurisprudenza: Cass. 25 novembre 2018, n. 5664
[64] D. PULITANÒ, *La responsabilità da reato degli enti: i criteri di imputazione* in Riv. it. dir. e proc. pen., fasc.2, 2002, pag. 431.

più incisivi in capo agli enti. Facciamo riferimento, in primo luogo, alla direttiva NIS e al *Cybersecurity act*[65]. La prima diretta agli operatori di servizi essenziali (OES) stabiliti nell'Unione europea[66] e ai *digital service providers* (DPS)[67], introduce una serie di notifica degli incidenti e impone agli Stati di introdurre delle sanzioni adeguate. Il *Cybersecurity act*, invece, è volto a introdurre sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC valutati nel loro ambito siano conformi a determinati requisiti di sicurezza. Sebbene ci occuperemo in maniera più approfondita di tali temi nel proseguimento di questo lavoro, giova qui anticipare che parte della dottrina prospetta sistemi integrati di *compliance*[68]. Con tale espressione fa riferimento alla previsione, accanto ai presidi organizzativi volti alla prevenzione di determinati reati di cui si occupa il decreto 231, di specifici obblighi di *compliance* oggetto di autonoma sanzione amministrativa[69]. D'altronde come abbiamo visto nel corso del primo capitolo, i settori della sicurezza nazionale cibernetica e della protezione dei dati personali, si connotano per una serie di obblighi che hanno l'obiettivo di spingere le imprese ad adottare una serie di misure di carattere tecnico e organizzativo, proprio al fine di prevenire violazioni ma muniti di sanzioni *ad hoc*, per cui tale tesi sembra fondata[70].

Si potrebbe trattare di un primo passo verso l'obbligatorietà del modello che adeguatamente regolata, potrebbe favorire l'ente in sede di valutazione giudiziale [71]. Si tratta di una prospettiva *de jure condendo*, che proveremo a vagliare più approfonditamente nel proseguimento di questo lavoro.

[65] Di tali atti mi sono occupata nel capitolo uno di questa tesi, a cui rinvio per una trattazione approfondita.
[66] Si tratta dei soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali;
[67] Si tratta delle persone giuridiche che forniscono servizi della società dell'informazione, delle persone giuridiche che forniscono servizi di *e-commerce, cloud computing* o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.
[68] A. GULLO, *I modelli organizzativi* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020, pagg. 284-285
[69] Ibidem
[70] Ibidem
[71] BARTOLI R., *Il criterio di imputazione oggettiva* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Giappichelli editore, Lavis, 2020, pag. 216.

Il modello organizzativo previsto dal decreto non deve essere soltanto elaborato e adottato formalmente, ma deve essere altresì efficacemente attuato. La corretta attuazione del modello richiede una verifica periodica e l'eventuale modifica dello stesso quando siano scoperte significative violazioni delle prescrizioni, ovvero quando intervengano mutamenti nell'organizzazione aziendale, nell'attività svolta o si registrino modifiche normative[72]. Un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal modello e un idoneo piano di informazione e formazione del personale[73]. Oltre all'adozione di modelli organizzativi idonei a prevenire la commissione dei reati l'articolo sei del decreto prevede che il compito di vigilare sul funzionamento e sull'osservanza del modello nonché di curarne l'aggiornamento, sia affidata ad un organismo dotato di autonomi poteri di iniziativa e controllo. Il comma 3 dell'art. 6 prevede la possibilità che i modelli organizzativi e di gestione siano adottati, garantendo le esigenze di cui al secondo comma della norma in commento, sulla base di codici di comportamento redatti dalle associazioni degli enti. Queste linee guida, come chiarito dalla Relazione governativa, svolgono il ruolo di "promuovere già all'interno delle categorie interessate il rispetto della legge e di implementare la formazione di codici tecnicamente strutturati che possano fungere da utile punto di riferimento operativo per i soggetti interessati". I codici etici delle associazioni devono essere comunicati al Ministro della giustizia, che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati. In particolare, si ritiene che tale controllo sia funzionale ad evitare la formazione di codici comportamentali meramente formali, inutili o inidonei. Tuttavia, ad oggi, l'adozione di tali modelli non è segno, in sede giudiziale, di idoneità del modello. "Il significato dell'introduzione dei modelli risiede nell'intento di garantire lo svolgimento delle attività nel rispetto della legge e scoprire ed arginare tempestivamente le situazioni di rischio che devono ricondursi ad un rischio così detto accettabile, secondo quanto stabilito dalle Linee guida di Confindustria"[74].

Sembra opportuno approfondire gli elementi fondamentali di tali modelli, tenendo presente che ogni modello organizzativo deve essere costruito *ad hoc* per l'ente,

[72] CORRIAS LUCENTE G., *Commento sub Art. 7 alla legge 48/2008* in *Cybercrime, Responsabilità degli enti e prova digitale* a cura di CORASANITI G. e CORRIAS LUCENTE G., Cedam, Padova, 2009, pag. 171
[73] Ibidem
[74] Ibidem

costituendo tali linee guida soltanto un valido documento comune denominatore. Per essere efficace, infatti, il modello deve tener conto della natura del settore economico, della complessità organizzativa della singola azienda e dell'area geografica in cui l'ente esercita la propria attività. Ecco perché successivamente, andremo ad analizzare cosa in concreto dovrebbe prevedere un modello organizzativo che intenda prevenire i reati informativi. Quello della *compliance* è, infatti, un settore in cui l'autonormazione svolge un ruolo fondamentale. "Soprattutto con riguardo alla criminalità dolosa (quella del profitto), l'ente, con un procedimento autenticamente maieutico, deve ritagliare cautele di taglio 'frappositivo', idonee a ridurre il rischio-reato. Dunque, si staglia sullo sfondo un complicato laboratorio 'cautelare', interamente autonormato. La prassi, sinora maturata, testimonia di un ricorso informativo alle linee-guida, ma sta di fatto che il modello resta pur sempre un abito da cucire su misura, che impone la mobilitazione di risorse umane ed economiche non trascurabili"[75]. L'adozione di un modello efficace presuppone il compimento di numerose attività: una fase preliminare di analisi dell' organizzazione societaria, attraverso un approfondito studio dell'organigramma aziendale e delle attività svolte dalle singole funzioni; l'individuazione delle aree cosiddette sensibili; l'analisi del sistema di controllo preventivo esistente; la elaborazione dei protocolli interni per la formazione, attuazione delle decisioni dell'ente, soprattutto nei processi per attività cosiddette sensibili, affinché i rischi identificati vengano portati ad un grado accettabile; la previsione di idonei corsi di formazione e di flussi informativi obbligatori verso l'organismo di vigilanza[76].

La legge 30/11/2017 n. 179, recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano avvenuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", ha aggiunto all'articolo sei[77] ulteriori previsioni dedicate alla tutela del segnalante di fatti illeciti di presunta rilevanza ai fini del Decreto. La normativa è ispirata alla regolamentazione in materia di pubblica amministrazione prevista dalle disposizioni relative alle misure di prevenzione e contrasto della corruzione che hanno attuato e rafforzato il sistema introdotto dalla l. n. 190/2012 in materia di tutela del dipendente pubblico che segnala illeciti. Il tema del *whistleblowing*, che impone alle

[75] C. PIERGALLINI, *Autonormazione e controllo penale in Diritto penale e processo* n.3/2015, pag. 265.
[76] G. CORRIAS LUCENTE, *Commento sub Art. 7 alla legge 48/2008*, cit., pag. 172
[77] Rinvio a nota 51 per il testo completo dell'art. 6 d.lgs. 231/2001

società di adottare misure al fine di garantire la riservatezza del soggetto che segnala il reato o violazioni del MOG e ad assicurare il corretto utilizzo dello strumento della segnalazione, costituisce un profilo di grande rilevanza per verificare l'applicazione del decreto. Infatti, le conseguenze sul piano lavoristico per la violazione della privatezza del segnalante appaiono di rilevanza tale da poter dissuadere le società dalla adozione di un modello di organizzazione che incida radicalmente sull'organizzazione dell'impresa, anche sotto il profilo dei rapporti con i lavoratori[78].

2.4 La responsabilità penale dell'Organismo di Vigilanza

L'ente, al fine di usufruire dell'esonero da responsabilità, deve provare di avere affidato il compito di vigilare sul funzionamento e l'osservanza del modello ad un organismo dotato di autonomi poteri di iniziative di controllo e deve dimostrare che tale organismo non abbia omesso o reso insufficiente questa vigilanza. Si tratta dell'Organismo di Vigilanza. La legge in realtà, pur sottolineando il fatto che l'organismo debba garantire l'effettività dei controlli non fornisce indicazioni specifiche sulla composizione dello stesso, potrebbe quindi trattarsi di un organo monocratico o collegiale, composto da un organo sociale già esistente o di essere istituito *ad hoc*[79]. I pochi richiami si desumono dall'art. 6 d.lgs. 231/2001, dove si fa riferimento alla titolarità in capo all'Organismo di autonomi poteri di iniziativa e controllo e si attribuisce ad esso il compito di vigilare sul funzionamento e l'osservanza del modello. Un richiamo ancora è contenuto nella lett. D), a proposito dei flussi normativi. Il comma 4 dell'art. 6 d.lgs. 231/2001 dispone che "Negli enti di piccole dimensioni i compiti indicati nella lettera b), del comma 1, possono essere svolti direttamente dall'organo dirigente". Inoltre, il comma 4-bis dello stesso articolo afferma che "Nelle società di capitali il collegio sindacale, il consiglio di sorveglianza e il comitato per il controllo della gestione possono svolgere le funzioni dell'organismo di

[78] D. FONDAROLI, *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001* in *Cybercrime* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M*., Utet giuridica, Milano, 2019, pag. 199

[79] Per una trattazione esaustiva delle questioni relative alla composizione dell'Organismo di Vigilanza rinvio a: A. GULLO*, I modelli organizzativi* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Giappichelli editore, Lavis, 2020; V. MONGILLO, L'Organismo di vigilanza, cit.; R. SACCHI, *L'organismo di vigilanza ex d. lgs. n. 231* in Giur. comm., fasc.6, 2012; RORDOF R., *L'Organismo di vigilanza nel quadro del D.lgs. n. 231/2001* in Le società n.1/2022.

vigilanza di cui al comma 1, lettera b)"[80]. Nulla ci dice il decreto sulla nomina dell'Organismo e sulla sua composizione, sui requisiti di qualificazione dei suoi componenti, sulla sua concreta operatività e sui suoi poteri, che vengono solitamente indicati nello Statuto e nel Regolamento interno dell'organo.

Il dibattito più acceso ha riguardato il tema delle competenze dei componenti e delle modalità di svolgimento dell'attività dell'Organismo. In sintesi, i caratteri che sembrano emergere sono quelli dell'onorabilità e della professionalità, dell'autonomia e dell'indipendenza e, infine, della continuità d'azione dell'Organismo[81]. L'Organismo di vigilanza, pertanto, deve essere autonomo e indipendente. L'indipendenza consiste nell'assenza di qualsiasi coinvolgimento nei processi decisionali che è chiamato a vigilare[82]. "Si tratta di un dato da sottolineare con vigore: sarebbe davvero difficile immaginare un organismo protagonista di una indipendente azione di controllo ed al contempo implicato nei processi decisionali della sfera gestoria"[83]. Sembra, inoltre preferibile la tesi secondo cui il requisito in esame dovrebbe riguardare ciascun componente dell'ODV e non l'Organismo nel suo complesso[84]. Con la richiesta di autonomia si intende sottolineare che il soggetto deve essere estraneo ad ogni forma di interferenza e di pressione dei vertici operativi. Da tale requisito discende la disponibilità di un *budget* adeguato da parte dell'OdV, un livello di compenso proporzionato al ruolo, l'accesso libero ai dati dell'impresa rilevanti rispetto ai compiti affidati all'ODV, la nomina di consulenti esterni o al compimento di *audit* o verifiche a sorpresa senza autorizzazioni specifiche, la possibilità di organizzare liberamente la propria struttura e la relativa attività dotandosi di un regolamento e approvando il programma annuale di

[80] Cfr. A. GULLO, *I modelli organizzativi*…, cit., pag. 276, il quale sottolinea che la identificazione tra ODV e collegio sindacale, pur possibile in base al dato normativo, è criticata poiché rischierebbe di porre il soggetto nella scomoda posizione di controllore e controllato, rispetto almeno a taluni reati presupposto (ad esempio le false comunicazioni sociali, tenuto conto degli obblighi di controllo contabile in capo ai sindaci); V. MONGILLO, *L'Organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche* in Resp. amm. delle società e degli enti, n. 4/2015, pag. 87.

[81] V. MONGILLO, *L'Organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche* in Resp. amm. delle società e degli enti, n. 4/2015, Pagg. 88 ss.; A. GULLO, *I modelli organizzativi*…, cit., pag. 278.

[82] A. GULLO, *I modelli organizzativi*…, cit., pag. 279; V. MONGILLO, L'organismo di vigilanza…, cit., pag. 88

[83] R. BLAIOTTA, *L'organismo di vigilanza: struttura, funzione e responsabilità in sistema penale* web, 16 novembre 2021.

[84] Ibidem

vigilanza[85]. Con il requisito della continuità d'azione si fa riferimento al fatto che l'Organismo debba svolgere un ruolo concreto nel sistema di controllo interno[86]. Infine, fondamentale è che tale organismo sia posto in grado di conoscere tutte le informazioni concernenti la vita dell'ente e che possieda le competenze necessarie per svolgere le proprie funzioni. Le principali funzioni dell'organismo possono così essere sintetizzate: valutare l'adeguatezza del modello, in relazione alle attività espletate dall'ente e alla sua organizzazione e quindi la sua idoneità a scongiurare la commissione degli illeciti; vigilare sulla effettività del modello, verificando che sia coerente con quanto disposto dai codici di comportamento; analizzarne il costante mantenimento nel tempo dei requisiti di solidità e funzionalità; curare l'aggiornamento del modello attraverso proposte di adeguamento dirette alle funzioni aziendali interessate, nonché la verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte[87]. La definizione dei compiti attribuiti all'organismo di vigilanza riveste una particolare importanza anche con riferimento alla delimitazione della responsabilità penale dei componenti dell'organismo stesso. Specie, con riferimento ai reati informatici, vedremo quanto possa essere rilevante tale figura, occorre pertanto chiederci se possa eventualmente affermarsi una sua responsabilità. Il tema non è nuovo al diritto penale d'impresa che si è interrogato circa la responsabilità di amministratori e sindaci[88]. Proprio la scarsa disciplina normativa in merito alla figura dell'OdV è alla base del dibattito sullo statuto della responsabilità. Non è in dubbio la possibilità di ammettere un concorso attivo ex art. 110 c.p., con la quale si farebbe riferimento, tuttavia, ad ipotesi di ridotta frequenza. In questo lavoro, pertanto ci soffermiamo sull'ipotesi in cui la condotta di partecipazione rilevante dell'OdV sia costituita da un comportamento omissivo. La responsabilità penale dei componenti dell'Organismo di Vigilanza per "omessa o insufficiente vigilanza" (art 6, c.1, lett. d d.lgs. 231/2001) sarebbe riconducibile allo schema del reato omissivo improprio e in particolare

[85] A. GULLO, *I modelli organizzativi…*, cit., pag. 279. V. MONGILLO, *L'Organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche* in Resp. amm. delle società e degli enti, n. 4/2015, pag. 88.

[86] Cfr. A GULLO, I modelli organizzativi…, cit., pag. 279; V. MONGILLO, L'Organismo di vigilanza…, cit., pag. 89

[87] V. MONGILLO, *L'Organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche* in Resp. amm. delle società e degli enti, n. 4/2015, pag. 84.

[88] In questo caso l'obbligo giuridico di impedimento viene rinvenuto negli artt. 2392 e 2403 c.c., per i primi, e negli artt. 1393 e 2394 c.c. per i secondi.

nel concorso per omissione. Possiamo pensare all'ipotesi dell'OdV, che sia venuto a conoscenza del fatto che un Amministratore della società stia per commettere un reato e volontariamente ometta di esercitare i poteri di controllo per impedirne la consumazione. Per poter giungere alla conclusione che sia possibile ascrivere una responsabilità penale a carico dell'OdV occorre interrogarci sulla titolarità o meno di una posizione di garanzia e di poteri giuridici di impedimento in capo a questa figura[89]. Inoltre, occorre accertare che tra l'evento (che in questo caso corrisponderebbe alla commissione dell'attività illecita altrui) e la condotta omissiva intercorra una connessione, cioè, "se e in che modo l'eventuale compimento dell'azione dovuta avrebbe inciso sul corso degli accadimenti e, in particolare, se avrebbe evitato la verificazione dell'evento lesivo"[90]. Sul giudizio, di natura ipotetica, che deve essere utilizzato per indagare il nesso di derivazione causale tra l'omissione e l'evento, è ampiamente intervenuta la Cass. a Sez. Unite[91]. In questa sede non ci soffermiamo su questo punto, poiché, nel caso di specie, il problema riguarda l'altro elemento richiesto, ci riferiamo alla posizione di garanzia, da cui originano gli obblighi giuridici di attivarsi e la sussistenza dei poteri giuridici di impedimento, la cui violazione consente l'affermazione della responsabilità penale per non aver impedito il reato.

In particolare, autorevole dottrina, con riferimento al concorso mediante omissione (artt. 40 c.p. e 110 c.p.), nota che "se nell'ambito del concorso punibile sono da ricondurre tutte le condotte che abbiano avuto un'efficacia condizionante rispetto al fatto di reato e se, in forza dell'art. 40, co. 2, il non impedimento di un evento, in presenza di un obbligo giuridico di attivarsi volto in tale direzione, è equiparato alla sua attiva causazione, ne segue che il non impedimento di un reato da parte del titolare di un obbligo di garanzia

[89] G. MARINUCCI E.DOLCINI, *Manuale di diritto penale*, cit., 409, i quali osservano che «deve sussistere una posizione di garanzia, cioè in capo ad un soggetto deve sussistere l'obbligo giuridico di impedire la commissione del reato da parte di altri: in assenza di un tale obbligo non c'è partecipazione del reato bensì una mera connivenza — cioè l'inerzia da parte di chi sappia che altri sta per commettere o sta commettendo un reato — o un altrettanto irrilevante adesione morale — cioè l'approvazione solo interiore del reato commesso da altri. (...) quanto al contenuto degli obblighi di impedimento, andrà desunto dalle norme giuridiche che fondano l'obbligo di garanzia. (...) in secondo luogo, l'omissione deve essere condizione necessaria per la commissione del reato da parte dell'autore: bisogna cioè accertare se l'azione doverosa che si è omesso di compiere avrebbe impedito la realizzazione del fatto concreto da parte dell'autore»; cfr. G. FIANDACA E. MUSCO, *Diritto penale*, cit., 606.; cfr. M. ROMANO G. GRASSO, *Commentario sistematico del Codice penale*, Milano, Giuffrè, 2012, pag. 186 ss.

[90] Così, G. FIANDACA E. MUSCO, *Diritto penale*, cit., 600; cfr. G. MARINUCCI E. DOLCINI, Manuale di diritto penale, cit., 206 e ss.

[91] Cass. pen., Sez. Un., 10 luglio 2002, FRANZESE, in Foro it., 2002

deve essere considerato come una condotta di partecipazione rilevante"[92]. La posizione di garanzia deve avere come contenuto l'impedimento di reati di quelli che si sono verificati e, inoltre, il reato commesso deve costituire lesione di quel bene per la cui tutela è prevista la posizione di garanzia[93]. Proprio con riferimento alla posizione di garanzia nella partecipazione omissiva, una parte della dottrina ha individuato un *tertium genus* (accanto alla posizione di protezione e a quelle di controllo di una fonte di pericolo), che ha come contenuto l'impedimento delle azioni illecite di terzi[94]. Mentre la titolarità delle posizioni di garanzia che hanno ad oggetto il controllo di una fonte di pericolo si ricollega all'esercizio di un potere di fatto su di essa, in questo caso il garante deve essere titolare di un potere giuridico di impedire il reato altrui[95].

Inoltre, parte della dottrina rileva come sia arbitrario, assegnare alla clausola dell'equivalenza tra il non impedire e il cagionare un'estensione illimitata nel concorso di persone. Se in presenza di un reato mono-soggettivo la regola generale dell'equivalenza ex 40 cpv. è limitata ai soli reati c.d. causali puri, che attentano ai beni di rango più elevato quali la vita e l'incolumità individuale e pubblica, non si comprende, allora, sulla base di quali criteri si possa, nell'ipotesi di responsabilità concorsuale, giungere fino al punto di includervi anche fattispecie di reato che offendono beni di natura diversa[96]. In dottrina, tuttavia, si rilevano argomenti contrari a questa tesi. Una parte di essa osserva che "per espressa ammissione della stessa dottrina tedesca, si tratta di una clausola ambigua, controversa e di scarso rilievo pratico, che comunque non è mai stata invocata — né dalla dottrina, né dalla giurisprudenza, né tanto meno dal legislatore storico — per negare in radice la possibilità di "convertire" i reati d'evento a forma vincolata in reati omissivi impropri (purché, naturalmente, sussista il primo, e fondamentale, requisito dell'obbligo giuridico di impedire l'evento). Va anzi sottolineato che sia la dottrina sia la giurisprudenza tedesche ammettono pacificamente la possibilità che reati a forma vincolata, quali ad es. l'estorsione, la violenza privata e soprattutto la truffa, vengano realizzati anche attraverso un'omissione"[97]. A supporto dell'esclusione della

[92] G. GRASSO M. ROMANO, *Commentario*…, cit., pag. 187
[93] G. GRASSO M. ROMANO, *Commentario*…, cit., pag. 188-189.
[94] Ibidem
[95] Ibidem
[96] G. FIANDACA E. MUSCO, *Diritto penale*, cit., pag. 596. Anche G. GRASSO*, Commentario*…, cit., pag. 191 risulta contrario a questa delimitazione
[97] G. MARINUCCI E. DOLCINI, *Manuale di diritto penale*, cit., pag. 200

delimitazione dell'operatività dell'art. 40, c 2 alle sole fattispecie causali pure, gli studiosi fanno riferimento all'art. 138 c.p.m.p. poiché alcune delle fattispecie ivi previste sono di mera condotta e il richiamo all'art. 40, comma 2 non può che essere letto nel senso che per tali ipotesi di reato risulta configurabile una responsabilità a titolo di compartecipazione omissiva[98]. Inoltre, anche con riferimento a talune ipotesi di reato prive di un evento naturalistico possano sussistere esigenze di tutela che giustificano pienamente la configurazione di una compartecipazione nel reato realizzata per omissione[99].

Secondo una parte della dottrina[100], per poter risolvere la questione risulterebbe importante stabilire se i poteri dell'OdV appartengano alla categoria degli obblighi di garanzia o degli obblighi di sorveglianza. Seguendo tale impostazione, l'obbligo di garanzia consiste nell'obbligo giuridico gravante su specifiche categorie di soggetti forniti degli adeguati poteri giuridici di impedire eventi offensivi di beni altrui, affidati alla loro tutela per l'incapacità dei titolari di proteggerli adeguatamente. Questo obbligo si distingue dall'obbligo di sorveglianza che è, invece, l'obbligo giuridico, gravante su specifiche categorie di soggetti, privi di poteri giuridici impeditivi, di vigilare su altrui attività per conoscere dell'eventuale commissione di fatti offensivi e di informare il titolare o il garante del bene[101]. La principale differenza attiene pertanto ai poteri, che in questo caso sono di mera vigilanza e di informazione sulla situazione di pericolo. Da queste argomentazioni discendono una serie di conseguenze. In primo luogo, in virtù del principio della responsabilità penale, l'inosservanza dell'obbligo di sorveglianza non dà luogo a responsabilità per non impedimento dell'evento, perché, in assenza dei poteri impeditivi, si tratterebbe di responsabilità per fatto altrui[102]. Il titolare dell'obbligo di sorveglianza non può neanche rispondere per concorso omissivo nel reato commesso dal

[98] G. GRASSO, *Commentario*…, cit., pag. 191
[99] Ibidem
[100] Cfr. I. LEONCINI, *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, Giappichelli, 1999, 179 e ss.; F. MANTOVANI, *Causalità, obbligo di garanzia e dolo nei reati omissivi* in Riv. it. dir. e proc. pen., fasc.4, 2004, pagg. 13-14; F. MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, di solidarietà, di libertà e di responsabilità personale* in Riv. it. dir. e proc. pen., fasc.2, 2001, pag. 5.
[101] F. MANTOVANI, *Causalità, obbligo di garanzia e dolo nei reati omissivi* in Riv. it. dir. e proc. pen., fasc.4, 2004, pag. 14; F. MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, di solidarietà, di libertà e di responsabilità personale* in Riv. it. dir. e proc. pen., fasc.2, 2001, pag. 5
[102] Ibidem

soggetto sottoposto a sorveglianza[103]. Infine, l'omessa sorveglianza è punibile nei casi espressamente previsti da specifiche norme della parte speciale del diritto penale, stante l'assenza di una previsione generale sull'obbligo di sorveglianza[104].

Importante è, inoltre, chiarire il concetto di "potere impeditivo". Alcuni autori considerano "potere impeditivo" quello a cui corrisponde un dovere di conformazione: ossia, quel potere il cui esercizio produce un effetto giuridico vincolante sull'attività del soggetto controllato[105]. "Conseguentemente esulano dalla categoria anzidetta quei poteri c.d. deboli, ossia quelli il cui esercizio produce solamente un'influenza sulle decisioni del soggetto controllato; a nulla rilevando che tale influenza possa aver indotto il soggetto controllato ad astenersi dall'illecito"[106].

Chiarito ciò analizziamo le posizioni degli studiosi. Cospicua dottrina ritiene che il legislatore non abbia configurato alcun potere impeditivo, collegiale e/o individuale, in capo all'organo[107].

L'adempimento degli obblighi di segnalazione previsti dal decreto 231 a carico dell'organismo di vigilanza non rappresenterebbe, pertanto, quell'azione doverosa richiesta per impedire il reato e configurare una responsabilità penale di tipo omissivo, ma è preordinata esclusivamente a ridurre il rischio di reato. L'organo di vigilanza, sebbene disponga di strumenti astrattamente incisivi, tra cui l'elaborazione di note

[103] Ibidem
[104] Ibidem
[105] V. PISANI, *I requisiti di autonomia e indipendenza dell'Organismo di Vigilanza istituito ai sensi del d.lgs. 231/2001*, in *La resp. amm. delle soc. e degli enti*, 1/2008, pag. 69
[106] N. NAPOLETANO, *Omesso impedimento del reato e illecito amministrativo dell'ente: quale responsabilità per l'Organismo di Vigilanza in caso di omesso o insufficiente controllo?* in giurisprudenzapenale.com n. 3/2020, pag 7
[107] F. CERQUA, *Commento sub art. 6 del d.lgs 231/2001* in Enti e responsabilità da reato a cura di CADOPPI A. GARUTI G. VENEZIANI P, Utet giuridica, Torino, 2010, pag. 136; A. GULLO, *I modelli organizzativi…*, cit.; V. MONGILLO*, L'organismo di vigilanza…*, cit., pag. 102; C. PIERGALLINI, *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, in Riv. trim. dir. pen. econ., 2002, 571 ss; F. GIUNTA, Controllo e controllori nello specchio del diritto penale societario, Riv. trim. dir. pen. econ., 2006, 610; F. CENTONZE, *Il problema della responsabilità penale degli organi di controllo per omesso impedimento degli illeciti societari (Una lettura critica della recente giurisprudenza)* in Riv. Soc., fasc. 2-3/2012; DE STEFANIS R., *Profili di responsabilità dell'Organismo di Vigilanza ai sensi del d.lgs. 231/2001* in Danno e responsabilità, n.4/2010; RORDOF R., *L'Organismo di vigilanza nel quadro del D.lgs. n. 231/2001* in Le società n.1/2022; PAONESSA C*., Il ruolo dell'organismo di vigilanza nell'implementazione dei modelli organizzativi e gestionali nella realtà aziendale* in La giustizia penale, fasc. VII, LUGLIO 2014; N. NAPOLETANO, *Omesso impedimento del reato e illecito amministrativo dell'ente: quale responsabilità per l'Organismo di Vigilanza in caso di omesso o insufficiente controllo?* in giurisprudenzapenale.com n. 3/2020, pag 9.

informative o la denuncia di accertate irregolarità, non possiede poteri sanzionatori o di natura strutturalmente impeditiva idonei ad incidere direttamente sull'altrui operato[108]. "L'OdV vanta esclusivamente poteri di sorveglianza e controllo, cosicché, una volta venuto a conoscenza di operazioni a rischio-reato, questo non può sostituirsi ai soggetti apicali, ma deve unicamente segnalare al vertice aziendale la violazione perché intervenga per bloccare l'illecito: spetterà, poi, all'organo dirigente decidere se correre o no il rischio della commissione del reato. Del resto, l'autonomia e l'indipendenza dell'Organismo di Vigilanza dai vertici aziendali sembra cogliersi proprio in questa sua estraneità alla gestione d'azienda"[109]. Sembra importante sottolineare in questa sede la *vexata questio* intorno alla natura di tale organo. Si sono contrapposti due diversi indirizzi: uno che qualifica l'OdV come un vero organo della società al pari del collegio sindacale o del revisore legale, la tesi maggioritaria, invece, lo classifica come mero ufficio della stessa. Nonostante quanto fino a questo momento detto, spesso la giurisprudenza tende ad attribuirgli un sindacato di merito sull'attività gestoria e un potere impeditivo delle condotte illecite. Questo finisce con il far assumere alla figura dell'OdV un ruolo di garante, rilevante sul piano della responsabilità penale. Facciamo riferimento al discusso caso Impregilo[110], concernente fatti di aggiotaggio informativo commessi dai vertici della società. Secondo la Corte di Cassazione, la funzione di controllo dell'organismo di vigilanza non era adeguata, poiché i comunicati stampa potevano essere emessi dagli apicali, senza che «all'organo di controllo fosse concesso di esprimere una *dissenting opinion* sul "prodotto finito"», pertanto la funzione dell'ODV sarebbe stata carente di autonomi ed effettivi poteri di controllo. I giudici di legittimità sembrano attribuire all'OdV un controllo nel merito dei singoli atti di amministrazione ed una funzione impeditiva dell'evento-reato. In base al disegno della corte l'ODV dovrebbe essere in possesso di poteri che lo renderebbero di fatto partecipe dei processi decisionali, ma questo entra in contrasto con la lettera della norma[111]. Un approccio non dissimile si

[108] Come poteri idonei a modificare il modello (esempio riportato in NAPOLETANO N., *Omesso impedimento del reato e illecito amministrativo dell'ente: quale responsabilità per l'Organismo di Vigilanza in caso di omesso o insufficiente controllo?* in giurisprudenzapenale.com n. 3/2020)
[109] N. NAPOLETANO, *Omesso impedimento del reato e illecito amministrativo dell'ente: quale responsabilità per l'Organismo di Vigilanza in caso di omesso o insufficiente controllo?* in giurisprudenzapenale.com n. 3/2020, pag 9.
[110] Cass. pen., Sez. V, 18 dicembre 2013 (dep. 30 gennaio 2014), n. 4677 in Diritto penale contemporaneo web
[111] V. MONGILLO, *L'organismo di vigilanza…,* cit., pag. 106

rinviene nella sentenza del Tribunale di Milano relativa al caso BMPS[112]: un caso di aggiotaggio e false comunicazioni sociali in relazione ad operazione finanziaria internazionale artificiosa. La pronunzia attribuisce all'OdV il sindacato nel merito dell'attività gestoria. Come nota Blaiotta: "Queste soluzioni interpretative non possono essere condivise perché: a) Sono avulse dalla realtà che si è tentato di tratteggiare: la collocazione, cioè, in un peculiare "luogo" dell'organizzazione, lontano dalle fucine nelle quali vengono agiti i processi decisionali. b) Attribuiscono all'OdV un ruolo disfunzionale (di controllo ed impedimento) che contrasta con il tenore della normazione e con la veste di indipendenza e autonomia cui si è fatto cenno; nonché con l'assenza di qualunque legittimazione nella sfera gestoria. c) Soprattutto, non hanno ben chiaro qual è il fondamento della responsabilità dell'ente: cosa esattamente si chiede all'istituzione e cosa realmente si punisce"[113].

Un orientamento minoritario, presente in dottrina ha individuato un potere impeditivo mediato in capo all'ODV che potrebbe consentire di predicare l'esistenza di una responsabilità omissiva per tutti coloro che sono parte necessaria, seppure non sufficiente, di una procedura impeditiva[114]. La posizione di garanzia in capo ai componenti dell'Organismo di Vigilanza discenderebbe direttamente dal Modello organizzativo, il quale, considerata la sua peculiare finalità di prevenzione del rischio-reato attribuirebbe, all'atto della nomina dell'OdV, quegli specifici ed effettivi poteri di ingerenza e di interferenza tipici della posizione di garanzia. Tuttavia, se accogliessimo tale orientamento dovremmo affrontare anche tutte le problematiche relative all'ammissibilità di una partecipazione colposa del componente dell'OdV nel delitto doloso dell'organo della società, poiché la responsabilità dell'OdV sarebbe riconducibile allo schema del

[112] Tribunale di Milano, Sezione II penale, 7 aprile 2021 (ud. ottobre 2020), n. 10748 in Giurisprudenza penale web

[113] R. BLAIOTTA, *L'organismo di vigilanza: struttura, funzione e responsabilità* in sistema penale web, 16 novembre 2021. Si sulla sentenza in esame anche: FRAGASSO B. FUSCO E., *Sul presunto obbligo di impedimento in capo all'organismo di vigilanza: alcune note a margine della sentenza BMPS* in Sistema penale web, n. 10/2020

[114] Cfr. GARGANI, *Imputazione del reato degli enti collettivi e responsabilità penale dell'intraneo: due piani irreali?* in Dir. pen. proc., 2002, 1061, 1066; A, NISCO*, Compliance e posizioni di garanzia: prime indicazioni dalla giurisprudenza tedesca*, in Cass. pen., 2010, 2435 ss.; A. NISCO, *Controlli sul mercato finanziario e responsabilità penali,* Bologna, 2009, 382 ss.; A, NISCO, *Responsabilità degli enti, riflessioni sui criteri ascrittivi soggettivi e sul nuovo assetto delle posizioni di garanzia nelle società* in Riv. trim. dir. pen. econ., 2004, 317 ss.

concorso per omissione nel delitto doloso[115]. Il legislatore, infatti, ha previsto un'apposita regola per consentire la configurazione della cooperazione nel delitto colposo ai sensi dell'art. 113 c.p., la quale sembra escludere implicitamente la cooperazione colposa nel delitto doloso[116].

Tenuto conto di tali difficoltà interpretative, in giurisprudenza si sta sviluppando un orientamento volto ad inquadrare l'omesso controllo nello schema del dolo eventuale. Pertanto, dietro la decisione di non osservare gli obblighi di sorveglianza imposti dalla legge, si potrebbe celare l'atteggiamento psicologico di chi avrebbe consapevolmente accettato il rischio del verificarsi di fatti dannosi[117]. Si tratta, tuttavia, di un *escamotage* volto a rivestire come doloso un comportamento che, invece, costituisce una chiara forma di agevolazione colposa di comportamenti criminosi altrui[118].

Sebbene si tratta di una posizione superata grazie all'intervento del legislatore, rileviamo che in passato alcun studiosi individuavano una eccezionale posizione di garanzia nel settore del riciclaggio, in considerazione del combinato disposto degli artt. 52 e 55 d.lgs. n. 231 del 2007. Tali norme prevedevano un obbligo di segnalazione esterno dell'OdV penalmente sanzionato. Tuttavia, tale orientamento, invece che convalidare la tesi della sussistenza di una posizione di garanzia in capo all'OdV, rappresentava piuttosto conferma della tesi opposta. Si trattava infatti di una ipotesi di reato omissivo proprio, fondata sulla violazione di uno specifico obbligo di sorveglianza, che di per sé, presuppone proprio l'assenza di un obbligo di garanzia[119].

---

[115] Sul delicato problema del concorso colposo nel delitto doloso, si veda, per tutti, FIANDACA-MUSCO, Diritto penale, cit., 515

[116] G. FIANDACA E. MUSCO, *Diritto penale,* cit., 515; Contro, Cass. pen., Sez. IV, 9 ottobre 2002 in Riv. pen., 2003, 107, ove si afferma che «in tema di concorso di persone nel reato, così come deve ritenersi ammissibile il concorso doloso nel reato colposo altrui (quale ipotizzabile nel caso di chi, assecondando e sostenendo l'altrui condotta colposa, si rappresenti ed accetti il possibile verificarsi, in conseguenza di essa, dell'evento tipico del reato, non previsto, invece, dall'autore diretto di detta condotta), deve parimenti ritenersi ammissibile l'ipotesi inversa, costituita dalla cooperazione colposa nel delitto doloso altrui, configurabile qualora, posta in essere da taluno una determinata condotta caratterizzata dall'inosservanza di obblighi dettati dalla comune prudenza e diligenza, oltre che da specifiche disposizioni normative, altri soggetti, nella situazione così creata, abbiano modo di cagionare dolosamente un determinato evento costituente reato».

[117] Cass. pen., sez. V, 4 maggio 2007 n. 23383, in Cass. pen., 2008.

[118] NAPOLETANO N., *Omesso impedimento del reato e illecito amministrativo dell'ente: quale responsabilità per l'Organismo di Vigilanza in caso di omesso o insufficiente controllo?* in giurisprudenzapenale.com n. 3/2020, pag. 17

[119] A. GULLO, *I modelli organizzativi*…, cit., pag. 283.

Il tema è stato comunque eliminato alla radice con le modifiche apportate al d.lgs. n. 231 del 2007 dal d.lgs. n. 90 del 2017 che ha attuato la IV Direttiva antiriciclaggio. Con la presente modifica i membri degli OdV sono stati eliminati dai destinatari degli obblighi di comunicazione, sottoponendo peraltro la relativa violazione a sanzione amministrativa. Alla luce di tali considerazioni, riteniamo pertanto difficile l'individuazione di una responsabilità dell'OdV, almeno da inquadrare nello schema del reato omissivo improprio. Abbiamo, invece, già all'inizio del presente paragrafo rilevato che non sorgono dubbi in merito alla possibilità di ammettere un concorso attivo ex art. 110 c.p. Inoltre, la multiformità dei casi offerti dalla prassi ci potrebbe restituire forme di responsabilità omissiva propria. Nell'ipotesi di specie l'OdV dovrebbe omettere un'azione che la stessa legge penale gli comanda di realizzare. In questo caso non gli verrebbe rimproverato il fatto di non aver impedito il verificarsi degli eventuali risultati dannosi connessi alla condotta omissiva, ma di non aver posto in essere l'azione doverosa. Ancora possiamo fare riferimento a quella parte della dottrina che ipotizza un Modello che introduca un potere generale di intervento in capo all'OdV nei casi d'impossibilità di riferire nell'immediatezza ai vertici aziendali o d'impossibilità dei vertici di agire con tempestività[120]. Non ci soffermiamo sulla legittimità o opportunità di tale ipotesi, ma sul fatto che in questo caso si possa delineare una delega formale e autorizzata di poteri decisionali dell'OdV da parte dell'ente, con tutte le conseguenze che la delega comporta sul piano della responsabilità[121]. Questa dottrina non esclude che in futuro alcune certezze circa l'ambito e l'oggetto dei poteri di vigilanza dell'OdV possano vacillare e possano aprirsi nuovi e imprevedibili scenari[122]. Quello che in questa sede sembra opportuno sottolineare è che nella prassi applicativa si possono presentare casi molto diversi, in relazione alla composizione di tale organismo, ai poteri ad esso conferiti, alla effettiva organizzazione dell'ente, al tipo di reati commessi. L'eventuale responsabilità dell'OdV dovrà, pertanto, essere vagliata tenendo in considerazione le circostanze del caso concreto. Infine, occorre rilevare che i singoli componenti dell'organo di controllo possono rispondere civilmente del loro operato nei confronti dell'ente. Infatti, l'ente collettivo, nell'ipotesi in cui la responsabilità penale sia stata giudizialmente accertata per

[120] A. GIAVAZZI, *Poteri e autonomia dell'Organismo di Vigilanza: prime incertezze, nuove incertezze*, in Le soc., n. 11/2012, pag. 1221
[121] Ibidem
[122] Ibidem

l'illecito amministrativo dipendente da reato, potrà esperire azioni civili di risarcimento del danno economico subito, in conseguenza di una sentenza di condanna, sia nei confronti dei componenti dell'OdV che, con la propria condotta, abbiano reso possibile la realizzazione dell'evento perché non abbiano vigilato secondo diligenza sull'osservanza dei protocolli di prevenzione; e sia nei confronti dell'autore materiale del reato-presupposto[123].

2.5 L'accertamento della colpa organizzativa: in attesa di un futuro migliore per gli enti

Una questione che necessita di approfondimento nell'ambito della nostra analisi è sicuramente quella relativa all'accertamento della colpa organizzativa e alla valutazione dell'idoneità ed efficace attuazione del modello di organizzazione e gestione poiché la dimostrazione di aver attuato un Modello adeguato potrebbe aiutare l'ente a discolparsi o ricevere un esimente. Sebbene, soprattutto in relazione ai reati informatici, sia auspicabile che le imprese non si limitino a recepire la *compliance* unicamente per evitare le sanzioni pecuniarie e interdittive comminabili ai sensi del d.lgs. n. 231/2001. È opportuno che tali soggetti giungano a concepire la sicurezza come un valore aggiunto, idoneo in alcuni casi a garantire la sopravvivenza dello stesso ente che, in assenza di adeguati meccanismi di prevenzione, dinnanzi a *cyber* aggressioni provenienti dal mondo esterno potrebbe uscirne irrimediabilmente danneggiato[124]. Purtroppo, ad oggi, nelle valutazioni condotte dai giudici gli enti sono riusciti difficilmente ad uscirne vincitori. La difficoltà nella trattazione della tematica nasce da un lato da una scarsa giurisprudenza che tende a valutare inidonei i modelli, dall'altro dallo sconforto della dottrina. Analizzeremo, pertanto, le opinioni degli studiosi, le scarse pronunce e le prospettive che ci riserva il futuro anche in considerazione dell'utilizzo sempre più incisivo della tecnologia.

In questa analisi faremo riferimento all'ente sano, dedito all'attività imprenditoriale consentita e incentivata dalla Costituzione, che tuttavia incorre occasionalmente nelle

[123] N. NAPOLETANO, *Omesso impedimento del reato e illecito amministrativo dell'ente: quale responsabilità per l'Organismo di Vigilanza in caso di omesso o insufficiente controllo?* in giurisprudenzapenale.com n. 3/2020, pag. 17

[124] G. FORNARI E. ANGIULI D. ATTANASIO, *Cybercrimes e responsabilità da reato degli enti: rischi penali e prevenzione* in fornariassociati.com, luglio 2020

maglie della legge penale. Diversamente nel caso in cui l'ente sia dedito esclusivamente o prevalentemente alla commissione di reati è prevista la "pena capitale" dell'interdizione definitiva dall'esercizio dell'attività (art. 16).

Il problema circa l'oggetto della nostra analisi è stato efficacemente espresso da V. Manes, il quale rileva che nell' analisi del modello organizzativo "si ha subito l'impressione che il decreto abbia fatto affidamento — forse troppo ingenuamente — su una vastità di orizzonti di scienza ed esperienza in capo al singolo giudice penale che appare davvero eccessiva, chiamandolo a valutare contesti altamente complessi, e strutturalmente interdisciplinari, nei quali si mescolano — assieme a competenze tecnico-giuridiche — competenze di organizzazione aziendale, informatiche, e molte altre, tutte necessarie — appunto — per la costruzione del modello. Ed infatti, nella prassi, ciò che accade è che questa valutazione viene delegata dal giudice ai suoi ausiliari, e fatalmente si sposta, o fa integrale affidamento, sulle analisi di consulenti tecnici e periti, analisi che però difficilmente riescono a correggere l'impronta che ha dato all'accertamento l'organo che ha investigato in sede penale o extra-penale"[125]. Del resto, il fatto che il decreto 231 si rivolgesse agli enti più vari e facesse riferimento ad un vasto catalogo di reati, ha dissuaso il legislatore dal fornire indicazioni precise. Svolgono, pertanto un ruolo fondamentale le linee guida elaborate dalle associazioni rappresentative. Ciascun ente, tuttavia, dovrà calibrare tali indicazioni alle proprie caratteristiche. Forse anche per questi motivi, la valutazione di idoneità del modello è stata accompagnata da un tendenziale silenzio giurisprudenziale e davvero rari sono i casi in cui il modello ha veduto riconosciuta la sua idoneità[126]. Sembra ravvisarsi una tendenza della giurisprudenza ad "elevare l'asticella sino a pretese oggettivamente e soggettivamente insostenibili per la *societas eiusdem*, specie se ci si misura con la realtà del panorama italiano"[127].

[125] V. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo* IN Giurisprudenza Commerciale, fasc.4, 1° agosto 2021, pag. 6.

[126] Per un caso in cui si è ritenuto correttamente assolto l'onere di adozione di modello idoneo, giungendo all'assoluzione dell'ente, tratto a giudizio per il fatto di soggetti sottoposti all'altrui vigilanza (ex art. 7, decreto 231) relativamente ad una ipotesi di omicidio colposo con violazione della normativa antinfortunistica, v. Trib. Catania, sez. IV, 14 aprile 2016, n. 2133 in www.penalecontemporaneo.it, 13 gennaio 2017, con nota di Orsina, Il caso "Rete ferroviaria italiana S.p.A.": un'esperienza positiva in tema di colpa di organizzazione.

[127] V. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo* IN Giurisprudenza Commerciale, fasc.4, 1° agosto 2021, pag. 7

L'impressione che se ne ricava è che la valutazione sul modello resti astratta, mentre la colpevolezza di organizzazione implica sempre la necessaria ricostruzione di una puntuale connessione tra *deficit* organizzativo e singolo fatto criminoso[128]. Questo potrebbe, ovviamente, disincentivare le imprese ad adoperarsi per l'adozione di un modello idoneo e ad affrontare costi economici certi, a fronte di conseguenze incerte[129].

Occorre, pertanto, soffermarci sul paradigma su cui si fonda il giudizio di idoneità del modello, per scongiurare il rischio che il mero evento-reato si trasformi in una condizione obiettiva di punibilità. In particolare, facciamo riferimento alla ipotesi ricostruttiva che sembra aver trovato crescente riscontro in dottrina e giurisprudenza. Il modello è quello di una responsabilità autonoma dell'ente focalizzata su una rimproverabilità essenzialmente organizzativa, che salda la responsabilità dell'ente al modello organizzativo e che rimanda allo schema dell'illecito omissivo colposo di evento[130]. Il giudice, dovrà, quindi seguire tutte le sequenze procedurali tipiche dell'illecito colposo[131]. A tal proposito parte della dottrina rileva i maggiori problemi già nel primo *step*: la violazione di una regola di corretta organizzazione e gestione idonea a prevenire la commissione del reato. In primo luogo, il controllo del giudice non ha ad oggetto l'intero Modello ma fa riferimento allo specifico reato. Si tratta di un controllo concreto e relativo e non astratto ed esteso all'intera organizzazione. Il legislatore ha individuato nel Modello il fondamentale strumento precauzionale per prevenire la commissione dei reati all'interno dell'ente e ha fissato le esigenze fondamentali che deve soddisfare (artt. 6 e 7 d.lgs. 231/2001). Alla luce di questo, la colpa sembrerebbe di natura specifica per inosservanza degli *standard* positivizzati dal legislatore[132]. Autorevole dottrina ritiene,

---

[128] C. PALIERO, *La società punita: del come, del perché e del per cosa*, in Riv. it. dir. proc. pen., 2008, 1516 ss.

[129] Le medesime perplessità sono esposte in: PALIERO C. E., *Soggettivo e oggettivo nella colpa dell'ente: verso la creazione di una "gabella delicti"?* in Le società 11/2015 che ripercorre i leading case: Re Impregilo e Thyssenkrupp

[130] C. PALIERO C. PIERGALLINI, *La colpa di organizzazione*, in La responsabilità amministrativa delle società e degli enti, fasc. 3, 2006

[131] Cfr. G. MARINUCCI E. DOLCINI, *Manuale di diritto penale. Parte generale*, cit., pagg. 308 ss.; V. MONGILLO, *Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione* in La responsabilità amministrativa della società e degli enti, fasc. 3/2011, pag. 72; V. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo* IN Giurisprudenza Commerciale, fasc.4, 1° agosto 2021, pag. 10.

[132] In tal senso in dottrina M.G. FLICK., *Giustizia penale ed economia pubblica e privata: profili problematici* in Cassazione Penale, fasc.10, 1° ottobre 2017, pag. 6

tuttavia, che la disciplina legislativa della responsabilità da reato degli enti non contiene vere e proprie regole cautelari, ma si limita a fornire clausole generali, che forniscono indicazioni che occorre poi adattare alle concrete esigenze dell'ente[133]. Pertanto, la colpa dell'ente nella sostanza si rivela colpa generica e non specifica[134]. Questa differenza si riflette sul metodo di accertamento. La verifica giudiziale di idoneità del modello penal-preventivo adottato dall'ente si risolve, secondo questo orientamento, in un giudizio normativo volto a controllare, non tanto l'eventuale violazione di precise regole cautelari di fonte legislativa (o secondaria), quanto la conformità delle regole prevenzionali auto-normate dall'ente alle migliori conoscenze, consolidate e condivise nel momento storico in cui è commesso l'illecito, in ordine ai metodi di neutralizzazione o di minimizzazione del rischio tipico[135]. Questo rende particolarmente arduo il compito, da un lato dell'ente chiamato a conformarsi al decreto 231 e, dall'altro del giudice chiamato a verificare, in sede processuale, l'idoneità *ex ante* del Modello a prevenire reati della stessa *species* di quello realizzato. Ad oggi, infatti, i requisiti di un'organizzazione virtuosa non rispondono a parametri di diligenza, prudenza o perizia sufficientemente determinati e riconoscibili e il giudice non è attrezzato, per cultura, formazione e prassi, a confrontarsi con le organizzazioni complesse. Questo rende le valutazioni giudiziali in *subiecta* materia intaccate da una difficilmente evitabile componente di soggettività che dà luogo a incertezze e disomogeneità applicative[136].

Nonostante autorevole dottrina sottolinea le difficoltà intrise nell'accertamento della colpa organizzativa dell'ente e nella valutazione giudiziale del MOG[137], può essere utile analizzare l'intera sequenza procedimentale che secondo parte della dottrina dovrebbe portare a risultati più equi per gli enti[138]. Il giudice, dovrà scandagliare la effettiva prevenibilità e prevedibilità dell'evento, la sua connessione con lo scopo di protezione

[133] V. MONGILLO, *Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione* in La responsabilità amministrativa della società e degli enti, fasc. 3/2011, pag. 73
[134] Ibidem
[135] F. D'ARCANGELO, *I canoni di accertamento dell'idoneità del modello organizzativo nella giurisprudenza*, in La resp. amm. delle soc. e degli enti, 2-2011, pp. 140 ss.
[136] V. MONGILLO, *Il giudizio di idoneità…*, cit., pag. 74
[137] Cfr. V. MONGILLO*, Profili critici…*, cit.
[138] Cfr. V. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo* IN Giurisprudenza Commerciale, fasc.4, 1° agosto 2021.

della disciplina oggetto di autonormazione, ossia la concreta impedibilità del fatto di reato così come la stessa esigibilità dell'adozione ed efficace attuazione di un modello organizzativo idoneo[139].

Superata la prima fase dell'individuazione della regola cautelare che si assume essere stata violata dalla verificazione dell'evento reato, secondo il modello (non *dell'homo eiusdem professionis et condicionis*, bensì) della *societas eiusdem negotii et condicionis*; il secondo passaggio prevede la ricostruzione della c.d. "causalità" della colpa, consistente nella verifica della connessione tra l'evento-reato che si è verificato e lo scopo della regola precauzionale violata. Quindi occorre accertare se il primo corrisponda al "tipo" di quelli che la cautela omessa o negligentemente attuata mirava a prevenire. Un problema che ancora oggi rimane aperto è se, nella peculiare dinamica che vede combinarsi la responsabilità dell'ente a responsabilità individuali (spesso dolose), l'accertamento debba accontentarsi di rintracciare non già un nesso causale rigoroso, bensì un "nesso di rischio", rispetto al quale la cautela omessa o negligentemente attuata avrebbe garantito una apprezzabile riduzione del rischio[140].

Il terzo passaggio, altrettanto decisivo consiste nella verifica sulla capacità concretamente impeditiva del c.d. comportamento alternativo lecito, per accertare se la regola violata possa essere ravvisata come reale antecedente colposo dell'evento-reato. Sotto questo profilo, l'accertamento dell'idoneità del modello dovrebbe rispondere alla seguente domanda: quand'anche il modello fosse stato adottato secondo un parametro di idoneità, adeguatezza, correttezza, sarebbe stato in grado di evitare quell'evento reato che si è verificato? Se la risposta dovesse essere negativa dovremmo concludere comunque per l'assenza di una possibilità di imputare quell'evento-reato alla disfunzione organizzativa dell'ente[141]. Infine, il quarto passaggio consiste nella verifica della concreta esigibilità del c.d. comportamento alternativo lecito, ossia l'adozione di un modello organizzativo idoneo che avrebbe avuto, nel caso di specie, effettiva capacità impeditiva. La verifica deve logicamente estendersi anche all'ipotesi contigua di aggiornamento del modello in

[139] V. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo* IN Giurisprudenza Commerciale, fasc.4, 1° agosto 2021, pag. 10
[140] Ibidem, pag 11.
[141] Ibidem, pag 11.

caso di novazioni legislative, così come di avanzamento delle conoscenze nomologiche sui rischi tipici, sino a concludere per l'assenza di rimproverabilità in capo all'ente ove l'illecito di evento non rientrava in concreto nella sfera di dominabilità dell'apparato organizzativo[142]. Il rispetto rigoroso della sequenza logica (e dogmatica) imposta dall'accertamento della colpa potrebbe far emergere una assenza di correlazione tra i difetti strutturali e procedurali e l'evento-reato concretamente verificatosi, e condurre ad escludere la "colpa di organizzazione" dell'ente, in una logica quanto più possibile ispirata ad una dimensione normativa di rimproverabilità. In questo contesto, persino l'assenza *tout court* del modello potrebbe non risultare dirimente, se ad esempio si accerta che quel reato si sarebbe comunque verificato o se comunque il reato realizzato sarebbe stato eccentrico, ancora se comunque l'organizzazione dell'ente, pur non formalizzata in un modello organizzativo, risulta comunque adeguata a prevenire quel rischio reato, in forza di ulteriori e diversi presidi preventivi previamente adottati[143].
Al contrario, punire l'ente per questo disinteresse nei confronti del rischio di reato "significa riconvertire la corresponsabilizzazione dell'ente sul paradigma dell'aumento del rischio, allontanandola dai dispostivi dell'illecito colposo ed elidendo, di fatto, il necessario accertamento causale"[144]. Il che non significa, ovviamente, voler incentivare alcuna forma di "disobbedienza giuridica". I vantaggi derivanti dalla corretta adozione di un modello organizzativo restano indubbiamente evidenti.

Tuttavia, occorre sempre tenere presente la questione relativa alla non obbligatorietà o meno del Modello organizzativo e di gestione. Una domanda che ci siamo posti in precedenza in relazione ai reati informatici, visti i recenti obblighi provenienti dagli atti sovranazionali, ma a cui non abbiamo saputo dare una risposta certa. Sul piano teorico la natura facoltativa del Modello appare coerente con l'impianto legislativo e in linea con le spinte della dottrina emergente, "che sembra convergere nel valorizzare un'accezione normativa della colpevolezza dell'ente, sostenendo un concetto di esigibilità che guardi

[142] V. MANES, *Realismo e concretezza…,* cit., pag 11.
[143] Per talune aperture in questa direzione v. ad es. Cass., 23 gennaio 2019, n. 11518, non negando rilievo a "le procedure di monitoraggio e controllo adottate dall'ente prima dell'adozione del modello di organizzazione".
[144] V. MANES, *Realismo e concretezza*, cit*.,* pag 14. In giurisprudenza Trib. Catania, 14 aprile 2016, n. 2133, cit., dove si è esclusa la responsabilità dell'ente anche se — al momento dell'evento dannoso — il MOG non risultava ancora adeguato alle novelle del 2007/2008 concernenti l'art. 25 septies d.lgs.

alla situazione di fatto in cui questo versi e diversamente graduabile in ragione della sua specificità"[145]. Soprattutto per le PMI l'imposizione di simili obblighi sarebbe non necessaria e non congrua rispetto alla realtà aziendale, motivo per cui autorevole dottrina auspica una totale esenzione[146]. In dottrina, tuttavia, vi sono tesi contrastanti. I sostenitori della non obbligatorietà del modello ritengono che l'ente potrebbe riuscire a minimizzare il rischio- reato anche senza passare per la formalizzazione dei modello. Altra parte della dottrina sottolinea che anche se l'adozione del Modello rappresentasse un mero onere, sarebbe difficile per l'ente andare esente da responsabilità in una situazione di totale inerzia. E non manca neanche chi ricollega all'assenza del MOG la responsabilità dell'ente: "Siamo in presenza di un tipo di responsabilità`, in definitiva ne´ 'dolosa', ne´ 'colposa', quanto di rischio; responsabilità`, peraltro, non tanto "da rischio illecito" (quale ad es. la *recklessness* del sistema anglosassone), quanto piuttosto "da rischio di illecito": il rischio consapevolmente o comunque riprovevolmente assunto di (lasciar) determinare un (qualsiasi) reato-presupposto"[147]. La soluzione a tale questione potrebbe sicuramente rappresentare una certezza in più sia per le imprese nel momento in cui decidano di adottare un MOG o meno, tanto per i giudici in sede di valutazione. La dottrina che stiamo analizzando propende per una visione positiva in cui il giudice valuta nel concreto l'organizzazione dell'aziende a prescindere dall'adozione formale del MOG; tuttavia, abbiamo anche contezza del fatto che se i giudici, nella maggior parte delle pronunce, tendono a valutare negativamente l'idoneità del Modello, difficilmente l'impresa potrebbe riuscire discolparsi in caso di totale assenza di un Modello formalizzato.

Non possiamo neppure trascurare la divergenza di struttura che, come si sa, il decreto segue nella modulazione della corresponsabilità dell'ente, declinando la distinzione tra soggetti posti in posizione apicale (art. 6) e soggetti sottoposti all'altrui direzione (art. 7). In effetti, mentre l'art. 7 sembra profilare con maggior chiarezza, ed in positivo, il paradigma della "colpa di organizzazione", l'art. 6 pare declinato su un paradigma "rovesciato" di colpevolezza, che sembrerebbe imposto, quanto ai soggetti apicali , dal

[145] Ombretta di giovine pag. 215
[146] F. CENTONZE, *La responsabilità degli enti e la piccola e media impresa*, in AA.VV *La responsabilità penale degli enti*, pag. 87
[147] C.E. PALIERO, *La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale* in Riv. trim. dir. pen. econ. 1-2/2018, pag.208

chiaro riferimento dell'art. 6, primo comma, del decreto, ove appunto si prevede che "l'ente non risponde se prova che [...]", evocando quella che è stata diffusamente identificata come una "presunzione di colpa organizzativa", declinata in chiave di vera e propria "inversione dell'onere della prova". Autorevole dottrina ritiene, tuttavia, che , in entrambi i casi, resta inalterata la funzione tipizzante che il "modello" svolge nel paradigma imputativo della responsabilità *ex delicto*, e come tale — sia per quanto concerne i soggetti apicali sia per quanto concerne i "sottoposti all'altrui vigilanza" — deve entrare nel *thema probandum*, secondo le sequenze indicate (evento-reato e regola cautelare-organizzativa pertinente, concretizzazione del rischio, prevedibilità e prevenibilità, etc.): la verifica processuale avrà in ogni caso ad oggetto "la funzione cautelare e il contenuto procedimentale su cui l'idoneità dell'intero sistema auto-normato si regge"[148].

Occorre soffermarci sulla difficoltà della valutazione giudiziale del modello nel caso vengano commessi reati dolosi, poiché i dubbi in merito a tali fattispecie si accrescono, tanto che parte della dottrina distingue tra i reati in attività e i reati decisione[149]. I primi sono di tipo colposo e in questo ambito l'accertamento è più semplice per la più facile "riconoscibilità del pericolo", agevolata dalla vicinanza dell'agente all'evento da prevedere ed evitare; pertanto, si tratta del settore meno problematico[150].

I problemi maggiori attengono al secondo settore che comprende i reati dolosi, poiché aumenta la distanza cronologica e quindi logica tra cautela ed evento-reato. Questa distanza rende più facile per il giudice ipotizzare *ex post* regole precauzionali che avrebbero impedito o reso più difficile la commissione del reato e traccia uno scenario in cui l'ente finisce per essere "impigliato nella fitta ragnatela che ha intessuto"[151]. Se per il giudice risulta facile individuare una fallacia nel modello, dall'altro lato la prevenzione da parte dell'ente è particolarmente ardua e l'individuazione delle cautele viene in genere effettuata intervenendo sui difetti che via via si rivelano nel sistema[152]. In questo ambito,

[148] V. MANES, *Realismo e concretezza*, cit.
[149] C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale* (parte II) in Cass. pen., fasc.2, 2013, pagg. 848 ss.
[150] O. DI GIOVIENE*, Il criterio di imputazione soggettiva* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020, pag. 223
[151] O. DI GIOVINE, *Il criterio di imputazione soggettiva*…, cit., pag. 222
[152] Cfr. C. PIERGALLINI, Paradigmatica dell'autocontrollo penale (parte II) in Cass. pen., fasc.2, 2013, pagg. 848 ss.

si mostrano quei problemi a cui abbiamo fatto prima cenno e il rischio che la valutazione del giudice, circa il nesso tra evento- reato e sistema cautelare, sia arbitrario e discrezionale si accresce. "Più in generale, i presidi cautelari possono essere così tanti, così formalizzati o formalizzabili e spesso così multifunzionali (tendono a prevenire diversi rischi-reato e – si noti- anche rischi diversi da quello- reato) da produrre quale effetto paradossale una semplificazione preterintenzionale e insostenibile del giudizio sulla c.d. concretizzazione del rischio. Con l'esito di veicolare logiche di ascrizione oggettivizzanti che in nome della massima tutela di valori, fissano sempre più in basso il livello di accettabilità del rischio"[153]. In sostanza, una volta commesso il reato, una lacuna nel Modello la si potrebbe trovare sempre[154]. Ad esempio, nel caso dei reati informatici, sarebbe sufficiente che un presidio sia ritenuto non più di ultima generazione, perché la cautela venga considerata inidonea.

___2.5.1 Possibili rimedi *de jure condendo*

Viste le difficoltà nella trattazione del tema, risulta interessante, analizzare i possibili rimedi *de jure condendo* che sono stati proposti per ovviare a questa intollerabile incertezza. La soluzione più ovvia sul piano penalistico consisterebbe nel chiedere al legislatore di riempire di contenuto le cautele 231, in modo da orientare l'azione dei destinatari del decreto (metodo già adottato in materia di infortunistica lavorativa. Art. 30 c.5 d.lgs. n. 81 del 2008[155]). Questa soluzione non è immune da critiche poiché vista la varietà di enti a cui il decreto si rivolge tali indicazioni non potrebbero che essere eccessivamente generiche.

Un'altra soluzione deriva dalla celebre proposta AREL[156], che fa gravare sull'ente l'onere/obbligo di definire il contenuto del Modello e prevede un meccanismo di

[153] O. DI GIOVINE*., Il criterio di imputazione soggettiva…*, cit., pag. 223
[154] M.G. FLICK, *Giustizia penale ed economia pubblica e privata: profili problematici* in Cassazione Penale, fasc.10, 1° ottobre 2017
[155] V. MONGILLO*, Il dovere di adeguata organizzazione della sicurezza tra responsabilità penale individuale e responsabilità da reato dell'ente: alla ricerca di una plausibile differenziazione* in AA.VV., *Infortuni sul lavoro e doveri di adeguata organizzazione: dalla responsabilità penale individuale alla «colpa» dell'ente*, a cura di A.M. Stile - A. Fiorella - V. Mongillo, Napoli, Jovene editore, 2014, pagg. 19 ss.
[156] Questa proposta è stata analizzata nel dettaglio da V. MONGILLO, *Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione* in *La responsabilità amministrativa della società e degli enti,* fasc. 3/2011, pagg. 83 ss.

"attestazione" anticipata del sistema preventivo, in grado, a certe condizioni, di determinare *ex se* l'esclusione della responsabilità dell'ente.

Autorevole dottrina ha, tuttavia, obiettato che non tutti gli ambiti del sistema 231 sono governati da leggi di natura, che garantiscono uno *standard* di predittività elevato dell'evento reato e criteri di accertamento di tipo scientifico[157]. In questi settori, pertanto, il sistema di certificazione non potrebbe funzionare. Inoltre, il sistema di certificazione potrebbe incontrare le resistenze della giurisprudenza, la quale potrebbe ritenere il modello certificativo idoneo in astratto a prevenire una specie di eventi, ma inidoneo in concreto a prevenire lo specifico evento che si è verificato[158].

Altra soluzione ha proposto di valorizzare il ruolo delle associazioni di categorie alle quali delegare il compito di formalizzare delle *best practices*. I modelli elaborati dalle associazioni sarebbero dotati di una presunzione d'idoneità relativa, vincibile ma argomentando in modo stringente[159]. Anche tale soluzione viene, tuttavia, criticata poiché da un lato questa omologazione sarebbe difficile da realizzare in una realtà multiforme come quella imprenditoriale italiana; dall'altra non è detto che tale sistema rappresenti per il magistrato una garanzia sufficiente di idoneità della *compliance*[160]. In questo ambito potrebbe valorizzarsi anche il ruolo del Ministro della giustizia cui già spetta il vaglio circa la congruità delle Linee guida elaborate dalle associazioni di categoria e che accentuerebbe l'attendibilità dell'autonormazione[161].

---

[157] C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale* (parte II) in Cass. pen., fasc.2, 2013, pagg. 864 ss.

[158] Cfr. M.G. FLICK, *Le prospettive di modifica del d.lgs. n. 231/2001, in materia di responsabilità amministrativa degli enti: un rimedio peggiore del male* in Cass. pen., fasc.11, 2010; V. MONGILLO, *Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione* in La responsabilità amministrativa della società e degli enti, fasc. 3/2011;

[159] C. PIERGALLINI, *Premialità e non punibilità nel sistema della responsabilità degli enti* in Diritto penale e processo, n. 4/2019, pag. 535; C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale* (parte II) in Cass. pen., fasc.2, 2013, pag. 865; M. COLACURCI*; L'idoneità del modello nel sistema 231, tra difficoltà operative e possibili correttivi* in Dir. pen. cont., n. 2/2016

[160] O. DI GIOVINE, *Il criterio di imputazione soggettiva*…, cit., pag. 227

[161] Come accaduto in materia di responsabilità sanitaria con la riforma Gelli- Bianco, che ha demandato ad istituti pubblici il compito di accreditare le linee guida predisposte dalle società scientifiche a presidio delle condotte mediche.

Altre proposte spingono verso l'assimilazione del sistema italiano a quello statunitense con l'introduzione di soluzioni premiali subordinate ad atteggiamenti di cooperazione dell'ente con l'autorità giudiziaria[162].

Un'ultima soluzione propone di allargare agli enti il procedimento di "messa alla prova"[163]. Tale proposta, tuttavia, non risolve uno dei principali problemi del sistema, quello che porta i giudici a ritenere il modello inidoneo o inefficace se è stato commesso un reato[164]. Inoltre, la proposta non risolve il problema dell'impreparazione giudiziaria a valutare l'idoneità dei modelli, sia nel caso in cui questi fossero già stati adottati prima della commissione del reato, sia quando vengano adottati successivamente in funzione riparatoria[165].

Il rischio di una valutazione puramente discrezionale e le numerose critiche anche alle possibili riforme ha spinto parte della dottrina a ritenere preferibile eliminare l'attuale forma di responsabilità penale a favore di obblighi specifici di *compliance* dei rischi-reato, la cui violazione dovrebbe essere sanzionata sul piano pecuniario[166]. Si tratta di una proposta definita dalla stessa dottrina che la propone fantascientifica, ma che esprime tutti i dubbi determinati da questa normativa.

Infatti, nel corso di questo ventennio nel decreto 231 sono stati inseriti, grazie anche agli interventi normativi dell'Unione europea, numerosi reati molto diversi tra loro. Questo comporta che se l'ente volesse davvero predisporre una *compliance* completa e effettiva dovrebbe utilizzare ingenti risorse proibitive anche per imprese dotate di notevoli capacità economico-patrimoniali e neppure così potrebbe eliminare ogni rischio di responsabilità[167]. Potrebbe accadere che un rischio- reato non perfettamente coperto, perché percepito come lontano si realizzi. Si auspica, pertanto che i giudici siano più equilibrati nella valutazione del MOG. In particolare, l'apprezzamento dell'esigibilità

[162] Cfr. O. DI GIOVINE, *Il criterio di imputazione soggettiva*…, cit., pagg. 227 ss, la quale espone le critiche che vengono mosse al sistema statunitense.
[163] Cfr. F. MAZZACUVA, *La diversione processuale per gli enti collettivi nell'esperienza anglo-americana* in Dir. pen. con. n. 2/2016; E. SCAROINA, *Prospettive di razionalizzazione della disciplina dell'oblazione nel sistema della responsabilità da reato degli enti tra premialità e non punibilità* in Dir. pen. con. n. 2/2020
[164] O. DI GIOVINE, *Il criterio di imputazione soggettiva*…, cit., pag. 230.
[165] O. DI GIOVINE, *Il criterio di imputazione soggettiva*…, cit., pag. 230
[166] O. DI GIOVINE, Il criterio di imputazione soggettiva…, cit., pag. 232.
[167] Cfr. O. DI GIOVINE, Il criterio di imputazione soggettiva…, cit., pag. 235; MONGILLO V., *Presente e futuro della compliance penale* in sistema penale web, 11 gennaio 2022

non andrebbe limitato al segmento di attività nel cui ambito è stato commesso il reato, ma la valutazione dovrebbe essere più ampia e complessiva[168].

2.6 Colpa di organizzazione e nuove tecnologie

Possiamo, in conclusione, cercare di interrogarci sulle ripercussioni delle nuove tecnologie sulla costruzione e valutazione giudiziale del Modello di organizzazione e gestione e sulla colpa di organizzazione. Nel contesto delle imprese digitalizzate questo profilo è di particolare interesse, tanto che si parla di "*compliance* digitale"[169]. Questa espressione fa riferimento alla gestione dei dati, al rispetto della normativa sulla riservatezza e alla prevenzione degli illeciti (compresi alcuni reati informatici). Altri autori, invece, fanno riferimento alla *compliance* integrata, per indicare l'utilizzo della tecnologia ed in particolare l'IA nelle strategie di prevenzione dei reati all'interno degli enti[170]. Il rapporto tra *compliance* e digitalizzazione è tuttavia contraddittorio. Da un lato la *compliance* digitale è uno strumento per prevenire i reati; dall'altro in materia di riservatezza rappresenta un limite generale alle misure di *compliance* attuabili in altri settori[171]. In questa sede, con l'espressione *compliance* digitale faremo riferimento all'impiego all'interno dell'ente di tecnologie basate sull'Intelligenza artificiale e in particolare alla IA applicata ai *Big data*. Mettendo da parte il tema della responsabilità penale della macchina, analizzeremo le ricadute dell'impiego dell'IA sul modello organizzativo e sulla colpa di organizzazione.

In primo luogo, l'uso della tecnologia, grazie alla sua capacità di esattezza e di maggiore effettività, potrà consentire il formarsi di *best practices* e, dunque la standardizzazione dei sistemi di *compliance*. In tale prospettiva, l'IA modificherà le modalità di controllo e di prevenzione dei reati. I *software* di intelligenza artificiale possono essere impiegati nell'analisi e valutazione *ex post* dei dati aziendali, al fine di identificare le aree

[168] C.E. PALIERO, *La società punita: del come, del perché, e del per cosa* in Riv. it. dir. e proc. pen., fasc.4, 2008, pag. 1533 ss.
[169] Cfr. A. NISCO, *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022; V. MONGILLO, MONGILLO V., *Presente e futuro della compliance penale* in sistema penale web, 11 gennaio 2022.
[170] A. GULLO, *I modelli organizzativi…*, cit., pag. 284 ss.; LETIZI M. SOANA G., *Le potenzialità del modello di corporate compliance integrato basato sulla tecnologia blockchain* in Il sole 24 ore, 21 dicembre 2020
[171] A. NISCO, *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022, pag. 2.

maggiormente a rischio-reato e intervenire, in ottica di aggiornamento e miglioramento, sul *compliance program* adottato[172]. Si tratta di una delle fasi iniziali della costruzione del modello organizzativo e all'interno della quale l'azienda potrebbe avvalersi dell'IA. In queste ipotesi, l'ente potrà basarsi su un patrimonio conoscitivo senza dubbio più completo e affidabile di quello ottenibile attraverso un'analisi condotta secondo metodologie tradizionali, con indiscutibili benefici in termini di riduzione dei tempi e dei costi connessi[173]. Questo potrebbe avere delle ricadute sul giudizio di idoneità dei modelli organizzativi. Ad esempio, il giudice potrebbe valutare il fatto che l'ente non abbia adottato misure tecnologiche o che quelle utilizzate non siano all'avanguardia. Inoltre, lo stesso giudizio di idoneità potrebbe avvalersi della tecnologia informatica. Tuttavia, la dottrina teme che ciò porti a fondare il rimprovero dell'ente su un'idea di "agente modello collettivo tecnologicamente avveduto"[174]. In primo luogo, occorre rilevare che l'IA lavora grazie all'utilizzo di grandi masse di dati raccolti nel passato, ma non è esente da pregiudizi. In particolare, l'utilizzo di tecnologie avanzate potrebbe generare la convinzione che la soluzione elaborata dalla macchina sia l'unica corretta. "Questa convinzione può essere tanto più fuorviante, se si considera che il risultato atteso riguarda la prevenzione di un comportamento descritto da norme penali soggette a interpretazione e, in molti casi, formulate in modo poco chiaro, se non indeterminato"[175]. I principali problemi attengono, alla mancanza di neutralità degli algoritmi di cui si serve l'IA e al dubbio circa la compatibilità del sistema predittivo di tipo informatico con un comportamento contrario a una norma, che può essere giudicato illecito solo al termine di un procedimento logico di sussunzione entro una fattispecie, che la macchina può emulare ma non risolvere compiutamente. Inoltre, non si possono escludere difetti di progettazione o funzionamento di queste tecnologie. Questa circostanza potrebbe mettere in crisi il criterio soggettivo di imputazione dell'illecito all'ente, la colpa di organizzazione. Infatti, nel caso in cui la commissione del reato presupposto dipenda dalla mancata segnalazione di quel determinato ambito di rischio da parte della macchina, ad esempio, per un difetto di progettazione o funzionamento non ascrivibile all'ente il

[172] A. GULLO, *I modelli organizzativi*…, cit., pagg. 286 ss.
[173] P. SEVERINO, Intelligenza artificiale e diritto penale in Intelligenza artificiale- il diritto, i diritti l'etica a cura di Ugo Ruffolo, Milano, Giuffrè, 2020, pag. 538
[174] A. NISCO, *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022, pag. 10
[175] A. NISCO, *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022, pag. 11

concetto di rimproverabilità soggettiva risulterebbe svuotato. Il soggetto collettivo si è limitato ad adottare un *software* prodotto da altri e la colpa di organizzazione si ridurrebbe alla erronea scelta del *software* o alla decisione stessa di automatizzare *in toto* la *compliance*[176]. Una soluzione prospettata è quella di includere degli esperti nel perimetro dell'organizzazione, elaborando, in sostanza una "*compliance* della *compliance*" digitale, aumentando il numero dei controlli. Tuttavia, anche per questi esperti potrebbe essere difficile fornire una spiegazione esaustiva del difetto organizzativo eventualmente occorso a causa o nonostante, l'impiego della tecnologia, poiché non possibile prevedere compiutamente le decisioni della macchina.

Con ciò, la *compliance* digitale si pone al centro tra la questione della ricostruzione di un'autentica colpa d'organizzazione e l'altra, altrettanto cruciale questione della impellente necessità di regolamentare l'IA. Nel futuro, sarà pertanto necessario, ricomprendere nell'ambito tematico della *compliance* digitale anche l'esigenza di regolamentarne l'uso prospettabile nelle organizzazioni d'impresa, cercando di mantenere fermo, fin dove possibile, il modello della "auto-regolazione regolata" che, faticosamente, si è cercato di sviluppare per la responsabilità degli enti. "Tenendo insomma avvinte "*governance* tecnologica" e "*governance* della tecnologia", di modo che non solo l'organizzazione d'impresa si avvalga delle nuove tecnologie, ma che anche la tecnologia possa avvalersi delle organizzazioni, ricevendone un assetto di regole condivise e condivisibili"[177].

2.7 Il destino delle multinazionali

Una riflessione che non possiamo esimerci dal fare, nella nostra indagine sulla responsabilità da reato degli enti con riferimento ai reati informatici attiene alla posizione assunta dalle multinazionali rispetto al decreto 231. Il progresso della tecnologia ha, infatti, spinto sempre più aziende ad espandersi nel mercato globale, con il risultato che in Italia operano numerose aziende estere che potrebbero rendersi autori dei reati di cui ci occupiamo. Inoltre, facendo sempre più uso della tecnologia, per il futuro, sembra potersi prospettare l'ipotesi che tali enti siano a chiamati a rispondere dei reati informatici.

[176] P. SEVERINO, *Intelligenza artificiale e diritto penale in Intelligenza artificiale- il diritto, i diritti l'etica* a cura di Ugo Ruffolo, Milano, Giuffrè, 2020, Pag. 538

[177] A. NISCO, *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022, pag.12

In particolare, è doveroso ricordare che la prevenzione dei reati dolosi, espressivi della criminalità del profitto, è essenzialmente implementata, nel panorama giuridico internazionale: a) per una (ridotta) parte da strumenti normativi e da *best practices* internazionali; e b) per altra (prevalente) parte, da atti di autonormazione privata. A differenza della criminalità colposa, in cui l'apparato di cautele è in ciascuno Stato oggetto di specifica disciplina normativa, per i reati dolosi non sono reperibili esaustivi cataloghi di cautele normativizzate agevolmente consultabili. "È la *societas* che, dopo aver guardato dentro sé stessa (*risk assessment*), individua i rischi-reato potenzialmente esistenti, ne misura il grado di avveramento (l'intensità) e, successivamente, forgia i corrispondenti presidi cautelari telelogicamente orientati a ridurre ragionevolmente i rischi emersi (*risk management*)"[178]. In questo contesto, da un lato, l'ente collettivo è chiamato a confrontarsi con la "nazionalità" dei diversificati regimi normativi e, dall'altro lato, con i sistemi di *compliance*, frutto di autonormazione.

Questo apre due questioni, la prima è quella relativa alla giurisdizione che cercheremo di risolvere successivamente, grazie ai più recenti approdi giurisprudenziali. La seconda riguarda l'obbligo o meno degli enti esteri di adottare i modelli organizzativi di cui agli artt. 6 e 7[179], che ci sembra opportuno risolvere in questa sede, essendoci nel precedente paragrafo occupati della valutazione di idoneità del MOG che deve essere condotta dal giudice.

La questione circa la valutazione dei Modelli organizzativi, in merito agli enti stranieri è particolarmente insidiosa e divide dottrina e giurisprudenza. In giurisprudenza, l'orientamento prevalente ritiene che un surrogato estero di un modello di organizzazione e gestione ex art. 6 d.lgs. 231/2001 non abbia alcuna rilevanza esimente[180]. Quindi l'ente straniero operante in Italia potrà andare esente da responsabilità soltanto se dimostri di aver adottato ed efficacemente attuato il Modello 231. "Pur dando atto che la legge

[178] C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021

[179] Cfr. C. PIERGALLINI, *Globalizzazione dell'economia, rischio reato e responsabilità ex crimine delle multinazionali* in Riv. trim. dir. pen. econ. 1-2/2020, pag. 157, il quale parla di un "rischio normativo multinazionale" con una morfologia "tentacolare", con le seguenti declinazioni: rischio "da giurisdizione"; rischio "disciplinare", riferibile ai sistemi di responsabilità sanzionatoria della societas; rischio "da *compliance*", integrato dal reticolato di disposizioni normative e non relative alla prevenzione e alla gestione del rischio reato.

[180] Trib. Lucca, 31 luglio 2017, n. 222 in giurisprudenzapenale.com.

tedesca e quella austriaca non prevedono l'obbligo di adottare i modelli organizzativi previsti dalla legge italiana, si è già chiarito come la scelta di tali società 'straniere' di operare in Italia non consenta loro di sottrarsi alla giurisdizione di questo Tribunale, né all'applicazione delle disposizioni del d.lgs. 231/2001"[181]. Secondo tale orientamento, il semplice fatto di operare in Italia comporta l'obbligo di rispettarne la legge. In altra sentenza i giudici utilizzano un esempio eloquente: "il conducente di un'automobile straniera fabbricata in un Paese in cui non sia in vigore l'obbligo delle cinture di sicurezza dovrà munirsi di tale dispositivo per circolare in Italia, altrimenti commettendo un'infrazione al Codice della Strada"[182]. Questa tesi, che trova spazio nelle aule dei tribunali, crea, tuttavia, una discriminazione tra enti stranieri e nazionali[183]. Neppure condivisibile appare la posizione di chi ritiene che la valutazione sull'ente debba avere riguardo alle regole di *compliance* per come previste nei paesi di appartenenza di ciascun ente, al fine di evitare che la giurisprudenza dichiari sempre inadeguati i modelli predisposti. Il criterio discretivo per verificare la conformità del Modello deve essere rappresentato dalla legge applicabile nel territorio dello Stato, non essendo concepibile una indagine da parte del giudice nazionale su sistemi normativi stranieri[184]. Autorevole dottrina ritiene che non si debba pretendere dall'ente straniero il Modello così come previsto nel nostro ordinamento. Se, già per gli enti italiani che operano nel nostro territorio, ci sembra che vi sia il rischio di alzare troppo l'asticella del modello idoneo ed efficacemente attuato, fino a basare la responsabilità da reato sul mero verificarsi dell'evento, per le società multinazionali la situazione sarebbe ancora più complessa. "In definitiva - vale la pena ripeterlo - se un ente estero dovesse rincorrere, nei più svariati mercati in cui opera, la diversificata congerie di atti a scopo preventivo, autonormati e non, ciò si tradurrebbe nell'imposizione di un obbligo oggettivamente insuscettibile di adempimento"[185]. Se venisse seguito un simile ragionamento verrebbe di fatto impedito all'ente l'esercizio del diritto alla difesa. Ecco perché l'ente, attratto dalla giurisdizione di uno Stato, come quello nostro, che incentra l'illecito della *societas* sulla colpevolezza

[181] Trib. Lucca, 31 luglio 2017, n. 222, pag. 1009 in giurisprudenzapenale.com
[182] Tribunale di Milano, 27/04/2004, (ord.) GIP Salvini – Imp. Siemens A.G
[183] E. STAMPACCHIA, *La responsabilità amministrativa degli enti con sede all'estero* in archiviodpc.dirittopenaleuomo.org, 4 ottobre 2013, Pag. 14
[184] A. SCARCELLA, *La c.d. "internazionalizzazione" della responsabilità da reato degli enti* in La resp. amm. delle soc. e degli enti, n.1/2014
[185] C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021, pag. 324

di organizzazione, deve potersi appellare, al rispetto della *compliance* preventiva del suo Paese, sia essa eteronormata che spontaneamente autonormata[186]. Questo *modus operandi* appare necessario sia per evitare fughe dal mercato italiano, sia per evitare di riservare agli enti esteri un trattamento peggiore di quello riservato agli enti, con sede principale in Italia, che operano all'estero. Questi ultimi, infatti, grazie al riferimento normativo alla sede nell'art. 4 d.lgs. 231/2001, potranno avvalersi dello strumentario difensivo predisposto negli artt. 6 e 7 d.lgs. 231/2001. Pertanto, prima di tutto, occorrerà verificare l'esistenza di una *compliance*, che, a prescindere dalla sua qualificazione nominalistica, trasmetti finalità di prevenzione dei rischi-reato attraverso non la mera esposizione dei valori perseguiti (alla stregua di un codice etico), ma con strumenti operativi aziendali (codici di comportamento, linee-guida, protocolli, procedure, ecc.) idonei a conseguire lo scopo preventivo. Successivamente, è da verificare l'effettività del sistema preventivo apprestato. La *compliance*, cioè, non deve risolversi nella istituzione di un apparato meramente burocratico-cartolare, bensì in una funzionalità operativa. Ricorrendo tali condizioni, non dovrebbero sussistere ostacoli al riconoscimento della sostanziale assimilabilità di un simile sistema prevenzionistico a quello delineato nel d.lgs. n. 231/2001. Li accumunano lo "scopo" (la riduzione ragionevole del rischio reato) e il "mezzo" (l'arsenale preventivo efficacemente ed effettivamente apprestato)[187]. "In questa prospettiva rileverebbe dunque anche quello che potrebbe definirsi il modello c.d. "equivalente" ovvero il complesso delle procedure e controlli astrattamente compatibili, indipendentemente dalla loro denominazione e primaria finalizzazione, con la *ratio* preventiva posta a fondamento del decreto"[188]. Anche Confindustria sembra condividere

[186] Cfr. C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021, pag. 325 e A. Alessandri, Attività di impresa e responsabilità penali, in Riv. it. dir. proc. pen., 2005, pag. 559.

[187] Cfr. A. F. TRIPODI, *Il diritto penale degli enti nello spazio: deantropomorfizzazione e globalizzazione a confronto* in archiviopenale.it n.1/2019; C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021; C. PIERGALLINI, *Globalizzazione dell'economia, rischio reato e responsabilità ex crimine delle multinazionali* in Riv. trim. dir. pen. econ. 1-2/2020; G. RUTA, *La responsabilità amministrativa degli enti stranieri e i limiti del principio di territorialità* in La responsabilità amministrativa delle società e degli enti - 4/2018; SCAROINA E., *Verso una responsabilizzazione del gruppo di imprese multinazionali?* in diritto penale contemporaneo, 23 luglio, 2018; E. STAMPACCHIA, *La responsabilità amministrativa degli enti con sede all'estero* in archiviodpc.dirittopenaleuomo.org, 4 ottobre 2013; M. RICCARDI, *L'internazionalizzazione della responsabilità "231" nel processo sulla strage di Viareggio: gli enti con sede all'estero rispondono per l'illecito da reato-presupposto "nazionale"* in giurisprudenza penale web, n.1/2018

[188] E. SCAROINA, *Verso una responsabilizzazione del gruppo di imprese multinazionali?* in diritto penale contemporaneo, 23 luglio, 2018, pag. 12

detta posizione laddove afferma che i modelli organizzativi adottati in base a leggi straniere "potranno ritenersi idonei a spiegare efficacia esimente laddove rispondano ai requisiti previsti dal decreto 231 e risultino efficacemente attuati"[189].

Una perplessità, tuttavia, potrebbe sorgere dalla figura dell'OdV, prevista dal decreto 231 e non rinvenibile in altri ordinamenti[190]. Del resto, è altamente improbabile che una società multinazionale si doti di questo organo per sole attività svolte in Italia[191]. Date per conosciute le caratteristiche strutturali (indipendenza, autonomia, professionalità, continuità d'azione) e funzionali (vigilanza sul funzionamento e l'osservanza del modello, cura del suo aggiornamento) dell'organismo di vigilanza, va osservato come già nel decreto n. 231 sia riconosciuta la fungibilità dell'organismo. Infatti, l'art. 6, comma 4-bis, prevede che le funzioni dell'organismo possono essere svolte, nelle società di capitali, dal collegio sindacale, dal consiglio di sorveglianza o dal comitato per il controllo della gestione, sì da rendere tutt'altro che 'esclusiva' la scelta di incardinare un organismo *ad hoc*[192]. A maggior ragione, deve essere riconosciuta una analoga fungibilità alle società estere, proprio tenendo presente che si è al cospetto di un istituto esclusivamente italiano. Sarà, pertanto, sufficiente, per l'ente estero, avere incardinato ed implementato funzioni di controllo interno sull'adeguatezza e sull'effettività della prevenzione. Autorevole

[189] Confindustria, Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo, 2014, pag. 11.

[190] Nella giurisprudenza italiana, tale questione si è posta immediatamente, in particolare nel procedimento che ha visto coinvolta la società tedesca Siemens per fatti di corruzione commessi in Italia: G.i.p. Trib. Milano, ord. 28 aprile 2004, in Foro it., 2004, II, 434.

[191] Sebbene V. MONGILLO, *L'Organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche* in Resp. amm. delle società e degli enti, n. 4/2015, pag. 85, sottolinea la capacità attrattiva di tale creazione a livello internazionale.

[192] Questa disposizione apre la questione della responsabilità dell'OdV, nel caso in cui questa funzione venisse svolta dal Collegio Sindacale, poiché la responsabilità penale dei membri del collegio è riconosciuta pacificamente dalla giurisprudenza. Il rischio, evidenziato in dottrina, era che la presenza nell'OdV di soggetti su cui gravano, a causa dell'appartenenza ad altro organo societario, una serie di poteri doveri, determinerebbe la moltiplicazione di occasione in cui si attiva, per il garante, l'obbligo di impedimento. Tuttavia, come nota Mongillo "Non è detto però che l'accresciuto rischio penale connesso all'assunzione delle funzioni di OdV da parte dei sindaci possa tradursi in un significativo disincentivo. Del resto, anche nell'assetto fisiologico dell'organismo deputato a vigilare sull'attuazione del Modello si richiedono flussi informativi tra OdV e organo sociale di controllo per quanto concerne le disfunzioni del Modello organizzativo ed eventuali illeciti rilevanti commessi da soggetti apicali o sottoposti. Situazioni di blocco informativo, in presenza di (reiterate) violazioni degli amministratori, potrebbero denotare proprio una «sudditanza» dei membri dell'OdV nei confronti del vertice aziendale; disfunzione a cui potrebbe, invece, permettere di ovviare proprio l'investitura del Collegio Sindacale, quale organo che normalmente dà le maggiori di garanzie di indipendenza e «distanza» dall'organo amministrativo" (Cfr. V. MONGILLO, *L'organismo di vigilanza*…, cit., pag. 105.

dottrina, individua funzioni che possono essere accostate all'OdV e che potrebbero aiutare il giudice nella valutazione del modello della società estera. Una funzione che, ad esempio, può essere paragonata all'OdV è quella dell'*internal audit*, che si è diffusa a livello internazionale. Tale figura ha il compito: a) di valutare i processi di *governance*; b) di contribuire al miglioramento di tali processi; c) di controllare i processi esposti a rischi, compresi quelli normativi, segnalando possibili azioni di miglioramento[193]. Dette funzioni di controllo devono essere condotte tramite un approccio sistematico e *risk-based*. Siamo in presenza di una figura connotata da indipendenza e che riproduce i compiti affidati all'OdV[194]. Inoltre, le società di capitale, italiane ed estere, quotate in borsa, sono altresì provviste di ulteriori importanti funzioni: *l'Enterprise Risk Assessment* (ERA) e *l'Enterprise Risk Management* (ERM). Proposte nel 2004 dal Co.S.O. (*Committee of Sponsoring Organisations of the Tradeway Commission*), hanno lo scopo di valutare e migliorare la gestione dei rischi aziendali, compresi quelli normativi, tra i quali il rischio penale[195]. Si inseriscono nell'ambito del Sistema del Controllo Interno (SCI), che contribuisce a mantenere l'organizzazione aziendale orientata alla salvaguardia dei seguenti obbiettivi: conformità delle operazioni alle leggi, ai regolamenti e alla normativa endoaziendale; affidabilità ed integrità delle informazioni, salvaguardia del patrimonio aziendale; efficacia ed efficienza delle operazioni. Possiamo, ancora, fare riferimento alla figura del *Compliance Officer*, di matrice anglo- statunitense, che supervisiona e gestisce le tematiche di *compliance* (compresa la prevenzione dei rischi-reato) all'interno dell'organizzazione, assicurando che la struttura sia conforme ai requisiti dettati dalla regolamentazione e che le risorse umane agiscano nel rispetto delle procedure interne[196]. Pur trattandosi di una funzione indipendente dai vertici della società è, tuttavia, da precisare che si è al cospetto di un "vertice" della società, che esercita funzioni direttive[197]. "Il *compliance officer* costituisce, infatti, un ufficio di controllo, una funzione ricoperta di regola da un *manager* interno all'azienda, che secondo le migliori

[193] C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021, pag. 326
[194] Ibidem
[195] Ibidem
[196] C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021, pag. 326
[197] Ibidem

prassi andrebbe individuato tra i dirigenti di più alto livello (*senior managers*)"[198]. Di conseguenza, manca il requisito dell'indipendenza[199]. La figura, tuttavia, più simile all'OdV, la ritroviamo nell'Organismo spagnolo[200]. Si tratta della figura *dell'oficial de cumplimento* prevista nel sistema spagnolo, che, come l'OdV, presenta i caratteri dell'autonomia e dell'indipendenza rispetto ai vertici della società[201]. Peraltro, autorevole dottrina rileva che il problema circa l'assenza della figura dell'OdV nelle società estere, è di più agevole soluzione grazie alla novella del 2011, che ha modificato l'art. 6 del decreto 231. Poiché, di norma il diritto societario dello Stato di provenienza dell'ente contemplerà, quantomeno, la costituzione di un organo di controllo sulla gestione, comunque denominato o configurato (comitato interno all'organo amministrativo, consiglio di sorveglianza, ecc.), assimilabile ad uno tra quelli menzionati dal nuovo comma 4 bis dell'art. 6[202]. Autorevole dottrina, pertanto, rileva che "la ricognizione delle esperienze internazionali sul terreno del "controllo interno" dimostra l'esistenza di una pluralità di funzioni, spesso operanti in sinergia, che paiono, ovviamente per analogia, accostabili ai compiti di vigilanza e controllo che il decreto n. 231 assegna al "neofita" organismo di vigilanza"[203]. Il giudice italiano, pertanto, potrebbe valutare l'idoneità del modello tenendo in considerazione la presenza di figure, che seppur non perfettamente sovrapponibili all'ODV, svolgono funzioni analoghe all'interno delle società estere[204].

Alla luce delle difficoltà emerse, sarebbe auspicabile, secondo parte della dottrina muoversi in modo non troppo dissimile da quanto avviene nell'ambito della colpa professionale del medico, governata da linee-guida e protocolli terapeutici e puntare al

---

[198] V. MONGILLO, *La vigilanza sull'attuazione del sistema aziendale di prevenzione dei reati in Italia e nei principali ordinamenti ispanoparlanti: circolazione dei modelli e specificità nazionali* in Dir. pen. cont.- Riv. Trim., 3/2018, pag. 153

[199] Cfr. V. MONGILLO, *La vigilanza sull'attuazione del sistema aziendale di prevenzione dei reati in Italia e nei principali ordinamenti ispanoparlanti: circolazione dei modelli e specificità nazionali* in Dir. pen. cont.- Riv. Trim., 3/2018, pagg. 148 ss.

[200] Cfr. V. MONGILLO, L'Organismo di vigilanza…, cit., pag. 85

[201] Cfr. C. PIERGALLINI, La gestione ermeneutica…, cit., pag. 327; V. MONGILLO, La vigilanza sull'attuazione del sistema aziendale…, cit., pagg. 161 ss

[202] Cfr. V. MONGILLO, *L'Organismo di vigilanza*…, cit., pag. 100

[203] C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021, pag. 327

[204] Cfr. art 322- bis c.p., il quale all'ultimo comma afferma che le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi. Si tratta, pertanto, di una situazione similare a quella da noi proposta con riferimento alla funzione dell'OdV.

confezionamento di modelli e protocolli "pilota", destinati a veicolare la nervatura delle cautele, sempre suscettibili, poi, di integrazioni di "dettaglio". Sarebbe, infine, opportuno che protocolli, così costruiti, fossero assistiti da una presunzione, *iuris tantum*, di idoneità preventiva, superabile dal giudice solo attraverso l'adempimento dell'obbligo di motivare la *dissenting opinion*. "In questa maniera, il giudizio di idoneità del modello si potrebbe conformare a quel paradigma che nel diritto penale individuale corrisponde al dominio della colpa specifica, forma di colpevolezza che ben si sposa con le prerogative - di serialità operativa, di rilevanza dei beni in gioco, di affinamento della relativa cornice nomologica - dell'attività di impresa e che, tornando conclusivamente sull'esigenza di contenimento del potere valutativo dell'organo giudiziario, garantirebbe un tipo di accertamento meno "libero" e una maggior fiducia nel sistema da parte degli enti"[205].

Altra soluzione, sarebbe quella di garantire l'armonizzazione dei *compliance program* a livello sovranazionale. Già a livello europeo abbiamo visto gli sforzi fatti per ampliare il catalogo di reati per i quali è prevista la responsabilità da reato degli enti e rendere omogenee le sanzioni previste, pertanto, non potrebbero essere escluse delle azioni, a livello europeo e internazionale, volte a garantire un'armonizzazione dei modelli organizzativi. Ad esempio, l'OSCE ha pubblicato la Guida alla *due diligence* per l'impresa responsabile (*Due Diligence Guidelines for Responsible Business*). Si tratta di uno strumento volto a dare un supporto pratico alle imprese sull'attuazione delle Linee guida OCSE per le imprese multinazionali. L'attuazione di queste raccomandazioni può aiutare le imprese a evitare e ad affrontare l'impatto negativo relativamente ai lavoratori, ai diritti umani, all'ambiente, alla corruzione, ai consumatori e al governo societario che possono essere associati alle loro operazioni, catene di fornitura e rapporti commerciali. La presente Guida intende altresì promuovere una visione comune presso i Governi e le parti interessate (*stakeholders*) circa il dovere di diligenza per la condotta d'impresa responsabile. I Principi guida delle Nazioni Unite sulle Imprese e i Diritti umani, nonché la Dichiarazione tripartita dell'Organizzazione Internazionale del Lavoro (OIL) di principi sulle imprese multinazionali e la politica sociale, contengono altresì raccomandazioni sul dovere di diligenza e questa Guida può aiutare le imprese ad attuarle.

[205] C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021, pag. 327

Inoltre, il 23 febbraio 2022 è stata adotta la proposta di direttiva europea che introduce nuove regole sulla "*due diligence*" aziendale, che mirano a rendere le imprese più responsabili rispetto alle violazioni dei diritti umani e dei danni ambientali. La proposta della Commissione prevede l'obbligo per le imprese di individuare i rischi e, se necessario, evitare, far cessare o attenuare gli effetti negativi delle loro attività sui diritti umani, come il lavoro minorile e lo sfruttamento dei lavoratori, e sull'ambiente, ad esempio l'inquinamento e la perdita di biodiversità. "Le nuove norme offriranno alle imprese certezza giuridica e parità di condizioni, garantendo maggiore trasparenza ai consumatori e agli investitori"[206]. Questi documenti costituiscono un esempio degli sforzi fatti a livello sovranazionale per guidare le imprese, garantendo un comportamento omogeneo. L'omologazione tra le discipline dei vari paesi faciliterebbe l'attività dei gruppi multinazionali e il compito per i giudici. Facciamo, ad esempio, riferimento all'ordinamento spagnolo, nel quale gli studiosi hanno appurato una sostanziale coincidenza dei requisiti previsti quanto all'idoneità del modello organizzativo e dell'organismo di vigilanza dall'art. 31 bis del *Código penal* rispetto a quelli descritti dagli artt. 6 e 7 del d.lgs. n. 231 del 2001[207]. Questo consente un agevole adeguamento per i gruppi le cui società operano in entrambi gli ordinamenti[208]. "Occorre responsabilizzare i legislatori nazionali affinché promuovano una omogeneizzazione dei rispettivi ordinamenti in vista di una più efficace lotta alla criminalità d'impresa attuata in ottica integrata e globale"[209].

2.8 La difficile individuazione dell'autore del reato nei reati informatici e l'applicazione dell'art. 8 d.lgs. 231/2001

[206] L. MACRI, Proposta di Direttiva sulla *due diligence* in materia di sostenibilità in ntplusdiritto.ilsole24ore.com, 1 marzo 2022.
[207] E. SCAROINA, *Verso una responsabilizzazione del gruppo di imprese multinazionali?* in diritto penale contemporaneo, 23 luglio, 2018
[208] E. COLAROSSI J. CORTINOVIS, *I modelli organizzativi in Spagna*, in Resp. amm. soc. enti, 2016, 4, 306; E. SCAROINA, *Verso una responsabilizzazione del gruppo di imprese multinazionali?* in diritto penale contemporaneo, 23 luglio, 2018, pag. 14; V. MONGILLO, *La vigilanza sull'attuazione del sistema aziendale di prevenzione dei reati in Italia e nei principali ordinamenti ispanoparlanti: circolazione dei modelli e specificità nazionali* in Dir. pen. cont.- Riv. Trim., 3/2018
[209] E. SCAROINA, *Verso una responsabilizzazione del gruppo di imprese multinazionali?* in diritto penale contemporaneo, 23 luglio, 2018, pag. 14

Prima dell'avvento del d.lgs. 231 del 2001, la commissione di crimini informatici non destava preoccupazione alle imprese poiché esse facevano affidamento sul fatto che il reo sarebbe facilmente rimasto anonimo. Adesso, invece, l'ente è imputabile anche in caso di non identificazione del reo, grazie all'art. 8 del d.lgs. 231. Tale profilo risulta di particolare interesse nell'ambito del *cybercrime* poiché "non sempre l'uso di un terminale o di una certa identità digitale per la commissione di un reato" può "rappresentare la prova del fatto che quel reato sia stato realizzato da chi normalmente ha la disponibilità di quel particolare *computer* o dalla persona alla quale appartiene quell'identità"[210]. Nei precedenti capitoli abbiamo già messo in luce quali sono le possibili insidie che riguardano i reati informatici e che potrebbero essere amplificati all'interno del contesto aziendale. In particolare, ci riferiamo al fatto che nell'azienda le *password* circolano tra dipendenti e dirigenti al fine di garantire i controlli o concedere autorizzazioni per il compimento di determinate operazioni economiche, di *marketing,* fiscali o simili. Diventa, pertanto, ancora più difficile individuare una persona fisica alla quale attribuire il possibile compimento del reato. "Proprio muovendo da questa consapevolezza, l'autonomia della responsabilità dell'ente agisce quale deterrente contro condotte variamente ostative della struttura giuridica, sia rivolte a favore di chi abbia realizzato il reato (nascondendone l'identità), sia dirette contro di esso (trasformando la risorsa umana in capro espiatorio)"[211]. L'adozione di adeguati modelli organizzativi dovrebbero avere lo scopo di ridurre al mimino questi rischi al fine di assicurare flussi decisionali e processi aziendali trasparenti. In questo modo saranno più facilmente individuabili le condotte non conformi. Tuttavia, l'applicazione dell'art. 8 è tutt'altro che semplice. Sebbene la norma faccia riferimento anche all'ipotesi dell'amnistia in questa sede ci occuperemo dell'ipotesi della mancata individuazione dell'autore del reato, dato lo stretto collegamento con le fattispecie di cui ci occupiamo.

La norma ex art. 8 chiarisce che la responsabilità a carico dell'ente, ancorché dipendente dalla commissione di un reato, costituisce un titolo autonomo di responsabilità. Se il meccanismo punitivo contemplato dal decreto 231 si basa sul legame tra vicende delle persone fisiche e quelle dell'ente, ciò non toglie che in alcune ipotesi, l'inscindibilità tra le due possa venire meno. Ai sensi dell'art. 8, infatti, la responsabilità dell'ente sussiste

[210] H. BELLUTA, Cybercrime…, cit., pag. 96.
[211] Ibidem

anche quando il soggetto non è identificabile o non è imputabile. Con riferimento alla mancata identificazione dell'autore del reato, la Relazione governativa precisa che "quello della mancata identificazione della persona fisica che ha commesso il reato è un fenomeno tipico nell'ambito della responsabilità d'impresa" e "la sua omessa disciplina si sarebbe tradotta in una grave lacuna legislativa, suscettibile di infirmare la *ratio* complessiva del provvedimento". La previsione di cui alla lettera a) è stata oggetto di numerose obiezioni. La prima censura che viene mossa è che la disposizione mal si concilierebbe con l'intero sistema di illecito amministrativo delineato dal d.lgs. 231/2001, la cui imputazione si articola su due livelli che operano a seconda del tipo di soggetto attivo del reato. Pertanto, se i meccanismi di ascrizione dell'illecito sono diversi a seconda della particolare posizione che il soggetto attivo del reato occupa nell'ambito dell'impresa, ci si chiede quale dei due debba essere applicato qualora egli non venga identificato[212]. Si sostiene, inoltre, che non potrebbe essere verificato l'elemento soggettivo del reo, né ricostruita la finalizzazione della sua condotta al fine di accertare l'esistenza del collegamento tra reato e interesse dell'ente. Tuttavia, c'è chi ritiene sia sufficiente la riconducibilità dell'agente ad una delle due categorie[213]. La più frequente ragione dell'autonoma responsabilità dell'ente risiede nella complessità dei processi produttivi e gestionali che, coinvolgendo una pluralità di persone, molto spesso impediscono di identificare il singolo autore o gli autori del reato. Inoltre, non si può trascurare il fenomeno patologico della "irresponsabilità individuale organizzata", espressione della tendenza ad adottare all'interno dell'ente meccanismi che impediscono, anche quando sarebbe possibile, l'identificazione dell'autore e degli autori del reato. Per quanto attiene all'accertamento della responsabilità dell'autore del reato presupposto, la Corte di Cassazione, valorizzando l'autonomia della responsabilità dell'ente anche sul versante processuale, ha precisato in una recente sentenza che " Deve dunque affermarsi il principio di diritto per cui, in tema di responsabilità da reato degli enti, l'autonomia della responsabilità dell'ente rispetto a quella penale della persona fisica che ha commesso il reato-presupposto, di cui D.lgs. n. 231 del 2001, art. 8, deve essere intesa nel senso che, per affermare la responsabilità dell'ente, non è necessario il definitivo e completo

[212] O. DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo* in *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2021, n. 231*, Milano, Giuffrè editore, 2010, pag. 140

[213] DE SIMONE, *La responsabilità da reato degli enti nel sistema sanzionatorio italiano: alcuni aspetti problematici* in Riv. Trim. dir. pen. economia, 2004, n. 3, pag. 657 ss.

accertamento della responsabilità penale individuale, ma è sufficiente un mero accertamento incidentale, purché risultino integrati i presupposti oggettivi e soggettivi di cui del medesimo Decreto artt. 5, 6, 7 e 8. Conseguentemente, la posizione processuale dell'ente imputato deve intendersi a sua volta come autonoma rispetto a quella dei coimputati persone fisiche, non gravando sul giudice alcun obbligo di valutare, a favore dell'ente, atti difensivi prodotti in favore di altri soggetti processuali[214].

Per quanto attiene alla valutazione di idoneità del modello, nel caso di specie, una soluzione ritiene di ravvisare una *culpa in re ipsa*, giacché il solo fatto che l'assetto organizzativo abbia consentito un'anonimizzazione dell'autore sarebbe segno evidente di una negligenza organizzativa[215]. Altra lettura conduce ad ammettere, comunque, una possibilità di discolpa in capo all'ente[216]. Tale orientamento distingue due ipotesi. La prima riguarda il caso in cui l'autore non è stato identificato a causa di una non trasparente organizzazione dell'ente che non ha consentito di risalire all'autore del reato. Questo caso richiama lo scenario del reato- presupposto commesso dagli apicali e la colpevolezza dell'ente si atteggia come colpa con previsione. "Se l'ente ha omesso di dotarsi di una trasparenza organizzativa significa che, pur prevedendo la possibilità di eventi-reati, li ha deliberatamente trascurati"[217]. La seconda ipotesi riguarda il caso in cui l'autore non è stato identificato nonostante l'organizzazione trasparente dell'ente. In questo scenario se il pubblico ministero si accontentasse di un generico rimprovero per colpa di organizzazione, si configurerebbe una vera e propria responsabilità oggettiva. Per evitare ciò, parte della dottrina richiama il concetto di colpa grave[218]. Il rimprovero all'ente sarà simile a quello rivolto al sanitario post-decreto Balduzzi o all'imprenditore nella bancarotta semplice. L'ente risponderà del reato presupposto "se e solo se in concreto abbia marcatamente mancato l'obiettivo *ex ante* di mappatura dei rischi-reato ed attuazione delle cautele; cioè, se in concreto era esigibile qualcosa di significativamente

[214] Cassazione penale sez. IV, 23/05/2018, (ud. 23/05/2018, dep. 09/08/2018), n.38363 in banca dati De Jure
[215] C.E. PALIERO, *La società punita: del come, del perché e del per cosa*, in Riv. it. dir. proc. pen., 2008, pag. 1525; C.E. PALIERO, *La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale* in Riv. trim. dir. pen. econ. 1-2/2018, pagg. 216 ss.
[216] BARTOLUCCI, *L'art. 8 d.lgs. 231/2001 nel triangolo di Penrose*, in www.penalecontemporaneo.it, 9 gennaio 2017, pagg. 14 ss.
[217] BARTOLUCCI, *L'art. 8 d.lgs. 231/2001 nel triangolo di Penrose*, in www.penalecontemporaneo.it, 9 gennaio 2017, pag. 18
[218] Ibidem

diverso rispetto alla condotta tenuta (dall'ente, in generale, o dall'Organismo di vigilanza, in particolare), con onere probatorio interamente in capo all'accusa"[219]. La previsione di cui all'art. 8 dovrebbe essere letta solo come autonomia della responsabilità dell'ente dalla responsabilità della persona fisica, "ma non dall'obiettiva realizzazione di un reato integro in tutti gli elementi che ne fondano lo specifico disvalore, considerando peraltro che la tipicità fattuale del "fatto di connessione", nella maggior parte dei casi, tramanderà segnali inequivoci sul retrostante tipo d'autore (se "apicale" o "subordinato")"[220].

Non può, tuttavia, che sorgere il dubbio circa l'applicazione dell'art. 8 ai reati dolosi di cui ci occupiamo. Infatti, se il reato presupposto deve essere realizzato in tutti i suoi elementi, ci chiediamo come possa essere accertato il dolo del fatto, se non si dispone del volto dell'autore. A tal proposito, una sentenza della Cassazione afferma che il reato-presupposto deve essere accertato ma, proprio in conseguenza dell'art. 8, che consente di prescindere dall'identificazione del colpevole, è anche possibile che l'accertamento si arresti al fatto obbiettivo tipico e alla sua antigiuridicità[221].

3. Prevenire in concreto i reati informatici: tra autonormazione privata e atti sovranazionali

In questa parte dell'elaborato ci concentreremo su ciò che le aziende possono o sono chiamate a fare per prevenire i crimini informatici. L'analisi procederà lungo due profili. Quello della prevenzione dei rischi da reato all'interno degli enti è uno dei pochi ambiti del settore penale in cui l'autonormazione privata gioca un ruolo fondamentale. Da un lato, cercheremo, pertanto, di comprendere, come possa essere costruito un modello organizzativo idoneo a prevenire i reati informatici. Dall'altro lato, vedremo quale ruolo gioca la *cyber-security* nel contesto delle aziende. Tali spunti sono fondamentali, viste le incertezze che ruotano intorno ai modelli organizzativi. Nonostante i possibili rimedi proposti e analizzati nei paragrafi precedenti, dai sistemi di certificazione all'estensione

[219] BARTOLUCCI, *L'art. 8 d.lgs. 231/2001 nel triangolo di Penrose*, in www.penalecontemporaneo.it, 9 gennaio 2017, pag. 18
[220] V. MANES, *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo* in Giurisprudenza Commerciale, fasc.4, 1° agosto 2021, pag.16
[221] Cass. sent. n. 28299/2016 in olympus.uniurb.it

della messa alla prova per l'ente, non si è ancora giunti, infatti, ad un risultato pienamente soddisfacente.

3.1 La *Cybercompliance*: La costruzione di un modello di organizzazione e gestione adeguato

Un aspetto su cui l'estensione della responsabilità da reato degli enti ai reati informati può incidere è sicuramente il Modello organizzativo. "Tuttavia, nel settore di cui trattasi la redazione dei protocolli dedicati alla prevenzione dei rischi informatici è particolarmente complessa sia in ragione dell'interconnessione con i profili di riservatezza…, nonché in forza delle necessarie competenze informatiche che posseggono gli autori di tali illeciti e che devono possedere necessariamente anche i soggetti deputati alla prevenzione della commissione degli stessi. Ciò in aggiunta all'evoluzione delle tecnologie e dei dispositivi in uso che aumentano esponenzialmente le possibilità di commissione di tali reati"[222]. Non possiamo, infatti, trascurare, da un lato, l'assoluta specificità propria della maggior parte dei reati informatici e dall'altro, l'utilizzo ad ogni livello, all'interno degli enti, di strumenti informatici. Basti pensare ad un ente che intende partecipare a gare di appalto: un valido modello 231 dovrà prendere in considerazione il rischio derivante dalla condotta dei vertici che per ottenere la vittoria di un appalto di servizi, ad esempio, si avvalgano di *cyber* criminali. Ma la difficoltà non risiede esclusivamente nel vasto uso della tecnologia in qualunque azienda, ma anche dal fatto che tali reati possono essere commessi anche attraverso dispositivi mobili come cellulari e ancora *devices* normati e regolamentati secondo una serie di rigide politiche aziendali redatte sulla base delle *best practice* enunciate dai principali *standard* internazionali in materia di sicurezza informatica. Occorre pertanto che gli enti si organizzino per ridurre al minimo la probabilità del verificarsi di questi eventi.

"Poiché il nostro sistema affida un peso giuridico ai modelli di organizzazione, gestione e controllo che le aziende sono tenute ad adottare, onde formalizzare i propri processi decisionali e organizzativi, nel rispetto dei principi della legalità e della trasparenza. E, non ultimo, onde precostituirsi un valido elemento esimente, attenuante da spendere in

[222] P. BALBONI F. TUGNOLI, *Reati informatici e tutela dei dati personali: profili di responsabilità degli enti* in *Giurisprudenza penale* n. 1-bis/2021, pag. 9

sede processuale penale. Il primo banco di prova per la società e gli enti deve essere l'adeguamento del modello ad una dettagliata *compliance* informatica"[223]. La tutela delle infrastrutture informatiche all'interno dell'aziende costituisce un'importante fase della predisposizione della strategia imprenditoriale, non solo per evitare sanzioni anche ingenti ma anche per non intralciare il c.d. *business continuity*, aumentando le perdite d'esercizio[224]. Pertanto, gli enti dovranno preoccuparsi di predisporre misure organizzative adeguate al fine di assicurare una maggiore affidabilità e qualità alla vita sociale e rimanere competitivi sul mercato, sebbene, la predisposizione di modelli volti a prevenire gli attacchi *cybercrime* risulta particolarmente complessa. "Certo è che, con riguardo al *cybercrime*, i richiesti modelli organizzativi, ad efficacia esimente o attenuante della responsabilità d'impresa, dovranno prefigurare le sedi, le modalità e le finalità del compimento dei relativi reati, così da predisporre una rete di controlli atti a garantire la massima trasparenza alle operazioni informatiche, sia a livello apicale, sia tra i dipendenti"[225]. Considerate l'elevate conoscenze tecniche richieste per prevenire questo tipo di reati è consigliabile affidare la progettazione e lo sviluppo del Modello a consulenti esterni, specialisti della materia, in grado di dare consigli mirati, capaci anche di diffondere una cultura della legalità di impresa. Infatti, non esiste un modello organizzativo che possa soddisfare le più disparate esigenze aziendali, al fine di esimersi dalla responsabilità da reato. Piuttosto, bisogna adeguare ogni procedura e documento, compreso il codice etico alla struttura, dimensione e natura dell'ente in modo da ridurre il rischio reato alla soglia del tollerabile[226]. Peraltro, nessun sistema può essere completamente sicuro, c'è sempre una percentuale di rischio da tenere in considerazione[227]. L'obiettivo è quello di raggiungere un livello accettabile di sicurezza che è definito dal bilanciamento di varie componenti, come il valore di quanto si intende difendere, l'investimento economico che si è disposti a sostenere, il livello di rischio che

[223] H. BELLUTA, Cybercrime…, cit., pag. 107.
[224] P. AMODIO, *Digital compliance: spunti di riflessione e di riforma sui controlli di prevenzione e protezione dell'O.D.V*. in *Filodiritto*, 7 giugno 2021
[225] H. BELLUTA, *Cybercrime*…, cit., pag. 90
[226] Ibidem.
[227] L. VELIA, *Commento sub art. 24-bis del d.lgs. 231/2001* in *Enti e responsabilità da reato* a cura di Lasco G., Velia L., Morgana M., Giappichelli Editore, Torino, 2017, pag. 265

si è disposti a tollerare[228]. È quindi necessario trovare un ragionevole compromesso tra gli interessi in gioco.

A tal proposito, occorre ricordarci che il d.lgs. 231/2001, all'art. 6, comma 2 predispone una serie di informazioni che riguardano la costruzione del MOG: "I modelli di cui alla lettera a), del comma 1, devono rispondere alle 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. Inoltre, il comma 3 consente agli Enti Collettivi di riferirsi, nel definire il Modello Organizzativo, Gestionale e di Controllo, a codici di comportamento elaborati dalla Associazioni di Categoria alle quali aderiscono e ritenuti idonei dal Ministero della Giustizia. Tali codici di comportamento non sono dei modelli *standard*, adottabili in quanto tali dagli Enti Collettivi, ma delle Linee-Guida cui riferirsi nell'elaborazione dello specifico Modello di cui deve dotarsi ciascun Ente. Pur con le ovvie differenze dovute alle caratteristiche tipiche di ogni Associazione, in generale da tali Linee-Guida emerge un *iter* procedimentale di applicazione del d.lgs. 231/2001 articolato in due fasi distinte: a) l'analisi dei rischi-reato (*risk assessment*); b) la gestione dei rischi-reato (*risk management*). Il già menzionato *iter* va seguito con riferimento a tutti i reati presupposti e quindi anche con riferimento ai reati informatici.

In primo luogo, bisognerà individuare le risorse che si vogliono destinare a questo scopo, realizzando un modello adeguato all'identità dell'ente in questione[229]. Questa valutazione dipende dall'impiego della tecnologia, sia nel versante interno ai processi produttivi, sia nel versante esterno rappresentato dalle relazioni che l'impresa intrattiene per ragioni processuali. Pertanto, la valutazione sarà differente a seconda che l'ente produca *software* o generi alimentari[230]. Inoltre, bisognerà individuare, con riguardo alle singole fattispecie

[228] BALBONI P. TUGNOLI F., *Reati informatici e tutela dei dati personali: profili di responsabilità degli enti* in *Giurisprudenza penale* n. 1-bis/2021, pag. 12
[229] G. DEZZANI, *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica,* in *La responsabilità amministrativa delle società e degli enti*, fasc. 1/2012, pag. 78.
[230] H. BELLUTA, Cybercrime…, cit., pag. 108

elencate nell'art. 24-bis d.lgs. 231 del 2001 i beni da proteggere e le aree di rischio (c.d. *risk assessment*) nelle quali potrebbe verificarsi il reato e valutare con il metodo della *gap analysis*, quali lacune all'interno della struttura possano avvantaggiare la commissione di reati[231]. Tale mappatura dei rischi impone l'attribuzione di uno specifico punteggio a ciascuna attività o processo sensibile (con riferimento a possibili modalità di commissione dei reati presupposto), oltreché di analisi di quali processi effettivamente possono essere oggetto di rischio per la realtà aziendale e verificare se, alla luce dei presidi in essere, vi sia anche un rischio residuo, ossia la possibilità di commissione dei reati alla luce delle misure correttive e dei protocolli in essere[232]. La mappatura si conclude con l'attribuzione di un livello di rischio esistente che dovrà essere mitigato tramite uno specifico presidio di controllo. In merito all'esito del lavoro di analisi si possono fare alcune considerazioni. In primo luogo, l'utilizzo della strumentazione informatica è ormai talmente generalizzato da estendersi ad ogni area e ad ogni processo operativo esistenti in qualunque tipo di Ente Collettivo. Ciò non significa che non sia possibile evidenziare aree/attività ove è maggiore la probabilità di una loro commissione (ad es.: l'area Acquisti nel caso di partecipazione dell'Ente a gare indette dalla Pubblica Amministrazione). Significa piuttosto che, analogamente a quanto va osservato riguardo i reati colposi derivanti da violazioni di norme antinfortunistiche non è possibile escludere a priori nessun settore di attività dell'Ente Collettivo dalla mappa di commissibilità di reati informatici presupposti. Inoltre, non è detto che la commissione di reati informatici presupposti avvenga mediante l'utilizzo dei mezzi informatici messi a disposizione dall'Ente Collettivo ai suoi collaboratori/dipendenti o ai suoi apicali ovvero nel normale svolgimento delle attività lavorative proprie dell'Ente. Gli agenti potrebbero utilizzare strumenti informatici di sua proprietà o comunque a sua disposizione e potrebbero agire operando al di fuori dell'Ente. In questi casi è evidente che non è possibile alcuna misura preventiva[233].

Con riferimento ai reati informatici, le aree di attività ritenute essere quelle più a rischio sono le seguenti.

---

[231] H. BELLUTA*, Cybercrime…*, cit., pag. 107.

[232] Cfr. Linee guida di Confindustria disponibili qui https://www.confindustria.it/.

[233] DEZZANI G. DELL'AGNOGNOLA L.*, L'implementazione del modello organizzativo, gestionale di controllo negli enti collettivi a seguito dell'inserimento di reati informatici fra i reati presupposto ex d.lgs. 231/2001 operato dalla legge 48/2008* in La responsabilità amministrativa degli enti, fasc. 3, 2009

1. La gestione dei sistemi informatici e telematici aziendali: In questo ambito potrebbero realizzarsi introduzioni abusive in questi sistemi per sottrarre dati ed informazioni all'interno dei pc utilizzati dai dipendenti, la produzione e diffusione a terzi di codici, parole chiave o altri mezzi idonei all'accesso al sistema informatico aziendale. Inoltre, introducendosi nei sistemi informatici di altre strutture, gli addetti potrebbero istallare dispositivi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o intercorrenti tra più sistemi, ovvero falsificare documenti informatici ad interesse e vantaggio della medesima società[234].
2. L'attività di analisi dei *competitors*: In questo ambito, distruggendo, deteriorando o rendendo, in tutto o in parte, inservibili i sistemi informatici dell'azienda concorrente, gli addetti alle attività di analisi dei *competitors* potrebbero agire per procurarsi abusivamente i codici di accesso ed introdursi nel sistema informatico di questi ultimi anche se protetto da misure di sicurezza per poi permanervi contro la volontà espressa o tacita di chi ha il diritto di estromettere eventuali terzi, al fine di ottenere un ingiusto vantaggio per l'azienda[235].
3. L'utilizzo dei sistemi informatici e telematici aziendali ed accesso della rete *internet*: All'interno della struttura aziendale, tutti i dipendenti autorizzati all'uso della rete *internet,* potenzialmente possono danneggiare i sistemi informatici, diffondere *malware* o altri programmi nocivi, introdursi illegittimamente in un sistema informatico protetto da misure di sicurezza, diffondere abusivamente codici o parole chiave idonei all'accesso ad un sistema informatico[236].
4. La trasmissione informatica o telematica di informazioni a Enti Pubblici: Gli addetti preposti alla trasmissione di dati alla Pubblica Amministrazione tramite sistemi informatici, possono inviare *malware* al fine di distruggere o cancellare informazioni o programmi informatici utilizzati dall'Ente Pubblico ed allo scopo

[234] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 41
[235] Ibidem
[236] Ibidem

di procurare all'azienda di appartenenza un ingiusto vantaggio, come differire l'informativa o le dichiarazioni rispetto alla scadenza stabilita[237].

Ognuna di queste aree dovrebbe essere presidiata con specifici protocolli per la mitigazione di specifici rischi. Altro passaggio fondamentale è fissare un certo *standard* di sicurezza entro la quale consentire agli apici e ai dipendenti di svolgere la propria attività informatica o telematica. Per evitare il verificarsi di *computer crimes* presupposto per l'applicazione delle sanzioni di cui al d.lgs. 231/01, la *policy* aziendale dovrebbe espressamente prevedere l'obbligo di utilizzare i *personal computer* dell'azienda per i soli ambiti inerenti all'attività lavorativa, di adoperare le unità di rete come aree di condivisione strettamente professionale, di non utilizzare e né tanto meno installare sulle macchine della società programmi distribuiti da soggetti non autorizzati, né mezzi di comunicazione propri, salvo esplicita autorizzazione del responsabile dei sistemi[238]. *Server* e postazioni *web* dell'azienda andrebbero protetti mediante l'impiego di *firewall*, sistemi antintrusione e di *software* antivirus di tipo centralizzato[239], che vanno poi costantemente aggiornati[240]. La *password* è uno strumento fondamentale per delimitare l'utilizzo dei diversi *dispositivi* aziendali poiché consentono al titolare di entrare in determinate aree operative. Per rendere sicuro il sistema delle *password* aziendali sarà necessario che queste siano conosciute esclusivamente dal personale preposto e modificate secondo cadenze stabilite. Spesso accade all'interno degli enti che la stessa posizione venga condivisa da più operatori. In questi casi, al fine di una più facile individuazione dell'autore del reato sarà necessario introdurre chiavi di accesso individuali da mantenere rigorosamente riservate. Solo in questo modo sarà possibile seguire le tracce dell'accaduto e poter verificare o escludere una responsabilità dell'ente.

Occorre, inoltre predisporre un sistema di autorizzazioni e di deleghe in modo da garantire l'attuazione del principio di separazione dei compiti durante tutto il processo. Questo

---

[237] Ibidem

[238] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 41; H. BELLUTA, Cybercrime…, cit., pag. 108.

[239] Si tratta di software antivirus dotati di una console di monitoraggio centralizzata che permettono all'amministratore di sistema la verifica ed il monitoraggio degli aggiornamenti e delle eventuali infezioni incorse al singolo sistema

[240] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 43

passaggio è fondamentale, in virtù, della tesi esposta nel secondo capitolo secondo cui il reato di accesso abusivo a un sistema informatico si realizza anche nel caso in cui il singolo sia legittimato all'accesso nel sistema senza però essere autorizzato a permanere ivi per il raggiungimento di finalità diverse da quelle al cui raggiungimento è finalizzato l'abilitazione all'ingresso. In questo caso il Modello Organizzativo di una società che svolga attività di assistenza informatica o raccolta di dati dovrà curare non solo che accedano a sistemi informatici esterni solo i soggetti abilitati, ma anche che costoro facciano il dovuto e legittimo uso dei dati così raccolti e che non approfittino della disponibilità delle chiavi di accesso per l'ottenimento di risultati diversi da quelli legittimi.

Peraltro, gli enti potrebbero anche decidere di predisporre misure di sicurezza di natura organizzativa. Facciamo riferimento a presidi fisici collocati nel luogo in cui si trova l'elaboratore, come ad esempio, l'accesso regolamentato dal *badge* di servizio o anche semplicemente da una chiave nella sala server o nella stanza ove è custodito il sistema che si intende proteggere.

Per facilitare i controlli e cercare di risalire all'autore del reato, tutte le attività devono essere documentate in modo adeguato, in particole con riferimento alle funzioni relative all'IT. Pertanto, occorrerà effettuare la copia di *backup* dei dati a frequenze prestabilite e registrare ogni accesso a dati sensibili[241]. La garanzia generale, quindi, riguarda la tracciabilità delle informazioni e la sicurezza che queste vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati. Sempre più diffusa è l'adozione di sistemi di *audit* automatico della struttura informatica. Si tratta di *software* progettati per tenere traccia di tutte le attività che avvengono sulla rete e permettono di ricostruire con estrema facilità e semplicità la movimentazione e/o alterazione di un dato. Attraverso questi *software* è possibile risalire all'uso di una risorsa e determinare la commissione di un reato[242].

[241] Ibidem

[242] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 43

Anche la formazione del personale e la parte del Modello relativa alle sanzioni disciplinari dovranno essere adeguate al fine di prevenire tali reati. L'Ente Collettivo che intenda dotarsi di un Modello Organizzativo, Gestionale e di Controllo mirato alla prevenzione dei reati presupposti, ovvero che intenda implementare il Modello già adottato e funzionante a seguito dell'entrata in vigore della legge 48/2008 deve inserire nel Codice Etico-Comportamentale principi e valori che sovraintendano all'utilizzo della strumentazione informatica nello svolgimento della sua attività e recepire nel Codice Etico- Comportamentale, almeno come richiamo, le modalità di utilizzo e le linee-guida di impiego degli strumenti informatici contenute nel Documento di *Policy* Aziendale sull'informatica di cui si è dotato, ovvero si deve dotare, così come suggerito dal Garante della Privacy in sue pronunce[243]. Dovrebbero essere organizzati specifici corsi di formazione in grado di illustrare le condotte lecite e le condotte *contra legem* rispetto all'utilizzo degli strumenti informatici. Un ottimo deterrente è determinato dall'esatta conoscenza delle pene inflitte poiché la percezione del reato nei *computer crimes* è estremamente ridotta. Spesso ciò che viene percepito come un'attività di normale svolgimento determina la commissione di un reato o di un illecito amministrativo. Ad esempio, si pensi all'installazione abusiva di un *software* che determini all'azienda un ingente risparmio e di conseguenza una concorrenza sleale nella realizzazione di un progetto. Tale condotta deve essere prevenuta dal Modello organizzativo in quanto potrebbe determinare un vantaggio per l'azienda che risulterebbe più competitiva a seguito del risparmio ottenuto[244]. L'adozione di una politica della sicurezza informatica, non va quindi vista dal punto di vista esclusivamente tecnico, ma anche giuridico. In questo contesto risulta fondamentale la figura dell'informatico giurista o di un informatico e di un giurista che collaborino per un'attenta pianificazione della prevenzione dei reati[245].

[243] BALBONI P. TUGNOLI F., *Reati informatici e tutela dei dati personali: profili di responsabilità degli enti* in *Giurisprudenza penale* n. 1-bis/2021, pag. 12.
[244] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 44
[245] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 45

Altro aspetto rilevante è la cooperazione pubblico- privato, la quale si manifesta in diversi modi. In *primis*, sotto forma di collaborazione tra autorità statuali e enti, attraverso la comunicazione in capo a determinati operatori degli incidenti informatici e attraverso l'adozione di misure dirette a contenere e gestire il rischio di minacce. Sotto questo profilo, non viene in rilievo esclusivamente il d.lgs. 231/2001 ma anche altri atti normativi, come la direttiva NIS e il *Cyber-act*, di cui abbiamo avuto modo di parlare nel primo capitolo e che si sono occupate del tema della *cybersecurity* a livello europeo. Documenti che mirano a rafforzare questo legame attraverso un sistema di notificazione degli incidenti, ispezioni da parte delle autorità competenti in caso di violazione degli obblighi previsti dagli atti sovranazionali e sanzioni adeguate. In tema di prevenzione dei reati occorre dire che l'azienda deve soprattutto preoccuparsi di evitare che gli attacchi ai sistemi e ai dati provengano dall'interno dell'ente. Nel caso di sospetto del reato, di provenienza interna ma anche esterna, occorrerà adottare tutte le misure necessarie per poter capire se un evento si è verificato e di che tipo di evento si tratta. Inoltre, si dovrà procedere a recuperare e memorizzare ogni fonte di prova digitale, per evitare eventi simili in futuro e per offrire supporto alle indagini. Anche questi elementi saranno oggetto di valutazione giudiziale in ordine alla idoneità del modello organizzativo dell'ente a prevenire il rischio di reati informatici.

Infine, poiché l'adozione, il rispetto e la messa in pratica del modello organizzativo devono essere controllati da un apposito organismo di vigilanza occorre che quest'ultimo sia posto nelle reali condizioni di conoscere e comprendere le dinamiche aziendali, comprese quelle informatiche. Seppure, come sottolinea Dezzani, questo flusso informativo deve rispettare le norme in materia di *privacy* dettate dal d.lgs. 196/2003[246]. Il problema principale che pare profilarsi su questo orizzonte comunicativo è dato dalla difficoltà di comprensione delle operazioni tecniche che sottostanno ad un eventuale reato informatico, al punto che, per non trasformare i flussi documentali verso l'organismo di controllo in un'operazione di mera estetica aziendale, potrebbe rendersi opportuna, nelle realtà aziendali a maggiore esposizione informatica un'integrazione della composizione dell'organismo stesso, con persona tecnicamente preparata. Ci riferiamo al *Chief*

[246] G. DEZZANI, *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica in mento "abusivi" nel sistema informatico e la responsabilità amministrativa delle persone giuridiche*, in *La responsabilità amministrativa delle società e degli enti*, fasc. 1/2012, pag. 79

Information Security Officer preposto ad occuparsi della sicurezza informatica. Solo insieme, queste due figure "potranno efficacemente verificare, esaminare e monitorare periodicamente, anche attraverso apposite interviste con i responsabili di settore, come disposto dagli organigrammi e dalle eventuali deleghe, la correttezza delle procedure, l'esistenza di clausole contrattuali relative alla gestione delle misure di sicurezza nonché la tracciabilità e la verificabilità di eventuali c.d. *near miss* in materia informatica ovvero, più latamente, qualsiasi evento legato alla procedura digitale potenzialmente idoneo a causare una falla all'interno del sistema aziendale"[247]. Altrimenti, l'OdV, potrebbe consultare periodicamente tecnici esterni, ai quali affidare il compito di esaminare le notizie o approfondire gli aspetti informatici e telematici delle operazioni aziendali[248]. "Pertanto, la figura dell'Organismo di Vigilanza, proprio in relazione ai reati ex art. 24-bis del D. lgs. N. 231/2001, diviene ancora più fondamentale rispetto a quanto non lo sia stata precedentemente assurgendo, sostanzialmente, a primo baluardo affinché i dati personali ed aziendali possano essere ampiamente tutelati e non distorti per altri fini se non quelli per cui sono stati precedentemente concessi"[249]. I citati accorgimenti di natura tecnica e procedurale potrebbero rappresentare l'antidoto al verificarsi di casi di mancata individuazione del soggetto attivo di un eventuale reato informatico, a cui potrebbe conseguire l'accollo della responsabilità in capo alla società stessa, soprattutto nei casi in cui quest'ultima non sia in grado di dimostrare di aver adottato ogni utile accorgimento al fine di evitare che tale circostanza potesse verificarsi e che l'autore del reato abbia agito per fini esclusivamente personali e non nell'interesse del proprio datore di lavoro. Dal punto di vista delle responsabilità, le citate soluzioni ed accorgimenti, potrebbero dimostrare, se non altro in prima battuta, che la società ha posto in essere quanto nelle sue possibilità per impedire che propri dirigenti e dipendenti commettessero un reato informatico ed evitare quella che viene definita imputabilità per *culpa in vigilando*. Non va sottaciuto come per le aziende l'essere individuate quali responsabili di violazioni di cui al d.lgs 231/2001, comporterebbe oltre all'esborso di importanti somme di danaro, anche sanzioni interdittive pesanti come la sospensione o la revoca delle autorizzazioni,

[247] P. AMODIO, *Digital compliance: spunti di riflessione e di riforma sui controlli di prevenzione e protezione dell'O.D.V*. in *Filodiritto*, 7 giugno 2021.
[248] H. BELLUTA, *Cybercrime…*, cit., pag. 110.
[249] P. AMODIO, *Digital compliance: spunti di riflessione e di riforma sui controlli di prevenzione e protezione dell'O.D.V*. in *Filodiritto*, 7 giugno 2021.

licenze o concessioni che sono risultate funzionali alla commissione dell'illecito, l'interdizione dall'esercizio dell'attività, il divieto di contrattare con la Pubblica Amministrazione, salvo i casi in cui ciò si renda necessario per conseguire le prestazioni di un pubblico servizio, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni o servizi. Tali rischi, rilevanti dal punto di vista oltre che squisitamente economico anche da quello del pericolo di non poter proseguire nell'attività produttiva, dovrebbero indurre oggi le aziende a progettare e attuare strategie preventive in grado di impedire la commissione di reati informatici all'interno dell'unità produttiva ed in caso ciò si verifichi ugualmente, di escludere una propria responsabilità o diretto coinvolgimento[250].

3.2 Il ruolo della *cybersecurity*

Nel corso di questi capitoli abbiamo visto come la sicurezza informatica abbia assunto un ruolo centrale nella legislazione sovranazionale e nazionale. In particolare, per il penalista essa costituisce "un oggetto di tutela dai contorni piuttosto ampi…un bene giuridico, per usare un lessico familiare, strumentale alla protezione di un'ampia gamma di beni finali – dalla riservatezza informatica, ai dati personali; dall'integrità dei dati e sistemi informatici e telematici, alla fede pubblica"[251]. Nel primo capitolo abbiamo analizzato i più importanti strumenti normativi sovranazionali in tema di *Cybersecurity*, ci riferiamo alla direttiva NIS e al *Cybersecurity Act* e alla proposta di direttiva NIS 2.0. Sulla scia tracciata dagli organismi europei anche il legislatore italiano è intervenuto in questa materia. Adesso riflettiamo su quali conseguenze gli atti di cui abbiamo già parlato e altri che nomineremo per la prima volta in questa sede potrebbero avere in materia di responsabilità da reato degli enti.

___3.2.1 La direttiva NIS e il d.lgs. 65/2018: riflessioni, critiche e prospettive future

[250] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 46

[251] A. GULLO, *I reati informatici* in *Responsabilità da reato degli Enti: diritto sostanziale* a cura di *Lattanzi G. Severino P.*, Giappichelli Editore, Lavis, 2020, pag. 381.

La direttiva NIS attuata in Italia con il D.lgs. n. 65/2018 ha avuto un ruolo fondamentale nei settori della *cybersecurity*, delle infrastrutture critiche e della *data protection*. Questi atti si rivolgono agli operatori di servizi essenziali e i fornitori di servizi digitali. In particolare, gli operatori di servizi essenziali vengono identificati attraverso i seguenti criteri: "a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; e c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio"[252]. Nell'allegato II della direttiva vengono individuati, inoltre, i settori interessati: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile; infrastrutture digitali.

La *ratio* di questo atto si discosta da quella del decreto 231. Infatti, non viene in gioco la prevenzione di specifiche figure di reato, né l'ente è chiamato a rispondere solo laddove sia ravvisabile un suo interesse o un suo vantaggio. La strategia è simile a quella di cui alla l. n. 190 del 2012 in tema di contrasto alla corruzione nel settore pubblico[253]. In *primis*, viene richiesto agli operatori di servizi essenziali in determinati settori e al titolare e al responsabile del trattamento dei dati, l'adozione di misure tecniche e organizzative adeguate a fronteggiare i rischi esistenti nei diversi ambiti di attività. Inoltre, sono imposti obblighi di comunicazione alle autorità degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti e dei *data breach*. Sono anche previste sanzioni amministrative la cui severità "non fa dubitare circa la loro riconducibilità alla nozione convenzionale di materia penale"[254], seppure le violazioni non necessariamente integrino illeciti penali[255].

Questo atto, seppur fondamentale, non è immune da critiche poiché non riesce a disporre una completa tutela ad ogni aspetto della vita digitale dell'individuo e delle persone giuridiche responsabili, a vario titolo, del trattamento delle informazioni digitali[256]. Inoltre, l'intervento del legislatore italiano sembra aver tradito le aspettative di armonizzazione e omogeneizzazione del legislatore sovranazionale. La direttiva NIS, agli

[252] Art. 5 direttiva Nis; Art. 4 d.lgs. 65/2018.
[253] A. GULLO, *I reati informatici…*, cit., pag. 390
[254] A. GULLO, *I reati informatici…*, cit., pag. 390.
[255] Ibidem
[256] P. AMODIO, *Digital compliance: spunti di riflessione e di riforma sui controlli di prevenzione e protezione dell'O.D.V*. in *Filodiritto*, 7 giugno 2021

articoli 14 e 16 pone un obbligo, in capo agli Stati membri affinché, gli operatori di servizi essenziali e i fornitori di servizi digitali "… adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni".

Il decreto legislativo 18 maggio 2018, n. 65, che ha recepito la direttiva nel nostro ordinamento, si è, nei fatti limitato a cambiare il destinatario delle previsioni dagli Stati membri alle entità incluse nell'ambito di applicazione, rimettendo agli operatori di servizi essenziali ed ai fornitori di servizi digitali la scelta di quali misure implementare, evitando di prendere posizione sugli indirizzi operativi. Un intervento più incisivo avrebbe permesso di individuare delle buone pratiche e dei criteri unitari di gestione del rischio. In questo modo sarebbe stato lo stesso Stato membro a individuare gli *standard* applicabili, dando una maggiore certezza alle imprese. Tuttavia, l'intervento sovranazionale della direttiva Nis ha sicuramente avuto delle ricadute sulle imprese, attraverso gli obblighi imposti e il rafforzamento del ruolo dell'Enisa[257].

Importanti sono anche le linee guida del Gruppo di cooperazione previsto dall'art. 11 della Direttiva. In particolare, tale organismo ha prodotto un lavoro di compilazione, denominato *Reference document on security measures for Operators of Essential Services*[258], che, tuttavia si limita a costituire, per espressa dichiarazione degli autori un "*reference document*" che fornisce agli Stati membri una rappresentazione di ciò che gli Stati membri adottano, con un approccio comune. Tuttavia, mentre la direttiva si pone come obiettivo la predisposizione di disposizioni minime comuni in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali[259], nel documento viene ricordato che gli Stati potrebbero desiderare applicare misure strettamente nazionali e diverse da quelle europee o internazionali (viene citato lo standard ISO 27001). Di fatto è stata notata una incapacità della Direttiva NIS a raggiungere gli obiettivi che si era

[257] F. DI MAIO, *Certificazioni di information security: analisi di supporto per le finalità esimenti de modello organizzativo* in Cybercrime e responsabilità da reato degli enti a cura di A. MONTI, Lavis, Giuffrè, 2022, pag. 217
[258] Il testo del documento è reperibile sul sito ec.europa.eu
[259] Considerando 2016, Direttiva 2016/1148

prefissata di omogenea applicazione ed innalzamento del livello generale di *cybersecurity*.

Dalle perplessità sorte intorno a questa direttiva è nata una Proposta di direttiva NIS 2.0, da noi analizzata nel primo capitolo. Nella relazione di accompagnamento alla proposta di direttiva si legge "La valutazione del funzionamento della direttiva NIS, condotta ai fini della valutazione d'impatto, ha identificato i seguenti problemi: 1) il basso livello di cyber-resilienza delle imprese operanti nell'UE; 2) i diversi livelli di resilienza tra Stati membri e tra settori; 3) il basso livello di consapevolezza situazionale comune e la mancanza di una risposta comune alla crisi". Ancora "La direttiva NIS ha concesso agli Stati membri un'ampia discrezionalità nello stabilire i requisiti di sicurezza e di segnalazione di incidenti per gli operatori di servizi essenziali. La valutazione mostra che in alcuni casi gli Stati membri hanno attuato tali requisiti in modi significativamente diversi, creando oneri aggiuntivi per le società operanti in più di uno Stato membro".

Il legislatore europeo, con questa proposta, cerca di dare un nuovo impulso alle logiche di standardizzazione, considerato un adeguato strumento di crescita, pensando sia alle certificazioni di prodotti e sistemi ICT, sia alla valutazione della conformità delle misure tecniche ed organizzative. Sarà, tuttavia, necessario attendere il processo di adozione della Direttiva e il suo recepimento negli ordinamenti nazionali, per verificare se questo sforzo sia idoneo a raggiungere gli obiettivi prefissati. In particolare, tale documento potrebbe garantire un passo in avanti verso l'armonizzazione dei *corporate compliance program*. Infatti, potrebbe finalmente essere individuato un parametro di riferimento che potrà consentire "il chiarimento definitivo sugli effettivi obblighi imposti agli operatori essenziali e quindi, l'esatta individuazione dei livelli minimi per valutare, ad esempio, un sistema di gestione della sicurezza delle informazioni, quale processo munito di capacità esimente in quanto strutturato su discipline comuni e armonizzate, individuate da autorità competenti come elementi idonei a garantire il pubblico interesse"[260].

___3.2.2 Il decreto *Cybersecurity* e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001

[260] F. DI MAIO, *Certificazioni di information security in Cybercrime e responsabilità da reato degli enti* a cura di A. MONTI, Lavis, Giuffrè, 2022, pag. 218

Di particolare rilievo, per la tematica qui affrontata, è la disciplina dettata dal d.l. 21 settembre 2019, n. 105 (convertito con la legge 18 novembre 2019, n. 133), che istituisce il c.d. parametro di sicurezza nazionale cibernetica e la nascita dell'Agenzia Nazionale per la sicurezza cibernetica, entrata nel nostro Ordinamento a seguito della conversione del Decreto-legge 14 giugno 2021, n. 82. La strategia nazionale si basa principalmente sulla prevenzione e sulla gestione delle crisi, al fine di accrescere il grado di resistenza delle organizzazioni e del sistema nazionale, in un'ottica di armonizzazione e con una visione europea e internazionale. Infatti, anche in questo caso i soggetti interessati sono sottoposti a obblighi di *compliance* preventiva. Peraltro, data l'assenza di un coordinamento tra gli atti, vi è il rischio di sovrapposizione agli obblighi imposti dal c.d Perimetro della sicurezza nazionale cibernetica di quelli provenienti dalla direttiva Nis. "Si diffonde per questa via un diverso meccanismo di corresponsabilizzazione dell'organizzazione fondato sulla mancata adozione di misure di *compliance*, con la creazione in prospettiva di binari sanzionatori ispirati a una logica di tutela anticipata rispetto a quella prevista dal d.lgs. n. 231 del 2001"[261].

L'art. 1 co. 1 del presente decreto così recita "Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, è istituito il perimetro nazionale di sicurezza cibernetica".

È stato previsto un articolato sistema di procedure e di controlli cui gli enti inseriti nel perimetro di sicurezza cibernetica dovranno ottemperare. Più nello specifico: ai sensi dell'art. 1, co. 2, lett. b), d.l. n. 105/2019, gli enti devono predisporre e aggiornare con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici; ai sensi dell'art. 1, co. 6, lett. a), d.l. n. 105/2019, gli enti devono dare apposita comunicazione al Centro di valutazione e certificazione nazionale (CVCN) qualora siano intenzionati a procedere con l'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per

[261] A. GULLO, *I reati informatici…*, cit., pag. 391.

l'espletamento di servizi informatici; ai sensi dell'art. 1, co. 6, lett. c), d.l. n. 105/2019, la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico svolgono attività di ispezione e verifica, impartendo, qualora necessario, specifiche prescrizioni.

Nel caso in cui, allo scopo di condizionare o ostacolare l'espletamento delle procedure e delle attività ispettive sopra indicate, vengano fornite informazioni, dati o elementi di fatto non rispondenti al vero o ne venga omessa la comunicazione, è applicabile la pena della reclusione da uno a tre anni (art. 1, co. 11, d.l. n. 105/2019).

L'introduzione del reato è recente e le opinioni degli studiosi non offrono molte certezze.

Secondo parte della dottrina la norma delinea diversi reati propri che si sostanziano in falsità ideologiche "rilevanti" ai fini della predetta disciplina extra-penale cui è accessoria, ed in un reato di omissione propria, tutti ascrivibili solo ai soggetti aventi sede nel territorio nazionale, che siano inclusi nel "perimetro di sicurezza nazionale cibernetica" quale definito e disciplinato da detta nuova normativa[262]. Alcuni studiosi, invece, ritengono che la disposizione si presenta, a prima vista, come reato comune, in quanto il soggetto attivo è identificato in "chiunque". Gli stessi, tuttavia, precisano che l'attività che il reo deve porre in essere al fine di conseguire l'illecito penale non appare effettivamente commissibile da chiunque, rendendosi necessario un ruolo qualificato per il soggetto interessato[263]. Potremmo ipotizzare quale autore di tale illecito l'organismo di vigilanza. Infatti, la condotta può manifestarsi nella duplice ipotesi commissiva o omissiva. Il reo potrebbe sia porre in essere attività volte a fornire informazioni, dati o elementi di fatto non rispondenti al vero e concretizzatesi in un *facere*, sia omettere di comunicare i medesimi entro i termini prescritti. Tuttavia, proprio l'ipotesi omissiva ci sembra quella che potrebbe realizzarsi con maggiore frequenza. Anticipiamo che tale reato è stato introdotto nel catalogo dei reati presupposto del decreto 231/2001. Il modello deve prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli. Se il modello deve essere costruito in modo da prevenire anche l'illecito in discorso, possiamo presumibilmente concludere che

[262] L. PICOTTI – M. R. VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in sistema penale web, 5 dicembre 2019
[263] T.E. ROMOLOTTI, *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001* in Rivista231, n. 1/2020, pag. 126

l'OdV sia destinatario delle informazioni a cui si fa riferimento e abbia la possibilità di compiere il reato.

Il dolo è specifico.

Alcuni studiosi hanno tuttavia criticato questa norma, poiché l'interprete avrebbe dovuto prevedere un'ipotesi di natura aggravata relativamente a colui che scientemente si è attivato per fornire informazioni fasulle rispetto al caso di chi si è astenuto dal fornire le informazioni richieste[264]. Altra dottrina rileva che si può parlare di reato di pericolo poiché il mero fornire o non fornire informazioni comporta una lesione al bene giuridico e di pericolo astratto, in particolare, non essendo necessaria una verifica della portata lesiva in concreto della condotta[265].

Il bene tutelato dalla norma non risulta di facile individuazione visto anche il mancato inserimento di tale disposizione all'interno del Codice penale. Individuato il fine del decreto, alcuni studiosi affermano che il bene da proteggere sia la sicurezza nazionale, la quale potrebbe essere pregiudicata da malfunzionamenti, interruzioni od impropri utilizzi di specifiche reti e sistemi informativi[266]. Tale profilo risulta per gli studiosi di rilevanza pratica. Infatti, non manca chi lamenta la scarsa determinatezza della fattispecie. Ricordiamo che la configurabilità del reato richiede attività o omissioni finalizzate ad ostacolare o condizionare l'espletamento di specifici provvedimenti o attività ispettive e di vigilanza. Tali procedimenti sono quelli di cui all'articolo 1, comma due lett. b; comma sei, lett. e comma sei, lett. c. Tuttavia, nessuna di queste norme prevede obblighi e comportamentali specifici. Si tratta infatti di disposizioni che si riferiscono ad ulteriori provvedimenti. Questo potrebbe in futuro portare a serie valutazioni in termini di legittimità della norma con riferimento al principio di tassatività e determinatezza che caratterizza il diritto penale[267]. L' individuazione del bene giuridico tutelato potrebbe essere utilizzata per interpretare correttamente la norma, anche al fine di supplire ai profili

[264] T.E. ROMOLOTTI, *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001* in Rivista231, n. 1/2020, pag. 126
[265] V. SASSI, *Sicurezza cibernetica e responsabilità ex D.lgs. 231/2001: la nuova fattispecie del D.L. 105/2019*, in quotidianogiuridico.it, 9 ottobre 2019
[266] T.E. ROMOLOTTI, *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001* in Rivista231, n. 1/2020, pag. 126
[267] T.E. ROMOLOTTI, *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001,* cit.; V. SASSI, *Sicurezza cibernetica e responsabilità ex D.lgs. 231/2001: la nuova fattispecie del D.L. 105/2019*, in quotidianogiuridico.it, 9 ottobre 2019.

di indeterminatezza che comporta la scelta legislativa adottata. "La domanda se la condotta contestata sia stata idonea a compromettere, almeno teoricamente, la sicurezza nazionale potrebbe pertanto divenire dirimente in futuro, al fine di determinare l'eventuale rilevanza penale"[268].

Altra parte della dottrina, individua, il bene giuridico tutelato nell'efficacia dei controlli, della vigilanza e dell'intervento da parte delle autorità preposte[269].

Ai fini della nostra indagine è importante rilevare l'inserimento del suddetto reato nell'ambito dei delitti presupposto ex art. 24- bis, d.lgs. n. 231/2001. Questo costituisce un esempio di come le imprese siano chiamate ad affrontare seriamente la tematica della sicurezza informatica, che adesso viene legata in modo diretto alla responsabilità da reato degli enti. Gli enti che potrebbero commettere tale reato sono: a) I soggetti rientranti nel perimetro sicurezza e che intendono esternalizzare alcune forniture o servizi; 2) centrali di committenza alle quali questi fanno ricorso; 3) fornitori di servizi che partecipano ai relativi bandi. Possiamo immaginare uno scenario in cui uno o più di questi soggetti potrebbe non volere eccessiva trasparenza con riferimento a rapporti in essere. Si pensi ad esempio ad un affidamento assegnato ad un operatore in modo non conforme alla normativa applicabile, secondo uno schema per cui la violazione dell'articolo uno, comma 11, potrebbe accompagnarsi, in concorso, ad ulteriori reati quali quelli di cui all'art. 317 ss. c.p. Ma potrebbe sussistere una certa contiguità anche tra la norma in esame e i reati informatici. Gli enti saranno, pertanto, tenuti a costruire il modello organizzativo in modo tale da prevenire anche questo tipo di reato. Ogni attività dovrà ricevere adeguati presidi in termini sia di trasparenza che di legittimità, garantendo all'ente una completa percezione dei rapporti in essere e delle relative implicazioni. Inoltre, dal momento che il reato viene commesso principalmente mediante lo scorretto utilizzo di informazioni e dati, sarà opportuno che il modello organizzativo si pronunci in merito alla bontà, completezza e verificabilità degli stessi, come pure sulla garanzia della corretta evidenza del relativo processo comunicativo.

[268] T.E. ROMOLOTTI, *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001* in Rivista231, n. 1/2020, pag. 127

[269] V. SASSI, *Sicurezza cibernetica e responsabilità ex D.lgs. 231/2001: la nuova fattispecie del D.L. 105/2019*, in quotidianogiuridico.it, 9 ottobre 2019.

Peraltro, anche in questo documento si evince la necessità di una standardizzazione della disciplina. Infatti, le minacce realizzate con le nuove tecnologie non conoscono confini tra i singoli paesi. Risulta imprescindibile una prospettiva globale e "le organizzazioni sono obbligate, dalla legge della sopravvivenza, ad operare in maniera coerente e comune"[270].

A tal proposito, è utile citare un altro documento il *Framework* Nazionale per la *Cybersecurity*, elaborato per la prima volta nel 2015 e frutto della collaborazione tra accademia, enti pubblici, e imprese private. Il *Framework*, ispirato al *Cybersecurity Framework* ideato dal NIST (*National Institute of Standards and Technology*), fornisce uno strumento operativo per organizzare i processi di *cybersecurity* nelle organizzazioni pubbliche e private di qualunque dimensione. Nel documento del 2015, seppure ricordiamo che è stata presentata una nuova versione del documento nel 2019, si legge: "Questo ecosistema di misure che vanno senza soluzione di continuità dal pubblico al privato, oltre a proteggere i nostri interessi economici nazionali, potrà essere di rilevanza cruciale all'interno di contenziosi legali tra imprese o di dispute internazionali tra Stati, dovuti ad attacchi *cyber*. Infatti, alleviare o aggravare la propria posizione dipenderà dalla "*duty-of-care*" o dalla "*negligence*" che uno stato, una azienda o entrambi avranno seguito nel corso del tempo per minimizzare il rischio *cyber*. Da questo punto di vista, il *Framework* Nazionale di *cybersecurity* rappresenta uno strumento per identificare le eventuali lacune nella gestione della *cybersecurity* di una organizzazione, sia essa nel settore pubblico che in quello privato e per definire un percorso di gestione del rischio che perduri al cambiare della minaccia e della tecnologia"[271].

___3.2.3 Riflessioni conclusive in materia di *Cybersecurity* e MOG

Gli atti analizzati, fanno riferimento alla prevenzione del rischio *cyber* slegato dai reati presupposto di cui al d.lgs 231/2001, ad eccezione dell'ultima fattispecie citata. Tuttavia, è pensabile un modello di organizzazione e gestione integrato, viste anche le aree di sovrapposizione tra le due normative. Le norme sulla *cybersecurity* da noi analizzate intendono tutelare la sicurezza informatica dei dati e delle reti, per la loro struttura

[270] F. DI MAIO, *Certificazioni di information security*…, cit., pag. 221.
[271] Par. 2.2., *Framework* nazionale per la cybersicurezza.

internazionale e per le conseguenze economiche che gli incidenti possono produrre nel mercato globale, siano essi conseguenza o meno di atti delittuosi. Quello che in questa sede preme sottolineare è che i sistemi informatici a rischio contengono informazioni, ma il bene giuridico da tutelare non è l'informazione bensì la riservatezza degli individui[272]. La tutela del bene giuridico della riservatezza e certamente anche della riservatezza informatica presuppone l'integrità e la sicurezza dei dati e dei sistemi informatici, come anche il potere di esercitare un controllo sul flusso delle informazioni che terzi possono conoscere e trattare[273].

La *cybersecurity* è pertanto uno strumento necessario per garantire la riservatezza. In tale contesto un modello organizzativo integrato consentirebbe di ridurre i costi e i contrasti tra le procedure. La mappatura e l'individuazione delle aree di rischio sono sicuramente utili tanto nella prevenzione dei reati, tanto nella predisposizione dei presidi organizzativi in tema di sicurezza informatica. L'OdV e il responsabile della sicurezza informatica potrebbero costituire un unico ufficio o almeno dovrebbe essere necessaria una funzione di raccordo[274]. La circolazione delle informazioni, infatti, faciliterebbe la prevenzione dei reati presupposto del decreto 231 ma anche degli eventi accidentali che rilevano ai sensi degli atti sovranazionali da noi citati.

Infine, possiamo fare un ultimo cenno alle certificazioni di sicurezza informatica, in particolare facciamo riferimento agli standard ISO. Tralasciando gli accorgimenti di carattere tecnico del funzionamento di tali certificazioni, occorre qui rilevare che l'adozione di uno *standard* autorevole possa aiutare le imprese a costruire un modello organizzativo che abbia anche rilevanza giuridica per le finalità esimenti di cui all'art. 6 del d.lgs. 231. Nonostante, la reticenza dimostrata dal legislatore a fare riferimento a queste certificazioni, già nel 2012 l'ENISA, in seguito all'emanazione da parte della Commissione della "strategia di sicurezza cibernetica dell'Unione Europea", aveva condotto delle ricerche per valutare l'opportunità di introdurre un approccio unitario ai

[272] A. POSTIGLIONE, *Riflessioni in tema di organizzazione e di controlli nell'ipotesi di adozione di un modello integrato di gestione dei rischi di data breach e cyber breach* in La resp. amm. delle società e degli enti, fasc. 4, vol. 15, 2020, pag. 209

[273] Ibidem

[274] C. TEDESCHI, *Cybersecurity, tutela dei dati personali e prevenzione dei reati nelle società di capitali: possibilità di un modello di organizzazione e gestione del rischio articolato e collegato* in La resp. amm. delle società e degli enti, fasc. 4, vol. 15, 2020

processi di certificazione delle organizzazioni. Questo dimostra l'incessante tendenza della standardizzazione in materia di *cybersecurity* che potrebbe avere un giorno dei risvolti anche con riferimento alla responsabilità da reato degli enti. Tuttavia, dobbiamo rilevare che attualmente tali certificazioni non sono ancora particolarmente diffuse tra le imprese, come risulta da uno studio condotto nel 2019 dall'organizzazione della standardizzazione internazionale con riferimento allo standard ISO/IEC 27001[275].

4. I controlli dei lavoratori tra prevenzione degli illeciti e tutela della riservatezza

L'introduzione dei reati informatici tra gli illeciti in grado di determinare la responsabilità dell'ente apre una ulteriore questione circa un potenziale contrasto tra la necessità di prevenire la criminalità d'impresa e l'aspettativa di riservatezza del lavoratore di cui si occupa il c.d. Statuto dei lavoratori (l. 20 maggio 1970, n. 70) e il c.d. Codice *Privacy* (d.lgs. 30 giugno 2003 n. 196). L'elaborazione e l'adozione dei protocolli di prevenzione del rischio di reato informatico passa, infatti, anche dalla regolamentazione e dal controllo dell'utilizzo di *internet* e della posta elettronica. Occorre dunque cercare un punto di equilibrio tra gli interessi in gioco, tenendo presente che la riservatezza del lavoratore non è più esclusivamente minacciata dal controllo del datore di lavoro frutto di un rapporto di tipo verticistico ma da un controllo che si espande a tutti i livelli operativi, dovuto alla necessità di adottare quei metodi organizzativi idonei a prevenire i reati. Questo rende difficile tracciare una linea di confine tra vita personale e vita professionale.

Proprio il rischio che il controllo realizzato attraverso l'utilizzo della tecnologia potesse permettere al datore di lavoro di acquisire informazioni sensibili non legate all'attività lavorativa ha spinto il Garante *Privacy* ad intervenire nel 2007[276]. Questo documento contiene delle indicazioni utili circa l'uso della posta elettronica e di *internet* nei luoghi di lavoro. Il Garante, in tali Linee Guida, richiama i principi generali del Codice *Privacy* applicabili al controllo sull'utilizzo delle strumentazioni informatiche centrali, ovvero i principi di necessità, correttezza, di pertinenza e non eccedenza. Inoltre, sottolinea che il trattamento da parte del datore di lavoro di dati personali relativi all'utilizzo delle

[275] www.iso.org

[276] Si fa riferimento alle Linee guida del Garante per posta elettronica e internet, pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007 disponibili sul sito www.garanteprivacy.it

strumentazioni informatiche aziendali deve ispirarsi ad un canone di trasparenza, dovendo pertanto escludersi a priori la legittimità di qualunque controllo di tipo occulto[277].

Abbiamo detto che uno dei capisaldi della tutela del lavoratore dai controlli a distanza è l'art. 4 dello Statuto dei lavoratori (l.300/1970). Tale norma nel corso del tempo, ha subito delle modifiche proprie per adeguarsi ai cambiamenti portati dalla tecnologia all'interno delle aziende e nel mondo del lavoro. Così come i criminali, abbiamo visto, si servono della tecnologia per agire, anche il controllo datoriale è mutato. Dall'accesso ai sistemi informatici alla navigazione in *internet*, dalla corrispondenza via *e-mai*l alla presenza sui *social network*. A tali possibilità tecnologiche ha corrisposto un'evoluzione della normativa anche penale in materia di riservatezza, a tutela del lavoratore. Il testo originario dell'art. 4 St. lav.[278] contemplava due distinte forme di controllo: i controlli "intenzionali", consistenti in una deliberata sottoposizione dell'attività lavorativa ad un controllo a distanza senza altri scopi legittimi, ed i controlli "preterintenzionali", effettuati dal datore di lavoro per ragioni di sicurezza o per ragioni di organizzazione o produttive, ma da cui possa derivare un controllo indiretto dell'attività lavorativa dei dipendenti. In base al primo comma del vecchio art. 4 era disposto il divieto assoluto di compiere controlli intenzionali, ovvero "l'uso di impianti audiovisivi e di altre apparecchiature per

[277] Nel dettaglio, il Garante stabilisce che compete al datore di lavoro l'onere di specificare le modalità di utilizzo delle strumentazioni informatiche fornite lavoratori, indicando chiaramente le modalità di uso delle stesse e se, in che misura e con quali modalità possano venire effettuati dei controlli. Tale onere deve essere perseguito dal datore di lavoro tramite una policy interna da sottoporre ad aggiornamento periodico, redatta in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente verso i singoli lavoratori della rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.

[278] Art. 4 Statuto dei lavoratori prima della modifica: 1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. 2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. 3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti. 4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui al precedente secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

finalità di controllo a distanza dell'attività dei lavoratori". Si trattava di una ipotesi di reato di pericolo concreto, pertanto, era sufficiente la predisposizione degli strumenti per il configurarsi della fattispecie, senza che fosse effettuato il controllo[279]. Il secondo comma, invece, si riferiva ad "impianti ed apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori". La relativa istallazione necessitava di un accordo con le rappresentanze sindacali aziendali o, in mancanza di queste, con la commissione interna, oppure, in difetto di accordo e su istanza del datore di lavoro, di un provvedimento dell'Ispettorato del lavoro. "La fattispecie penale sanzionava l'istallazione in assenza di tali presupposti, atteggiandosi a reato di pericolo astratto, posto che ad esser punita era la mera "possibilità" di un controllo, insita nell'istallazione in difetto dell'accordo o dell'autorizzazione"[280]. La riforma del 2015 ha concentrato la tutela penale in un'unica fattispecie, il cui contenuto va ora dedotto da tre distinte disposizioni (art. 171 Codice *Privacy* e artt. 4 e 38 St. lav.). Questa modifica ha risposto a tre esigenze. "In primo luogo, la necessità di aggiornare la norma alle innovazioni tecnologiche intervenute (anche) nel mondo del lavoro, di cui è figlia una ridefinizione degli "strumenti" di controllo presi in considerazione. In secondo luogo, l'intento di rimediare ai contrasti provocati dal ricorso alla discussa categoria dei controlli "difensivi", aggiungendo la tutela del patrimonio aziendale alle esigenze legittimanti il controllo a distanza. Infine, nell'ambito di un più generale riassetto dei rapporti con la normativa in materia di riservatezza, l'introduzione di una disciplina relativa all'utilizzabilità delle informazioni acquisite tramite il controllo"[281]. L'art. 4 St. lav. un tempo rubricato "Impianti audiovisivi", fa ora riferimento ad "Impianti audiovisivi e altri strumenti di controllo". La disposizione è stata riscritta e formalmente collegata all'art. 171, d.lgs. 196/2003 (Codice *Privacy*), che ha recepito la relativa contravvenzione. L'art. 4 ora prevede: "1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per

[279] A. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico* in Sistema penale web, 20 dicembre 2021

[280] A. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico…*, cit.

[281] A. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico…*, cit.

la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi. 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 1962".

La disposizione è stata riscritta e formalmente collegata all'art. 171 del Codice Privacy, rubricato "violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori", il quale stabilisce che: "La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge". Si tratta di una norma incriminatrice dalla conformazione alquanto singolare, dal momento che non descrive il comportamento incriminato né fissa la relativa sanzione, ma si limita a richiamare e a porre in relazione le disposizioni da cui trarre tali elementi. Per di più, mentre entrambe le disposizioni richiamate risultano collocate nello Statuto dei lavoratori, il loro collegamento avviene in un contesto normativo distinto, il d.lgs. 196/2003, dedicato ad una materia diversa, sia pure indubbiamente connessa ad alcuni profili disciplinati dallo statuto. In particolare, è resa ardua la riconoscibilità del precetto che va tuttora ricavato dall'art. 4, comma 1 St. lav. Nella nuova norma, le attività non sono oggetto di un divieto, ma risultano esercitabili in attuazione di taluni requisiti. In particolare, sono sorte perplessità in merito all'apparente abolizione del divieto di effettuare controlli intenzionali. Si ritiene, tuttavia, che tale divieto sia sopravvissuto, benché in maniera implicita. Si dispone, infatti, che

"gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza […] possono essere impiegati esclusivamente" per determinate finalità. Ne consegue che risulta vietato ogni impiego per finalità diverse da quelle consentite[282]. "Il precetto, dunque, risulta essere "sfuocato", "sfumato", dai contorni non del tutto chiari e, quanto meno, non del tutto precostituiti in via di principio, mancando l'esplicito divieto generale. Le conseguenze non sono di poco conto, in considerazione della struttura e della tecnica di formulazione della fattispecie penale, la quale si limita a richiamare la disciplina extra-penale che, a sua volta, opera un rinvio ai contenuti degli accordi o dei provvedimenti autorizzativi. A prima lettura non può sfuggire la frizione con il principio di legalità e, più nello specifico, con quelli di determinatezza e precisione del precetto normativo giuridico"[283]. Alla luce di tale complesso quadro normativo, risultano vietati l'impiego e l'istallazione di impianti audiovisivi e di altri strumenti di controllo, in mancanza di due ordini di requisiti. Un requisito di carattere sostanziale inerente all'impiego dello strumento, riconducibile ad una delle tre esigenze tassativamente indicate dalla norma (intese come scopi in senso oggettivo del controllo, non come mere finalità soggettivamente perseguite dal datore): esigenze organizzative e produttive, sicurezza del lavoro, tutela del patrimonio aziendale. E un requisito di carattere procedurale, in base al quale l'istallazione dello strumento deve essere preceduta dall'accordo con le associazioni sindacali o in subordine dall'autorizzazione dell'Ispettorato del lavoro. "Funzione di tali requisiti è garantire un bilanciamento tra

[282] Cass. pen., sez. III, 8 settembre 2016, n. 51897 in De jure: " …Con la rimodulazione dell'art. 4 dello Statuto dei Lavoratori, è solo apparentemente venuto meno il divieto esplicito di controlli a distanza, nel senso che il superamento del divieto generale di detto controllo non può essere predicato sulla base della mancanza, nel nuovo art. 4, di una indicazione espressa (com'era nel previgente art. 4, comma 1) di un divieto generale di controllo a distanza sull'attività del lavoratore, avendo la nuova formulazione solamente adeguato l'impianto normativo alle sopravvenute innovazioni tecnologiche e, quindi, mantenuto fermo il divieto di controllare la sola prestazione lavorativa dei dipendenti, posto che l'uso di impianti audiovisivi e di altri strumenti di controllo può essere giustificato "esclusivamente" a determinati fini, che sono *numerus clausus*, (cioè per esigenze organizzative e produttive; per la sicurezza del lavoro e per la tutela del patrimonio aziendale) e alle condizioni normativamente indicate, sicché residua un regime protezionistico diretto a salvaguardare la dignità e la riservatezza dei lavoratori, la cui tutela rimane primaria nell'assetto ordinamentale e costituzionale, seppur bilanciabile sotto il profilo degli interessi giuridicamente rilevanti con le esigenze produttive ed organizzative o della sicurezza sul lavoro". In dottrina si veda R. FLOR, "Diritto penale e controlli a distanza dei lavoratori dopo il c.d. Jobs Act" in Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act a cura di LEVI A., Milano, Giuffré, 2016

[283] FLOR R., "*Diritto penale e controlli a distanza dei lavoratori dopo il c.d. Jobs Act*" in *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act* a cura di LEVI A., Milano, Giuffré, 2016, pag. 170

potere datoriale di controllo e interessi del lavoratore, sì che, dal punto di vista penalistico, presupposti e forme dell'autorizzazione, letti ovviamente a contrario, configurano condizioni di illiceità espressa della condotta, operative già sul piano della tipicità; per converso, in presenza dei requisiti di forma e di sostanza dell'autorizzazione, il reato non sussiste per mancanza del fatto tipico"[284]. I fatti penalmente rilevanti sono pertanto determinati dalle violazioni, sostanziali e procedurali, dei limiti posto dal nuovo art. 4. Tra i requisiti oggettivi che legittimano l'installazione di impianti audiovisivi e altri strumenti di controllo, alle esigenze organizzative e produttive e alla sicurezza del lavoro, si aggiungono quelle richieste per la tutela del patrimonio aziendale. Si tratta della discussa categoria dei controlli c.d. difensivi, diretti all'accertamento di comportamenti illeciti anche di terzi estranei. Finora la prevenzione e le esigenze organizzative costituivano i due elementi caratterizzanti da una parte i controlli difensivi e dall'altra quelli preterintenzionali, ma a seguito dell'introduzione della responsabilità *ex crimine* degli enti, la linea di demarcazione tra i diversi controlli e quindi tra le discipline applicabili non è più così netta. Si assiste alla commistione tra prevenzione, divenuta obiettivo primario della *compliance* aziendale e organizzazione. Prima dell'intervento di modifica del 2015 parte della giurisprudenza[285] metteva in dubbio che questo tipo di controlli necessitasse della validazione ex art. 4 capoverso dello Statuto dei lavoratori. La disciplina dei controlli difensivi è mutata sotto l'evoluzione "garantista" della giurisprudenza[286] in accordo con la dottrina[287] e anche per questo tipo di controlli è stato richiesto l'accordo sindacale o l'autorizzazione ministeriale[288]. La riforma, tuttavia, non è

[284] NISCO A., *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico* in sistemapenale.it

[285] Si veda Cass., sez. lav., 27 maggio 2015, n. 10955

[286] Si veda Cass. 1° ottobre 2012, n. 16622 in adapt.it: "Il divieto di controlli a distanza ex art. 4, della legge n. 300 del 1970, implica, dunque, che i controlli difensivi posti in essere con il sistema informatico Blue's 2002, ricadono nell'ambito dell'art. 4, comma 2, della legge n. 300 del 1970, e, fermo il rispetto delle garanzie procedurali previste, non possono impingere la sfera della prestazione lavorativa dei singoli lavoratori".

[287] Si veda R. FLOR, FLOR R., "*Diritto penale e controlli a distanza dei lavoratori dopo il c.d. Jobs Act*" in *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act* a cura di LEVI A., Milano, Giuffré, 2016

[288] Anche il Garante della Privacy nelle sue linee guida del 2007 era arrivato a questa conclusione partendo dai principi di necessità e di non eccedenza del controllo che sono enunciati all'art. 3 del Codice Privacy. Appariva quindi necessaria l'elaborazione di una dettagliata *policy* aziendale circa l'utilizzo di Internet e di posta elettronica, da comunicare obbligatoriamente ai lavoratori, ai sensi dell'art. 13 Codice Privacy. In assenza di una simile politica di *privacy* elettronica, al datore di lavoro non sarebbe consentito procedere con monitoraggi del dipendente, poiché quest'ultimo, in questo caso, avrebbe una ragionevole aspettativa di riservatezza delle proprie navigazioni e comunicazioni.

riuscita a dissipare ogni dubbio. Recentemente la Cassazione è tornata sulla questione. La decisione in esame trae origine dal ricorso di una lavoratrice sanzionata con licenziamento per giusta causa a seguito di alcuni accertamenti effettuati dalla Fondazione per cui prestava la propria attività lavorativa. I controlli erano stati giustificati dalla diffusione di un *virus* nella rete locale, effettivamente risultato correlato ad un *file* rinvenuto nel *computer* aziendale in uso alla lavoratrice che, dai suoi *download*, aveva iniziato a propagarsi nella rete della Fondazione, criptando *file* all'interno di vari dischi di rete, rendendoli illeggibili e inutilizzabili. Secondo quanto emerge dalla sentenza, in occasione dei controlli effettuati dall'amministrazione del sistema informatico, "venivano in rilievo numerosi accessi – da parte della lavoratrice – a siti che all'evidenza erano stati visitati per ragioni private, per un tempo lungo, tale da integrare una sostanziale interruzione della prestazione lavorativa"[289]. In questo contesto si contrappone la tutela della riservatezza del lavoratore, da un lato e il diritto del datore di lavoro di tutelare il proprio patrimonio e la propria attività imprenditoriale "funzionalmente collegata, in maniera diretta, con il lavoro svolto dai propri dipendenti"[290]. Anche l'attività imprenditoriale costituisce un interesse di primaria importanza poiché il potere di controllo del datore di lavoro potrebbe essere anche diretto alla tutela di altri diritti fondamentali. Infatti, i *devices* elettronici, come il *computer*, potrebbero costituire strumenti per la commissione dei reati informatici, di cui ci siamo occupati e per i quali è prevista la responsabilità degli enti collettivi. La corte interviene per stabilire se questa tipologia di controlli possa collocarsi al di fuori del nuovo art. 4 dello Statuto dei lavoratori. La cassazione propone un'ulteriore suddivisione, tra controlli difensivi "in senso lato" e "in senso stretto". I primi consisterebbero nei controlli «a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto di tale patrimonio»; data la loro natura, essi richiedono necessariamente il rispetto delle previsioni di cui all'art. 4 dello Statuto (per come novellato nel 2015). Invece, i secondi, cioè i controlli difensivi in senso stretto, sarebbero quelli «diretti ad accertare specificamente condotte illecite ascrivibili – in base a concreti indizi – a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro»[291]. Secondo la

[289] Cass. 22 settembre 2021, n. 25732, par. 2
[290] COLAPIETRO C. GIUBILEI A., *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della cassazione* in *Labour & Law Issues*, vol. 7, no.2, 2021, pag. 196
[291] Cass. 22 settembre 2021, n. 25732, par. 31.

Suprema Corte, sono proprio questi ultimi controlli che, anche quando vengono svolti con strumenti tecnologici, «non avendo ad oggetto la normale attività del lavoratore, si [situano], anche oggi, all'esterno del perimetro applicativo dell'art. 4»[292]. La corte rileva che mentre la procedura richiesta dall'art. 4 per l'installazione dell'impianto di controllo sarebbe coerente con la necessità di consentire un controllo sindacale su scelte che riguardano l'organizzazione dell'impresa, mentre meno senso avrebbe applicare la medesima procedura nel caso di eventi straordinari ed eccezionali costituiti dalla necessità di accertare e sanzionare gravi illeciti di un singolo lavoratore[293]. La corte pertanto mette un punto sulla sopravvivenza dei controlli difensivi; tuttavia, precisa che «in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e della riservatezza del lavoratore»[294]. A sostegno di tale tesi richiama le considerazioni emerse nell'ambito della giurisprudenza della Corte europea dei diritti dell'uomo.

In particolare, viene richiamata la recente sentenza Lopez Ribalda e altri c. Spagna[295], nella quale i giudici di Strasburgo hanno in sostanza ritenuto legittima la sorveglianza occulta effettuata dal datore sul luogo di lavoro anche in assenza del previo rispetto delle disposizioni in tema di controllo a distanza dei lavoratori, a condizione, tuttavia, che possa ritenersi proporzionata, valorizzando la sussistenza nel caso concreto di alcune condizioni così sintetizzabili: a) la preventiva emersione di concreti indizi tali da segnalare la presenza di illeciti in atto da parte dei dipendenti; b) l'effettuazione del controllo al limitato e unico scopo di accertare gli illeciti in atto, e con modalità proporzionate e coerenti con tale esclusiva finalità; c) l'interruzione della sorveglianza occulta una volta terminata l'indagine.

La corte successivamente richiama un'altra sentenza della Corte EDU emessa nel caso Barbalescu c. Romania[296] la quale conferma come tale soluzione ermeneutica sia coerente con i principi sanciti dall'art. 8 della Convenzione, che consente simili controlli, nelle dette situazioni, se proporzionati e ragionevoli rispetto ai richiamati scopi. In quest'ultima pronuncia, in particolare, i giudici, avevano fornito una nozione estensiva del "Diritto al

[292] Cass. 22 settembre 2021, n. 25732, par. 32
[293] Cass. 22 settembre 2021, n. 25732, par. 33
[294] Cass. 22 settembre 2021, n. 25732, par. 37
[295] Corte EDU, Grande camera, Lopez Ribalda e altri c. Spagna, 17 ottobre 2019 in rivistalabor.it
[296] Corte EDU, Grande Camera, Barbulescu c. Romania, 5 settembre 2017 in rivistalabor.it

rispetto della vita privata e familiare" ex art. 8 CEDU, includendo anche la "vita professionale". La Cassazione prosegue, poi, individuando in maniera puntuale le condizioni che devono sussistere affinché i controlli di natura difensiva "in senso stretto" possano essere esercitati legittimamente. Il controllo deve essere mirato ed attuato *ex post*, ossia solo dopo che nel datore di lavoro sia sorto il sospetto della commissione di un atto illecito da parte del lavoratore[297]. L'attività di controllo è legittima solo se verte su informazioni riferite a fatti avvenuti a partire dal momento in cui il datore di lavoro ha motivo di dover accertare la commissione di un illecito e non su informazioni che si riferiscono ad un periodo antecedente. In quest'ultimo caso, i dati risulterebbero acquisiti in violazione delle prescrizioni di cui all'art. 4 dello Statuto e sarebbero, dunque, inutilizzabili. La sentenza ha il merito di fare chiarezza sui confini dei controlli datoriali in un periodo storico in cui la riservatezza del lavoratore è attaccata su più fronti. Il primo riguarda il mutamento dei modelli organizzativi e produttivi. Infatti, nelle società contemporanee, in cui i dati svolgono un ruolo determinante, soprattutto per l'attività d'impresa, anche la sfera personale del lavoratore risulta più vulnerabile[298]. Infatti, nei processi di identificazione, selezione, ripartizione e valutazione dei candidati e dei lavoratori si stanno progressivamente abbandonando i metodi tradizionali, basati sul, giudizio soggettivo, a favore di analisi basate su grandi masse di dati[299]. Il secondo fronte che rende la sfera personale del lavoratore più vulnerabile è quello del progresso tecnologico. La pronuncia della Cassazione tenta di porre al riparo la sfera personale del lavoratore da quelle indebite intromissioni del datore di lavoro che i nuovi mezzi tecnologici renderebbero facilmente realizzabili. Ciò è possibile garantendo un controllo mirato e soprattutto attuato *ex post*. "In questo modo, si circoscrive l'attività di controllo solo a quei dati strettamente necessari per tutelare gli interessi aziendali e non si consente l'accesso a tutte quelle informazioni superflue e personali che il lavoratore rischia di disseminare nel tempo e che gli strumenti dell'era digitale incamerano e memorizzano durante il rapporto di dipendenza"[300]. Da questo punto di vista, la Cassazione

[297] Cass. 22 settembre 2021, n. 25732, par. 44
[298] COLAPIETRO C. GIUBILEI A., *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della cassazione* in *Labour & Law Issues*, vol. 7, no.2, 2021, pag. 205.
[299] COLAPIETRO C. GIUBILEI A., *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della cassazione* in *Labour & Law Issues*, vol. 7, no.2, 2021, pag. 205
[300] COLAPIETRO C. GIUBILEI A., *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della cassazione* in *Labour & Law Issues*, vol. 7, no.2, 2021, pag. 207

sembrerebbe aver individuato un equo bilanciamento tra i contrapposti interessi che vengono in rilievo nell'ambito dei controlli difensivi, assicurandosi che sia preso adeguatamente in considerazione il peso di una potenziale lesione della dignità e della riservatezza del lavoratore.

Occorre, inoltre, mettere in evidenza la modifica introdotta al nuovo secondo comma dell'art. 4. Dalla lettera della disposizione in base alla quale il comma 1 " non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze" sembra doversi desumere la sua applicazione non solo ad ogni *device* fornito o utilizzato dal lavoratore per svolgere l' attività lavorativa, quali *smartphones, tablets, laptops,* sistemi GPS per autovetture o autoarticolati, ovvero *softwares* gestionali o spazi informatici aziendali, quali *email, social networks* o *cloud area,* ma anche a sistemi di registrazione delle presenze quali l'uso di *badges* elettronici, impianti di autenticazione biometrica o altri strumenti di rilevazione audio-visiva. Inoltre, nel caso dello *smart-working* la "registrazione" riguarderebbe l'accesso al sistema informatico dell'azienda e/o ai suoi *servers* attraverso *Internet* e meccanismi di autenticazione logica. L'uso di tali sistemi di autenticazione e di *softwares* in grado di consentire all'operatore di svolgere attività da remoto, infatti, comporta non solo la registrazione dell'accesso, ma anche il possibile monitoraggio e la conseguente archiviazione delle operazioni poste in essere. Sottrarre tutto questo comparto di attività alla disciplina limitativa dell'art. 4 significherebbe, di fatto, annullare ogni forma di protezione per il lavoratore. La questione è complessa. Se da un lato la disposizione appare meno garantista, dall'altro lato i limiti posti all'adozione di strumenti di controllo a distanza potrebbero condurre ad una valutazione di inidoneità del modello organizzativo dell'ente. Altrimenti si sarebbe potuta verificare la situazione paradossale in cui il fallimento dell'accordo sui mezzi di monitoraggio con le RSA, avrebbe potuto condurre ad un addebito di responsabilità dell'ente in ragione dell'inidoneità del modello organizzativo. Il rischio è che gli adempimenti imposti dalla normativa lavoristica limitino le possibilità auto-organizzative dell'ente e le conseguenze del *deficit* prevenzionistico conseguente sarebbero tutte caricate sull'ente. Questo intervento del legislatore delegato contiene la portata garantista dei diritti del lavoratore operata dalla recente giurisprudenza in materia, andando invece maggiormente incontro alle esigenze di *compliance* dell'impresa e quindi in accordo con gli adempimenti del d.lgs. 231/2001.

Le perplessità sorte sul secondo comma dell'art. 4 hanno spinto il Ministero del lavoro a intervenire. Nel comunicato stampa del 18 giugno 2015 è stato messo in evidenza che la norma non "liberalizza" i controlli datoriali ma si limita a fare chiarezza sul concetto di "strumenti di controllo a distanza" e sui limiti di utilizzabilità dei dati raccolti attraverso tali strumenti, in linea con le indicazioni che il Garante della *Privacy* ha fornito negli ultimi anni. Sempre per il Ministero del Lavoro, la modifica all'articolo 4 dello Statuto dei Lavoratori si limiterebbe infatti a chiarire che non possono essere considerati "strumenti di controllo a distanza" gli strumenti che vengono assegnati al lavoratore "per rendere la prestazione lavorativa" come *pc, tablet* e cellulari. Infatti, l'accordo o l'autorizzazione non servono se lo strumento viene considerato quale mezzo che "serve al lavoratore" per adempiere la prestazione ma, nel momento in cui tale strumento viene modificato, anche aggiungendo *software* di localizzazione o filtraggi o altre applicazioni, per controllare il lavoratore diventa strumento che "serve al datore" per controllarne la prestazione per cui le modifiche effettuate diventano lecite solo in ricorrenza di particolari esigenze e previo accordo sindacale o autorizzazione dell'Ispettorato. Ad esempio, è stato considerato strumento di controllo non strettamente funzionale alla prestazione un *proxy* di navigazione, installato sul *computer* aziendale, che consenta al datore di lavoro di tenere traccia delle informazioni inerenti alle navigazioni degli utenti della rete aziendale, con conseguente necessità di autorizzazione e del rispetto dell'obbligo di informazione di cui all'art. 4, comma 3 dello Statuto[301]. Più complessa diviene la distinzione tra strumento di lavoro e strumento di controllo, quando un unico *software* è utilizzato per l'attività lavorativa, ma risulta munito di una funzione integrata che consente il simultaneo controllo sull'efficienza della prestazione. In questo caso è stato osservato che, se quest'ultima funzione acquisisce "autonomia" e "specifica operatività" rispetto alle funzioni connesse alla prestazione servirebbero i requisiti procedurali previsti dall'art. 4, comma 1[302]. Problematico appare, infine, l'utilizzo dei *social network* per monitorare l'attività lavorativa. Si rientrerebbe nell'utilizzo di uno strumento di lavoro, quando il *social network* sia impiegato per incrementare la comunicazione interaziendale, sì da rendere legittimo il controllo dell'attività senza la procedura autorizzativa. Un altro caso è quello in cui l'azienda si avvalga dei *social network* per finalità connesse al *business*,

[301] Così Trib. Torino (lav.), in Riv. it. dir. lav., 2019, II, p. 3 ss.
[302] NISCO A., Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico in sistemapenale.it, 20 dicembre 2021

l'utilizzo dei quali, tuttavia, non rappresenta un mezzo di esecuzione dell'attività di lavoro da parte dei prestatori. Il datore potrebbe accedere al *social*, ad esempio, per verificare eventuali anomalie nel traffico dei dati in *internet* idonee a causare il malfunzionamento della rete aziendale o la diffusione tramite la rete di informazioni aziendali riservate o compromettenti per l'immagine del datore. Di conseguenza, in tali ipotesi, il controllo potrebbe essere giustificato in quanto finalizzato alla tutela del patrimonio aziendale.

Controversa si prospetta soprattutto l'ultima ipotesi, riferita ad un utilizzo di *social network* per la tutela del patrimonio aziendale tramite profili *fake* appositamente costruiti dal datore per accertare le condotte illecite, ovviamente senza previa informazione al dipendente. Tale ipotesi è tata ricondotta dalla giurisprudenza alla categoria dei controlli "occulti" difensivi[303]. Da questa casistica, che non pretende di essere esaustiva, comprendiamo quanto sia difficile nei nuovi contesti aziendali in cui si fa uso della tecnologia distinguere tra strumento di lavoro e di strumento di controllo e quanto l'intervento del ministero abbia scarso rilievo pratico. In questa sede, non può non venirci in mente l'accelerazione nel ricorso allo *smart-working*[304] dovuto alla pandemia da Covid-19. La prestazione, in questo caso, si svolge attraverso la connessione in rete e nei fatti ogni strumento di lavoro può convertirsi in forma di controllo. E la tendenza è destinata ad accentuarsi a causa degli sviluppi in tema di IA applicati al contesto lavorativo. Sul piano penalistico ne risultano effetti poco preventivabili. Da un lato, il datore è esposto al rischio di incorrere nella sanzione penale, tenendo conto che il reato previsto dall'art. 171 Codice privacy risulta già integrato dalla mera "installazione" dello strumento di controllo e che, trattandosi di contravvenzione, è imputabile anche a titolo di colpa. Dall'altro lato, il lavoratore può trovarsi esposto a strumenti riconducibili al comma 2° dell'art. 4 St. Lav., il cui impiego produce dati, magari inutilizzabili ai fini del

[303] Cass. civ. sez. lav., 27 maggio 2015, n. 10955, in DeJure.

[304] La definizione di smart working nell'ordinamento giuridico italiano è contenuta nella l. 81/2017 e fa riferimento alla flessibilità organizzativa, sulla volontarietà delle parti che sottoscrivono l'accordo individuale e sull'utilizzo di strumentazioni che consentano di lavorare da remoto (come ad esempio: pc portatili, tablet e smartphone). In particolare, l'art. 18, comma 1, l. 81/2017definisce il lavoro agile quale» modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva».

rapporto di lavoro (se non vi è stata un'adeguata informativa), ma acquisibili in sede penale (come vedremo più avanti). "Simili effetti derivano da un disallineamento della fattispecie penale dal substrato empirico per cui era stata concepita, al punto che la distinzione tra strumento prestazionale e strumento di controllo, più che incerta, rischia di divenire radicalmente indimostrabile, almeno in un processo penale. Nell'ottica di un complessivo ripensamento del rapporto di lavoro, sollecitato dal nuovo contesto tecnologico, sarebbe sì auspicabile continuare a garantire una ragionevole tutela al lavoratore – nei "luoghi" non fisici dove è eseguita la prestazione –, ma rimodulandone i connotati anche in vista delle esigenze di certezza del datore[305]. In ogni caso occorre, ai sensi del nuovo comma 3, che il lavoratore sia informato sulle modalità d'uso degli strumenti e di effettuazione dei controlli, il che deve essere esplicitato in apposito disciplinare interno da redigere in modo chiaro e senza formule generiche, pubblicizzato adeguatamente verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori e sottoposta ad aggiornamento periodico, sulla falsa riga della *policy* per *internet* e la posta elettronica. "Non può tacersi, però, che in assenza di specifiche disposizioni normative disciplinanti il trattamento dei dati nell'esercizio dell'attività di controllo e oltretutto in assenza di formante giurisprudenziale, la compiuta armonizzazione della disciplina lavoristica con quella in materia di riservatezza e trattamento dei dati personali sarà di fatto demandata ai datori di lavoro e agli operatori del diritto, chiamati ad un arduo compito esegetico"[306].

4.1 Le ricadute sulla responsabilità da reato degli enti

Occorre adesso focalizzarci sulle ricadute di questa normativa sulla responsabilità da reato degli enti, tenendo in considerazione il contesto tecnologico in cui si realizzano i reati informatici. Bisogna premettere che, in assenza di un esplicito raccordo tra i testi normativi, non solo il reato di cui all'art. 171, ma nessun altro reato del Codice *privacy* rientra tra i reati presupposto della responsabilità dell'ente, nonostante la rubrica dell'art.

[305] NISCO A., Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico in sistemapenale.it, 20 dicembre 2021
[306] RIZZI R. VENTURA A., *La tutela della privacy del lavoratore controllato a distanza, alla luce della nuova disciplina sulla protezione dei dati personali* in fondazionenazionalecommercialisti.it, pag. 29

24-bis del decreto 231 faccia riferimento al trattamento illecito dei dati. Ai sensi dell'ultima disposizione citata, l'ente potrà rispondere, solo se il controllo datoriale sfoci in uno dei reati contro la riservatezza, da noi analizzati. Va comunque rilevato che la violazione dell'art. 4 St lav. può comportare l'applicazione di sanzioni amministrative nei confronti delle società da parte del Garante per la privacy, per via del richiamo operato dall'art. 114 Codice Privacy, che a sua volta costituisce norma nazionale di maggior tutela ai sensi dell'art. 88 GDPR sul trattamento dei dati nell'ambito dei rapporti di lavoro. Avvalendosi di tale strumento, il Garante è intervenuto nell'ambito dei servizi di consegna a domicilio tramite i c.d. "*rider*", gestiti mediante una piattaforma digitale ed altri strumenti relativi all'assistenza dei clienti, utilizzati (secondo il Garante) in modo difforme dal disposto dell'art. 4 St. lav. 91. Il contenuto afflittivo di tali sanzioni può di fatto eguagliare quello delle sanzioni ex decreto 231, ma il meccanismo di ascrizione della responsabilità non passa attraverso i modelli organizzativi che, notoriamente, contraddistinguono il sistema delineato dal decreto 231. Più che la mancata inclusione dell'art. 171 Codice Privacy nel decreto 231, in questa sede preme evidenziare l'omessa considerazione, da parte del legislatore, delle complesse interazioni tra modelli organizzativi e adempimenti inerenti alla riservatezza del lavoratore. "Nessun dubbio sul fatto che l'obbligo (o onere) di predisporre il modello organizzativo supponga il rispetto della normativa sulla *privacy* e dello Statuto dei lavoratori, ma, ad uno sguardo più attento, il rapporto tra siffatti adempimenti è percorso da una latente antinomia, sia nella fase antecedente che nella fase successiva alla commissione di un reato"[307]. I modelli organizzativi implicano sempre più spesso il ricorso a tecnologie di tipo informatico, come ad esempio l'uso di programmi in grado di processare i dati aziendali allo scopo di individuare anomalie, di tracciare le attività compiute dai dipendenti, al fine di evitare comportamenti elusivi o di ricostruire eventuali infrazioni, nonché di gestire i flussi informativi interni all'ente. La *compliance* aziendale concorre dunque allo sviluppo di nuove tecnologie di controllo del lavoro. Il che accentua, in primo luogo, le difficoltà insite nella distinzione tra strumento di lavoro e strumento di controllo poiché la nozione di strumento di lavoro dipende, seppure parzialmente, dal contesto organizzativo considerato. Questo ci spinge a chiederci se l'impiego di uno strumento idoneo a

[307] NISCO A., Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico in sistemapenale.it, 20 dicembre 2021

monitorare l'attività del lavoratore, quale destinatario del modello organizzativo, possa essere ricondotto per ciò solo al comma 2 dell'art. 4, in quanto funzionale alla *compliance* aziendale. A tale interrogativo, si ritiene, alla luce di quanto espresso poco prima, che debba essere data risposta negativa[308]. Specie nell'ambito della prevenzione dei reati informatici, che richiedono l'applicazione di strumenti (*hardware* e *software*) volti a tracciare gli accessi e le modalità di utilizzo dei dispositivi aziendali da parte del lavoratore, oltre che finalizzati alla manutenzione della rete da parte dei responsabili IT, la situazione si complica poiché mezzo prestazionale e misura di sicurezza tecnologica si compenetrano. Ma in un futuro non molto lontano, il complesso delle attività riconducibili alla *compliance* sarà sempre più gestito tramite tecnologie quali *Blockchain* ed Intelligenza artificiale. "Il fenomeno, etichettato "*digital criminal compliance*", potrebbe comportare la sottoposizione dei dipendenti ad una capillare attività di controllo elettronico, i cui risultati potrebbero spingersi oltre la generica previsione di un rischio illecito in ambito aziendale, sino a tradursi in una vera e propria profilazione di lavoratori singoli o di gruppi, in base alla specifica attitudine a commettere infrazioni. Si delineerebbe, con ciò, l'improprio affidamento al datore di lavoro di un'attività corrispondente all'accertamento della pericolosità criminale (su base tecnologica): scenario inquietante, che esigerebbe un più profondo ripensamento degli strumenti normativi a tutela del lavoratore"[309]. In questa sede ci limitiamo a constatare che in mancanza di un espresso raccordo con la disciplina statutaria, da un lato, e di un vero e proprio "obbligo" di adottare i modelli organizzativi secondo contenuti legislativamente predefiniti, dall'altro, la mera inclusione di uno strumento di controllo in un *compliance program* non è di per sé sufficiente ad esimere il datore dagli obblighi sanciti dall'art. 4 comma 1 St. lav. Secondo l'analisi della più recente giurisprudenza che abbiamo condotto, non può essere invocata la categoria dei controlli difensivi, incompatibile con la generica finalità di prevenire illeciti aziendali. Va anzi riconosciuto come l'adozione di un modello organizzativo attecchisca proprio nelle esigenze elencate dall'art. 4, comma 1 St. lav.: di tipo organizzativo, relative alla sicurezza del lavoro, nonché alla tutela del patrimonio aziendale (in quanto il modello consente all'ente di evitare in tutto o in parte

[308] NISCO A., Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico in sistemapenale.it, 20 dicembre 2021

[309] NISCO A., Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico in sistemapenale.it, 20 dicembre 2021

le sanzioni a contenuto patrimoniale previste dal decreto 231). Da questo punto di vista, la riduzione del rischio reato rientra nei compiti organizzativi primari dell'organo di gestione, ottemperando ai quali è necessario che esso tenga in debita considerazione gli interessi dei lavoratori. In sostanza, finché si consideri l'adozione del modello organizzativo *ante delictum*, l'eventuale allestimento di presidi tecnologici volti al monitoraggio dell'attività lavorativa non è sottratta alle rituali autorizzazioni. Diversamente possiamo dire nel caso dell'attività di indagine successiva alla notizia di un'infrazione, come accade ad esempio a seguito di una segnalazione interna ex art. 6, comma 2-bis d.lgs. 231/2001 (*whistleblowing*). L'attività di indagine interna riceve una disciplina frammentaria nell'ambito del d.lgs. 231/2001. Nonostante il quadro normativo incerto, non è escluso che l'impiego di uno strumento di controllo, privo di autorizzazione, possa ricadere nell'ambito dei controlli difensivi poiché si tratta di attività strumentale all'esercizio della difesa dell'ente, che può ricavarne un'attenuazione o l'esonero della responsabilità. Tuttavia, si auspica un intervento del legislatore che definisca i limiti entro i quali l'ente può difendersi indagando e regoli organicamente il rapporto tra difesa dell'ente e diritti del lavoratore. Tale regolazione dovrebbe tenere in conto che la riservatezza è in una certa misura connaturato alle indagini interne, almeno nella fase iniziale, e questo, ad oggi, potrebbe portare ad un contrasto con l'ambito di operatività dell'art. 4 St. lav. L'assetto normativo vigente lascia insoddisfatti entrambi i soggetti del rapporto. Da un lato, il datore di lavoro sottostà al rischio di violare il disposto dell'art. 4 St. lav., con le relative conseguenze penali, salvo confidare in un'incerta estensione dei controlli difensivi in chiave scriminante. Dall'altro lato, i lavoratori fruiscono di un'ambigua protezione processuale, in quanto l'inutilizzabilità degli elementi probatori ottenuti attraverso i controlli non autorizzati è circoscritta al rapporto di lavoro. Questo significa che tali elementi potrebbero restare inutilizzati in un procedimento disciplinare attivato a seguito dell'infrazione del modello organizzativo, e tuttavia essere posti alla base dell'accusa (e di un'eventuale condanna) in sede penale. È chiaro, dunque, che qui non è solo in pericolo la *privacy* dei dipendenti, ma piuttosto il loro diritto di difendersi da prove documentali formatesi nel corso delle indagini interne, con relativi rischi di autoincriminazione. Dall'altro lato è tempo al stesso in discussione

il contrapposto interesse dell'ente a dimostrare di aver attuato un sistema disciplinare "idoneo" ai sensi dell'art. 7, comma 4 lett. b), del decreto 231[310].

5. Delitti informatici e processo penale *de societate*

Nel precedente capitolo abbiamo affrontato un importante nodo della nostra indagine: il *locus commissi delicti* in relazione ai reati informatici. Si tratta di un argomento non semplice da affrontare poiché le classiche categorie del diritto penale non possono applicarsi in modo lineare a questo tipo di reati, a causa della loro afisicità e astrattezza. Anche con riguardo alla responsabilità da reato degli enti, si pongono problemi similari. In merito a tale tipo di illeciti, è infatti davvero difficile individuare l'autore e il luogo di consumazione del reato[311]. Come nota Belluta la volatilità delle informazioni che viaggiano attraverso i sistemi informatici e la capacità di *hacker* e *cracker*[312] di occultare la propria presenza rende arduo individuare il *locus commissi delicti* e il giudice competente per territorio[313]. Laddove non sia in altro modo possibile individuare l'autore del reato occorrerà applicare le regole suppletive ex art 9 c.p.p., sino ad arrivare "al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'articolo 335 c.p.p."[314]. Dal canto suo il legislatore ha cercato di rispondere all'aterritorialità dei reati informatici con "una risposta investigativa altrettanto sganciata dal territorio inteso in senso fisico"[315]. Difatti l'art. 11 comma 1 l. 48/2008[316] ha assegnato le funzioni investigative al c.d. procuratore distrettuale per tutti i reati informatici in modo da garantire la

[310] DEL PUNTA R., "La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 151/2015)" in Rivista italiana di diritto del lavoro, n.1/2016, pag. 84.
[311] L. LUPARIA*, Processo penale e tecnologia informatica* in *Diritto dell'Internet*, fasc. 3/2008, pag. 227.
[312] In merito alla differenza tra queste due figure rinvio a I. Salvadori, *L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cracking* in *Rivista italiana di diritto e procedura penale*, 2008, pagg. 1243 ss.
[313] H. BELLUTA, *Responsabilità degli enti e cybercrime*…, cit., pag. 98.
[314] In tal senso H. BELLUTA, *Responsabilità degli enti e cybercrime*…, cit., pag. 98
[315] Ibidem.
[316] Art. 11 l. 48/2008: "All'articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma: «*3*-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 640-*ter* e 640-*quinquies* del codice penale, le funzioni indicate nel comma 1, lettera *a)*, del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente»".

specializzazione di alcuni uffici a discapito del criterio dell'attribuzione distrettuale che garantisce l'unitarietà. Una adeguata competenza e apparecchiatura tecnologica risulta essenziale in questo ambito. Non mancano tuttavia alcune criticità nell'applicazione della normativa. Se venissero costituiti *pool* specializzati in materia di criminalità informatica occorrerebbe riorganizzare le risorse[317]. In secondo luogo, l'allargamento delle attribuzioni distrettuali potrebbe provocare disfunzioni in termini di eccessivo carico di lavoro[318]. Infine, nell'impossibilità di applicare i normali criteri in materia di competenza vista la difficoltà di individuare il *locus commissi delicti*, accadrà spesso che il giudice competente sarà quello distrettuale, ossia il giudice del luogo in cui opera il pubblico ministero che per primo ha iscritto la notizia di reato[319]. Nella legge 48 del 2008 troviamo tuttavia una rilevante lacuna. Invero, il legislatore, alla distrettualizzazione dell'ufficio procura, non ha fatto corrispondere un'analoga previsione che riguardasse l'esercizio delle funzioni di giudice per le indagini e l'udienza preliminari, "creando una dissimmetria foriera di rallentamenti"[320]. Una modifica al codice di procedura panale è intervenuta al fine di garantire una migliore gestione delle fasi preliminari. Ci riferiamo alla legge 24 luglio 2008 n. 125, che in sede di conversione del d.l. 23 maggio 2008 n. 92 ha aggiunto il comma 1-quater all'art. 328 c.p.p. il quale così recita: "Quando si tratta di procedimenti per i delitti indicati nell'articolo 51, comma 3-quinquies, le funzioni di giudice per le indagini preliminari e le funzioni di giudice per l'udienza preliminare sono esercitate, salve specifiche disposizioni di legge, da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente". Queste disposizioni vengono applicate con tutte le loro criticità nel caso di procedimenti a carico di enti in relazione alla commissione di reati informatici. Non possiamo, tuttavia, negare la specialità della materia trattata che richiede un ulteriore sviluppo dell'indagine. L'individuazione del giudice competente nel caso di specie avviene secondo la regola disposta dall'art. 36 d. lgs. 232 del 2001 il quale afferma: "La competenza a conoscere gli illeciti amministrativi dell'ente appartiene al giudice penale competente per i reati dai

[317] L. LUPARIA, *La ratifica della convenzione cybercrime del consiglio d'Europa- I profili processuali* in *Diritto penale e processo*, fasc. n. 6/2008, pag. 723. Critiche vengono mosse anche da S. Lorusso e A.E. Ricci., *Le novità del pacchetto sicurezza- I profili processuali* in *Diritto penale e processo,* fasc. n. 12/2008, pag. 1487

[318] Ibidem

[319] H. BELLUTA, Responsabilità degli enti…, cit., pag. 100.

[320] Ibidem

quali gli stessi dipendono". Questo significa che una volta individuato il giudice competente per il reato presupposto in base alle osservazioni effettuate in questo paragrafo e in quello dedicato nel precedente capitolo, sarà possibile individuare il giudice dell'illecito amministrativo. La *ratio* di tale diposizione è data dall'unitarietà del fatto da cui hanno origine la responsabilità della persona fisica, da un lato, e la responsabilità amministrativa per la persona giuridica nel cui ambito il delitto è stato realizzato. Per tali ragioni, il legislatore ha preferito questa forma di competenza per derivazione al fine di garantire una cognizione tendenzialmente unitaria delle regiudicande. Noi ci occupiamo, però di crimini informatici, intrinsecamente transnazionali. Anche una società italiana può commettere reati informatici all'estero e viceversa. Viene, a tal proposito in rilievo, l'art. 4 del d.lgs. 231 del 2001, il quale afferma al comma 1: " Nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale, gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto". Trattando di una materia in cui i reati vengono prevalentemente commessi all'estero, il legislatore ha cercato di individuare la risposta più efficace alle esigenze transfrontaliere che connotano spesso l'azione criminale informatica, oltre che quella d'impresa. "Infatti, ha sganciato la responsabilità degli enti dalla collocazione territoriale dei reati presupposto, facendo leva sulla diversa condizione in forza della quale si esige soltanto che l'ente abbia la propria sede principale in Italia"[321]. Non è stata, invece, disciplinata l'ipotesi opposta di cui ci occuperemo nel paragrafo successivo.

Per quanto attiene, all'ufficio del pubblico ministero, nel procedimento a carico dell'ente viene individuato in un magistrato appartenente all'ufficio di Procura istituito presso il giudice competente territorialmente. Nel caso dei reati informatici, tuttavia, le funzioni dell'accusa verranno trasferite al Procuratore distrettuale. Sembra di dover concludere che l'auspicata specializzazione delle Procure distrettuali in materia di indagini informatiche dovrebbe finire con il prevalere sull'altrettanto auspicabile competenza specifica a svolgere indagini in materia di responsabilità degli enti[322]. Per poter accertare la responsabilità da reato informatico degli enti, occorre, da un lato, un'adeguata preparazione tecnica e investigativa, dall'altro la capacità di districarsi tra strutture

[321] H. Belluta, *La responsabilità degli enti e computer crimes…*, cit., pag. 102.
[322] H. Belluta, *La responsabilità degli enti e computer crimes…*, cit., pag. 103.

aziendali complesse e modelli organizzativi, di gestione e controllo, il cui preliminare esame, in sede di indagini preliminari, può comunque spettare al pubblico ministero. Questo è uno dei motivi, per cui i procedimenti ex d.lgs. 231 del 2001 sono ancora in numero assai ridotto.

5.1 Le società estere operanti in Italia: il recente approdo giurisprudenziale relativo al disastro di Viareggio

In questa sede occorre approfondire il tema della possibilità che anche le società straniere operanti in Italia possano essere chiamate a rispondere ai sensi del d.lgs. 231/2001 per reati commessi nel nostro territorio, poiché con riferimento alla criminalità informatica è un'ipotesi facilmente prospettabile. Tripodi sottolinea l'importanza di tale questione. Il tema risulta essere "suggestivo perché intercetta, ovvero in esso si riassumono, due *topoi* della modernità giuridica: la globalizzazione dell'economia, riflessa nella transnazionalità dell'attività imprenditoriale; la deantropomorfizzazione del diritto penale, riflessa nel rivoluzionario prodotto legislativo del 2001. Delicato per gli effetti sul piano politico-economico che è in grado di determinare"[323]. Infatti, le società estere potrebbero essere indotte ad operare nel nostro territorio in ragione dei rischi penali collegati alla soluzione della questione. Sul punto è intervenuta una recente sentenza della Suprema corte[324] che ha ribadito la tesi già affermata da Cass. Pen., sez. VI, 11 febbraio 2020, n. 116226[325].

Per comprendere l'iter argomentativo svolto, occorre fare un passo indietro e richiamare le posizioni della dottrina sul punto. Premettiamo che la questione non è di facile trattazione poiché manca una specifica regolazione nel decreto 231. Analizziamo, quindi, i diversi orientamenti rispetto al modo di concepire il rapporto tra reato presupposto della responsabilità amministrativa e l'illecito dell'ente[326] .

---

[323] A.F. TRIPODI, *Il diritto penale degli enti nello spazio: deantropomorfizzazione e globalizzazione a confronto* in archiviopenale.it n.1/2019, pag. 1

[324] Cass., sez. IV penale, sent. 8 gennaio 2021 (dep. 6 settembre 2021), n. 32899 in sistema penale web

[325] Cass. Pen., sez. VI, 11 febbraio 2020, n. 116226 in sistema penale web

[326] Per una ricostruzione generale dei termini del dibattito cfr.: C. PIERGALLINI, *Globalizzazione dell'economia, rischio reato e responsabilità ex crimine delle multinazionali* in Riv. trim. dir. pen. econ. 1-2/2020; G. DI VETTA, *Il giudice border guard nei «grandi spazi»: prospettive critiche intorno alla responsabilità degli enti*, in Giur. Pen., 2021, 1bis, pp. 10ss.; S. MANACORDA, *Limiti spaziali della responsabilità degli enti e criteri di imputazione,* in Rivista italiana di diritto e procedura penale, 1/2012;

La prima tesi considera il reato presupposto e l'illecito amministrativo come fenomeni inscindibili e, pertanto, riconduce il *locus commissi delicti* dell'illecito amministrativo dipendente da reato al medesimo luogo in cui viene posto in essere il reato presupposto da parte dell'autore persona fisica[327].

La seconda considera come non strettamente interdipendenti il reato della persona fisica e l'illecito della persona giuridica. Secondo questa impostazione, il fondamento della responsabilità amministrativa degli enti si radicherebbe nella "colpa d'organizzazione" connessa alla mancata/inadeguata adozione del modello organizzativo. La giurisdizione italiana e, di conseguenza, il regime sanzionatorio previsto dal citato decreto, dipenderebbero allora dal fatto che nel territorio italiano sia radicato il centro decisionale dell'ente (luogo in cui, quindi, si verifica la carenza organizzativa)[328]. In altre parole, per l'applicabilità della normativa italiana, sarebbe necessario che, oltre al reato presupposto, anche la lacuna organizzativa si fosse verificata in Italia[329].

Accanto a tali posizioni, una dottrina minoritaria ha prospettato una posizione intermedia, in base alla quale ai fini dell'applicabilità della legge italiana in materia di responsabilità degli enti esteri si dovrebbe fare riferimento al c.d. interesse economico: secondo questo orientamento, l'ente, per poter rispondere alla luce della nostra normativa, deve essere 'presente' nel territorio italiano e, per far sì che tale requisito sia soddisfatto, basterebbe che il reato-presupposto della responsabilità amministrativa sia stato commesso in Italia nel suo interesse[330].

N. LANDI, Il rispetto del d.lgs. 231/2001 nelle imprese multinazionali operanti in Italia, in Rivista 231, 2, 2019, pp. 82 ss.

[327] In dottrina: C.E. PALIERO, La responsabilità penale della persona giuridica nell'ordinamento italiano: profili sistematici, in «*Societas puniri potest*». La responsabilità da reato degli enti collettivi, a cura di F. PALAZZO, Padova, 2003, p. 17 ss., citato da C. PIERGALLINI, *Globalizzazione dell'economia, rischio reato e responsabilità ex crimine delle multinazionali* in Riv. trim. dir. pen. econ. 1-2/2020. In giurisprudenza: Cass., S.U., 27 marzo 2008 in Riv. it. dir. proc. pen., 2008, p. 1738 ss. Aspre critiche a tale impostazione sono state di recente mosse da T. Padovani, *La disciplina italiana della responsabilità degli enti nello spazio transnazionale*, in Riv. It. Dir. e Proc. Pen., fasc.2, 1° giugno 2021, pp. 409 ss.

[328] S. Manacorda, *Limiti spaziali della responsabilità degli enti e criteri d'imputazione*, cit., pp. 99 ss.

[329] Cfr. E. AMODIO, *Rischio penale d'impresa e responsabilità degli enti nei gruppi multinazionali*, in Rivista italiana di diritto e procedura penale, 2007, p. 1294 ss.; A. ALESSANDRI, *Attività di impresa e responsabilità penali*, in Riv. it. dir. proc. pen., 2005, pag. 559; F. MUCCIARELLI, Il fatto illecito dell'ente e la costituzione di parte civile nel processo ex d.lgs. 231/2001, in Dir. pen. proc., 2011, p. 440 ss.

[330] Tale tesi è sostenuta da: G. RUGGIERO, Brevi note sulla validità della legge punitiva amministrativa nello spazio e sulla efficacia dei modelli di organizzazione nella responsabilità degli enti derivante da reato, in Riv. Trim, di Dir. Pen. Dell'Economia, 3-4, 2004, p. 991. Critico rispetto a tale impostazione: S. MANACORDA, Limiti spaziali della responsabilità degli enti e criteri d'imputazione, cit., p. 99 ss., che

La Cassazione, nel caso in commento, ha dato seguito all'unanime indirizzo giurisprudenziale che fa riferimento al luogo di commissione del reato presupposto. In particolare, la corte fa riferimento all'art. 4 del decreto che disciplina la situazione opposta in cui il reato-presupposto sia stato commesso all'estero nell'interesse o a vantaggio di un ente avente la sede principale in Italia. Secondo la corte "non vi sono ragioni per ritenere che alle persone giuridiche si applichi una disciplina speciale rispetto a quella vigente per le persone fisiche, che permetta loro di non essere assoggettate ai principi di obbligatorietà e di territorialità della legge penale codificati agli artt. 3 (…) e 6, comma primo, cod. pen"[331]. Pertanto, secondo la Cassazione, anche i principi di obbligatorietà e territorialità della legge penale si applicherebbero pacificamente anche alle persone giuridiche e qualora si ritenesse che tali principi non si applicassero agli enti, si realizzerebbe un'ingiustificata disparità di trattamento fra la persona fisica straniera (pacificamente soggetta alla giurisdizione nazionale in caso di reato commesso in Italia) e la persona giuridica straniera (in caso di reato-presupposto commesso in Italia). Anche la previsione dell'art. 36 prova la decisività del luogo di consumazione del reato. Questo si deduce al primo comma, il quale dispone che "la competenza a conoscere gli illeciti amministrativi dell'ente appartiene al giudice penale competente per i reati dai quali gli stessi dipendono"[332]. L'art. 34 del decreto rinvia per intero alle disposizioni del codice di procedura penale in quanto compatibili, e quindi anche all'art. 1 c.p.p. che attribuisce al giudice italiano la giurisdizione su tutte le violazioni commesse in Italia, qualunque sia la nazionalità del suo autore. I giudici fanno riferimento alla precedente sentenza della Cass. che era intervenuta sul tema e nella quale era stato osservato che la responsabilità dell'ente è sì autonoma ma anche "derivata" dal reato, di tal che la giurisdizione va

osserva come tale tesi sia "degna di apprezzamento per lo sforzo di valorizzare il criterio ascrittivo autonomo richiesto dall'art. 5 del decreto legislativo, ma pecca per una eccessiva oggettivizzazione, che non tiene adeguatamente conto di quella componente di colpevolezza tutta normativizzata degli articoli 6 e 7. Ancorando il locus commissi delicti dell'ente a quello della persona fisica c'è il rischio che si reintroducano surrettiziamente nel nostro ordinamento ipotesi di automatismi nella responsabilità che mal si conciliano con lo sforzo profuso dal nostro legislatore per dissociare, autonomizzandolo, il rimprovero mosso all'ente collettivo rispetto alla persona fisica".

[331] Cass. Pen., n. 32899/2021, cit., p. 329.

[332] In dottrina accoglie questa tesi C. PIERGALLINI, *Globalizzazione dell'economia, rischio reato e responsabilità ex crimine delle multinazionali* in Riv. trim. dir. pen. econ. 1-2/2020, pag. 160

apprezzata rispetto al reato-presupposto, a nulla rilevando che la colpa di organizzazione e dunque la predisposizione di modelli non adeguati sia avvenuta all'estero[333].

La corte fa proprie le argomentazioni e le conclusioni alle quali è pervenuta la sentenza Calò, ma ritiene necessario integrare con alcune considerazioni. In primo luogo, la Corte mette in evidenza che l'intenzione del legislatore nell'articolo quattro non era quella di ritrarre la giurisdizione nazionale, bensì di espanderla. Nella relazione governativa al decreto 231 si legge che l'opzione espansionistica è "conforme al progressivo abbandono, nella legislazione internazionale, del principio di territorialità ed alla correlativa, sempre maggiore affermazione del principio di universalità". La volontà del legislatore, quindi, è stata quella di reprimere gli illeciti dell'ente avente sede principale in Italia, anche se il reato presupposto è commesso all'estero. Ciò dimostra che per quel legislatore era pacifica la giurisdizione del giudice nazionale per gli illeciti amministrativi correlati ai reati commessi in Italia. L'*iter* logico seguito dalla corte segue due considerazioni. La prima, di carattere formale, è suggerita dalla qualificazione assegnata dal legislatore alla responsabilità degli enti, esplicitamente indicata come amministrativa. La natura amministrativa può aver indotto a non fare menzione di 'giurisdizione', che tipicamente attiene a rapporti tra autorità giudiziarie, e ad inquadrare il tema della titolarità della cognizione dell'illecito amministrativo dell'ente (così definito anche nello stesso articolo 36) nell'ambito concettuale della competenza. Incidentalmente può essere osservato anche che solo per il reato commesso all'estero si può ipotizzare una possibile questione di giurisdizione, ricorrente allorquando la relativa cognizione risulta assegnata ad organo giurisdizionale estero. Ma la considerazione certamente decisiva è di carattere sostanziale. Essa ha ad oggetto il ruolo del reato presupposto nella fattispecie dell'illecito dell'ente e il luogo di commissione di quest'ultimo.

[333] Cass. Pen., sez. VI, 11 febbraio 2020, n. 116226 in sistema penale web. Anche in dottrina si rileva che: "l'idea di radicare la giurisdizione laddove si è consumata la colpa di organizzazione muova da una completa volatilizzazione del disvalore di evento nella struttura dell'illecito dell'ente, vuoi ricostruito in un'ottica concorsuale, vuoi in una dimensione monosoggettiva. Una simile impostazione non riesce, però, ad offuscare il fatto che l'art. 6 c.p. richiama genericamente l'evento nella sua dimensione naturalistica, causalmente correlato all'azione o all'omissione, a prescindere, dunque, dalla qualificazione del suo ruolo nell'ambito della fattispecie oggettiva. Ne deriva, pertanto, che l'evento, sia che venga considerato come elemento costitutivo del 'tipo', sia che degradi a mera condizione obbiettiva di punibilità, non può che fungere da elemento di connessione territoriale, ai sensi dell'art. 6 c.p." citazione tratta da: C. PIERGALLINI, *Globalizzazione dell'economia, rischio reato e responsabilità ex crimine delle multinazionali* in Riv. trim. dir. pen. econ. 1-2/2020, pag. 162

La corte sottolinea che l'ente risponde per un fatto proprio in forza di un rapporto di immedesimazione organica che lega la persona fisica autrice del reato con la *societas*, che la colpa d'organizzazione assume una funzione non dissimile da quella assunta dalla colpa nel reato (che è elemento costitutivo del fatto tipico, e nucleo della colpevolezza) e che "il luogo di consumazione dell'illecito dell'ente è quello in cui si consuma il reato presupposto*"*[334]. "Non vi è stata necessità di prevedere disposizioni che regolassero esplicitamente il tema della giurisdizione sull'illecito dell'ente perché esso è risolto dal nesso di dipendenza con il reato presupposto, sicché il potere di conoscerne è in capo al giudice nazionale se e in quanto egli ha giurisdizione su quest'ultimo"[335]. Sono numerose le disposizioni del decreto 231 che attestano l'assoluta centralità accordata dal legislatore al reato presupposto, a partire dalla configurazione della responsabilità dell'ente come 'dipendente' da reato. Proprio il rapporto di dipendenza ha indotto il legislatore a stabilire che l'autorità titolare del potere di cognizione sul reato; quindi, il giudice avente giurisdizione sul medesimo ed inoltre competente, abbia il potere di cognizione anche sul dipendente illecito amministrativo. La Corte ha, infine sottolineato che, qualora il legislatore avesse scelto di radicare la giurisdizione per l'illecito dell'ente nel luogo di commissione della condotta (ovvero nel luogo della mancata adozione del modello organizzativo, che coincide con il centro gestionale e decisionale dell'ente), non sarebbe stata necessaria l'introduzione dell'art. 4 del Decreto 231, che ha per presupposta l'integrazione in Italia della colpa d'organizzazione, di talché la giurisdizione del giudice italiano per il reato commesso all'estero ne sarebbe stata una fisiologica conseguenza.

6. Davvero gli enti non hanno mai commesso reati informatici?

L'introduzione dei reati informatici nel d.lgs. 231/2001 non ha trovato pieno accoglimento tra gli studiosi. Le maggiori perplessità sono legate al fatto che sia più probabile che l'ente sia vittima del reato informatico piuttosto che autore e lo dimostra l'assenza di giurisprudenza. La critica mossa, dunque, è che l'attuale previsione legislativa sia rivolta a tutelare situazioni del tutto marginali[336]. La stessa dottrina dubita della

[334] Cass. Pen., n. 32899/2021, cit., p. 335
[335] Cass. Pen., n. 32899/2021, cit., p. 335
[336] G. CORRIAS LUCENTE, *Commento sub Art. 7 alla legge 48/2008* in *Cybercrime, Responsabilità degli enti e prova digitale* a cura di CORASANITI G. e CORRIAS LUCENTE G., Cedam, Padova, 2009, pag.190 ss.

possibilità concreta di adottare modelli adeguati relativi ai reati informatici (considerati troppo specifici e potenzialmente commissibili da chiunque) non essendo possibile isolare un'area o funzione dell'ente di rischio reato intrinseco o prevalente come avviene per gli altri reati[337]. "Per rispettare a fondo gli obblighi derivanti dall'art. 24 bis d.lgs. 231/2001 sarebbe necessario adottare misure e controlli particolarmente impegnativi e tali, comunque, da non garantire la prevenzione in senso globale, per la peculiarità della materia che, a mio parere, doveva rimanere estranea alle disposizioni del decreto n. 231, ovvero, essere limitata ad una serie di reati informatici che statisticamente risultino commessi con frequenza dall'ente nel proprio interesse"[338]. A queste critiche altra parte della dottrina, nonché molta parte dei professionisti di settore, replica che l'introduzione dell'articolo 24 bis all'interno del d.lgs. 231/2001, al contrario è una scelta saggia, da vedersi in un'ottica preventiva, in un presente (ed un futuro) in cui lo sviluppo delle tecnologie è destinato ad aumentare esponenzialmente. Un autorevole autore afferma come il fondamento politico criminale dell'art. 24 bis risieda nella persona giuridica come "referente criminologico" privilegiato in materia di reati informatici, dato che "tali delitti il più delle volte sono commessi nell'ambito delle attività di persone giuridiche o enti, le cui (spesso ingenti) risorse economiche o materiali vengono frequentemente strumentalizzate a fini illeciti"[339]. In una società caratterizzata da unità produttive e commerciali altamente informatizzate, l'uso improprio o l'abuso da parte dei dirigenti e dipendenti degli strumenti informatici loro affidati per l'esercizio delle specifiche funzioni all'interno dell'azienda, rappresenta uno dei più elevati fattori di rischio con riferimento al problema della sicurezza aziendale. Soprattutto in quelle realtà aziendali che sfruttano la tecnologia per orientarsi verso l'automazione ed ottimizzazione dei processi, sono tutt'altro che trascurabili le possibilità che i reati informatici possano essere commessi anche da soggetti apicali[340]. Se da un lato la mancanza di giurisprudenza potrebbe fare propendere per la prima tesi, dall'altro lato il legislatore ha probabilmente deciso di estendere la responsabilità a questi tipi di reati in modo da sollecitare l'ente ad

[337] Ibidem
[338] Ibidem
[339] F. RESTA, Cybercrime e cooperazione internazionale nell'ultima legge della legislatura, in Giur. Merito 2008 p. 2157
[340] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 40

aumentare la sicurezza informatica all'interno della propria struttura e così tutelare interessi penalmente rilevanti, anche alla luce delle pressioni sovranazionali. Risulta fondamentale, inoltre, prevenire questo tipo di reati in quanto il reato informatico è trasversale e propedeutico alla commissione di altri reati classici: si pensi all'aggiotaggio o all'abuso di informazioni privilegiate commessi grazie a reati informatici anteriori e concatenati a questi, come l'intercettazione o l'accesso abusivo a sistema. Secondo questa impostazione di pensiero, la *compliance* 231 andrebbe vista come un'opportunità di riorganizzazione interna aziendale ed accolta come una sfida positiva, non come un onere. Inoltre, si è abituati a vivere il crimine informatico come una minaccia esterna, occorrerebbe, invece, rendersi conto che attualmente anche un "colletto bianco" può commetterlo. I reati informatici presupposto per l'applicazione delle sanzioni del d.lgs. 231/2001 potrebbero essere compiuti dagli stessi addetti alla funzione IT[341], abusando, in modo illecito, dei propri diritti di accesso a sistemi informatici interni alla struttura operativa economica[342]. Per questi motivi, tali reati appaiono, forse, come i più trasversali tra i cd. "*white collar crimes*".

Tracciato questo quadro, è lecito domandarsi il motivo della difficoltà di reperire pronunce giurisprudenziali. Infatti, anche nei codici specifici, ci si limita ad indicare l'articolo senza fare riferimento alla giurisprudenza in materia e le ricerche tra le varie banche dati non producono alcun risultato. In realtà le motivazioni dietro questa assenza sono complesse e legate alla volontà stessa delle aziende, nonché ad un "*corporate ethos*" (non solo italiano) che calpesta sistematicamente l'etica informatica. Da sempre le aziende nel nostro Paese hanno colpevolmente sottovalutato e preso in scarsa considerazione i reati informatici a dispetto di tutti gli atti nazionali e sovranazionali da noi analizzati. Scarse sono state, infatti, le risorse utilizzate per predisporre soluzioni idonee ed efficaci che impedissero la commissione di questi reati. Spesso gli enti collettivi, si sono dimostrati addirittura restii ad adottare le misure minime di sicurezza introdotte obbligatoriamente dal Documento programmatico sulla sicurezza, con cui il modello

[341] Nel caso in cui reato informatico è compiuto da un amministratore di sistema il fatto costituisce aggravante ed in molti casi può essere perseguito d'ufficio.
[342] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 40

organizzativo in materiale informatico si deve integrare ed uniformare[343]. Le aziende, non avendo nessuna consapevolezza di che cosa potrebbe accadere dal punto di vista della responsabilità "amministrativa" dell'ente in caso di carenza o peggio totale mancanza di un modello organizzativo sul punto, sono attualmente decisamente poco propense a effettuare investimenti nell'ambito della sicurezza informatica e della prevenzione dei reati di cui si è detto[344]. Si aggiunga anche che la società vittima dell'attacco, di solito, non denuncia, convinta che la sua notizia *criminis* non dia inizio ad alcun processo, portando quasi sicuramente ad una archiviazione. Come in molti casi di criminalità informatica senza volto, dove l'autore materiale della condotta non viene identificato. Inoltre, la società bersaglio non denuncia alle autorità competenti l'eventuale crimine subito, in quanto tale denuncia equivarrebbe ad ammettere pubblicamente la debolezza e la violabilità dei propri sistemi, con il rischio del ritorno di una pubblicità negativa, le cui conseguenze possono anche superare (soprattutto in termini economici e di immagine) il danno sofferto[345]. Altre ragioni sono da individuare nella scarsa attivazione delle procure in relazione agli illeciti ex d.lgs. n. 231/2001 e dal frequente ricorso ai procedimenti speciali, anche se la materia dei provvedimenti cautelari ha consentito ampio spazio di intervento giudiziario[346]. A questo proposito, è interessante guardare all'approccio contrario delle *corporation* americane, che lungi dal cercare di stare lontano dai riflettori, sperando che reati informatici capitino a qualcun altro, fanno della propria sicurezza un vanto, reagendo in modo proattivo a situazioni di crisi, rafforzando in questo modo la propria posizione sul mercato e con gli investitori. Alla luce di queste considerazioni appare maggiormente evidente, ora, l'illogicità del sillogismo comune: nessuna giurisprudenza, uguale inesistenza del reato.

---

[343] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag. 40

[344] G. DEZZANI, L. PICCINNI, *La società "connessa": problematiche legate alla sicurezza aziendale ed alle necessità di prevenzione dei reati presupposti*, in La responsabilità amministrativa delle società e degli enti, n. 1, 2001, pp. 117 ss.

[345] G. DEZZANI, L. PICCINNI*, Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2, 2011, pag.40

[346] D. FONDAROLI, *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001* in *Cybercrime* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M*., Utet giuridica, Milano, 2019, pag. 203

A titolo esemplificativo e in assenza di giurisprudenza, si possono comunque ipotizzare alcune casistiche di applicazione pratica dell'art. 24 bis d.lgs. 231/2001[347]. Con riferimento all'accesso abusivo a un sistema informatico (art. 615-ter c.p..) delineiamo le seguenti ipotesi.

Un dipendente della società X o un suo appaltatore (concorso della società), con il benestare di *Cybersecurity* e dei vertici aziendali accede abusivamente ai sistemi informatici dei concorrenti. In particolare, questa condotta potrebbe essere attuata da un nuovo dipendente, proveniente da una società concorrente, che acceda ancora al sistema di questa con le proprie credenziali. L'interesse della società potrebbe essere uno dei seguenti: (i) acquisire a scopo di spionaggio industriale informazioni a carattere commerciale e/o industriale, costi di produzione, *mailing list* clienti, liste di fornitori, utili a elaborare strategie di *marketing* o altro (es. *recruiting* o *benchmarking)* e/o la documentazione relativa ai loro prodotti/progetti; (ii) distruggere informazioni, impedirne la trasmissione alla PA per conseguire un vantaggio competitivo.

Un altro caso potrebbe essere quello di un dipendente della società X (es. appartenente alla funzione *Customer Operation Services*) che con il benestare di *Cybersecurity* e dei vertici aziendali accede abusivamente alle quantità di sicurezza e all'anagrafica cliente nell'ambito della monetica (acquisisce *password*, codici delle carte di pagamento, informazione relative ai pagamenti (e al tipo di pagamenti) effettuati dal titolare della carta e le diffonde a terzi. L'interesse della società potrebbe essere quello di utilizzare i dati dei titolari come utilità corruttive di soggetti strategici per la società o come strumenti di intimidazione nei confronti di concorrenti di soggetti che possono far avere un vantaggio alla società.

Ancora, nell'ambito della monetica, la società X, accordandosi con la società controllata produttrice di carte e con un *merchant* compiacente favorisce la clonazione di carte, fornendo il relativo flusso informatico alla controllata produttrice di carte e divide con il merchant l'incasso realizzato con la carta clonata (il *merchant* compiacente provvede al

[347] Faremo ora riferimento ad una serie di esempi tratti da: SANTORIELLO C., *I reati informatici e la responsabilità delle società ex d.lgs. 231/2001* in La responsabilità amministrativa delle società e degli enti, fasc. 1, vol. 15, 2020

prelievo immediato e poi cessa l'attività). L' interesse della società è quello della creazione di fondo nero/provvista.

Con riferimento al reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 *quinquies* c.p.), possiamo fare le seguenti ipotesi. Un dipendente della società X (anche dall'esterno) o un appaltatore all'uopo incaricato (concorso della società X) diffonde, all'interno del sistema informatico appartenente all'azienda concorrente, un *software* malevolo (ad es. un *virus*, un *trojan virus*, un worm, una *logic bomb*, uno *spyware*, un *keylog* o un *software* di monitoraggio remoto) mediante un supporto rimovibile o tramite posta elettronica, che possa danneggiarlo; causa un *denial of service* ad un *competitor* (per esempio attraverso lo *spamming* cagionando la saturazione intenzionale delle risorse informatiche a seguito di un elevato numero di comunicazioni, così da provocare l'interruzione del servizio di comunicazione e altre eventuali disfunzioni ovvero attraverso il *netstrike* (che si realizza attraverso contemporanei e ripetuti accessi da parte di una moltitudine di utenti presso uno stesso sito *web* fino ad occuparlo e a renderlo inefficiente). L'interesse della società X potrebbe essere quello di danneggiare la concorrenza.

Altro caso: Un dipendente della società X (anche dall'esterno) o un appaltatore all'uopo incaricato (concorso della società X) diffonde nei sistemi della stessa società X un virus idoneo a danneggiare il funzionamento o ad interrompere il funzionamento del sistema informatico aziendale. L'interesse della società X è distruggere documenti «sensibili» in relazione ad un procedimento penale a carico della società X.

Altra ipotesi: Un dipendente della società X (anche dall'esterno) o un appaltatore all'uopo incaricato (quindi con il concorso della società X) diffonde nei sistemi della stessa società X un virus idoneo a criptare i dati trattati in chiaro dal *Customer Operation Services* pretendendone il riscatto. L'interesse della società X è il seguente: la società X paga il riscatto con un bonifico a sé stessa in un paese *off-shore* e si costituisce un fondo nero per generare una provvista.

Un ultimo caso. La società X simula una richiesta di *change* da parte di un cliente al fine di rispondere alla richiesta di un soggetto strategico per la stessa società X. Es. modificare i parametri dati alla società X dalla banca per la rilevazione delle operazioni sospette ai

fini antiriciclaggio. Interesse della società X: favorire un soggetto strategico per la società X.

Analizzata questa casistica, ci soffermiamo su un caso di cronaca recente, di cui non possediamo ancora le sentenze dei giudici, che riguarda proprio l'oggetto della nostra indagine. Facciamo riferimento al caso "Leonardo", una tra le aziende più note al mondo in ambito di prodotti per la difesa e per la *cybersecurity*. In particolare, era stato inserito in una serie di *pc*, un *malware* sufficientemente sofisticato da non essere riconosciuto dai sistemi *antivirus* aziendali, che consentiva di intercettare tutto quello che veniva digitato sulle tastiere dei *computer* infetti mediante la tecnica dello *screen capturing*. Il materiale veniva poi diretto ad una pagina *web* ora sequestrata. Nel corso dell'indagine condotta dal CNAIPIC e dal Compartimento della Polizia di Napoli un ex dipendente e un dirigente Responsabile del Cert (*Cyber Emergency Response Team*) della società Leonardo S.p.A., organismo deputato alla gestione degli attacchi informatici, sono stati sottoposti a misure restrittive. Allo stato, i capi di imputazione risultano essere relativi ai delitti di accesso abusivo a sistema informatico, intercettazione illecita di comunicazioni telematiche e trattamento illecito di dati personali per il primo e di depistaggio per il secondo. Tuttavia, ci possiamo chiedere se possa configurarsi un'ipotesi di responsabilità da reato degli enti a carico della stessa azienda. Sicuramente i reati ex artt. 615 ter c.p. e 617 quater c.p. rientrano tra i reati presupposto individuati all'art 25 bis d.lgs. 231. Sussiste anche il rapporto qualificato tra l'azienda e l'autore del reato richiesto dal decreto. I giudici dovranno, invece, interrogarsi sul requisito dell'interesse o vantaggio. Inoltre, bisognerà valutare l'eventuale possibilità per la società di esimersi da responsabilità, qualora sussistano le condizioni di cui agli artt. 6 e 7 d.lgs. 231/2001.

Conclusioni e prospettive future

1. Facciamo il punto della situazione

L'obiettivo che ci siamo posti all'inizio di questo lavoro era quello di intersecare le tematiche legate ai reati informatici posti a tutela dei beni giuridici di nuovo conio, la riservatezza informatica e sicurezza informatica, con la disciplina della responsabilità da reato degli enti. I motivi che ci hanno spinto a scegliere questo tema li abbiamo scandagliati nell'introduzione al lavoro di tesi, adesso cerchiamo di mettere insieme i pezzi e di tirare le fila del discorso. Farlo non è semplice, per ogni punto fermo, abbiamo trovato una questione aperta e nonostante le numerose riforme e gli innegabili sforzi del legislatore nazionale e sovranazionale ma anche della giurisprudenza e della dottrina, percepiamo di essere solo all'inizio di questo percorso in cui il diritto incontra i problemi di una società sempre più connessa.

Guardare tali problematiche da una visione sovranazionale ha conferito un contributo prezioso al nostro lavoro. Le sentenze della Corte europea dei diritti dell'uomo e della Corte di giustizia, ci hanno consentito di definire il contesto della tematica da noi affrontata. Abbiamo seguito l'evolversi del diritto alla riservatezza sino alla sua declinazione nel diritto alla protezione dei dati personali e con le sentenze da noi analizzate sono stati affrontati i problemi sorti all'interno dei singoli Stati e che hanno sollevato questioni di compatibilità con il diritto dell'Unione. Ad accomunare tali vicende, diverse tra loro, il contrasto tra gli individui che demandavano maggiori garanzie per la *privacy* e le esigenze di sicurezza degli Stati. In questi anni milioni e milioni di dati sono stati accumulati soprattutto grazie ai servizi di comunicazione telefonica, tanto da far pensare ad una vera società sorvegliata. In tale contesto, i giudici hanno sottolineato l'importanza di mettere in equilibrio gli interessi in gioco. Il rapporto tra sicurezza e *privacy* non deve essere visto come un'inconciliabile opposizione. Esse costituiscono, piuttosto, "due facce della stessa medaglia, ovverosia quella della protezione dei diritti essenziali dell'individuo nel più ampio quadro dei bisogni di tutela di una società globale interessata da gravi minacce alla sua stessa esistenza: minacce che impongono, quindi, di

riconsiderare ragionevolmente i confini e i contenuti delle stesse libertà del singolo e delle esigenze di protezione della sicurezza collettiva"[1]. In conclusione, possiamo dire che l'espressione "*privacy* vs. sicurezza" sia in realtà molto meno idonea a descrivere la realtà di quanto non possa farlo piuttosto l'affermazione contraria e cioè che "*privacy* è sicurezza".

Una volta chiarito questo intricato rapporto, l'analisi degli atti sovranazionali ci ha permesso di fare luce sugli strumenti approntati dall'Unione nella lotta al *Cybercrime*. La convezione di Budapest, la decisione 2005/22/GAI e infine la direttiva 2013/40/UE, hanno avuto un importante ruolo propulsore e hanno rappresentato un importante punto di riferimento per i legislatori nazionali. Quello che si evince dall'analisi di questi atti è la necessità di cooperazione tra gli Stati. L'impiego della tecnologia sfuma i confini tra le nazioni e in tale contesto una normativa quanto più omogenea tra gli Stati appare essenziale per contrastare in maniera concreta la criminalità informatica e risolvere i conflitti di giurisdizione. Fondamentali sono le definizioni che abbiamo ritrovato in questi atti e che grazie alla loro ampiezza consentono di essere impiegate da legislatori diversi. Inoltre, non si manca di fare riferimento all'introduzione di una responsabilità da reato degli enti. Allargare la responsabilità da reato degli enti, includendo anche i reati informatici appare necessario in una società sempre più digitalizzata. Proprio nell'impresa può nascere l'occasione di commettere tali reati, sebbene siano tanti i dubbi che sorgono dall'estensione di questo catalogo.

Infine, all'interno di questo capitolo, ci siamo occupati di quegli atti volti a costruire un'Unione europea più resiliente dal punto di vista della sicurezza informatica. I destinatari di tali atti sono i fornitori di operatori di servizi essenziali e fornitori di servizi digitali, che ora sono sottoposti a veri obblighi e sanzioni. In questo contesto assumono un ruolo sempre più incisivo i CSIRT e l'ENISA. Anche in questo ambito, inoltre, è stata sottolineata l'importanza di una cooperazione tra gli Stati. In verità, abbiamo constatato che un simile obiettivo non può dirsi raggiunto. Le perplessità sorte intorno alla direttiva Nis hanno portato alla proposta di una direttiva Nis 2.0, che ha puntato sugli obblighi in capo agli operatori di servizi essenziali, ampliandone l'elenco e ha rafforzato il ruolo

[1] M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza*, in medialaws.eu, 2018.

dell'ENISA. Con riguardo a tale ultimo atto dovremo attendere la sua attuazione per poter verificare le conseguenze. Certo è che tali discipline non possono non intersecarsi con la responsabilità da reato degli enti di cui ci occuperemo nel corso del terzo del capitolo. Sebbene tali atti non siano volti alla prevenzione dei reati presupposto inseriti nel decreto 231 del 2001, possibili sono le ricadute sui Modelli di Organizzazione che le imprese andranno a costruire. Le conseguenze verranno da noi analizzate nel corso del capitolo 3, in questa sede abbiamo avuto l'occasione di notare che tali atti potrebbero fornire degli importanti parametri per la costruzione dei MOG e prevenzione dei reati informatici. Inoltre, in vista di obblighi sempre più incisivi e sanzioni più severe le imprese saranno invogliate a investire nella costruzione di modelli che siano in grado di contrastare efficacemente i reati informatici.

Nel corso del secondo capitolo, siamo passati al piano nazionale e abbiamo prestato attenzione agli strumenti penalistici posti a tutela della riservatezza. Di particolare interesse la trattazione in merito ai nuovi beni giuridici della riservatezza e sicurezza informatica. In particolare, il primo fa riferimento "al nuovo interesse all'esclusività (o possibilità autonoma di controllo e limitazione) dell'accesso, utilizzo, trattamento di dati e sistemi informatici in quanto tali, che si giustifica per la (ben maggiore) utilità così garantita al titolare, di fronte all'altrimenti "strutturale" accessibilità, facilità di circolazione ed ampiezza di diffusione- proprio attraverso le connessioni e procedure automatizzate- dei dati e delle informazioni, spesso (ma non necessariamente) di rilevante valore economico e patrimoniale, ovvero personale, politico, ideologico, militare, ecc…"[2]. La protezione della riservatezza informatica, tuttavia, dipende anche dal raggiungimento di un elevato livello di sicurezza dei mezzi e dei sistemi informatici. Riservatezza e sicurezza informatica finiscono, così, per intersecarsi e sovrapporsi.

Avevamo anticipato nell'introduzione di questo lavoro, che un ruolo da protagonista in questo capitolo avrebbe avuto la fattispecie dell'accesso abusivo a un sistema informatico. La questione che ci siamo posti riguarda la configurabilità o meno del delitto previsto dall'art. 615- ter c.p., nel caso in cui il soggetto agente sia formalmente abilitato ad accedere ad un sistema informatico o telematico, ma vi si introduca o si mantenga al

[2] L. PICOTTI., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati* in *Il diritto penale dell'informatica nell'epoca di Internet* a cura di PICOTTI L., Padova, CEDAM, 2004, pag. 78

suo interno per uno scopo diverso da quello consentito. Con una prima sentenza la Cassazione a sez. unite ha provato a dirimere i contrasti, appoggiando l'orientamento secondo cui anche un *insider* può essere condannato per tale reato nel caso in cui abbia ecceduto le prescrizioni impartite dal titolare e, pertanto, violando lo *ius excludendi alios* del titolare del sistema[3]. Nonostante tale primo intervento, è continuato il contrasto in seno alla giurisprudenza. Successivamente la Cassazione a sez. unite è intervenuta nel caso specifico di un pubblico ufficiale affermando che l'accesso ad un sistema informatico per ragioni estranee a quelle di ufficio si traduce per il pubblico ufficiale in una condotta abusiva, ponendosi in un rapporto di "*ontologica incompatibilità*" con la funzione svolta[4]. In verità, anche tale sentenza è stata oggetto di critiche anche per l'eventualità dell'applicazione retroattiva di un *overruling* sfavorevole. Tuttavia, la giurisprudenza successiva ha escluso tale ipotesi. Peraltro, una recente riforma dell'associazione professori di diritto penale ha proposto di riformulare l'art. 615- ter c.p., al fine di risolvere la questione della rilevanza penale delle condotte dei c.d. *insider.* Secondo tale riforma il riferimento all' accesso in assenza di autorizzazione dovrebbe essere preferito rispetto all'attuale introduzione in violazione delle misure di sicurezza poste a protezione del sistema. Tali condotte verrebbero punite poiché tali soggetti spingendosi oltre i limiti dell'autorizzazione, accedono di fatto "senza autorizzazione" a parti o spazi riservati che sarebbero loro preclusi dal titolare o dall'ambito delle loro competenze. Il carattere abusivo o, meglio, "non autorizzato dell'intrusione" in un sistema informatico da parte dell'*insider*, verrebbe stabilito sulla base della violazione di specifici regolamenti interni, norme o disposizioni aziendali anche di natura contrattuale o comunque norme extra-penali. La mancanza di autorizzazione costituirebbe una clausola di illiceità speciale che contribuisce alla tipizzazione oggettiva del fatto di reato. In questo modo si eviterebbero gli errori emersi da alcuni giudici che hanno dato rilevanza alle finalità personali o soggettive dell'*insider*. Inoltre, verrebbe eliminato il riferimento al "mantenimento" nel sistema informatico, viste le difficoltà interpretative ed ermeneutiche a cui ha dato luogo.

Di particolare interesse la questione relativa al *locus commissi delicti* nel *cyberspace.* Una peculiarità dei reati informatici è che consentono la deterritorializzazione dell'utente, il

[3] Cass. Sez. un., 7 febbraio 2012 n. 4694, consultabile sul sito www.dirittopenalecontemporaneo.it
[4] Cass., sez. unite, sent. 18 maggio 2017 n. 41210, in diritto penale contemporaneo, fasc. 10/2017

quale può trovarsi a molta distanza dal luogo in cui si estrinseca l'accadimento materiale o in più luoghi contemporaneamente[5]. Altra caratteristica è la detemporalizzazione delle attività che possono essere pianificate e svolte senza un collegamento tra l'agente e il sistema informatico[6]. Date tali caratteristiche, ci siamo chiesti nell'introduzione di questo lavoro in che modo potesse essere individuato il luogo di commissione del reato. In primo luogo, abbiamo riportato alla mente i principi in materia, fissati nel nostro ordinamento, grazie alle norme del Codice penale e di procedura penale. In seguito, abbiamo fatto riferimento agli atti sovranazionali, quali la Convenzione di Budapest e la direttiva 2013/40/UE, che si occupano anche del tema della giurisdizione e costituiscono un importante tentativo di armonizzazione. L'indagine, esposti i vari orientamenti e superate le teorie più estreme, che da un lato vedono in *Internet* una realtà priva di ogni forma di localizzazione, dall'altro negano la particolarità dei reati commessi *online* dal punto di vista spaziale, si concentra sull'individuazione del *locus commissi delicti* nel reato di accesso abusivo ad un sistema informatico, poiché intorno a questo caso si è divisa la giurisprudenza tra coloro i quali ritengono che il *locus commissi delicti* coincide con il luogo nel quale si trova il soggetto che si introduce nel sistema[7], e coloro i quali fanno riferimento al luogo in cui è fisicamente collocata la banca dati oggetto dell'intrusione[8]. La Cass. a sezioni unite, nel 2015, risolve il contrasto giurisprudenziale nel senso che il *locus commissi delicti* coincide con il luogo in cui si trova il soggetto che si introduce nel sistema informatico, suscitando, tuttavia, aspre critiche. Abbiamo, da ultimo, delineato, la proposta di autorevole dottrina, secondo cui, la competenza dovrebbe essere riconosciuta al giudice del luogo in cui la vittima possiede il proprio centro di interessi (domicilio, sede dell'azienda ecc., a seconda dello "spazio informatico" violato, ossia "privato", "aziendale" ecc.), in quanto riconducibile a quell'area virtuale di espressione della sua intera personalità umana. Nel corso del lavoro, abbiamo evidenziato i vantaggi di tale teoria, che si adatta alla complessità della fattispecie analizzata, al principio di territorialità ed infine sembra trovare sostegno nelle fonti europee (cfr. art.12 direttiva

[5] R. FLOR, "*La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*" in *Cybercrime* a cura di Cadoppi A, Canestrari S., Manna A., Papa M., Utet giuridica, Milano, 2019, pag. 141.
[6] Ibidem
[7] Sent. Cass., sez. un., 26 marzo 2015, n. 17325 reperibile sul sito eius.it
[8] Cass. Sez. 1, n. 40303 del 27/05/2013 in banca dati De Jure; Cass., sez. 3, n. 23798 del 24/05/2012 in banca dati De Jure

2013/40/UE e art. 22 Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001).

Infine, nel terzo capitolo, ci siamo occupati di Responsabilità da reato degli enti e abbiamo provato a intersecare tale tematica con le problematiche relative ai reati informatici trattati nel capitolo 2. Abbiamo delineato, grazie agli studi degli esperti del settore, quali potrebbero essere gli scenari futuri che vedano gli enti protagonisti di contenziosi che abbiano ad oggetti i reati informatici. In verità, tali previsioni potrebbero presto concretizzarsi. Infatti, in una società caratterizzata da unità produttive e commerciali altamente informatizzate, l'uso improprio o l'abuso da parte dei dirigenti e dipendenti degli strumenti informatici loro affidati per l'esercizio delle specifiche funzioni all'interno dell'azienda, rappresenta uno dei più elevati fattori di rischio con riferimento al problema della sicurezza aziendale. Recente è il caso del *cyber* attacco subito dalla Leonardo S.P.A che potrebbe rappresentare il primo caso italiano di responsabilità da reato degli enti per reati informatici ad essere sottoposto al vaglio dei giudici.

In tale contesto è stata affrontata la questione relativa alla responsabilità da reato degli enti in relazione ai reati informatici. Partendo dalla disciplina prevista dal decreto legislativo 231 del 2001, carica di tutte le sue zone d'ombre come quella relativa all'obbligatorietà o meno del modello, o alla responsabilità dell'OdV, abbiamo cercato di analizzare le ricadute che le tecnologie di ultima generazione potranno avere sull'accertamento della colpa organizzativa. Centrale nel nostro lavoro la costruzione di un Modello di organizzazione e gestione che possa consentire alle imprese di prevenire i reati informatici e riuscire a superare positivamente la valutazione giudiziale. Abbiamo dedicato particolare attenzione a questa parte del lavoro poiché un MOG idoneo ed efficace potrebbe consentire all'ente di andare esente da responsabilità. La sua costruzione nell'ambito della prevenzione dei reati informatici non può che risentire dell'influenza di quegli atti sovranazionali di cui ci siamo occupati nel primo capitolo. Ci riferiamo alla direttiva NIS, al *Cybersecurity Act* e alla proposta di direttiva NIS 2.0. Sebbene tali documenti facciano riferimento ad obblighi volti a prevenire, in via più generale gli incidenti informatici, ci fanno percepire l'importanza che sta via via assumendo il valore della sicurezza informatica anche nel giudizio da parte delle autorità dell'attività svolta dall'ente. Il mancato rispetto di tali normative, pertanto, nel caso in cui

si realizzassero i presupposti della responsabilità da reato degli enti, potrebbero essere percepiti dal giudice come indifferenza nei confronti della normativa prevista dal decreto 231. Inoltre, date le peculiarità dei reati informatici abbiamo preso in considerazione l'ipotesi in cui un ente estero commetta un reato informatica in Italia. Sono stati presi in considerazione, sia i problemi di giurisdizione che si è tentato di risolvere grazie ad un recente intervento giurisprudenziale che ha riguardato il disastro di Viareggio, tanto i problemi relativi alla mancata adozione da parte della società estera del modello di organizzazione e gestione così come previsto dalla normativa italiana. Con riferimento a tale ultima questione, mentre la giurisprudenza prevalente ritiene che operare in Italia comporti l'adeguamento alle relative leggi[9], autorevole dottrina afferma che non si possa pretendere dall'ente straniero il Modello così come previsto dal nostro ordinamento[10]. Sarebbe sufficiente, in base a tale teoria supportata anche da Confindustria, un modello equivalente. Anche la soluzione dei problemi strettamente legati alla giurisdizione non è semplice. Delineati i vari orientamenti abbiamo descritto l'ultimo intervento della Cassazione a sez. unite., che conferma la tesi prevalente secondo cui occorre fare riferimento al luogo di commissione del reato presupposto, e non già in quello in cui si radica la "colpa di organizzazione". Le complesse questioni ci hanno spinto a ritenere necessaria ancora una maggiore cooperazione tra gli Stati con l'obiettivo di armonizzare la disciplina dei *compliance program* a livello europeo e sovranazionale. Questo consentirebbe di rispondere alle problematiche legate alla commissione dei reati informatici nell'ambito degli enti e alla crescente globalizzazione del mercato.

Queste, in sintesi, le principali questioni affrontate nel corso di questo lavoro. Ma nell'analizzare tali tematiche non possiamo non concludere con uno sguardo ad un futuro che non è più così lontano e su cui occorre interrogarci. Così come il *computer* e *internet* hanno apportato una vera rivoluzione nella società e i giuristi hanno dovuto interrogarsi su cosa il diritto potesse fare per fronteggiare i nuovi rischi, oggi l'impiego dell'Intelligenza artificiale e dei Big Data dona nuova linfa al dibattito. Cerchiamo, in

[9] Trib. Lucca, 31 luglio 2017, n. 222 in giurisprudenzapenale.com; Tribunale di Milano, 27/04/2004, (ord.) GIP Salvini – Imp. Siemens A.G

[10] E. STAMPACCHIA, *La responsabilità amministrativa degli enti con sede all'estero* in archiviodpc.dirittopenaleuomo.org, 4 ottobre 2013; A. SCARCELLA, *La c.d. "internazionalizzazione" della responsabilità da reato degli enti* in La resp. amm. delle soc. e degli enti, n.1/2014; . C. PIERGALLINI, *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021.

conclusione di questo lavoro, di analizzare quali problematiche aprono l'impiego di tali strumenti per la *privacy* degli individui e quale ruolo possono avere all'interno del settore penalistico. Mi rendo conto che più e più volte nel corso di questo lavoro è risultato necessario utilizzare il condizionale, che sono stati molti più gli aspetti che hanno diviso gli studiosi che quelli sui cui essi sono stati concordi; tuttavia, non possiamo esimerci dallo smuovere ancora una volta le nostre certezze per capire quali potrebbero essere i risvolti dell'impiego delle nuove tecnologie sulle tematiche da noi analizzate.

2. Alcune riflessioni sulle ricadute dell'IA nell'oggetto della nostra indagine

2.1 Chiariamo alcuni concetti

Prima di affrontare una qualunque questione dobbiamo chiarire che cosa si intenda per Intelligenza Artificiale e per *Big data*. I Big data non sono altro che una quantità massiva di dati "dalle dimensioni talmente ampie da sfuggire alle abilità di raccolta, archiviazione, gestione ed analisi degli strumenti tradizionali a ciò finalizzati"[11]. Si tratta delle materie prime impiegate dall' intelligenza artificiale. Chiarire quest'ultimo concetto non è opera semplice, dal momento che manca una definizione univoca e universalmente condivisa[12]. L'intelligenza artificiale costituisce attualmente la massima espressione tecnologica contemporanea[13].

La Commissione europea ci fornisce una prima definizione di carattere generale nel 2018. Per IA si intendono quei "sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in *software* che agiscono nel mondo virtuale (per esempio assistenti vocali, *software* per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'IA in dispositivi *hardware* (per esempio in *robot* avanzati, auto a

[11] MONDINI RUSCONI, *Big data. Privacy, gestione e tutele*, Altalex editore, Milano, 2018, pag. 15
[12] C. TREVISI, *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo* in medialaws.eu, 25 giugno 2018; D. IMBRUGLIA, *L'intelligenza artificiale (IA) e le regole* in medialaws.eu, 24 dicembre 2020
[13] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020, pag. 76

guida autonoma, droni o applicazioni dell'Internet delle cose)"[14]. Questa definizione è volutamente ampia allo scopo di includere ogni sistema in grado di reagire alle variabili ambientali e di migliorare le prestazioni sulla base dell'esperienza acquisita[15]. Di conseguenza, l'IA rappresenta "quel settore dell'informatica con oggetto la teoria, le tecniche e le metodologie che permettono di progettare sistemi *hardware* e *software* in grado di elaborare delle prestazioni "assimilabili" all'intelligenza umana", dimodoché "l'idea è quella di fare sì che le "macchine" - intese nella loro duplice componente - possano essere in grado di compiere operazioni e "ragionamenti" complessi"[16]. In altri termini, gli strumenti di IA hanno la capacità di "fornire prestazioni assimilabili a quelle dell'intelligenza umana e, cioè, l'abilità di risolvere problemi o svolgere compiti e attività tipici della mente e del comportamento umano"[17].

La «Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi», adottata nei giorni 3-4 dicembre 2018 dalla Commissione europea per l'efficienza della giustizia (Cepej), istituita dal Comitato dei ministri del Consiglio d'Europa nel 2002, la intende come l'«insieme di metodi scientifici, teorie e tecniche finalizzate a riprodurre mediante le macchine le capacità cognitive degli esseri umani. Gli attuali sviluppi mirano a far svolgere alle macchine compiti complessi precedentemente svolti da esseri umani»[18]. Nello stesso documento viene poi distinta l'intelligenza forte dall'intelligenza debole. La prima capace di contestualizzare problemi specializzati di varia natura in maniera completamente autonoma; la seconda capace di compiere alte prestazioni nell'ambito di addestramento. Diversamente, la distinzione nell'ambito dell'intelligenza artificiale tra forte e debole è talora utilizzata per contrapporre i casi di equivalenza con le capacità umane a quelli in cui si mira alla semplice soluzione di

[14] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni. L'intelligenza artificiale per l'Europa, in www.eur.lex.europa.eu

[15] C. LIMITI*, Intelligenza Artificiale: implicazioni etiche in materia di privacy e diritto penale* in iusinitinere.it, 9 febbraio 2021

[16] C. PARODI, V. SELLAROLI, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco* in Diritto penale contemporaneo, fasc. 6/2019

[17] A. TRAVERSI**,** *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice robot?* In questionegiustiza.it

[18] Commissione Europea per L'efficienza Della Giustizia (CEPEJ), Carta etica per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente, App. III, Glossario, p. 47

problemi applicativi ma non vengono in rilievo *robot* o androidi[19]. Quello che sottolineano gli studiosi, tuttavia, è che l'IA non è un umanoide simile in tutto e per tutto all'essere umano ma si tratta di algoritmi in grado di elaborare milioni di dati e fornire, sostanzialmente su basi statistiche, risposte[20]. L'*input* resta quello umano: è quest'ultimo che sceglie l'obiettivo che l'applicazione di IA deve perseguire.

Una recente sentenza del Consiglio di Stato è intervenuta su questi concetti[21]. In particolare, l'organo giurisdizionale intervenuto per giudicare l'esatta perimetrazione tecnica della nozione di "algoritmo di trattamento" nell'ambito e nel contesto di una procedura nazionale di gara per la fornitura di *pacemaker* di alta fascia, approfondisce la stessa nozione di algoritmo evidenziando le differenze di carattere ontologico rispetto alla nozione di intelligenza artificiale. La corte rileva che l'algoritmo in via generale può essere definito come una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato. Tuttavia, osserva che la nozione, quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. Il grado e la frequenza dell'intervento umano dipendono dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare. Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di *machine learnig* e crea un sistema che non si limita solo ad applicare le regole *software* e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico.

Nel 21 aprile 2021 la Commissione Europea ha presentato una proposta di regolamento che stabilisce norme armonizzate in materia di intelligenza artificiale e che modifica alcuni atti legislativi dell'Unione. L'art. 3 della proposta definisce il sistema di "intelligenza artificiale" come il *software* sviluppato con una o più tecniche e approcci elencati nell'allegato I e che può, per una data serie di obiettivi definiti dall'uomo, generare

[19] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020, pag. 77

[20] C. TREVISI, *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo* in medialaws.it, 25 giugno 2018

[21] Consiglio di Stato, sentenza 4-25 novembre 2021, n. 7891

risultati quali contenuto, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono. Dall'analisi del considerando ed anche dall'analisi della stessa definizione sembra che la Commissione europea voglia accogliere una definizione piuttosto circostanziata di intelligenza artificiale delimitandone con una certa precisione i confini, invece quando esaminiamo l'allegato I richiamato dalla definizione scopriamo che si fa riferimento sia ad approcci tipici del *machine learning*, compreso l'apprendimento supervisionato, non supervisionato e profondo come il *deep learning*; sia ad approcci basati sulla logica e sulla conoscenza, tra cui rappresentazione della conoscenza, programmazione (logica) induttiva, basi di conoscenza, motori deduttivi e inferenziali, ragionamento (simbolico) e sistemi esperti nonché persino approcci statistici, stima *bayesiana*, metodi di ricerca e ottimizzazione. Probabilmente la Commissione al fine di evitare problematiche interpretative ha voluto ampliare al massimo la nozione di intelligenza artificiale ricomprendendo in essa sia l'intelligenza artificiale forte, intesa a duplicare la mente negli elaboratori, cioè a creare *computer* in grado di comprendere e di possedere stati cognitivi, sia l'intelligenza artificiale debole intesa a realizzare sistemi informatici capaci di prestazioni normalmente attribuite all'intelligenza umana, pur senza assumere alcuna analogia tra le menti e i sistemi informatici.

Per quanto attiene, invece, alle caratteristiche principali dell'intelligenza artificiale sembra essere raggiungibile un livello minimo di accordo tra gli studiosi[22]. Le caratteristiche sarebbero le seguenti: a) l'uso di grandi quantità di dati e informazioni; b) una elevata capacità logico-computazionale; c) l'uso di nuovi algoritmi, come quelli del *deep learning* e dell'auto-apprendimento, che definiscono metodi per estrarre conoscenza dai dati per dare alle macchine la capacità di prendere decisioni corrette in vari campi di applicazione. Chiariti tali concetti preliminari, ci addentriamo nelle questioni giuridiche.

2.2 L'impiego dell'IA nel sistema giudiziario

L'analisi che ci apprestiamo a svolgere ha ad oggetto la prevenzione e predizione dei reati per mezzo dell'IA. Occorre pertanto analizzare gli atti e i riferimenti normativi che si sono occupati dell'impiego dell'IA nel sistema giudiziario. Tale trattazione non ha la

[22] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020, pag. 77

pretesa di essere esaustiva, ma ha l'obiettivo di mettere in luce i possibili rischi per la *privacy* ma anche per altri diritti fondamentali a cui queste moderne tecnologie possono dare luogo.

La spinta crescente verso l'impiego di algoritmi nel campo della giustizia è alimentata *dai* risparmi di tempo e di costi che i *softwares* consentono di realizzare ma anche da una particolare fiducia nei confronti delle capacità della macchina. Tuttavia, non si possono nascondere le delicate questioni relative alla tutela dei diritti fondamentali dell'individuo e ai principi garantistici del giusto processo sollevate dal loro utilizzo. In particolare, ciò che desta preoccupazione è la discrezionalità soggettiva che si riscontra lungo tutto l'arco che procede dalla raccolta dei dati ai risultati definitivi basati sui medesimi. La neutralità dell'Intelligenza artificiale è solo apparente[23]. Risulta, pertanto, di fondamentale importanza il tema delle garanzie individuali che vanno osservate dal momento della raccolta dei dati personali fino all'uso dei risultati della loro elaborazione.

Nell'aprile del 2019 la Commissione Europea ha pubblicato le *Ethics Guidelines for Trustworthy AI*, in cui sono stati delineati quattro principi da rispettare al fine di assicurare uno sviluppo dell'intelligenza artificiale affidabile: rispetto dell'autonomia umana, *fairness*, prevenzione dei danni ed esplicabilità. Seppur non concernenti in particolare i sistemi utilizzati in ambito giuridico, questi principi rappresentano un importante tentativo di risolvere alcune delle questioni più problematiche inerenti all'impiego degli strumenti di IA nelle politiche pubbliche, tra cui le discriminazioni che potrebbero derivare dai *bias* contenuti nei *software*, l'opacità dei processi computazionali e il possibile condizionamento del risultato algoritmico sulla decisione umana. Essi disegnano pertanto un prezioso quadro etico volto a promuovere un approccio "antropocentrico" all'intelligenza artificiale e il rispetto dei diritti fondamentali delineati dalla Carta di Nizza[24].

Riguardano invece nello specifico le problematiche relative all'impiego dell'intelligenza artificiale nei sistemi giudiziari alcuni lavori recentemente elaborati nel contesto del Consiglio d'Europa. Tra questi, degno di nota è lo studio dottrinale *Algorithms and*

[23] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020, pag. 78

[24] F. C. GASTALDO, *Lo statuto della giustizia digitale nella Carta etica della CEPEJ* in iusinitinere.it, 2 aprile 2021

Human Rights[25], redatto nel 2017 dal comitato di esperti sull'intelligenza artificiale, che nella sezione *fair trial* e *due process* ha approfondito i profili più critici degli strumenti di IA impiegati nel processo penale statunitense. Le principali preoccupazioni evidenziate dal comitato attengono alla tenuta dei principi della presunzione di innocenza, della parità delle armi e del contraddittorio, come anche al pericolo che sistemi nati come strumenti di supporto alla decisione possano essere impropriamente impiegati dai giudici per delegare la decisione a strumenti tecnologici non adeguati a tale scopo.

Il più importante riconoscimento dei sistemi di intelligenza artificiale e la possibilità di un suo consapevole utilizzo nell'ambito dei sistemi giudiziari, tuttavia, è rinvenibile nella *Carta Etica europea per l'uso dell'intelligenza artificiale nei sistemi giudiziari e nei loro ambienti* adottata dalla Commissione europea per l'efficienza nella giustizia (CEPEJ) il 4 e 5 dicembre 2018. La Carta nello specifico definisce un quadro di principi utili a intraprendere e affrontare lo sviluppo dell'intelligenza artificiale nei processi giudiziari nazionali e va letto nell'ambito del più vasto sistema di garanzie costituito dalla CEDU e dalla normativa generale sul trattamento dei dati personali (Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 – GDPR). Questo strumento di *soft law* si articola in 5 principi e 4 Appendici: una, contenente uno studio approfondito dello stato dell'arte e delle problematiche aperte sull'uso dell'intelligenza artificiale nei sistemi giudiziari, la seconda contenente una griglia sui possibili utilizzi dell'intelligenza artificiale nei sistemi giudiziari, la terza che reca un glossario, la quarta una *checklist* di autovalutazione della compatibilità dei modelli di utilizzo con i principi recati dalla Carta. Essa si rivolge, non solo ai legislatori degli Stati membri, chiamati a stabilire una cornice normativa in materia, ma anche ai soggetti privati e pubblici coinvolti nella realizzazione o nell'impiego degli strumenti informatici. L'obiettivo della Carta non è di proibire o disincentivare l'introduzione dell'IA nei sistemi giudiziari, bensì di incoraggiarne le applicazioni che possono apportare un miglioramento in termini di efficienza e qualità della giustizia, garantendone però un uso responsabile e rispettoso dei

[25] Committee of expert of Internet Intermediaries, *Algorithms and Human Rights*. *Study on the Human Rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, Council of Europe, 2017, https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html.

diritti fondamentali enunciati dalla Convenzione europea dei diritti dell'uomo e dalla Convenzione n.108 del Consiglio d'Europa sulla protezione dei dati personali.

Il primo principio affermato nella Carta Etica, sicuramente il più importante, stabilisce che la progettazione e l'applicazione degli strumenti di intelligenza artificiale devono sempre essere compatibili con il rispetto dei diritti fondamentali. I testi di riferimento in materia sono la Convenzione n.108 del Consiglio d'Europa sulla protezione dei dati personali e la Convenzione Europea dei Diritti dell'Uomo, con particolare attenzione ai diritti fondamentali connessi all'amministrazione della giustizia, tra cui il diritto di accesso a un tribunale, il diritto ad un equo processo, che comprende i principi del contraddittorio e della parità delle armi, il principio di legalità e il principio dell'indipendenza giudiziale. Per garantire il rispetto del primo principio, la CEPEJ suggerisce soprattutto l'elaborazione di norme che operino sin dalle fasi iniziali di progettazione e di "addestramento" degli algoritmi, con lo sviluppo di un approccio "*ethical-by-design*" o "*human-rights-by-design*". La seconda disposizione sancisce il principio di non discriminazione. Si sottolinea con particolare enfasi la necessità di assicurare che gli strumenti di IA non conducano ad un aggravamento delle discriminazioni esistenti o ad analisi o usi deterministici. Particolare attenzione dovrebbe essere prestata nei casi in cui ai fini delle analisi predittive siano impiegati dati "sensibili", tra cui rientrano per esempio l'origine razziale o etnica, le condizioni socioeconomiche, le opinioni politiche, la fede religiosa o filosofica, l'appartenenza a un sindacato o i dati genetici, biometrici, sanitari o relativi alla vita o all'orientamento sessuale di un individuo. Al contempo secondo la CEPEJ sarebbe anche opportuno, proprio ai fini di limitare tali pericoli, incoraggiare l'impiego virtuoso delle tecniche di apprendimento automatico con l'instaurazione di analisi multidisciplinari in materia. Il terzo principio affermato dalla Carta Etica attiene alla necessità di garantire la sicurezza e la qualità degli algoritmi impiegati nei sistemi giudiziari. Fondamentale è esercitare attente verifiche sull'affidabilità delle fonti e sull'integrità dei dati forniti in *input* agli strumenti di IA: le informazioni utilizzate dovrebbero dunque sempre provenire da fonti certificate, l'intero processo di costruzione dell'algoritmo dovrebbe essere tracciabile e verificabile e gli algoritmi dovrebbero essere memorizzati e archiviati in ambienti tecnologici sicuri al fine di evitare qualunque alterazione dei dati da essi elaborati, anche involontaria. Di grande rilevanza è il principio di trasparenza, imparzialità e equità, secondo cui i processi

computazionali dei *software* devono sempre essere accessibili, comprensibili e verificabili. Il quinto principio della Carta impone dunque di assicurare che gli utilizzatori siano sempre informati e in grado di controllare le proprie scelte. Affinché ciò effettivamente avvenga, essi dovrebbero sempre essere messi in condizione di poter risalire alle informazioni elaborate dalla macchina e restare liberi di discostarsi autonomamente dal risultato da essa fornito, considerando le particolarità del caso concreto. I destinatari della decisione automatizzata, invece, dovrebbero sempre essere avvisati in linguaggio chiaro e comprensibile del carattere vincolante o meno delle soluzioni proposte dagli strumenti di intelligenza artificiale, delle varie opzioni disponibili e del loro diritto all'assistenza legale e al ricorso a un tribunale.

In una prospettiva più politica, si colloca invece il «Libro bianco sull'intelligenza artificiale -Un approccio europeo all'eccellenza e alla fiducia» del 19 febbraio 2020, con il quale la Commissione europea sostiene il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi relativi con lo scopo di definire le opzioni strategiche su come raggiungere gli stessi.

Inoltre, facciamo riferimento a una risoluzione del Parlamento europeo sull'intelligenza artificiale nel diritto penale e sul suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, risalente al 6 ottobre 2021. In particolare, la risoluzione punta 5 aspetti importanti: il rischio di discriminazione derivante dall'uso dell'IA, la necessità di condurre valutazioni d'impatto, la trasparenza, i sistemi di polizia predittiva ed il divieto di sorveglianza di massa biometrica. Nell'interazione tra IA e diritto penale, pertanto, le maggiori questioni ruotano pertanto intorno ai rischi per i diritti fondamentali ed in particolare per la *privacy* degli individui. Il Parlamento europeo riconosce che i risultati forniti dai sistemi di intelligenza artificiale sono necessariamente influenzati dalla qualità dei dati utilizzati e che tali pregiudizi intrinseci sono inclini ad aumentare gradualmente e quindi a perpetuare e amplificare le discriminazioni esistenti, in particolare per le persone appartenenti a determinati gruppi etnici o comunità dette "razzializzate". Inoltre, i deputati chiedono che sia condotta una valutazione d'impatto obbligatoria sui diritti fondamentali prima dell'attuazione o della diffusione di qualsiasi sistema di intelligenza artificiale per le forze dell'ordine o la magistratura, al fine di valutare eventuali rischi per i diritti e le libertà delle persone fisiche. Per quanto riguarda la trasparenza, il Parlamento europeo chiede che gli algoritmi siano "spiegabili", trasparenti, tracciabili e che la verifica

sia una parte necessaria della supervisione, al fine di garantire che lo sviluppo, la diffusione e l'uso dei sistemi di intelligenza artificiale per la magistratura e le forze dell'ordine siano conformi ai diritti fondamentali e siano considerati affidabili dai cittadini, nonché al fine di garantire che i risultati generati dagli algoritmi di IA possano essere resi intelligibili agli utenti e agli individui soggetti a tali sistemi. Inoltre, si rileva che la polizia predittiva è tra le applicazioni di intelligenza artificiale più utilizzate nel settore delle forze dell'ordine, tuttavia, essa non può rispondere alla domanda di causalità e non può fare previsioni affidabili sul comportamento individuale, e quindi non può costituire l'unica base per un intervento. Pertanto, il Parlamento europeo si oppone all'uso dell'intelligenza artificiale da parte delle autorità di contrasto per fare previsioni comportamentali su individui o gruppi sulla base di dati storici e comportamenti passati, appartenenza a gruppi, posizione o altre caratteristiche simili, cercando in tal modo di identificare le persone che potrebbero commettere un crimine. I sistemi di intelligenza artificiale possono offrire grandi opportunità nel campo dell'applicazione della legge, in particolare migliorando i metodi di lavoro delle forze dell'ordine e delle autorità giudiziarie e combattendo in modo più efficiente determinati tipi di reato, in particolare la criminalità finanziaria, il riciclaggio di denaro e il finanziamento del terrorismo *online*, l'abuso e lo sfruttamento sessuale dei bambini, nonché alcuni tipi di criminalità informatica, contribuendo così alla sicurezza e all'incolumità dei cittadini dell'Unione europea. Allo stesso tempo, però, possono comportare rischi significativi per i diritti fondamentali delle persone e qualsiasi sistema generalizzato di IA ai fini della sorveglianza di massa sarebbe da considerarsi sproporzionato. Sebbene questa risoluzione non rientri direttamente nel diritto dell'UE, essa fornisce un'indicazione molto chiara che il Parlamento adotterà una linea forte quando si tratterà di adottare atti legislativi che riguardano questioni di polizia predittiva e sorveglianza di massa biometrica.

Importante nella regolazione dell'impiego dell'IA nel sistema giudiziario è il GDPR, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. In particolare, facciamo riferimento all'art. 22 rubricato "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione", il quale dispone che: "1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo

significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato". In conclusione, l'articolo 22 è il tentativo del legislatore di disciplinare le condizioni in cui è consentito l'uso esclusivo di una decisione fondata sul trattamento automatizzato di dati e informazioni.

___2.2.1 La prevenzione della criminalità mediante l'IA

L'IA può svolgere un ruolo fondamentale nella prevenzione dei reati. Nel settore di *law enforcement*[26], è sorta l'esigenza di sfruttare il potenziale offerto dai c.d. *big data* e quindi di gestire e analizzare enormi quantità di informazioni attraverso la tecnologia. La raccolta dei dati consente pertanto di prevenire i reati, purché tali strumenti siano adeguatamente regolati. Il Libro Bianco dell'Agenzia per l'Italia Digitale del marzo 2018, L'intelligenza artificiale al servizio del cittadino, sottolinea che: «...pur rappresentando una miniera di informazioni, i dati hanno bisogno di strumenti adeguati per poter essere sfruttati in tutto il loro potenziale. In particolare, servono modelli e metodi di recupero e filtraggio delle informazioni fondati su tecnologie semantiche e ontologie condivise».

[26] Il Concept Paper dell'Annual Police Experts Meeting (APEM) del 2019, organizzato dall'OSCE e dedicato al tema "Artificial Intelligence and Law Enforcement: an Ally or an Adversary?", evidenzia che «The increasing amount of data obtained and stored by the police has also called for more sophisticated methods and tools for data management and analysis, identification of patterns, prediction on risks, and development of strategies to allocate human and financial resources where they are most needed». Il documento è reperibile su https://www.osce.org/chairmanship/429596.

Parliamo di quel fenomeno definito *predictive o big data policing*, affermatosi prima negli Stati Uniti e oggi anche in Italia[27]. Per "polizia predittiva" possiamo intendere l'insieme delle attività rivolte allo studio e all'applicazione di metodi statistici con l'obiettivo di "predire" chi potrà commettere un reato, o dove e quando potrà essere commesso un reato, al fine di prevenire la commissione dei reati stessi[28]. Tali *software* coadiuvano gli agenti di polizia nella formulazione di previsioni circa il compimento di determinate tipologie di reati, grazie all'incrocio di dati provenienti da banche dati delle forze dell'ordine, *social networks e Internet* e all'impiego della tecnica di *machine learning*[29]. Ad esempio, *White Collar Crime Early Warning System* è un *software* appositamente impiegato per la prevenzione di reati economici a Manhattan[30]. La predizione può riguardare l'individuazione di luoghi sospetti (*crime hotspot*) o l'elaborazione di profili criminali individuali di persone a rischio, a seconda che il *software* si basi sul *place- based system* o sul *person- based system*[31]. Il *Big data policing* funziona in termini corrispondenti. Anche in questo caso si tratta di previsioni algoritmiche che dovrebbero consentire agli organi statali la prevenzione dei reati. La differenza tecnologica rispetto al *predictive policing* consiste nella quantità e qualità dei *record* di dati che sono impiegati. In questo caso vengono elaborate ampie serie di dati apparentemente disgiunti. Sebbene il loro impatto sulla diminuzione del tasso di criminalità sia sicuramente apprezzabile, questa attività di monitoraggio potrebbe entrare in tensione con alcuni diritti fondamentali dell'individuo. In primo luogo, emerge una possibile frizione con la tutela della *privacy*, a causa della mole di dati raccolti e processati, con l'eventualità di possibili discriminazioni nel caso in cui gli indici di pericolosità si fondino sul pregiudizio dell'appartenenza del soggetto a determinate categorie etniche ovvero sulla sua provenienza da contesti sociali ritenuti a rischio[32]. Inoltre, affiorano talune criticità in relazione alle modalità oggettive di funzionamento dei

[27] Alla Questura di Napoli si deve l'elaborazione di X-LAW, mentre alla questura di Milano di Key Crime.
[28] F. BASILE, Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine in Diritto penale e Uomo, pag. 10.
[29] P. SEVERINO, *Intelligenza artificiale e diritto penale* in Intelligenza artificiale: il diritto, i diritti e l'etica, Milano, Giuffrè, 2020, pag. 540
[30] In Italia è stato elaborato X-LAW dalla Questura di Napoli e KeyCrime dalla Questura di Milano.
[31] Per un approfondimento circa l'impiego di tali sistemi rinvio a F. BASILE, Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, in Dir. pen. uomo, 29 settembre 2019
[32] P. SEVERINO, *Intelligenza artificiale e diritto penale* in Intelligenza artificiale: il diritto, i diritti e l'etica, Milano, Giuffrè, 2020, pag. 541.

predictive policing systems. È stato notato che l'intensificazione dei controlli in una zona calda, cui consegua l'effettiva rilevazione di reati, determinerà in modo inevitabile che l'algoritmo acquisendo tali dati, innalzerà ulteriormente il tasso di rischiosità di quella zona, con il pericolo che si trascurino le iniziative di prevenzione in altre aree[33]. Altra problematica attiene ad un possibile difetto di funzionamento dell'IA. Peraltro, mancano precise indicazioni normative sul legittimo uso della c.d. polizia predittiva, con la conseguenza che il *modus operandi* e il grado di influenza di tali strumenti nelle strategie di *crime prevention* sono integralmente rimessi alle scelte dei singoli *police officers*. La recente iniziativa promossa dall'OSCE e dedicata al tema dell'"*Artificial Intelligence and Law Enforcement"* costituisce, tuttavia, un passo avanti nell'ottica della cooperazione e scambio di *best practices*. Nel documento di presentazione del Convegno annuale di esperti di Polizia si legge: "nei loro sforzi per aumentare l'efficienza e l'efficacia e per stare al passo con le innovazioni tecnologiche, le autorità e le agenzie di *law enforcement* di tutto il mondo stanno esplorando sempre più i potenziali dell'IA per il loro lavoro. La crescente quantità di dati ottenuti e archiviati dalla polizia ha anche richiesto metodi e strumenti più sofisticati per la loro gestione e analisi, per l'identificazione di modelli (*pattern*), la previsione dei rischi e lo sviluppo di strategie per allocare le risorse umane e finanziarie dove sono maggiormente necessarie. Anche se l'uso dell'IA nel lavoro delle forze dell'ordine è un argomento relativamente nuovo, alcuni strumenti basati sull'intelligenza artificiale sono già stati testati e sono persino attivamente utilizzati dai servizi di polizia di diversi Paesi del mondo. Questi includono *software* di analisi di video e immagini, sistemi di riconoscimento facciale, di identificazione biometrica, droni autonomi e altri *robot* e strumenti di analisi predittiva per prevedere le "zone calde" del crimine o anche per identificare potenziali criminali futuri, in particolare i criminali ad elevata pericolosità"[34].

___2.2.2 L'impiego dell'IA nel processo penale

[33] F. BASILE, Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, in Dir. pen. uomo, 29 settembre 2019, pag. 13.

[34] Il documento completo di presentazione del 2019 OSCE Annual Police Experts Meeting: Artificial Intelligence and Law Enforcement: An Ally or an Adversary? può essere letto sulla rivista diritto penale e uomo, 23 settembre 2019)

Altro tema che ha suscitato interesse negli ultimi tempi è quello dell'utilizzo degli algoritmi predittivi nel processo penale. Facciamo riferimento all'affiancamento al giudice di algoritmi impiegati per valutare la pericolosità sociale e il rischio di recidiva di un individuo, ma anche a fini decisionali (c.d. *automated decision systems*). Negli Stati Uniti l'utilizzo di tali algoritmi è una realtà consolidata. In Estonia, nel 2019 ha debuttato il giudice *robot*. Si tratta, pertanto, di una tematica con cui occorre fare i conti e che potrebbe apportare indubbi vantaggi in termini di celerità della giustizia, senza tuttavia nascondere le preoccupazioni per i diritti fondamentali. In questa sede, cercheremo di mettere in luce tali problematiche, rinviando ad autorevole dottrina per i relativi approfondimenti[35]. In primo luogo, la standardizzazione delle informazioni rischia di far passare dal "diritto penale del fatto" al "diritto penale d'autore", mentre la loro selezione e le loro correlazioni possono consacrare eventuali preconcetti[36]. Infatti, non si può ignorare che gli algoritmi predittivi possono entrare in conflitto con l'art. 3 Cost, ma anche con il diritto alla *privacy* e determinare una sorta di "militarizzazione" nella sorveglianza di determinate zone o di determinati soggetti[37]. In caso di crimini seriali, infine, la profilazione della persona cui venga addebitato un reato con l'impiego di algoritmi predittivi sarebbe utilizzabile altresì per sospettarlo di precedenti illeciti, desunti dall'archivio informatico e dalla sua elaborazione. Il rischio è quello di cadere in una teoria lombrosiana 2.0[38]. Sulla stessa linea, autorevole dottrina afferma che "L'algoritmo potrebbe rafforzare i c.d. stereotipi impliciti, fisiologicamente presenti nella persona che deve effettuare un giudizio, aumentando il rischio di un approccio proprio del diritto penale d'autore e del nemico… il tutto in violazione, innanzitutto del principio di uguaglianza, del principio di offensività del diritto penale del fatto (sancito dall'art. 25,

[35] F. BASILE, Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine, in Dir. pen. uomo, 29 settembre 2019; A.M. MAUGERI*, L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali* in Archivio penale 2021, n.1; D. POLIDORO*, Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale* in Archivio penale n. 3/2020; SEVERINO P., *Intelligenza artificiale e diritto penale* in Intelligenza artificiale: il diritto, i diritti e l'etica, Milano, Giuffrè, 2020; G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020

[36] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020, pag. 81

[37] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020, pag. 82

[38] A. GIANNINI, Lombroso 2.0: On AI and Prediction of Dangerousness in Criminal Justice in RIDP, Vol.92/2021

comma 2 Cost.) e del principio di colpevolezza, correttamente inteso come colpevolezza del fatto"[39].

Altro problema è la mancanza di trasparenza, emersa in un noto caso che negli Stati Uniti ha consentito di affrontare le problematiche legate all'impiego della giustizia predittiva[40]. Un soggetto aveva ricevuto una condanna sulla base delle valutazioni compiute attraverso l'algoritmo COMPAS. Avverso la decisione il reo presentava ricorso per violazione del suo diritto al giusto processo. In particolare, lamentava di non poter controllare i processi algoritmici perché protetti da segreto industriale; di non essere stato punito individualmente perché COMPAS lavorava con dati di gruppo generalizzati; e che l'algoritmo prendeva in considerazione anche il sesso della persona da valutare, una variabile inammissibile perché discriminatoria rispetto al genere. Tuttavia, la Corte suprema del Wisconsin ha respinto il ricorso e anche la Corte suprema degli Stati Uniti alla fine non ha accettato il caso. La motivazione alla base di tale rifiuto sta nel fatto che l'individuo non dovrebbe godere di alcun "diritto alla spiegazione" rispetto a una previsione algoritmica del rischio se egli sia in grado di supervisionare i suoi *input* e sia informato circa i suoi *output.* L'uso di dati aggregati nonché l'inclusione del genere nella previsione algoritmica del rischio non sono stati criticati, in quanto ciò ne migliora l'accuratezza e non persegue un obiettivo discriminatorio. Inoltre, è stato chiarito che un giudice può tenere in considerazione una prognosi algoritmica del rischio, ma non la considera vincolante. Si tratta, ovviamente di un caso controverso, tuttavia per il futuro si prevede un impiego sempre più massiccio degli algoritmi, i quali dovrebbero garantire l'obiettività, la neutralità e la coerenza nell'applicazione del diritto. "Per evitare effetti di sovrastima e/o rischi di falsi positivi, e per consentire alla difesa di verificare la scientificità e l'accuratezza di un enigmatico database o di un dato generato da un determinato processo computazionale si dovrebbe ammettere nei confronti dell'algoritmo la valutazione peritale, - non diversamente da ogni acquisizione scientifica che entri nel

[39] A.M. MAUGERI*, L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali* in Archivio penale 2021, n.1, pagg. 12- 13.
[40] Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis, Case no. 2015AP157-CR, 5 April-13 July 2016

processo penale-, e comunque la sua fondatezza empirica dovrebbe essere valutata in contraddittorio, ne rispetto dei diritti della difesa"[41].

In Italia possiamo citare la sentenza del Consiglio di Stato, n. 2270/2019, che affronta la questione del diritto di accesso delle parti interessate all'algoritmo. Il Consiglio di Stato ha affermato il principio della conoscibilità dell'algoritmo ma anche della necessità che sia tradotto in una regola giuridica conoscibile e comprensibile in piena conformità con il principio di legalità/precisione dell'ordinamento penale[42].

Proprio per le conseguenze determinate da tali problematiche, l'impiego della macchina in sede giurisdizionale dovrebbe essere assoggettato a un controllo umano significativo rappresentato dalle seguenti imprescindibili condizioni: "1) che il suo funzionamento sia reso pubblico e vagliato conformemente ai criteri di *peer review*; 2) che sia noto il potenziale tasso di errore; 3) che adeguate spiegazioni traducano la "formula tecnica" costitutiva dell'algoritmo nella sottesa regola giuridica, così da renderla leggibile e comprensibile dal giudice, dalle parti e dai loro difensori; 4) che sia salvaguardato il contraddittorio sulla scelta degli elementi archiviati, sui loro raggruppamenti e sulle correlazioni dei dati elaborati dall'apparato di intelligenza artificiale, particolarmente in relazione all'oggetto della controversia; 5) che la loro accettazione da parte del giudice fosse giustificata alla luce di quanto emerso in giudizio e per la *quaestio facti* valutato secondo il principio del libero convincimento"[43].

Alcuni studiosi mettono in luce un'altra questione. Anche se il processo decisionale fosse supportato dagli algoritmi, con la possibilità per il giudice di superare la decisione dell'algoritmo con la propria si determinerebbe comunque una prevalenza della decisione algoritmica. Infatti, il giudice, per paura di reazioni negative se la propria prognosi si rivelasse sbagliata, perché ad esempio un soggetto che è stato rilasciato torna a commettere reati, verrebbe indotto ad avvalersi degli algoritmi[44].

---

[41] A.M. MAUGERI*, L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali* in Archivio penale 2021, n.1, pag. 20

[42] Consiglio di Stato, Sez. VI, Sent. 8 aprile 2019, n. 2270 in medialaws.it

[43] G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo* in Diritto penale contemporaneo n.4/2020, pag. 84

[44] C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società* in Rivista italiana di diritto e procedura penale, n. 4/2019, pag. 22

Oltre ai rischi di discriminazione e per la *privacy* si profila anche la necessità che tali algoritmi siano messi in sicurezza. Si parla, infatti, di *oracle attack*, con i quali i criminali si procurano le previsioni elaborate dai *software* di *Predictive* o *Big data policing*, adattando di conseguenza il loro comportamento criminale (ad esempio commettendo il furto esattamente dove l'algoritmo non si aspetta). Per cui occorre anche predisporre adeguati strumenti di sicurezza informatica al fine di prevenire gli *hackeraggi* e gli *oral attacks.*

2.3 Intelligenza artificiale e responsabilità penale

L'impiego dell'Intelligenza artificiale apre anche il problema della responsabilità penale. Pensiamo ai *robot* impiegati nel settore medico-chirurgico, alle *self-driving cars*, agli algoritmi di giustizia predittiva, ma anche ai sistemi impiegati all'interno delle società come *CorpTech*, sistemi in grado di prendere decisioni complesse di grande rilievo sociale. Questo tipo di sistemi mette in crisi le tradizionali categorie del diritto penale. La difficoltà della questione non ha, tuttavia, impedito agli studiosi di affrontare il problema. Senza alcuna pretesa esaustiva, indagheremo gli scenari che si aprono nel futuro.

L'IA si configura come una c.d. *dual-use techonology* in quanto può essere impiegata sia per svolgere attività lecite, sia per svolgere attività illecite. Questi *software* possono sostituirsi, in tutto o in parte, all'uomo ad esempio nel compimento di attività illecite sul *web*. Pensiamo ad esempio agli attacchi di *spear pishing*. L'IA favorisce inoltre l'emersione di nuove forme di aggressione a beni giuridici tradizionali o di nuovo conio, quali la riservatezza e la sicurezza informatiche[45]. Questi *softwares* possono essere programmati per accedere abusivamente a sistemi informatici, per porre in essere attacchi distribuiti in rete (c.d. *distributed denial of service attacks*) o diffondere pericolosi *malware* e *ransomware*. Le c.d. *social media bots* contribuiscono in modo significativo alla proliferazione in rete dell'*hate speech* e di campagne di disinformazione, alimentate da *fake news*, create con l'obiettivo di manipolare l'opinione pubblica, di creare consenso politico o di destabilizzare gli equilibri geopolitici. Esemplare la vicenda del social

[45] 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'epoca di Internet*, Padova, 2004, p. 21 ss., p. 70 ss.; e I. SALVADORI, I reati contro la riservatezza informatica, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), Cybercrime, Torino, 2019, p. 656 ss., p. 660 ss.

Twitter "Tay" di *Microsoft*, che ha rapidamente imparato dall'interazione con gli altri utenti a dirigere *twitter* osceni ad un'attivista femminista. Parte della dottrina ritiene che date le peculiarità connesse all'IA, dovrebbe configurarsi una nuova categoria di reati, i c.d. *Artificial Intelligence Crimes*[46]. L'intelligenza artificiale ha, pertanto, anche dei riflessi sui reati informatici di cui ci siamo occupati nel corso del secondo capitolo, ma anche in relazione a quella categoria a cui abbiamo fatto cenno dei c.d. reati informatici in senso ampio, tanto in relazione alla modalità d'azione, quanto in relazione alla responsabilità penale.

Rispetto ai *softwares* tradizionali che utilizzavano un linguaggio di regola trasparente, oggi, l'IA può compiere attività che neppure i loro programmatori, sviluppatori e produttori avevano previsto. Ma non solo, la struttura interna dell'IA può essere volutamente occultata per evidenti ragioni di natura economica o connesse alla tutela di segreti industriali, dei brevetti, del *copyright*, ecc. Di regola, però, l'opacità tecnologica è connaturata all'IA per la complessità dei sistemi che operano sulla base di c.d. *black box algorithms* e trattano in tempi rapidissimi una mole enorme di dati (*big data*)[47]. Il problema della responsabilità penale è complicato anche dal fatto che sono numerose le figure che intervengono in fase di progettazione, sviluppo, sperimentazione, produzione, distribuzione ed utilizzo dei *softwares*. Pertanto, "Da un lato la responsabilità (anche penale) che sorge in conseguenza degli eventi dannosi connessi con il funzionamento e l'utilizzo degli a.a. tende a diffondersi e distribuirsi tra più "operatori" (sviluppatori, programmatori, collaudatori, produttori, utilizzatori, ecc.), il cui agire "concorre", sul versante causale, a produrre l'evento lesivo e, in determinati casi, si "somma" a quello dell'agente artificiale. Dall'altro lato, nella ricostruzione del processo eziologico, il concreto apporto di ogni singolo "operatore", nella complessità della struttura interna degli a.a., diventa difficile da provare sul piano oggettivo causale e dell'imputazione soggetti"[48]. Occorre, inoltre, precisare che gli agenti di intelligenza artificiale vengono

[46] B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pag. 327
[47] Cfr. I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021, pag. 89
[48] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021, pag. 90

classificati in base al livello di automazione e autonomia, dal primo al quinto livello[49]. Mentre per gli agenti che rimangono sotto il controllo dell'uomo, la responsabilità sarà sempre degli operatori. In queste ipotesi, il soggetto che controlla il sistema di IA ha il dovere di evitare danni a terzi, si configura, pertanto, una posizione di garanzia, inquadrabile nella categoria delle posizioni di controllo, imperniata sul governo della fonte di pericolo[50]. Per gli agenti su cui l'uomo ha difficoltà ad esercitare un controllo si potrebbe configurare un vuoto di responsabilità. Nonostante le proposte avanzate, in particolare citiamo lo studioso israeliano Gabriel Hallevy[51], al momento la teoria secondo cui l'agente artificiale possa essere considerato autore di reato sembra essere stata accantonata. Infatti, ad oggi, sembra difficile riconoscere ad un agente artificiale una effettiva libertà di autodeterminazione. "Anche gli a.a. più evoluti non hanno ancora una autocoscienza tale da consentirgli di comprendere il disvalore sociale delle loro azioni e di cogliere la funzione precettiva delle norme penali"[52]. Inoltre, ogni tentativo di muovere all'agente artificiale un rimprovero penale per aver commesso un fatto costitutivo di reato è destinato a naufragare contro lo scoglio insuperabile dell'art. 27 Cost., nella parte in cui sancisce che «la responsabilità penale è personale». In forza del principio costituzionale di colpevolezza, per il ricorso allo *jus puniendi* non basta la commissione di un fatto (oggettivo) tipico ed antigiuridico, ma occorre che esso possa essere personalmente rimproverato al suo autore (umano). L'inflizione della pena presuppone la attribuibilità psicologica e la rimproverabilità del fatto di reato al soggetto che lo ha posto in essere e la sanzione penale inflittagli deve tendere alla sua rieducazione (art. 27, co. 3, Cost.). Difficilmente l'irrogazione di una sanzione penale potrebbe svolgere quella funzione di prevenzione generale e speciale che è chiamata a svolgere. Ed anche con riferimento alla

[49] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021, pagg. 92 ss. In tal senso si veda anche CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale* in disCrimen, 27 marzo 2019, pag. 3

[50] C. PIERGALLINI, PIERGALLINI C., *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020, pag. 1751

[51] CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale* in disCrimen, 27 marzo 2019, pag.8; BORSARI R., *Intelligenza Artificiale e responsabilità penale: prime considerazioni* in medialaws, 3 novembre 2019 analizzano la tesi di Gabriel Hallevy.

[52] Ibidem, pag. 96

responsabilità civile, in ordine al risarcimento del danno, il programma di intelligenza artificiale non avrebbe un patrimonio di cui poter disporre con il quale risarcire il danno[53].

Ci occupiamo pertanto della distribuzione della responsabilità penale tra l'uomo e gli agenti e facciamo quindi, ora, riferimento all'IA come strumento e non autore di reato[54]. Tale tema risulta interessante ai fini della nostra indagine poiché tali strumenti possono essere utilizzati per compiere anche i reati di cui ci siamo occupati nel corso di questo lavoro, ma può avere delle ricadute in ordine alla responsabilità da reato degli enti e alla responsabilità dei vertici e dei dipendenti all'interno degli enti.

Non solleva particolari problemi, il caso in cui l'operatore decida di impiegare l'IA per commettere un reato o per arrecare offesa a terzi. In questo caso si configurerà una responsabilità a titolo doloso, anche nell'ipotesi di c.d. *aberratio causae*, vale a dire di divergenza tra il decorso causale prefigurato dall'agente e quello effettivamente realizzatosi nel caso concreto[55]. Riportiamo l'esempio del soggetto che utilizzi un drone a pilotaggio da remoto con l'intenzione di far cadere un ordigno esplosivo sulla casa in cui vive un preciso soggetto. Nel caso in cui il drone, per un difetto di funzionamento, dovesse cadere su un altro edificio facendo delle vittime, l'evento andrebbe comunque imputato, a titolo doloso, al soggetto. A rilevare, sul piano penale, sarebbe la causazione dell'evento preso di mira con la sua azione e non le modalità concrete con le quali si è verificato[56].

Il comportamento degli agenti di intelligenza artificiale è, nella maggior parte dei casi prevedibile da parte di un "operatore", pertanto, in caso di errore di programmazione o di

---

[53] G. FINOCCHIARO, *Intelligenza artificiale e responsabilità* in Contratto e impresa 2/2020, pag. 730

[54] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021; CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale* in disCrimen, 27 marzo 2019; BORSARI R., *Intelligenza Artificiale e responsabilità penale: prime considerazioni* in medialaws, 3 novembre 2019; C. PIERGALLINI, *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020; B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021.

[55] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021, pag. 101; CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale* in disCrimen, 27 marzo 2019, pag.8; BORSARI R., *Intelligenza Artificiale e responsabilità penale: prime considerazioni* in medialaws, 3 novembre 2019

[56] Ibidem

funzionamento potrà configurarsi un'ipotesi di responsabilità a titolo colposo per coloro che hanno programmato, sviluppato, prodotto o collaudato il *software*[57]. Occorre osservare, inoltre, che questo settore condivide molti dei peculiari problemi connessi con la responsabilità penale per danno da prodotto, poiché l'evento dannoso è in genere conseguenza di errori umani posti in essere nelle complesse ed articolate attività, spesso plurifrazionate, di programmazione, di sviluppo, di collaudo e/o di produzione[58]. Si pongono pertanto le problematiche legate alla responsabilità per danno da prodotto ma anche nuove questioni legate alle peculiarità dell'IA. In primo luogo, bisognerà intervenire sul concetto di "difettosità", considerando l'eventualità di poter comprendere all'interno del concetto di "difetto" le inaspettate deviazioni nel processo decisionale in cui è inserito l'agente artificiale[59]. Inoltre, si dovrà trovare il modo di superare il limite posto dall'art. 7 della direttiva 85/374/CEE che, escludendo la responsabilità del produttore per difetti sorti successivamente alla messa in commercio del prodotto, limiterebbe l'applicabilità del regime di *product liability* a tutti quei casi in cui l'evento lesivo sia cagionato da un'evoluzione emergente e successiva del comportamento della macchina[60]. Dovrebbe, pertanto, essere prevista una normativa specifica che in materia di *product safety*, introduca specifici obblighi di monitoraggio e revisione periodica degli agenti artificiali[61]. Inoltre, al pari dell'ambito dei danni derivanti da prodotti difettosi, diventa estremamente problematico ricostruire l'eziologia del fatto lesivo ed individuare i soggetti responsabili di ogni contributo causale. All'interno delle organizzazioni complesse che operano nel settore dell'IA e del ML vi è una inevitabile ripartizione di poteri e compiti (decisionali, organizzativi, operativi, di vigilanza, di consulenza, ecc.), ai quali corrispondono specifiche posizioni di garanzia, in forza delle quali ciascun

[57] Ibidem, pag. 102

[58] Cfr. C. PIERGALLINI, *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020; Tesi di dottorato di R. BERTOLESI, Intelligenza artificiale e responsabilità penale per danno da prodotto, 2019 (tesi di dottorato di Diritto penale nell'ambito del Corso di dottorato di ricerca in Scienze Giuridiche "Cesare Beccaria" dell'Università degli Studi di Milano - Curriculum di diritto penale e processuale penale - XXXII ciclo); B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021

[59] B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pag. 342. Si veda anche Commissione europea, Report Liability for artificial intelligence, pag. 27

[60] B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pag. 342.

[61] Ibidem

garante risponderà degli errori e delle omissioni ravvisabili nell'adempimento delle proprie funzioni. Ad una potenziale responsabilità per la causazione attiva di eventi vietati si affianca così una responsabilità omissiva, nella peculiare forma commissiva mediante omissione, per il loro mancato impedimento ex art. 40 cpv. c.p. In seno all'organizzazione complessa si dovrà individuare una rete di garanti, sui quali incombe un obbligo di controllo su determinate fonti di pericolo. Tali posizioni di garanzia sorgono non solo in relazione a coloro che assumono poteri decisionali ed organizzativi (c.d. soggetti apicali), ma anche in capo a coloro che, pur privi di autonomia decisionale (c.d. soggetti subordinati), detengono il sapere tecnico-scientifico, necessario per sviluppare la complessa struttura interna degli *a.a*. (programmatori, consulenti informatici, ecc.). Su tali soggetti graverà l'obbligo di adottare norme cautelari e di prevenzione volte a evitare il verificarsi dei rischi insiti nella progettazione, nello sviluppo, nella produzione, nel collaudo o nella messa in circolazione ed utilizzazione degli di tali sistemi. Il mancato rispetto degli obblighi di protezione potrà essere fonte di una responsabilità (omissiva) in relazione ad eventi lesivi concreti, verificatisi in conseguenza dell'utilizzo di un a.a. o del suo "autonomo" operare, purché rappresentino lo sviluppo del pericolo insito nella fonte da controllare e siano obiettivamente prevedibili ed evitabili.

Vi è, ancora, chi richiama la responsabilità da reato degli enti e l'art. 8 del d.lgs. 231. Laddove a causa di una c.d. "irresponsabilità individuale organizzata" non sia possibile identificare l'autore del fatto antigiuridico (colposo o doloso) penalmente rilevante e rientrante nel novero dei c.d. reati-presupposto di cui agli artt. 24 ss. d.lgs. n. 231/2001, l'evento dannoso, da ricondurre ad una attività "collettiva", potrà essere imputato alla persona giuridica (azienda, impresa, ecc.) per non averlo impedito mediante una adeguata organizzazione d'impresa. Si dovrà comunque dimostrare, alla stregua dell'art. 5, co. 1, d.lgs. n. 231/2001, che il reato-presupposto è stato commesso nell'"interesse" o a "vantaggio" dell'ente[62].

[62] I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021; Si veda anche C. PIERGALLINI, *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020 e B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021 che individuano anche le problematiche legate al rapporto tra Intelligenza artificiale e responsabilità da reato degli enti.

I problemi dell'individuazione dell'autore del reato e dell'accertamento della responsabilità, anche penale, nell'ambito dell'IA sono ulteriormente accentuati, come si è avuto modo di evidenziare dalla tendenziale opacità che ne connota la struttura interna. Due sono le principali conseguenze sul piano giuridico-penale. La c.d. *technological opacity* impedisce, in primo luogo, di determinare con precisione, nell'ambito della sommatoria di più "concause", i comportamenti degli "operatori" da mettere in correlazione causale con l'offesa cagionata. In secondo luogo, essa ostacola l'individuazione di una legge di copertura in grado di spiegare scientificamente il decorso causale in un contesto caratterizzato da una elevata complessità tecnologica e da una inevitabile interazione tra molteplici "operatori" (*many hands problem*).

La questione è più complicata nel caso in cui l'intelligenza artificiale fosse dotata di livelli più elevati di autonomia, tale da rendere oggettivamente impossibile prevedere *ex ante* il comportamento. Di fronte a situazioni di incertezza scientifica si potrebbe essere anche essere indotti a fare appello al principio di precauzione[63] e a porre dei limiti all'impiego dell'IA, ma questo potrebbe bloccare lo sviluppo di questo settore[64]. Tra gli studiosi che mettono in connessione l'intelligenza artificiale alla responsabilità penale per danno da prodotto, vi è chi rileva che a questo *gap* conoscitivo potrebbe sopperire l'installazione di scatole nere, teleologicamente orientate a 'schiarire', *ex post*, la ricostruzione della dinamica del fatto lesivo[65]. Nondimeno, ci si chiede se, ove il danno sia da ricondurre al cd. fattore robotico (cioè ad una azione/decisione autoappresa, estranea all'originario disegno operativo), questo non possa atteggiarsi alla stregua di un fattore causale sopravvenuto interruttivo del nesso causale, secondo quanto previsto dall'art. 41, comma 2, c.p.[66]. Altro modo per limitare gli addebiti colposi rimproverabili agli operatori potrebbe consistere "nella limitazione del loro dovere di diligenza", ritenendo pertanto

[63] Tra i diversi contributi in materia segnalo: A. MASSARO, Principio di precauzione e diritto penale: nihil novi sub sole? in penalecontemporaneo.it, 9 maggio 2011; E. CORN, Il principio di precauzione nel diritto penale, Torino, Giappichelli, 2013

[64] Per una riflessione sulle limitazioni all'autonomia tecnologica si veda B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pagg. 354 ss.

[65] C. PERGALLINI, *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020, pag. 1758; R. BERTOLESI, Intelligenza artificiale, cit., 211.

[66] C. PIERGALLINI, *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020, pag. 1758; contra B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pag. 358.

che gli operatori che si attengono ai severi *standard* previsti dalla proposta di Regolamento europeo e dalle altre fonti giuridiche rilevanti (come la normativa in materia di sicurezza dei prodotti) abbiano adempiuto al loro dovere di diligenza, anche se rimangono consapevoli (insieme a tutti i consociati) della permanenza di alcuni rischi[67]. Secondo tale tesi, il diritto penale dovrebbe fare un passo indietro a favore di forme di responsabilità di natura civilista. L'IA, però, potrebbe arrecare gravi danni a beni giuridici di primaria importanza, pertanto, escludere ogni forma di tutela penale non sembra la soluzione più auspicabile[68]. Come vediamo, il problema è di difficile soluzione. Certo è che vista la grande varietà di soggetti coinvolti, si dovrebbe propendere per la costruzione di forme di responsabilità collettiva o diffusa, prendendo a modello l'elaborazione che ha contrassegnato la disciplina della responsabilità penale degli enti[69]. Nonostante, la stessa dottrina che propone tale soluzione, non manchi di sollevare le criticità di simili parallelismi[70]. Inoltre, è necessario partire dagli obblighi che devono ricadere sull'operatore nella costruzione di un IA responsabile, intesa quale sistema "socio-tecnico" conforme ai "principi di ART" (accountability, responsability e transparency)[71]. Alcuni spunti interessanti si ricavano dal concetto di *Legal Protection by Design*, con cui "si richiede uno sforzo di traduzione dei principi giuridici, in specie per la tutela dei diritti fondamentali, dal linguaggio naturale a quello computazionale attraverso la formulazione di requisiti tecnici e impostazioni di *default* che vadano ad informare le architetture *data-driven* della nostra società"[72]. Questa teoria consente un coinvolgimento del diritto fin dalle fasi di *design* degli artefatti e dei processi della realtà socio-tecnica in cui viviamo, per garantirne la contestabilità.

---

[67] Cfr. I. SALVADORI, *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021; CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale* in disCrimen, 27 marzo 2019

[68] Cfr. B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pag. 359

[69] Ibidem, pag. 363

[70] Cfr. B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pag. 363, ma anche C. PERGALLINI, *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020; SEVERINO P., *Intelligenza artificiale e diritto penale* in Intelligenza artificiale: il diritto, i diritti e l'etica, Milano, Giuffrè, 2020

[71] B. PANATTONI*, Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021, pag. 364

[72] Ibidem

Altra osservazione che possiamo compiere è che l'intelligenza artificiale oltre a strumento per compiere reato, può costituire l'oggetto del reato. Sebbene non vi siano norme che facciano espresso riferimento all'IA, gli a.a. più complessi (ad es. MASs), composti da uno o più dispositivi di tipo *hardware* e *software,* sono da equiparare ad un sistema informatico o telematico. Pertanto, a tutela degli a.a. potranno applicarsi, laddove ne sussistano tutti i presupposti, i reati cibernetici (*cyber crimes*) che hanno ad oggetto dati ovvero sistemi informatici. Si pensi, a titolo esemplificativo, ad un *hacker* che si introduca senza autorizzazione nel sistema informatico che gestisce una *self-driving car*. In questo caso la condotta potrà configurare un'ipotesi di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-ter c.p. Lo stesso dicasi per il criminale informatico che, fuori dai casi consentiti dalla legge, installi uno *spyware* atto ad intercettare i dati informatici che vengono scambiati da più s.i.a. ovvero che proceda ad intercettare le comunicazioni informatiche tra a.a. interconnessi, mediante il *Cloud*, ad altri dispositivi. In questo caso potranno venire in rilievo le fattispecie che puniscono le intercettazioni non autorizzate di dati informatici (artt. 617-quater, 617-quinquies, 617-sexies c.p.).

In conclusione, ad oggi appare ancora opportuno affermare l'antico dogma del *machina delinquere non potest,* tuttavia i futuri sviluppi della tecnologia potrebbero porre il problema definito "*Responsibility gap*[73]" rispetto a quelle offese che non possono essere attribuite al programmatore o utilizzatore. Del resto, nella Risoluzione del Parlamento europeo del 2017, era già stata avanzata la proposta di considerare l'istituzione di uno *status* giuridico specifico per i *robot*, ossia per il riconoscimento della "personalità elettronica dei *robot* che prendono decisioni autonome o che interagiscono in modo indipendente con terzi"[74]. Risoluzione che, tuttavia, non ha trovato l'appoggio di un cospicuo gruppo di esperti. Riportiamo le previsioni di Hawking in una intervista alla BBC, nel 2014: "…lo sviluppo dell'intelligenza artificiale completa potrebbe decretare la fine della specie umana [...] Decollerebbe da sola, riprogettandosi a ritmo sempre crescente. Gli esseri umani, limitati dalla lenta evoluzione biologica, non riuscirebbero a

[73] Si tratta di un concetto introdotto da Andreas Matthias nel 2004 e sviluppato da Rob Spawwor nel 2007, secondo cui tecnologie complesse come gli algoritmi di machine learning generano degli *outcomes* per i quali nessuno può essere ritenuto responsabile, creando così una situazione che non è eticamente né socialmente accettabile.

[74] Parlamento europeo, Risoluzione del 16 febbraio 2017 recante "raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica"

tenere il passo e verrebbero rimpiazzati". Ci chiediamo, quindi, in un futuro l'IA cesserà di essere *res* e diverrà persona?

2.4 L'impiego dell'IA nelle società

Un altro ambito su cui l'IA potrebbe aprire nuovi scenari con riguardo alle tematiche da noi analizzate è il suo impiego all'interno degli enti. Si tratta di un tema di cui ci eravamo occupati nel corso del terzo capitolo e a cui faccio rinvio per l'analisi del tema relativo a colpa di organizzazione e IA (cap. 3; par. 2.6 "Colpa organizzativa e nuove tecnologie). Riprendiamo il discorso in questa sede con una prospettiva più ampia alle problematiche riguardanti l'impiego dell'IA all'interno delle società, per dare uno sguardo alle prospettive future anche in questo campo. Peraltro, quanto detto fino ad ora a proposito dell'IA può avere delle ricadute anche in questo specifico settore, tanto per quanto attiene alla prevenzione dei reati, tanto per quanto attiene alla responsabilità penale.

In primo luogo, una problematica su cui l'IA ha dei riflessi è quella del controllo dei lavoratori e del loro diritto alla *privacy,* specie alla luce delle novità introdotte dal *data protection reform package*[75], il quale potrebbe essere compromesso per effetto dell'attività di sorveglianza generalizzata che l'analisi algoritmica di ingenti quantità di dati aziendali comporterebbe[76]. L'avvento della pandemia e la diffusione dello *smart-working*, ha sicuramente dato nuova linfa al dibattito. Il Garante spagnolo (AEPD), infatti, ha ritenuto di dover sanzionare una catena di supermercati che aveva optato per l'implementazione e l'utilizzo di un sistema di intelligenza artificiale (riconoscimento facciale) per controllare l'ingresso nei negozi, così finendo per elaborare i dati personali (e particolari, quelli biometrici per la *face recognition*) tanto dei dipendenti, quanto dei clienti (sia maggiorenni che minorenni). Nel caso specifico, inoltre, l'utilizzo di tali strumenti di controllo era addirittura finalizzato alla verifica circa la presenza o meno dei suddetti dati all'interno di un *data base* contenente soggetti con pendenze giudiziarie.

[75] Facciamo riferimento al GDPR 2016/679/UE e alla Direttiva 2016/680/UE sulla protezione dei dati personali nell'attività di prevenzione, indagine, accertamento e perseguimento di reati, i quali impongono, rispettivamente, agli artt. 22 e 11, il divieto di decisione basate unicamente sul trattamento automatizzato, compresa la profilazione. Tale divieto è stato recepito dal nostro ordinamento da parte dell'art. 8 del D. Lgs. 18 maggio 2018, n. 51, attuativo della citata direttiva.

[76] P. SEVERINO, Intelligenza artificiale e diritto penale in Intelligenza artificiale- il diritto, i diritti l'etica a cura di Ugo Ruffolo, Milano, Giuffrè, 2020, pag. 539.

Altro caso ha riguardato l'Italia, dove nel 2021 il Garante *privacy* ha sanzionato per 2,6 milioni di euro una società (*Foodinho Srl*) del gruppo *Glovo*, uno dei maggiori *player* del settore della *instant delivery*. La società faceva uso di un sistema di IA per assegnare le consegne senza che fossero previste garanzie sulla correttezza ed esattezza dei risultati nonché la possibilità di un intervento correttivo umano, causando gravi discriminazioni[77].

Inoltre, ci si potrebbe servire dell'IA, per la prevenzione dei reati, impiegando all'interno delle organizzazioni private dei *software* di IA per la valutazione e gestione del rischio-reato[78]. Questi sistemi di prevenzione potrebbero essere utilizzati soprattutto nel campo dei reati informatici. Infatti, la crescente digitalizzazione delle imprese ha comportato l'innalzarsi del tasso tecnologico della condotta criminale e le misure preventive devono essere adeguate a questo contesto[79]. Abbiamo parlato nel corso di questo lavoro di tesi di *digital compliance*[80], per riferirci all'impiego dell'IA all'interno dei *compliance program*. L'IA è utilizzata per processare enormi quantità di dati interni ed esterni all'ente, così da individuare segnali di allarme e indici di anomalia, sintomatici di possibili condotte illecite, specie nell'ambito della lotta alla corruzione[81]. In linea generale, la versatilità degli strumenti in questione permette alle imprese di adattarli alle proprie esigenze. In primo luogo, i *software* di intelligenza artificiale possono essere impiegati nell'analisi e valutazione *ex post* dei dati aziendali, al fine di identificare le aree maggiormente a rischio-reato e intervenire, in ottica di aggiornamento e miglioramento, sul *compliance program* adottato. In queste ipotesi, l'ente potrà basarsi su un patrimonio conoscitivo senza dubbio più completo e affidabile di quello ottenibile attraverso un'analisi condotta secondo metodologie tradizionali, con indiscutibili benefici in termini di riduzione dei tempi e dei costi connessi[82]. La società potrebbe, inoltre, utilizzare l'algoritmo per rilevare

[77] BERTI R. ZUMERLE F., *Rider, no a discriminazioni dell'algoritmo: il Garante privacy sanziona Glovo per 2,6 milion*i in cybersecurity360; 9 LUGLIO 2021. La decisione del Garante privacy è reperibile sul sito garanteprivacy.it

[78] Cfr. R. TREZZA, *L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231: vantaggi "possibili" e rischi "celati"* in Giurisprudenza penale, n. 1-bis/2021

[79] NISCO A., *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022, pag. 5

[80] NISCO A., *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022

[81] Per una compiuta analisi dell'argomento, v. BIRRITTERI, *Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri*, in Dir. pen. cont. - Riv. trim., 2019, 2, 290 ss., il quale ipotizza l'applicabilità di predictive algorithms del rischio di corruzione anche nel settore pubblico

[82] P. SEVERINO, Intelligenza artificiale e diritto penale in Intelligenza artificiale- il diritto, i diritti l'etica a cura di Ugo Ruffolo, Milano, Giuffrè, 2020, pag. 538

eventuali condotte illecite *ex ante*, vale a dire, integrando tali strumenti all'interno delle procedure operative di *risk detecting* contenute nel modello. Grazie alle ben note capacità del *software,* ciò contribuirebbe senz'altro a rafforzare l'idoneità preventiva del *compliance program*, in quanto il potenziale criminale si troverebbe di fronte a un meccanismo di controllo difficile da aggirare, se non mediante un'elusione fraudolenta dello stesso[83]. Non mancano, tuttavia, le criticità. In primo luogo, la scelta in sé di avvalersi dell'algoritmo nella fase di individuazione del rischio-reato potrebbe ritorcersi contro l'azienda stessa tutte le volte in cui i vertici dovessero rimanere inerti di fronte a un pericolo che, segnalato dal sistema, trovi poi effettiva concretizzazione. In questo caso, il giudice potrebbe agevolmente concludere nel senso della mancata attuazione del modello. Inoltre, i sistemi di predizione dei reati ma anche i sistemi di controllo a cui abbiamo fatto prima cenno, si basano sull'archiviazione di grandi masse di dati, che potrebbero determinare una profilazione di attitudini criminali di massa, che determinerebbero una trasposizione delle inquietudini suscitate dai sistemi di *predictive policing*. Il primo argine a questo possibile sviluppo è costituito dalla normativa in materia di riservatezza. Va ricordato, a tal riguardo, che l'22 GDRP prevede un diritto alla trasparenza e alla "spiegazione" delle decisioni automatiche. Quello che, in questa sede, è importante sottolineare è il fatto che tale disciplina si estenda alle decisioni adottate in un contesto privato, quale è l'impresa che adotti un sistema automatizzato di prevenzione dei reati. Inoltre, è chiaro che gli adempimenti relativi alla *compliance* non possono scriminare eventuali delitti a tutela della riservatezza informatica e della segretezza della corrispondenza. Dal punto di vista dei controlli sui lavoratori, un ruolo peculiare riveste anche l'art. 4 dello Statuto lavoratori (l. 300/1970) che, in combinazione con l'art. 171 del Codice privacy (d.lgs. 196/2003), punisce già solo l'installazione di strumenti di controllo non autorizzati. Per effetto di riforme innescate dal c.d. *Jobs Act*, però, l'autorizzazione non è necessaria, se lo strumento di controllo coincide con uno "strumento di lavoro": nozione, quest'ultima, estremamente problematica, che rende dunque incerto il perimetro della tutela assicurata al dipendente[84]. Tutto ciò, però, ancora non basta a una piena tutela delle posizioni individuali colpite da decisioni automatizzate.

[83]P. SEVERINO, Intelligenza artificiale e diritto penale in Intelligenza artificiale- il diritto, i diritti l'etica a cura di Ugo Ruffolo, Milano, Giuffrè, 2020, Pag. 538

[84] Rinvio a A. NISCO, *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico*, in Sist. pen., 20 dicembre 2021.

Non a caso, la Proposta di regolamento europeo in materia di IA lascia supporre che l'utilizzo di questi sistemi rientrerà nella categoria dei sistemi di IA ad alto rischio, per l'impatto che essi potrebbero avere sul futuro delle persone controllate e dunque sui loro diritti fondamentali.

Infine, un tema in cui l'impiego dell'Intelligenza artificiale incrocia quello della responsabilità da reato degli enti è quello della responsabilità penale. Accantonato il tema della soggettività giuridica della macchina, come pure di un suo improbabile parallelo con quella dell'ente, cerchiamo di riflettere sui potenziali effetti dell'AI nella distribuzione della responsabilità tra uomo ed ente e all'interno dell'ente. Questa tematica si lega anche ai reati informatici di cui ci siamo occupati. In questo caso, essendo che la condotta viene realizzata tramite strumenti tecnologici, la responsabilità potrebbe risalire al programmatore, installatore ed infine all'ente (anche attraverso l'art. 8 del decreto 231[85]), colpevole di non aver presieduto a questi processi o di non aver predisposto le adeguate contromisure tecnologiche.

In primo luogo, l'IA potrebbe avere delle ricadute sulla ridefinizione dei compiti organizzativi degli amministratori. Gli studiosi prospettano l'entrata dell'IA nei consigli di amministrazione come sostegno ai vertici nello svolgimento della loro attività. Un esempio è il *software* Corptech. La tecnologia potrebbe aiutare gli amministratori nell'adempiere ai loro obblighi informativi o, più in generale, nell'attuazione di processi di *governance* e sistemi di controllo. In sintesi, l'IA parrebbe poter sollevare gli amministratori dai compiti di *compliance*. Da ciò potrebbe derivare, innanzitutto, una rimodulazione della responsabilità degli amministratori: la diligenza, la correttezza e l'obbligo di agire informati andrebbero valutati anche alla luce delle conoscenze acquisibili tramite questi sistemi[86]. Con particolare riferimento all'obbligo di dotare la società di assetti organizzativi adeguati (art. 2086 c.c.), sorge la questione se l'algoritmo possa essere visto come un requisito da integrare necessariamente nell'organizzazione, o se il ricorso a una tecnologia in grado di individuare tempestivamente dei segnali di allarme possa incidere sul corretto adempimento di tali obblighi organizzativi. La risposta

[85] S. PREZIOSI, *Responsabilità da reato degli enti e intelligenza artificiale* in Rivista 231, n. 4/2020
[86] Cfr. L. ENRIQUES, *Governance* societaria algoritmica e responsabilità degli amministratori in *XXVI Lezioni di diritto dell'intelligenza artificiale* a cura di RUFFOLO U., Chieri, Giappichelli editore, 2021; L. ENRIQUES, *Responsabilità degli amministratori e ruolo degli algoritmi: brevi annotazioni sul senno di poi 4.0* in Intelligenza artificiale: il diritto, i diritti e l'etica, Milano, Giuffrè, 2020

che si tende attualmente a dare a un tale quesito è negativa. Ma, nella misura in cui la *compliance* digitale prometta di conferire maggiore effettività ai presidi organizzativi, questa conclusione non può essere ritenuta definitiva. Non appare dunque prematuro chiedersi se possano esserci riflessi sulla responsabilità penale degli amministratori, in particolare sulla responsabilità omissiva dei membri non esecutivi del CdA. Difatti, poiché il *software* "prescrive" azioni capaci di intervenire in tempo reale sulle fonti di rischio, la tecnologia pare accorciare la "distanza organizzativa" tra condotta omissiva e reato non impedito. Le possibili ripercussioni di tutto ciò sull'imputazione dell'evento non sono inimmaginabili: il sistema informatico potrebbe individuare l'azione doverosa, supponendone l'efficacia "impeditiva", e potrebbe favorire la percezione di segnali di allarme, o comunque suscitare, in eventuali inquirenti, l'impressione che tali segnali fossero evincibili da un suo corretto utilizzo. Si pensi, ad esempio, all'applicazione di tecnologie come *machine learning* e *deep learning* nella scoperta degli indici predittivi d'insolvenza e alle ripercussioni che l'impiego di tali sistemi potrebbe avere, in futuro, nella ricostruzione delle responsabilità per omesso impedimento dei reati di bancarotta. Deve invece escludersi che alla IA possa essere conferita una delega di funzioni, come pure che un sistema informatico possa essere nominato amministratore di società (al di là di qualche noto caso mediatico), per le stesse problematiche messe in luce nel paragrafo precedente, infatti, non avendo il sistema capacità giuridica, non possono essergli attribuiti quei requisiti soggettivi di indipendenza, diligenza etc. riferibili agli amministratori[87]. In sostanza, non è ammissibile un "*roboboard*", ma, lo sviluppo dell'IA rende ipotizzabile la creazione di *board* di (umani) esperti di nuove tecnologie nell'ambito del CdA. Ci possiamo, pertanto, chiedere se sarebbe possibile sostituire l'Organismo di vigilanza (previsto dall'art. 6 d.lgs. 231/2001) con un sistema informatico basato sull'IA. Invero, le stesse ragioni che si oppongono alla creazione di un *roboboard* vietano l'istituzione di un "OdV algoritmico". L'OdV (composto da umani) potrebbe, tuttavia, dotarsi di tecnologie in grado di individuare rischi di non conformità del MOG, nel modo più rapido ed efficace. Come pure, non escludono che, nelle realtà di ridotte dimensioni, nelle quali il compito della vigilanza sul modello può essere assunto dagli

[87] A. NISCO, *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022

stessi amministratori, questi ultimi debbano adempiervi sulla base dei più avanzati sistemi tecnologici.

Infine, l'impiego dell'IA potrebbe avere delle ricadute sulla colpa di organizzazione. Su questo tema valgono le considerazioni effettuate nel corso del capitolo 3 a cui rinvio. In primo luogo, la circostanza che una *corporation* possa scegliere di affidarsi integralmente a *software* algoritmici potrebbe mettere in crisi il criterio soggettivo di imputazione dell'illecito all'ente, la colpa di organizzazione. Infatti, nel caso in cui la commissione del reato presupposto dipenda dalla mancata segnalazione di quel determinato ambito di rischio da parte della macchina, ad esempio, per un difetto di progettazione o funzionamento non ascrivibile all'ente il concetto di rimproverabilità soggettiva risulterebbe svuotato. Il soggetto collettivo si è limitato ad adottare un *software* prodotto da altri e la colpa di organizzazione si ridurrebbe alla erronea scelta del *software* o alla decisione stessa di automatizzare in toto la *compliance*[88]. Ciò che è importante tenere presente è la necessità di un bilanciamento che consenta di impiegare l'IA per innalzare l'efficacia preventiva dei modelli organizzativi, senza sacrificare la corretta allocazione della responsabilità del soggetto collettivo. Occorre, per affermare la responsabilità dell'ente, verificare l'esistenza di un contributo specifico di quest'ultimo. Sarebbe opportuna l'introduzione di una disciplina specifica affinché l'ente che si adoperi nella prevenzione del rischio possa nutrire una ragionevole aspettativa, in ottica premiale, di andare esente da responsabilità[89].

3. Che cosa ci aspettiamo dal futuro?

Siamo giunti al termine di questo lavoro d'indagine. Concludiamo questo lavoro ripercorrendo gli interrogativi e le aspettative dei giuristi nelle tematiche da noi analizzate.

Grazie alle sentenze della Corte Edu e della Corte di giustizia abbiamo notato la scarsa rilevanza data, spesso, dagli Stati al diritto alla vita privata e alla protezione dei dati personali con normative che consentivano, di fatto, una conservazione generalizzata dei

[88] P. SEVERINO, Intelligenza artificiale e diritto penale in Intelligenza artificiale- il diritto, i diritti l'etica a cura di Ugo Ruffolo, Milano, Giuffrè, 2020, Pag. 538
[89] P. SEVERINO, Intelligenza artificiale e diritto penale in Intelligenza artificiale- il diritto, i diritti l'etica a cura di Ugo Ruffolo, Milano, Giuffrè, 2020, Pag. 540

dati. Le condanne hanno dato un nuovo indirizzo in materia di *data retention* e per il futuro ci aspettiamo una maggiore sensibilità a queste tematiche, anche in vista dei nuovi rischi *privacy* sorti con l'impiego dei Big Data e dell'IA.

A livello nazionale, il legislatore, grazie anche all'impulso dato dagli atti emanati a livello europeo ha introdotto nel Codice penale nuove fattispecie poste a tutela della riservatezza e sicurezza informatica. In particolare, dalle ricerche condotte abbiamo appurato la frequenza con cui vengono realizzati accessi abusi ad un sistema informatico (art 615- ter c.p.), dato che ci fa comprendere come questo intervento fosse necessario. Tuttavia, le complesse questioni giurisprudenziali e le critiche mosse da autorevole dottrina, hanno messo in luce anche la necessità di una revisione delle fattispecie. Il legislatore, intervenuto nel 2021, tuttavia, non è riuscito a cogliere questa profonda esigenza di riforma e le modifiche introdotte non sono riuscite a dissipare i dubbi che con molta probabilità si riproporranno nelle aule di giustizia.

Altra complessa questione a cui nel corso di questo lavoro abbiamo cercato di rispondere, grazie al supporto delle sentenze della Corte di Cassazione e della dottrina è quella relativa all'individuazione del *locus commissi delicti,* nei reati informatici. L'ambientazione di tali problematiche è quella delineata da A. Garapon nella sua ultima opera, "La despazializzazione della giustizia", in cui analizza gli sconvolgimenti prodotti dalla globalizzazione, dalla rivoluzione digitale e dalla crisi sanitaria. Sconvolgimenti che provocano una rivoluzione nel rapporto tra diritto e spazio. L'ultimo intervento della Corte di Cassazione, da noi analizzato non è riuscito a spegnere il dibattito e sebbene autorevole dottrina abbia proposto una soluzione inedita, basata su un'interpretazione evolutiva del principio di territorialità che potrebbe incontrare vasto consenso, date le difficoltà nella trattazione del tema, sarebbe sicuramente opportuno un intervento legislativo che consideri le peculiari caratteristiche dei *cybercrimes*.

Per quanto attiene alla materia della responsabilità da reato degli enti, a più di vent'anni dalla sua introduzione sono tanti i dubbi che animano gli studiosi. Dal futuro ci aspettiamo che gli enti percepiscano la *cybersecurity* come un valore aggiunto e questo consenta di prevenire i reati informatici che mettono a rischio la *privacy* degli individui. Sicuramente, gli strumenti sovranazionali da noi analizzati, hanno dato un impulso in questo senso, introducendo sanzioni e obblighi che tuttavia, non riguardano in senso stretto reati

presupposto del decreto 231, ma in via più generale gli incidenti informatici. Quello che possiamo evincere da questo lavoro è, tuttavia, l'assenza di parametri certi che siano di aiuto alle imprese nella costruzione dei modelli di organizzazione e gestione e che riescano ad orientare i giudici nel giudizio di idoneità ed efficacia del MOG. Proprio su questo punto abbiamo cercato di intervenire al fine di individuare le misure che in concreto consentano la prevenzione di tale tipo di reati. Per il futuro possiamo pensare a *compliance program* integrati che tengano conto della prevenzione dei reati informatici, degli incidenti informatici in senso ampio presi in considerazione dagli strumenti sovranazionali e nazionali e infine delle problematiche legate alla *privacy*. Peraltro, anche in questo campo si auspica un'armonizzazione a livello europeo e sovranazionale, al fine di semplificare i contenziosi riguardi le imprese nell'attuale mercato globalizzato.

Infine, nelle conclusioni di questo lavoro abbiamo delineato le ricadute che l'intelligenza artificiale ha avuto e avrà nelle tematiche di nostro interesse e le questioni aperte dall'impiego di queste avanzate. Sebbene risulti difficile mettere dei punti fermi in materia, l'IA offre interessanti spunti di riflessioni. I dati sono il nuovo petrolio e l'IA si serve di grandi masse di dati, i *Big data* per funzionare. I beni giuridici tradizionali e di nuovo conio (riservatezza informatica e sicurezza informatica) sono, pertanto, esposti a nuovi rischi. Non sappiamo se le previsioni di Hawking si concretizzeranno e il futuro sarà dominato dai *robot.* Quello che è certo, è che l'Intelligenza viene già impiegata nelle organizzazioni pubbliche e private, fornendo un valido supporto alle attività, ma mettendo in pericolo la *privacy* di ciascuno di noi. Come accaduto per il *computer* e *Internet*, si pongono complesse pertanto questioni di bilanciamento tra diritti fondamentali. Delicate, inoltre, le questioni legate ai profili di responsabilità penale delle persone fisiche e di responsabilità da reato degli enti. Quello che abbiamo imparato nel corso di questo lavoro, è che quando si parla di tecnologia, guardare alla tematica da una prospettiva internazionale risulta imprescindibile. Ci aspettiamo, pertanto, una forte cooperazione tra gli Stati e una disciplina quanto più armonizzata a livello europeo e internazionale.

Bibliografia

ACCIAI R., *Il diritto alla protezione dei dati personali*, Santarcangelo di Romagna, Maggioli editore, 2004

ACCINNI G.P., *L'oggettiva incertezza della valutazione di idoneità dei modelli organizzativi* in La resp. amm. delle soc. e degli enti, n. 4/2018

ACCORDATI A., *Una sconfitta (di misura) in tema di controllo sulla dosimetria sanzionatoria: nota a Corte cost. n. 117/2021* in iusinitinere.it, 12 ottobre 2021

AETERNO S., Commento sub art. 4 alla legge 48/2008 in *Cybercrime, Responsabilità degli enti e prova digitale* a cura di CORASANITI G. e CORRIAS LUCENTE G., Padova, Cedam, 2009.

AETERNO S., *Le fattispecie di danneggiamento informatico* in *Sistema penale e criminalità informatica* a cura di L. Luparia, Milano, Giuffrè, 2009

AETERNO S., CUNIBERTI M., GALLUS G.B., MICOZZI F.P, *Cybercrimine: prime note sulla legge di ratifica della Convenzione di Budapest* in altalex.com, 8 maggio 2008

AETERNO S., *Aspetti problematici dell'art. 615-quater c.p.* in *Cassazione penale*, n.4/2000

AGNINO F., *Cybersecurity: le novità della legge n. 133/2019* in Ilpenalista.it, 2019

ALESSANDRI A., *Attività di impresa e responsabilità penali*, in Riv. it. dir. proc. pen., 2005

ALMA M. M. PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici* in Diritto penale e processo, n.4/1997

AMODIO P., *Digital compliance: spunti di riflessione e di riforma sui controlli di prevenzione e protezione dell'O.D.V*. in filodiritto.com, 7 giugno 2021

AMODIO E., *Rischio penale d'impresa e responsabilità degli enti nei gruppi multinazionali*, in Rivista italiana di diritto e procedura penale, 2007

ANTOLISEI F., *Manuale di diritto penale*, Milano, Giuffrè, 2016

APARO M. FUCITO F., *I reati presupposto* in *Trattato di diritto penale d'impresa* a cura di D'AVIRRO A. DI AMATO A., Lavis, CEDAM, 2009

AULETTA T., *Riservatezza e tutela della personalità*, Milano, Giuffrè, 1978.

BADODI D., Commento sub art 24-ter d.lgs 231/2001 in *Enti e responsabilità da reato a cura* di CADOPPI A. GARUTI G. VENEZIANI P, Torino, Utet giuridica, 2010

BAFFA G. CECCHINI F., *Limiti spaziali di validità della responsabilità "da reato" degli enti: applicabilità del d.lgs. n. 231/2001 all'ente "italiano" per reato commesso all'estero e all'ente "straniero" per reato commesso in Italia* in Giurisprudenza penale web, n. 7-8/2018

BALBONI P. TUGNOLI F., *Reati informatici e tutela dei dati personali: profili di responsabilità degli enti* in Giurisprudenza penale n. 1-bis/2021

BALZANO A., *Tutela della Sicurezza Pubblica vs Tutela della Privacy: un bilanciamento necessario* in diritto.it, 20 ottobre 2020

BAMBERGER K.A., *Technologies of Compliance: Risk and Regulation in a Digital Age* in Texas Law Rev., 88, 4, 2010,

BARBIERI A., *Whistleblowing e internal investigation: una prospettiva di collaborazione dell'ente* in sistema penale web, n. 6/2020

BARTOLI R., *Il criterio di imputazione oggettiva* in *Responsabilità da reato degli enti*, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020

BASILE F., *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine* in diritto penale e uomo, 20 settembre 2019

BASSI A. D'ARCANGELO F., *Il sistema della responsabilità da reato dell'ente: disciplina e prassi applicativa*, Giuffrè, 2020

BASSINI M. POLLICINI O., *La corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico* in Diritto penale contemporaneo, 9 gennaio 2017

BASTIA P., *I modelli organizzativi dei gruppi internazionali* in *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2021, n. 231*, Milano, Giuffrè editore, 2010

BELLACOSA V., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in Diritto penale contemporaneo, 2 febbraio 2015

BELLOCCI M., MAGNANESI S., PASSAGLIA P., RISPOLI E., *Tutela della vita privata: realtà e prospettive costituzionali* in Quaderno predisposto in occasione dell'incontro trilaterale delle Corti costituzioni spagnola, portoghese e italiana, Lisbona,1° –4 ottobre 2006 disponibile online https://www.cortecostituzionale.it/documenti/convegni_seminari/STU_190_Vita_privata.pdf

BELLUTA H., *Cybercrime e responsabilità degli enti* in *Sistema penale e criminalità informatica* a cura di Luparia L., Milano, Giuffrè, 2009.

BELTRANI S., *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della convenzione di Budapest* in La responsabilità amministrativa delle società e degli enti fasc. 4/2008

BERGHELLA F. BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici* in Cassazione penale, n.9/1995, pag. 2329

BERTI R. ZUMERLE F., *Rider, no a discriminazioni dell'algoritmo: il Garante privacy sanziona Glovo per 2,6 milion*i in cybersecurity360, 9 luglio 2021

BERTOLESI R., *Intelligenza artificiale e responsabilità penale per danno da prodotto,* 2019 (tesi di dottorato di Diritto penale nell'ambito del Corso di dottorato di ricerca in Scienze Giuridiche "Cesare Beccaria" dell'Università degli Studi di Milano - Curriculum di diritto penale e processuale penale - XXXII ciclo).

BERTOLESI R., *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere* in diritto penale contemporaneo, fasc. 10/2017

BERTOLUCCI M.A., *L'art. 8 d.lgs. 231/2001 nel triangolo di Penrose* in Diritto penale contemporaneo, 9 gennaio 2017

BETTINI M.N., *Impianti audiovisivi e strumenti di controllo fra esigenze aziendali e tutela della sfera personale del lavoratore* in Annali 17/2016, Napoli, Editoriale scientifica, 2016

BIRRITTERI E., *Controllo a distanza del lavoratore e rischio penale* in sistema penale web, 16 febbraio 2021

BIRRITTERI E., *Big data analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri* in Diritto penale contemporaneo n. 2/2019

BLAIOTTA R., *L'organismo di vigilanza: struttura, funzione e responsabilità* in sistema penale web, 16 novembre 2021

BLONDA D., *La disciplina della privacy nel panorama internazionale* in jei.it, 1 agosto 2006

BOMBELLI G. COSTA P. PIZZOLATO F., *Sicurezza e tecnologia*, Giuffrè, Milano, 2017

BONGIORNO G., Organismo di Vigilanza ex 231: natura e responsabilità in diritto.it, 28 dicembre 2018

BORGOBELLO M., *Il reato di accesso abusivo a sistema informatico di cui all'art. 615-ter c.p. alla luce della giurisprudenza più recent*e in Giurisprudenzapenale.com, 21 febbraio 2021.

BORRUSO R. BUONOMO G. CORASANITI G. D'AIETTI G., *Profili penali dell'informatica*, Milano, Giuffrè, 1994

BORSARI R., *Intelligenza Artificiale e responsabilità penale: prime considerazioni* in medialaws, 3 novembre 2019

BRASCHI S., *La consumazione del reato,* Milano, Cedam, 2020

BRAVO F., *Indagini informatiche e acquisizione della prova nel processo penale* in Rivista di Criminologia, Vittimologia e Sicurezza v.3, n. 3, settembre 2009

BRIGHI R. e CHIARA P., *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea* in federalismi.it, 8 settembre 2021.

BRIZZI F., *Privacy: la tutela penale dei dati personali*, Milano, Giuffrè, 2020

BRIZZI F, *Privacy* in Ilpenalista.it, 2019

BURCHARD C., *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società* in Rivista italiana di diritto e procedura penale, n. 4/2019

CAGGIANO G., *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione* in rivista di diritto dei media, n. 2/2018

CALDIROLA D, *Il diritto alla riservatezza*, Padova, Cedam, 2006

CAPITANI F.G., *Il reato informatico si verifica nel luogo dell'accesso abusivo e non in quello di ubicazione del server* in Diritto & Giustizia, fasc.18/2015

CAPPELLINI A., *Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale* in disCrimen, 27 marzo 2019

CAPUZZO G., "*Do Algorithms dream about Electric Sheep?" Percorsi di studio in tema di discriminazione e processi decisori algoritmici tra le due sponde dell'Atlantico* in www.medialaws.it

CAROTTI B., *La Corte di Giustizia costruisce un ponte tra riservatezza e comunicazioni elettroniche*, Giornale di diritto amministrativo, n. 4/2017.

CAROTTI B., *Il caso Schrems, o del conflitto tra riservatezza e sorveglianza di massa* in Giornale di diritto amministrativo, n. 3/2016

CASELLATO M., DI MAIO A., LA MUSCATELLA A., *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali* in Cassazione Penale, fasc.7, 1° luglio 2019

CATAUDELLA A, *La tutela civile della vita privata*, Milano, Giuffrè, 1972

CATERINI M., *La proporzione nella dosimetria della pena da criterio di legiferazione a canone ermeneutico* in antoniocasella.eu

CECCACCI G., *Limiti di spazio della responsabilità da reato degli enti: Il reato commesso in Italia nell'interesse o a vantaggio di società avente sede all'estero* in Cassazione Penale, fasc.12/2020

CENTONZE F- MANTOVANI M., *Dieci proposte per una riforma del d. lgs. n. 231/2001*, in La responsabilità "penale" degli enti. Dieci proposte di riforma, Bologna, Il Mulino, 2016

CENTONZE F., *Il problema della responsabilità penale degli organi di controllo per omesso impedimento degli illeciti societari (Una lettura critica della recente giurisprudenza)* in Riv. Soc., fasc. 2-3/2012

CERQUA F., *Commento sub art. 6 del d.lgs 231/2001* in Enti e responsabilità da reato a cura di CADOPPI A. GARUTI G. VENEZIANI P, Torino, Utet giuridica, 2010

CERQUA F., *Commento sub art. 7 del d.lgs 231/2001* in *Enti e responsabilità da reato a cura* di CADOPPI A. GARUTI G. VENEZIANI P, Torino, Utet giuridica, 2010

CIAMPI C., *Cybersecurity: Politiche globali, Compliance normativa, Logiche organizzative e modelli di gestione* in Rivista elettronica di diritto, economia e management, n. 3/2013

CIRILLO G.P., *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Cedam, Padova, 2004

CHARRIE A., DU CROO DE JONGH L. ROY S. QUEST L., *The Risks and Benefits of Using AI to Detect Crime*, in *Harvard Business Review* (https://hbr.org/), August 9, 2018.

COLACURCI M.; *L'idoneità del modello nel sistema 231, tra difficoltà operative e possibili correttivi* in Dir. pen. cont., n. 2/2016

COLAPIETRO C. GIUBILEI A., *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della cassazione* in *Labour & Law Issues*, vol. 7, n.2/2021

COLAROSSI E. CORTINOVIS J., *I modelli organizzativi in Spagna*, in Resp. amm. soc. enti, n.4/2016

CONSULICH F., I*l principio di autonomia della responsabilità dell'ente. Prospettive di riforma dell'art. 8* in La responsabilità amministrativa delle società e degli enti - 4/2018

CONSULICH F., *Vigilantes puniri possunt. I destini dei componenti dell'Organismo di vigilanza tra doveri impeditivi e cautele relazionali* in Riv. trim. dir. pen. econ. 3/2015

CONTALDO A. MULA D., *Cybersecurity law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, Pacini giuridica, 2020

CONTALDO A. PELUSO F., *Cybersecurity: la nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa, Pacini Giuridica, 2018

CORASANTI G., *La tutela penale dei sistemi informativi e telematici* in privacy.it

CORASANITI G., *Commento sub Art. 1 alla legge 48/2008* in *Cybercrime, Responsabilità degli enti e prova digitale* a cura di CORASANITI G. e CORRIAS LUCENTE G., Padova, Cedam, 2009.

CORN E., Il principio di precauzione nel diritto penale, Torino, Giappichelli, 2013

CORRIAS LUCENTE G., *Commento sub Art. 7 alla legge 48/2008* in *Cybercrime, Responsabilità degli enti e prova digitale* a cura di CORASANITI G. e CORRIAS LUCENTE G., Padova, Cedam,2009.

COZZA M. ONORATI C. O., *I reati in tema di comunicazioni* in *Diritto penale dell'informatica* a cura di PARODI C., SELLAROLI V., Giuffrè, Milano, 2020

CRIMI S., *Commento sub art 24 bis d. lgs. 231/2001* in *Enti e responsabilità da reato* a cura di Cadoppi A. Garuti G. Veneziani P., Lavis, Utet giuridica, 2010.

CRISCUOLO C. "*Potere di controllo e computer aziendale"* in Rivista italiana di diritto del lavoro, n.2/2019

CUOMO I., IZZI B., *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in Cass. pen., fasc.3/2002

CUOMO L., *Accesso abusivo a sistema informatico e competenza territoriale* in Ilpenalista.it, 24 giugno 2015

CUOMO N., TRIBERTI C., *Criminalità informatica: approvata la legge* in Il corriere giuridico, n. 5/1994

D'ADAMO V., *L'accesso abusivo ad un sistema informatico o telematico effettuato da soggetto munito di chiave d'accesso* in Archivio Penale, n.2/2011.

D'ARCANGELO F., *La introduzione di uno standard legale per la valutazione di idoneità dei modelli organizzativi* in La responsabilità amministrativa delle società e degli enti, n.4/2018

D'ARCANGELO F., I canoni di accertamento dell'idoneità del modello organizzativo nella giurisprudenza, in La resp. amm. delle soc. e degli enti, n.2/2011

D'AVIRRO A., *I modelli organizzativi. L'organismo di vigilanza* in Trattato di diritto penale dell'impresa. Vol. X, a cura di A. D'Avirro- A. D'Amato, Padova, CEDAM, 2009

DEL PUNTA R., "*La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 151/2015)"* in Rivista italiana di diritto del lavoro, n.1/2016

DE MARCHI P.G., *I nuovi reati informatici*, Torino, Giappichelli editore, 2009

DE MARTINO P., *Le sezioni unite sul luogo di consumazione dell'accesso abusivo a un sistema informatico* in Diritto penale contemporaneo web, 11 maggio 2015

DE ROBBIO C. AGNINO F, *I reati informatici in ambito aziendale* in "*Diritto penale dell'informatica: reati della rete e sulla rete"* a cura di C. Parodi e V. Bellaroli, Milano, Giuffrè, 2020

DE ROBBIO C., *Giurisdizione e competenza in materia penale* in Giur. merito, fasc.12/2013

DE SIMONE G., *La responsabilità da reato degli enti: natura giuridica e criteri oggettivi di imputazione* in Diritto penale contemporaneo web

DE STEFANIS R., *Profili di responsabilità dell'Organismo di Vigilanza ai sensi del d.lgs. 231/2001* in Danno e responsabilità, n.4/2010

DESTITO V.S., DEZZANI G., SANTORIELLO C., *Diritto penale delle nuove tecnologie*, Padova, Cedam, 2007

DE VERO G*., Struttura giuridica e natura giuridica dell'illecito di ente collettivo dipendente da reato: luci e ombre nell'attuazione della delega legislativa* in Riv. it. dir. e proc. pen., fasc.4/2001

DEZZANI G., PICCINNI L., *La società connessa: problematiche legate alla sicurezza aziendale e alle necessità di prevenzione dei reati presupposto* in La responsabilità amministrativa degli enti, fasc. 1/2011

DEZZANI G., PICCINNI L., *Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito di applicazione del d.lgs. 231/2001* in La responsabilità amministrativa degli enti, fasc.2/2011

DEZZANI G., *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica* in La responsabilità amministrativa delle società e degli enti, fasc. 1/2012

DEZZANI G. SANTORIELLO C., *Il reato di accesso e trattenimento abusivi nel sistema informatico e responsabilità amministrativa delle persone giuridiche* in La responsabilità amministrativa delle società e degli enti, fasc.1/2012

DEZZANI G. DELL'AGNOGNOLA L*., L'implementazione del modello organizzativo, gestionale di controllo negli enti collettivi a seguito dell'inserimento di reati informatici fra i reati presupposto ex d.lgs. 231/2001 operato dalla legge 48/2008* in La responsabilità amministrativa degli enti, fasc. 3/2009

DIAMANTIS M.E., *The Extended Corporate Mind: When Corporations Use AI to Break the Law* in scholarship.law.unc.edu

DI GIOVINE O., *Il criterio di imputazione soggettiva* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020

DI GIOVINE O., *Lineamenti sostanziali del nuovo illecito punitivo* in *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2021, n. 231*, Milano, Giuffrè editore, 2010

DI LANDRO, A.C., *Big data: rischi e tutele nel trattamento dei dati personali*, Napoli, Edizioni scientifiche italiane, 2020

DI MAIO F., Certificazioni di *information security: analisi di supporto per le finalità esimenti de modello organizzativo* in *Cybercrime e responsabilità da reato degli enti* a cura di A. MONTI, Lavis, Giuffrè, 2022

DI VETTA G., *Il giudice border guard nei «grandi spazi»: prospettive critiche intorno alla responsabilità degli enti*, in Giurisprudenza Penale Web, n-1-bis/2021

DI VETTA G., *La responsabilità degli enti nella prospettiva dei «grandi spazi» Profili transnazionali del d.lgs. n. 231/2001* in Archivio penale, n. 1/2021

DOGLIAN M., *Il volto costituzionale della sicurezza* in astrid-online.it

ENRIQUES L., *Governance* societaria algoritmica e responsabilità degli amministratori in *XXVI Lezioni di diritto dell'intelligenza artificiale* a cura di RUFFOLO U., Chieri, Giappichelli editore, 2021

ENRIQUES L., *Responsabilità degli amministratori e ruolo degli algoritmi: brevi annotazioni sul senno di poi 4.0* in Intelligenza artificiale: il diritto, i diritti e l'etica, Milano, Giuffrè, 2020

FENUCCI T., *Quanto spazio c'è per un diritto individuale della sicurezza nell'ordinamento costituzionale italiano?* in federalismi.it, 2015

FIANDACA G. MUSCO E., *Diritto penale: parte generale*, Bologna, Zanichelli, 2019

FIANDANESE C, *Criminalità informatica* in Ilpenalista.it, 2018

FINOCCHIARO G., *Intelligenza artificiale e responsabilità* in Contratto e impresa n.2/2020

FINOCCHIARO G., *La memoria della rete e il diritto all'oblio* in Il diritto dell'informazione e dell'informatica, n.3/2010

FIORELLA A. SELVAGGI N., *Compliance programs e dominabilità aggregata del fatto. Verso una responsabilità da reato dell'ente compiutamente personale* in Diritto penale contemporaneo, n. 3-4/2014

FLICK M.G., *Giustizia penale ed economia pubblica e privata: profili problematici* in Cassazione Penale, fasc.10, 1° ottobre 2017

FLICK M.G., *Le prospettive di modifica del d.lgs. n. 231/2001, in materia di responsabilità amministrativa degli enti: un rimedio peggiore del male* in Cass. pen., fasc.11/2010

FLOR R., *Data retention e giustizia penale in Italia* in *"Diritto penale dell'informatica: reati della rete e sulla rete*" a cura di C. Parodi e V. Bellaroli, Milano, Giuffrè, 2020

FLOR R., *Cyber-criminality: le fonti internazionali ed europee* in *Cybercrime* a cura di Cadoppi A, Canestrari S., Manna A., Papa M., Milano, Utet giuridica, 2019

FLOR R., *La legge penale nello spazio, fra evoluzione tecnologia e difficoltà applicative* in *Cybercrime* a cura di Cadoppi A, Canestrari S., Manna A., Papa M., Milano, Utet giuridica, 2019

FLOR R., *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di Internet*, n. 3/2019

FLOR R., *La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere* in Diritto penale e processo n.4/2018

FLOR R., "*Riservatezza informatica*" in treccani.it, 2017

FLOR R., "*Diritto penale e controlli a distanza dei lavoratori dopo il c.d. Jobs Act*" in *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act* a cura di LEVI A., Milano, Giuffré, 2016

FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle sezioni unite* in Diritto penale e processo, n. 10/2015

FLOR R., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?* in Diritto dell'informazione e dell'informatica n. 4/2014

FLOR R., *Art 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico* in Diritto penale e processo, n.1/2008

FLOR R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente* in Riv. it. dir. e proc. pen., fasc.2-3/2007

FLOR R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios* in Diritto penale e processo n.1/2005

FONDAROLI D., *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001* in *Cybercrime* a cura di Cadoppi A, Canestrari S., Manna A., Papa M., Milano, 2019, Utet giuridica

FONDAROLI D., *La tutela penale dei "beni informatici"* in Diritto dell'informazione e dell'informatica, 1996, pagg. 291-322

FORMICI G., *Lavoratori e tutela della privacy: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza* in Osservatorio costituzionale, fasc. 1/2018

FORNARI G. ANGIULI E. ATTANASIO D., *Cybercrimes e responsabilità da reato degli enti: rischi penali e prevenzione* in fornariassociati.com, luglio 2020

FRAGASSO B. FUSCO E., *Sul presunto obbligo di impedimento in capo all'organismo di vigilanza: alcune note a margine della sentenza BMPS* in Sistema penale web, n. 10/2020

FRANZONI M., *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale* in Juscivile.it, 2021

FROSINI T.E., *Diritto all'oblio e Internet* in Federalismi.it, n.1/2014

FROSINI T.E., *Il diritto costituzionale della sicurezza,* in forumcostituzionale.it

FUMO M., La condotta nei reati informatici in "Archivio penale", aa. LXV, n.3/2013

GALANTE A., *L'overruling delle Sezioni unite in tema di accesso abusivo ad un sistema informatico* in Giurisprudenza italiana, n. 3/2018

GALDIERI P., *Il domicilio informatico: l'interpretazione dell'articolo 615-ter c.p. tra ragioni di carattere sistematico e "forzature"* in Dir. informatica, fasc.1/2013

GARAPON A., *La despazializzazione della giustizia*, Milano, Mimemis edizioni, 2021

GARGANI A., *Imputazione del reato agli enti collettivi e responsabilità penale dell'intraneo: due piani irrelati?* in Dir. pen. proc., fasc. 9/2002

GASTALDO F.C., *Lo statuto della giustizia digitale nella Carta etica della CEPEJ* in iusinitinere.it, 2 aprile 2021

GAZZETTA C., *Sicurezza, terrorismo e cittadinanza: la nuova legislazione francese antiterrorismo e l'impegno internazionale contro i cd. foreign fighters*, in Democrazia e sicurezza, n. 3/2015

GHINI P. MAGLIO M., *Smart working: opportunità e criticità tra riservatezza delle informazioni e controlli a distanza* in La responsabilità amministrativa delle società e degli enti, fasc. 3/2020

GHINI M. LEDDA F., *L'importanza della regolamentazione dell'uso degli strumenti elettronici, di internet e della posta elettronica in azienda, anche ai fini della prevenzione della responsabilità amministrativa da reato informatici* in La responsabilità amministrativa delle società e degli enti, fasc. 3, vol.4, 2009

GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa* in Diritto penale contemporaneo, 29 maggio 2019

GIANNINI A., *Lombroso 2.0: On AI and Prediction of Dangerousness* in Criminal Justice in RIDP, vol.92/2021

GIAVAZZI A., *Poteri e autonomia dell'Organismo di Vigilanza: prime incertezze, nuove incertezze*, in Le soc., n. 11/2012

GIUNTA F., *Controllo e controllori nello specchio del diritto penale societario*, Riv. trim. dir. pen. econ., 2006

GIUPPONI T.F., *Sicurezza personale, sicurezza collettiva e misure di prevenzione. La tutela dei diritti fondamentali e l'attività di intelligence* in forumcostituzionale.it

GRAMANO E., La rinnovata ed ingiustificata vitalità della giurisprudenza in materia di controlli difensivi in Diritto delle relazioni industriali, n.1/2018

GRASSO G. ROMANO M., *Commentario sistematico del Codice penale*, Milano, Giuffrè, 2012

GROTTO M., *La rilevanza penale del controllo datoriale attraverso gli strumenti informatici* in *Il diritto dell'informatica e dell'informazione*, anno XXX, fasc. 1/2014

GULLO A., *I reati informatici* in *Responsabilità da reato degli Enti: diritto sostanziale* a cura di LATTANZI G. SEVERINO P., Lavis, Giappichelli Editore, 2020

GULLO A., *I modelli organizzativi* in Responsabilità da reato degli enti, vol.1 a cura di LATTANZI G.- SEVERINO P., Lavis, Giappichelli editore, 2020

HOBBES T., *Il Leviatano*, 1651.

IMBRUGLIA D., *L'intelligenza artificiale (IA) e le regole* in medialaws.eu, 24 dicembre 2020

INGRAO A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata* in *Diritto e processo del lavoro* collana diretta da BARBIERI M., DALFINO D., LECCESE V., PINTO V., TRISORIO LIUZZI G., VOZA R., Cacucci editore, Bari

LA MANNA A., *La c.d. responsabilità amministrativa delle persone giuridiche: il punto di vista del penalista*, in Rivista trimestrale di diritto penale dell'economia, n. 3/2003

LANDI D., *Il rispetto del d.lgs. 231/2001 nelle imprese multinazionali operanti in Italia*, in Rivista 231, n. 2/2019

LANZIERI M., *I nuovi reati informatici*, Milano, Altalex editore, 2010

LASCO G., Commento sub art. 8 d.lgs. 231/2001 in *Enti e responsabilità da reato* a cura di LASCO G., LORI V., MORGANTE M., Trofarello, Giappichelli Editore, 2017.

LASCO G., Commento sub art. 7 d.lgs. 231/2001 in *Enti e responsabilità da reato* a cura di LASCO G., LORI V., MORGANTE M., Trofarello, Giappichelli Editore, 2017.

LA ROSA M., *Teoria e prassi del controllo interno ed esterno sull'illecito dell'ente collettivo* in Riv. it. dir. e proc. pen., fasc.4, 2006

LEDDA F., GHINI P., *Normativa sulla responsabilità amministrativa degli enti e normativa sulla privacy: punto di contatto* in La responsabilità amministrativa delle società e degli enti, fasc. 3, vol.4, 2009

LEONCINI, *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, Giappichelli, 1999

LETIZI M. SOANA G., *Le potenzialità del modello di corporate compliance integrato basato sulla tecnologia blockchain* in Il sole 24 ore, 21 dicembre 2020

LIMITI C., *Intelligenza Artificiale: implicazioni etiche in materia di privacy e diritto penale* in iusinitinere.it, 9 febbraio 2021

LOCKE J., *Secondo trattato sul governo*, 1689.

LORIA V., Commento sub art. 24-bis d.lgs. 231/2001 in *Enti e responsabilità da reato* a cura di LASCO G., LORI V., MORGANTE M., Trofarello, Giappichelli Editore, 2017.

LORUSSO S. RICCI A. E., *Le novità del pacchetto sicurezza- I profili processuali* in Diritto penale e processo, fasc. n. 12/2008

LUPARIA L., *La ratifica della convenzione cybercrime del consiglio d'Europa- I profili processuali* in Diritto penale e processo, fasc. n. 6/2008

LUPARIA L., *Processo penale e tecnologia informatica* in Diritto dell'Internet, fasc. 3/2008

MANACORDA S., *Limiti spaziali della responsabilità degli enti e criteri di imputazione*, in Rivista italiana di diritto e procedura penale, n. 1/2012

MANCINI L.V. PAGNOTTA G., *Cyberattack: tecniche di prevenzione, rilevazione e mitigazione* in *Cybercrime e responsabilità da reato degli enti* a cura di A. MONTI, Lavis, Giuffrè, 2022

MANES V., *Realismo e concretezza nell'accertamento dell'idoneità del modello organizzativo* in Giurisprudenza Commerciale, fasc.4, 1 agosto 2021

MANES V.- TRIPODI A*., L'idoneità del modello organizzativo* in "*La responsabilità penale degli enti: dieci proposte di riforma*" a cura di CENTONZE F.- MANTOVANI M., Bologna, Il mulino, 2017

MANTOVANI F., *Diritto penale: delitti contro la persona*, Milano, Cedam, 2019

MANTOVANI M., *Il d.lgs. 231/2001 e gli incentivi alla persona giuridica: il punto di vista dell'impresa* in "La responsabilità penale degli enti: dieci proposte di riforma" a cura di CENTONZE F.- MANTOVANI M., Bologna, Il mulino, 2017

MANTOVANI F., *Causalità, obbligo di garanzia e dolo nei reati omissivi* in Riv. it. dir. e proc. pen., fasc.4, 2004

MANTOVANI F., *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, di solidarietà, di libertà e di responsabilità personale* in Riv. it. dir. e proc. pen., fasc.2/2001

MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica* in Critica del diritto, n. 4/1994

MANZARI M., *La convenzione di Budapest: l'alba di una normativa di contrasto al cybercrime* in bptmavvocati.it

MARINUCCI G. DOLCINI E. GATTA G.L., *Diritto penale parte generale*, Milano, Giuffrè, 2021

MARINUCCI G. DOLCINI E., *Trattato di diritto penale parte speciale*, Vicenza, Cedam, 2015

MARINUCCI G., "*Societas puniri potest": uno sguardo sui fenomeni e sulle discipline contemporanee,* in Riv. it. dir. proc. pen., fasc. 4/2002

MARTINELLI S., *Il controllo a distanza del lavoratore e le nuove tecnologie* in Ciberspazio e diritto, vol. 16, n. 53/2015

MARTORANA M., *Intelligenza Artificiale e diritto penale, la risoluzione del Parlamento europeo* in altalex.com, 12 novembre 2021

MARTORANA M., *Fine del Privacy Shield: la Corte di Giustizia invalida la decisione di adeguatezza* in Altalex.com, 5 agosto 2020.

MASSARO A., *Diritto penale e privacy*, Pisa, Pacini Giuridica, 2020

MASSARO A., *Principio di precauzione e diritto penale: nihil novi sub sole?* in penalecontemporaneo.it, 9 maggio 2011

MAUGERI A.M*., L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali* in Archivio penale 2021, n.1

MAZZACUVA F., *La diversione processuale per gli enti collettivi nell'esperienza anglo-americana* in Dir. pen. con. n. 2/2016

MAZZACUVA N., *Alcune riflessioni su intelligenza artificiale e diritto penale sostanziale* in *XXVI Lezioni di diritto dell'intelligenza artificiale* a cura di RUFFOLO U., Chieri, Giappichelli editore, 2021

MELIS F., *Il diritto all'oblio e i motori di ricerca nel diritto europeo* in Giornale di diritto amministrativo, n.2/2015

MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in "*Rivista trimestrale di diritto penale dell'economia"*, 1992, pagg 365-377

MINUCUCCI G., *Reati informatici e responsabilità degli enti: vecchi e nuovi scenari* in disCrimen, 29 aprile 2022

MIRAGLIA V., *Il controllo a distanza dell'attività dei lavoratori: il limite invalicabile* in Giurisprudenza italiana, giugno 2018

MONDINI RUSCONI, *Big data. Privacy, gestione e tutele*, Altalex editore, Milano, 2018

MONGILLO V., *Presente e futuro della compliance penale* in sistema penale web, 11 gennaio 2022

MONGILLO V., *Imprese multinazionali, criminalità transfrontaliera ed estensione della giurisdizione penale nazionale: efficienza e garanzie "prese sul serio"*, in Giornale di diritto del lavoro e di relazioni industriali, n. 2/2021

MONGILLO V., *La responsabilità penale tra individuo ed ente collettivo*, Torino, Giappichelli, 2018

MONGILLO V., *La vigilanza sull'attuazione del sistema aziendale di prevenzione dei reati in Italia e nei principali ordinamenti ispanoparlanti: circolazione dei modelli e specificità nazionali* in Dir. pen. cont.- Riv. Trim., 3/2018

MONGILLO V., *L'Organismo di vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche* in Resp. amm. delle società e degli enti, n. 4/2015

MONGILLO V., *Il dovere di adeguata organizzazione della sicurezza tra responsabilità penale individuale e responsabilità da reato dell'ente: alla ricerca di una plausibile differenziazione* in AA.VV., Infortuni sul lavoro e doveri di adeguata organizzazione: dalla responsabilità penale individuale alla «colpa» dell'ente, a cura di A.M. Stile - A. Fiorella - V. Mongillo, Napoli, Jovene editore, 2014.

MONGILLO V., *Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione* in La responsabilità amministrativa della società e degli enti, fasc. 3/2011

MONGILLO V., *Profili critici della responsabilità da reato degli enti alla luce dell'evoluzione giurisprudenziale* in La responsabilità amministrativa della società e degli enti, fasc.4/2009

MONTALENTI P., *Organismo di vigilanza e sistema dei controlli* in Giur. comm., fasc.4/2009.

MONTE N. VACIAGO G., *Informatica e tutela della riservatezza* in *Diritto penale dell'informatica* a cura di PARODI C. SELLAROLI V., Milano, Giuffrè, 2020

MONTERIN A., *Dell'incertezza nei trasferimenti di dati personali verso gli Stati Uniti*, la Nuova Giurisprudenza Commentata, n. 1/2021.

MONTESQUIE, *Lo spirito delle leggi*, 1748.

MORSELLI C., *Accesso abusivo a un sistema informatico e telematico: un'analisi critica rispetto all'interpretazione giurisprudenziale,* in Ilpenalista.it, 2020

MORALE PRATS F., *Presupposti politico criminali per una tutela penale della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo),* in Diritto dell'informazione e dell'informatica, n.2/1986

MUCCIARELLI F., *Ricomporre il nesso spezzato: giurisdizione e legge applicabile alle imprese multinazionali* in Rivista delle Società, fasc.2-3, 1 aprile 2021

MUCCIARELLI F., *Una progettata modifica al d.lgs. n. 231/01: la certificazione del modello come causa di esclusione della responsabilità* in Le società, n. 10/2020

MUCCIARELLI F., *Il fatto illecito dell'ente e la costituzione di parte civile nel processo ex d.lgs. 231/2001*, in Dir. pen. proc., n. 4/2011.

MUCCIARELLI F., *I computer-crimes nel disegno di legge 1657/1984*, in Rivista italiana di diritto e procedura penale, 1986

MUSCO E., *Le imprese a scuola di responsabilità tra pene pecuniarie e misure interdittive*, in Dir. e giust., n. 23/2001

NAPOLETANO N., *Omesso impedimento del reato e illecito amministrativo dell'ente: quale responsabilità per l'Organismo di Vigilanza in caso di omesso o insufficiente controllo?* in giurisprudenzapenale.com, n. 3/2020

NATALINI A., "*Giro di vite" sui reati informatici, spettro applicativo ad ampio raggio* in Guida al diritto, n. 7, 26 febbraio 2022

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, CEDAM, 2006

NISCO A., *Riflessi della compliance digitale in ambito 231* in sistemapenale.it, 14 marzo 2022

NISCO A., *Prospettive penalistiche del controllo a distanza sull'attività lavorativa nell'attuale contesto normativo e tecnologico* in sistemapenale.it, 20 dicembre 2021

NISCO A., *Compliance e posizioni di garanzia: prime indicazioni dalla giurisprudenza tedesca*, in Cass. pen., n. 6/2010

NISCO A., *Controlli sul mercato finanziario e responsabilità penali*, Bologna, 2009

NISCO A., *Responsabilità amministrativa degli enti: riflessioni sui criteri ascrittivi soggettivi e sul nuovo assetto delle posizioni di garanzia nelle società`*, in Riv. trim. dir. pen. econ., n. 1-2/2004

NOCERA A, *Whistleblowing. Primi orientamenti giurisprudenziali e prospettive di tutela europea*, in Ilpenalista.it, 2018

ONORATI C. O., COZZA M. F., *I reati in tema di comunicazione* in *Diritto penale dell'informatica: reati della rete e sulla rete* a cura di C. Parodi e V. Bellaroli, Milano, Giuffrè, 2020

ORDILE A., *Le nuove frontiere del diritto penale dell'informatica* in osservatoriopenale.it

OROFINO M., *Diritto alla protezione dei dati personali e sicurezza*, in medialaws.eu, 2018.

PADOVANI T., *La disciplina italiana della responsabilità degli enti nello spazio transnazionale* in Riv. It. Dir. Proc. penale, n. 2/2021

PADUA G., *Intelligenza artificiale e giudizio penale: scenari, limiti e prospettive* in processo penale e giustizia, n.6/2021

PALIERO C.E., *La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale* in Riv. trim. dir. pen. econ., n. 1-2/2018

PALIERO C. E., *Soggettivo e oggettivo nella colpa dell'ente: verso la creazione di una "gabella delicti"?* in Le società, n.11/2015

PALIERO C.E., *Responsabilità degli enti e principio di colpevolezza al vaglio della Cassazione: occasione mancata o definitivo de profundis?* In Le società 4/2014

PALIERO C.E., *La società punita: del come, del perché, e del per cosa* in Riv. it. dir. e proc. pen., fasc.4, 2008

PALIERO C.E., *Il d.lgs. 8 giugno 2001, n. 231: da ora in poi, societas delinquere (et puniri) potest*, in Corr. giur., 2001

PANATTONI B., *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale* in diritto dell'informatica, fasc.2/2021

PAONESSA C*., Il ruolo dell'organismo di vigilanza nell'implementazione dei modelli organizzativi e gestionali nella realtà aziendale* in La giustizia penale, fasc. VII, LUGLIO 2014.

PAPA M., *Future crimes: intelligenza artificiale e rinnovamento del diritto penale* in Criminalia, 4 marzo 2020

PARODI C., SELLAROLI V., *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco* in Diritto penale contemporaneo, fasc. 6/2019

PASCARELLI R., Commento sub art. 8 del d.lgs. 231/2001 *in Enti e responsabilità da reato* a cura di CADOPPI A. GARUTI G. VENEZIANI P, Torino, Utet giuridica, 2010

PECORELLA C., *Reati informatici*, in Enc. Dir., Annali X, 2017

PECORELLA C., *Impiego dell'elaboratore sul luogo di lavoro e tutela penale della privacy* in www.penalecontemporaneo.it

PECORELLA C., *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico* in Diritto penale contemporaneo, 11 ottobre 2013

PECORELLA C, *L'attesa pronuncia delle sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo* in Cassazione penale n.11/2012

PECORELLA C, *Diritto penale dell'informatica*, Padova, Cedam, 2006

PERRIONE F., *Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Bărbulescu 2* in *Labor: il lavoro nel diritto*, 23 febbraio 2018

PESTELLI G., *Brevi note in tema di accesso abusivo ad un sistema informatico o telematico* in *Cassazione Penale* n. 6/2012

PETRINI D., *La responsabilità penale per i reati via internet*, Napoli, Casa editrice Jovene, 2004

PICA G., *Diritto penale delle tecnologie informatiche*, Torino, Utet, 1999

PICOTTI L., *I delitti informatici previsti dal d.lgs. 231/2001* in *Cybercrime e responsabilità da reato degli enti* a cura di A. MONTI, Lavis, Giuffrè, 2022

PICOTTI L., *Cybercrime e diritto penale* in *Diritto penale dell'informatica: reati della rete e sulla rete* a cura di C. Parodi e V. Bellaroli, Milano, Giuffrè, 2020

PICOTTI L., *Reati informatici, riservatezza, identità digitale* in www. aipdp.it, 2020

PICOTTI L., FLOR R., SALVADORI I., *Reati contro la riservatezza e la sicurezza informatiche, nonché l'identità digitale* in www. aipdp.it, 2020

PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme* in *Cybercrime* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M.*, Milano, Utet giuridica, 2019

PICOTTI L. – VADALÀ R.M., *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in sistema penale web, 5 dicembre 2019

PICOTTI L., *La tutela penale della persona e nuove tecnologie*, Padova, CEDAM, 2013

PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali* in Giurisprudenza di merito, fasc.12/2012

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa* in Diritto penale e processo, n.6/2008

PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale* in Diritto dell'internet, n. 2/2005

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

PICOTTI L., *Profili penali delle comunicazioni illecite via internet* in Dir. informatica, fasc.2, 1999

PIERGALLINI C., *La "maggiore età" della responsabilità dell'ente: nodi ermeneutici e pulsioni di riforma* in Archivio penale, n.1/2021

PIERGALLINI C., *La gestione ermeneutica del rischio normativo internazionale nel contesto della responsabilità da reato degli enti* in Le società n.3/2021

PIERGALLINI C., *Intelligenza artificiale: da mezzo ad autore del reato?* In Rivista Italiana di Diritto e Procedura penale, fasc. 4/2020

PIERGALLINI C., *Globalizzazione dell'economia, rischio reato e responsabilità ex crimine delle multinazionali* in Riv. trim. dir. pen. econ., n. 1-2/2020

PIERGALLINI C., *Premialità e non punibilità nel sistema della responsabilità degli enti* in Diritto penale e processo, n. 4/2019

PIERGALLINI C., Voce "Colpa" in Enciclopedia del diritto, Annali X, 2017

PIERGALLINI C., *Autonormazione e controllo penale* in Diritto penale e processo, n.3/2015

PIERGALLINI C, *I delitti contro la riservatezza informatica* in *Trattato di diritto penale parte speciale* a cura di G. Marinucci E. Dolcini, Vicenza, CEDAM, 2015.

PIERGALLINI C., *I delitti contro la riservatezza della corrispondenza e delle comunicazioni* in *Trattato di diritto penale parte speciale* a cura di G. Marinucci E. Dolcini, Vicenza, CEDAM, 2015

PIERGALLINI C., *Paradigmatica dell'autocontrollo penale* (parte II) in Cass. pen., fasc.2, 2013

PIERGALLINI C., *Paradigmatica dell'autocontrollo penale*, (parte I), in Cass. pen., fasc.1, 2013

PIERGALLINI C., *I modelli organizzativi* in Reati *e responsabilità degli enti. Guida al d.lgs. 8 giugno 2021, n. 231*, Milano, Giuffrè editore, 2010

PIERGALLINI C., *I reati presupposto della responsabilità dell'ente e l'apparato sanzionatorio* in *Reati e responsabilità degli enti. Guida al d.lgs. 8 giugno 2021, n. 231*, Milano, Giuffrè editore, 2010

PIERGALLINI C., *Societas delinquere et puniri non potest: la fine tardiva di un dogma*, in Riv. trim. dir. pen. econ., 2002

PIERGALLINI C., *La disciplina della responsabilità amministrativa delle persone giuridiche e delle associazioni* in Diritto Penale e Processo, n. 11/2001

PISANI N., *Struttura dell'illecito e criteri di imputazione* in *Trattato di diritto penale d'impresa* a cura di A. D'AVIRRO e A. DI AMATO, Verona, Cedam, 2009

PISANI V., *I requisiti di autonomia e indipendenza dell'Organismo di Vigilanza istituito ai sensi del d.lgs. 231/2001*, in La resp. amm. delle soc. e degli enti, n.1/2008

PIZZETTI F., *La decisione della corte di giustizia sul caso Google Spain: più problemi che soluzioni* in Federalismi.it, n. 1/2014

PLANTAMURA V., *La tutela penale delle comunicazioni informatiche e telematiche* in Diritto dell'informatica, n.6/2006

POLICELLA E.O., *Il controllo dei dipendenti tra Codice privacy e Statuto dei lavoratori* in Il lavoro nella giurisprudenza n. 10/2004

POLIDORO D., *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale* in Archivio penale n. 3/2020

POLLICINO O., *Corte di giustizia e giudici nazionali: il moto "ascendente", ovverosia l'incidenza delle "tradizioni costituzionali comuni" nella tutela apprestata ai diritti dalla - dell'Unione* in Consulta Online, n.3/2015.

POLLICINO O., *Un digital right to privacy preso troppo sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain* in Diritto dell'informatica e dell'informazione, n. 4/2014

POLLICINO O., *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale* in Federalismi.it, n.3/2014

POSTIGLIONE A., *Riflessioni in tema di organizzazione e di controlli nell'ipotesi di adozione di un modello integrato di gestione dei rischi di data breach e cyber breach* in La resp. amm. delle società e degli enti, fasc. 4, vol. 15, 2020

PRESSACO L., *La relazione annuale del membro nazionale italiano presso Eurojust (2020)* in Cassazione Penale, fasc.6, 1 giugno 2021, pag. 2199

PREZIOSI S., *Responsabilità da reato degli enti e intelligenza artificiale* in Rivista 231, n. 4/2020

PRINCIPATO G., *La imperfetta sovrapponibilità della giurisdizione per le persone fisiche e per gli enti stranieri: riflessioni a margine di una sentenza della cassazione sull'art. 4 d.lgs. 231/2001* in sistemapenale web, 6 maggio 2020

PULITANÒ D., *Diritto penale: tutela della persona*, Torino, Giappichelli editore, 2019

PULITANÒ D., *La responsabilità da reato degli enti: i criteri di imputazione* in Riv. it. dir. e proc. pen., fasc.2, 2002

PULITANÒ D., Voce "*la responsabilità amministrativa degli enti*" in Enciclopedia del diritto, aggiornamento VI, 2002

QUATTROCOLO S., *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche* in La legislazione penale, 22 marzo 2018

RAZZANTE R. CRISTALLINI A., *Cybercrime. Tra economia e diritto*, Pisa, Pacini editore, 2021

RAMIREZ BARBORSA P.A; *Corporate criminal law, artificial intelligence and big data: the Huawei case and its implications for global society* in rivistas.unaerp.br

RENNA V. C., *La vigilanza ex d.lgs. 231/2001 e la privacy GDPR* in Amministrazione e contabilità dello Stato e degli enti pubblici, 14 luglio 2021

RESTA F., *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura* in Giurisprudenza di merito, fasc. 9/2008

RICCARDI M., *L'internazionalizzazione della responsabilità "231" nel processo sulla strage di Viareggio: gli enti con sede all'estero rispondono per l'illecito da reato-presupposto "nazionale"* in giurisprudenza penale web, n.1/2018

RIZZI R. VENTURA A., *La tutela della privacy del lavoratore controllato a distanza, alla luce della nuova disciplina sulla protezione dei dati personali* in fondazionenazionalecommercialisti.it

RODOTÀ S., *Riservatezza* in enciclopedia treccani.it

RODOTÀ S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice della privacy*, in "*Europa e diritto privato*", 2004

RODOTÀ S., *Tecnologie e diritti*, Bologna, Il mulino, 1995

ROMOLOTTI T.E., *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001* in Rivista231, n. 1/2020

RORDOF R., *L'Organismo di vigilanza nel quadro del D.lgs. n. 231/2001* in Le società n.1/2022

ROSSI S., *Tutela della riservatezza e limiti ai controlli difensivi* in Giurisprudenza italiana, febbraio 2018

RUBECHI M, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni* in federalismi.it, n. 23/2016

RUGGIERO G., *Brevi note sulla validità della legge punitiva amministrativa nello spazio e sulla efficacia dei modelli di organizzazione nella responsabilità degli enti derivante da reato,* in Riv. Trim, di Dir. Pen. Dell'Economia, 3-4, 2004

RUGGIERO V., *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in Giurisprudenza di merito, n. 1/2002

RUTA G., *La responsabilità amministrativa degli enti stranieri e i limiti del principio di territorialità* in La responsabilità amministrativa delle società e degli enti, n. 4/2018

SACCHI R., *L'organismo di vigilanza ex d. lgs. n. 231* in Giur. comm., fasc.6, 2012.

SALCUNI G., *La valutazione di idoneità dei modelli ed il requisito dell'elusione fraudolenta* in Riv. trim. dir. pen. econ. 4/2015

SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale* in Rivista italiana di diritto e procedura penale, fasc.1/2021

SALVADORI I., *I reati contro la riservatezza informatica* in "*Cybercrime"* a cura di *Cadoppi A, Canestrari S., Manna A., Papa M.*, Milano, Utet giuridica, 2019

SALVADORI I., *L'Accesso abusivo a un sistema informatico o telematico: una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica* in *Tutela della persona e delle nuove tecnologie* a cura di L. Picotti, Padova, CEDAM, 2013

SALVADORI I., *Quando un insider accede abusivamente a un sistema informatico o telematico? Le sezioni unite precisano l'ambito di applicazione dell'art. 615- ter c.p.*, in Rivista semestrale di diritto penale dell'economia, 2012, n. 1-2

SALVADORI I., *L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cracking* in Rivista italiana di diritto e procedura penale, 2008

SANTORIELLO C., *I reati informatici e la responsabilità delle società ex d.lgs. 231/2001* in La responsabilità amministrativa delle società e degli enti, fasc. 1, vol. 15, 2020

SANTORIELLO C., *La condanna dell'ente in caso di mancata individuazione del soggetto colpevole del reato: da previsione inapplicabile a norma sanzionatoria della colpa di organizzazione* in La responsabilità amministrativa delle società e degli enti fasc. 4, vol. 11/2016

SANTORIELLO C., *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti* in La responsabilità amministrativa delle società e degli enti, fasc. 3/2009

SASSI V., *Sicurezza cibernetica e responsabilità ex D.lgs. 231/2001: la nuova fattispecie del D.L. 105/2019*, in quotidianogiuridico.it, 9 ottobre 2019

SCAFFARDI L., *Data retention e diritti della persona*, costituzionalismo.it, fasc. 2/2017

SCALISI A., *Il diritto alla riservatezza*, Milano, Giuffrè editore, 2002

SCARCELLA A., *La c.d. "internazionalizzazione" della responsabilità da reato degli enti* in La resp. amm. delle soc. e degli enti, n.1/2014

SCAROINA E., *Prospettive di razionalizzazione della disciplina dell'oblazione nel sistema della responsabilità da reato degli enti tra premialità e non punibilità* in Dir. pen. con. n. 2/2020

SCAROINA E., *Verso una responsabilizzazione del gruppo di imprese multinazionali?* in diritto penale contemporaneo, 23 luglio, 2018

SCIUBA M.L., *Osservazioni a Cass. Pen., 26 marzo 2015, sez. UU, N. 17325* in Cassazione Penale, n.10/2015

SEMINARA S., *Locus commissi delicti, giurisdizione e competenza nel cyberspace* in flamminiiminuto-chiocci.it

SEMINARA S. *La responsabilità penale degli operatori su internet* in juseinternet.it, 19 gennaio 2000

SEVERINO P., *Intelligenza artificiale e diritto penale* in Intelligenza artificiale: il diritto, i diritti e l'etica, Milano, Giuffrè, 2020

STAMPACCHIA E., *La responsabilità amministrativa degli enti con sede all'estero* in archiviodpc.dirittopenaleuomo.org, 4 ottobre 2013

STIANO A., *Ancora sul bilanciamento tra la tutela del diritto alla privacy e l'utilizzo di strumenti di sorveglianza di massa: tra garanzie procedurali e sostanziali* in rivista di diritto internazionale, n.3/2021

STUMPO G.R., *Verso un sistema armonizzato della certificazione della sicurezza cyber di prodotti, processi e servizi ITC. Analisi del Regolamento UE 2019/881,* in ictsecurirymagazine.com, 25 maggio 2020

TEDESCHI C., *Cybersecurity, tutela dei dati personali e prevenzione dei reati nelle società di capitali: possibilità di un modello di organizzazione e gestione del rischio articolato e collegato* in La resp. amm. delle società e degli enti, fasc. 4, vol. 15, 2020

TEROLLI E., *Privacy e protezione dei dati personali UE vs. USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II",* Diritto dell'informatica e dell'informazione, fasc. 1, 1 febbraio 2021

TOSI E., *Privacy digitale*, Milano, Giuffrè, 2019

TRAVERSI A., *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice robot?* in questionegiustiza.it

TREZZA R., *L'intelligenza artificiale come ausilio alla standardizzazione del modello 231: vantaggi possibili e rischi celati* in giurisprudenza penale web, n.1-bis/2021

TREVISI C., *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo* in medialaws.eu, 25 giugno 2018

TRIPODI A. F., *Il diritto penale degli enti nello spazio: deantropomorfizzazione e globalizzazione a confronto* in archiviopenale.it n.1/2019

TRONCONE P, *La tutela penale della riservatezza e dei dati personali*, Napoli, Edizioni scientifiche, 2020

TRONCONE P, *Il delitto di trattamento illecito dei dati personali*, Torino, Giappichelli editore, 2011

TROJSI A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo* in dirittifondamentali.it, fascicolo 2/2020

TUFO M., *Potere di controllo datoriale vs. privacy del lavoratore: alla ricerca delle coordinate di ammissibilità dei controlli occulti* in Studium iuris, n.7-8/2020

UBALDI A., *Accesso abusivo e detenzione/diffusione di codici di accesso: concorso apparente di reati* in Diritto & Giustizia, fasc. 91/2019

UBERTAZZI T.T., *Il diritto alla privacy: natura e funzioni giuridiche,* Padova, Cedam, 2005

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

VALERIANI A., *NIS 2: verso una nuova strategia in ambito cybersecurity,* in Iusintinere.it, 28 dicembre 2020

VELIA L., *Commento sub art. 24-bis del d.lgs. 231/2001* in *Enti e responsabilità da reato* a cura di Lasco G., Velia L., Morgana M., Torino, Giappichelli Editore, 2017

VENEZIANI P., Commento sub art. 5 del d.lgs 231/2001 in *Enti e responsabilità da reato* a cura di CADOPPI A. GARUTI G. VENEZIANI P, Utet giuridica, Torino, 2010

VIZZARO D., *I reati informatici nell'ordinamento italiano* in www.danilovizzaro.it

ZALIN M., *È opportuno introdurre un sistema di certificazione dei modelli 231?* in La responsabilità amministrativa delle società e degli enti, n. 4/2018

Giurisprudenza

ITALIANA

Tribunale di Milano, Sezione II penale, 7 aprile 2021 (ud. 15 ottobre 2020), n. 10748 in Giurisprudenza penale web

Tribunale Salerno sez. I, 17 gennaio 2020, n.166 in banca dati De Jure

Tribunale Milano sez. IV, 01 ottobre 2018, n.8862 in banca dati "De Jure"

Trib. Torino, sez. lav., 18 settembre 2018, n. 1664, in Riv. it. dir. lav., 2019, II.

Trib. Lucca, 31 luglio 2017, n. 222 in giurisprudenzapenale.com

Tribunale Roma, 16 aprile 2014 in banca dati De Jure

Tribunale Bari sez. uff. indagini prel., 11 dicembre 2009 in banca dati De Jure

Corte appello Bologna sez. II, 27 marzo 2008 in banca dati DeJure

Corte di appello di Bologna, 30 gennaio 2008, in Guida al diritto, 48/2008

Tribunale Nola, sez. uff. indagini prel., 14 dicembre 2007, n.488 in banca dati De Jure

Tribunale Nola, 11 dicembre 2007 in banca dati De Jure

Tribunale Milano sez. II, 28 settembre 2007 in banca dati De Jure

Tribunale Milano sez. III, 19 marzo 2007 in banca dati De Jure

Tribunale di Milano, 28 luglio 2006 in banca dati DeJure

Tribunale Torino, 20 giugno 2006 in banca dati De Jure

Tribunale Bologna sez. I, 22 dicembre 2005, n.1823 in banca dati DeJure

Tribunale Trapani, 22 dicembre 2005 n. 892 in banca dati De Jure

Tribunale Bologna, 21 luglio 2005, n.1823 in banca dati DeJure

Tribunale Viterbo, 05 luglio 2005 in banca dati De Jure

Tribunale La Spezia, 23 settembre 2004 in banca dati DeJure

Tribunale di Milano, 27/04/2004, (ord.) GIP Salvini – Imp. Siemens A.G in olympus.uniurb.it

Tribunale Torino, 30 settembre 2002 in banca dati De Jure

Tribunale Milano, 10 maggio 2002 in banca dati De Jure

Tribunale Torino, 08 aprile 2002 in banca dati DeJure

Corte appello Milano, 15 giugno 2001 in banca dati DeJure

Tribunale Milano, 10 ottobre 2000 in banca dati Dejure

Tribunale di Milano, 14 marzo 2000 in banca dati Dejure

Cass., Ufficio del Massimario e del Ruolo, relazione alla legge 23 dicembre 2021, n. 238, 21 marzo 2022 in sistemapenale.it

Cass. pen., sez. VI, 23 novembre 2021 n. 5541 in banca dati DeJure

Cass. pen., sez. IV, 20 maggio 2021, n.30231 in banca dati DeJure

Cass. pen. sez. V, 30 aprile 2021, (ud. 30/04/2021, dep. 06/07/2021), n.25683 in banca dati DeJure

Cass. pen. sez. I, 27 aprile 2021, (ud. 27/04/2021, dep. 18/06/2021), n.24095 in banca dati DeJure

Cass. Sez. Lav., 22 settembre 2021, n. 25732 in wikilabour.it

Cass., sez. IV penale, sent. 8 gennaio 2021 (dep. 6 settembre 2021), n. 32899 in sistema penale web

Cass., sez. III, sent. 14 dicembre 2020 n., 3255 in sistemapenale.it

Cass. pen. sez. V, 29 settembre 2020, (ud. 29/09/2020, dep. 04/11/2020), n.30735 in banca dati De Jure

Cass. pen. sez. V, 19 febbraio 2020, n.17360 in banca dati De Jure

Cass. pen., sez. VI, 11 febbraio 2020, n. 116226 in sistema penale web

Cass. pen., sez. V, 30 settembre 2019, n.49142 in banca dati De Jure

Cass. 27 novembre 2019, n. 49775 in sistemapenale.it

Cass. pen., sez. V, 22 novembre 2019, (ud. 22/11/2019, dep. 27/01/2020), n.3236 in banca dati De Jure

Cass. pen., sez. II, 29 maggio 2019, n.26604 in banca dati De Jure

Cass. pen., sez. V, 25 marzo 2019, n.18284 in banca dati De Jure

Cass. pen., sez. V, 27 febbraio 2019, n. 8541 in fglaw.it

Cass. pen., 14 gennaio 2019, n.21987, sez. II in banca dati DeJure

Cass. pen., sez. V, 02 ottobre 2018, n.2905 in banca dati De Jure

Cass. pen., sez. VI, 25 settembre2018, n.54640 in banca dati DeJure

Cass. pen., sez. V, 09 luglio 2018, n. 47510 in banca dati DeJure

Cass. pen., sez. IV, 23 maggio 2018, (ud. 23/05/2018, dep. 09/08/2018), n.38363 in banca dati De Jure

Cass. pen., sez. V, 24 aprile 2018, n. 37857 in banca dati DeJure

Cass. pen., sez. V, 16 aprile 2018, (ud. 16/04/2018, dep. 12/09/2018), n.40470 in banca dati DeJure

Cass. pen., sez. V, 23 marzo 2018, n.20485 in banca dati De Jure

Cass. pen., sez. III, 28 febbraio 2018, n. 9072 in iusinitinere.it

Cass. pen, sez. III, 31 gennaio 2018 in Giurisprudenza italiana, giugno 2018

Cass. pen., sez. II, 9 gennaio 2018 n. 295 in dpei.it

Cassazione civile, sez. lav., 10 novembre 2017, n. 26682 in Giurisprudenza italiana, febbraio 2018

Cass. pen., sez. II, 5 ottobre 2017 n. 295 in dpei.it

Cass. pen., sez. VI, 13 settembre 2017 n. 41768 in giurisprudenzapenale.com

Cass., sez. unite, sent. 18 maggio 2017 n. 41210, in diritto penale contemporaneo, fasc. n. 10/2017

Cass. pen., sez. III, 24 febbraio 2017 n. 9132 in informaimpresa.it

Cass. pen. sez. V, 02 febbraio 2017, n.12603 in banca dati De Jure

Cass., sez. II pen., 9/12/2016, n. 52316 in banca dati De Jure

Cass. pen., Sez. 6, 07 luglio 2016, n. 28299 in olympus.uniurb.it

Cass. pen., sez. III, 8 settembre 2016, n. 51897 in De Jure

Cass. pen., sez. V, 18 dicembre 2015, (ud. 18/12/2015, dep. 29/01/2016), n.4059 in banca dati De Jure

Cass. pen., sez. V, 28 ottobre 2015, n.13057 in banca dati De Jure

Cass. pen., sez. V, 04 giugno 2015, n.34993 in banca dati De Jure

Cass. sez. lav. 27 maggio 2015, n. 10955 in adapt.it

Cass., sez. un., 26 marzo 2015, n. 17325 in eius.it

Cass. pen., sez. V, 30 gennaio 2015, n.29091 in banca dati De Jure

Cass. pen., sez. V., 20 giugno 2014, n. 44390 in sites.les.univr.it

Cass., sez. VI pen., 20 dicembre2013, n. 3635 in aodv231.it

Cass. pen., sez. V, 18 dicembre 2013 (dep. 30 gennaio 2014), n. 4677 in Diritto penale contemporaneo

Cass., 28 novembre 2013, n. 10265 in www.studiolegaletosello.it

Cass., 15 novembre 2013, n. 45969 in banca dati De Jure

Cass. pen., sez. II, 03 ottobre 2013, n.47021 in banca dati DeJure

Cass. pen., Sez. I, 27 settembre 2013 n. 40303 in penale.it

Cass., relazione n. III/01/2013 del 22 agosto 2013 in cortedicassazione.it

Cass. sez. 1, 27 maggio 2013 n. 40303 in banca dati De Jure

Cass. pen., Sez. V., 24 aprile 2013, n. 22024 in sites.les.univr.it

Cass., 1 ottobre 2012, n. 16622 in adapt.it

Cass., sez. 3, n. 23798 del 24 maggio 2012 in banca dati De Jure

Cass. 23 febbraio 2012, n. 2722 in avvocatomandico.it

Cass. sez. un., 7 febbraio 2012 n. 4694 in dirittopenalecontemporaneo.it

Cass. pen., sez. un., 27 ottobre 2011, n.4694 in banca dati De Jure

Cass. SS. UU., 29 settembre 2011, in banca dati De Jure

Cass. pen., sez. IV, 18 gennaio 2011, n.24583 in banca dati De Jure

Cass. pen., sez. VI, 13 ottobre 2010, n.38667 in banca dati De Jure

Cass. pen., sez. V, 10 dicembre 2009, n.2987 in banca dati De Jure

Cass. pe., sez. IV, 17 novembre, 2009, n. 36083 in olympus.uniurb.it

Cass. pen., sez. V, 13 febbraio 2009, n.18006 in banca dati De Jure

Cass. pen., sez. VI, 08 ottobre 2008, n.39290 in banca dati De Jure

Cass. pen., sez. V, 30 settembre 2008, n.1727 in banca dati De Jure

Cass. pen., sez. V, 08 luglio 2008, n.37322 in banca dati De Jure

Cass. pen., sez. V, 29 maggio 2008, n.26797 in banca dati De Jure

Cass. pen., sez. II, 21 febbraio 2008, n. 36721 in banca dati De Jure

Cass., sez. V, 20 dicembre 2007, n. 2534 in banca dati De Jure

Cass. pen., sez. V, 11 dicembre 2007 in Cass. pen., 2008, p. 4669

Cass. pen., sez. V, 06 febbraio 2007, n.11689 in banca dati De Jure

Cass. pen., sez. II, 30 gennaio 2006, n. 3615 in altalex.com

Cass., pen. sez. II, 20 dicembre 2005 n. 3615 in banca dati De Jure

Cass. pen., sez. V, 19 maggio 2005, n.4011 in banca dati De Jure

Cass. pen., sez. II, 17 dicembre 2004, n.5688 in banca dati DeJure

Cass. pen., sez. II, 17 gennaio 2003, n.36288 in banca dati DeJure

Cass. pen., Sez. Un., 10 luglio 2002, in Foro it.

Cass. pen., sez. V, 07 novembre 2000, n.12732 in penale.it

Cass. pen., sez. VI, 04/10/1999, n.3065 in banca dati De Jure

Cass. sez. I civile, 27 maggio 1975, n. 2129, Soraya Esfandiari c. Rusconi Editore in jstor.org

Corte cost., 15 maggio 2021 in www.cortecostituzionale.it

Corte cost., 23 gennaio 2019, n. 37, in www. cortecostituzionale.it

Corte cost. 15 luglio 2004, n. 222, in Giur. cost., 2004, pag. 2340 ss.

Corte cost. 10 aprile 2001, n. 105, in Giur. cost., 2001, pag. 675 ss.

Corte cost., 19-23 febbraio 1996, n. 42 in www.cortecostituzionale.it

Consiglio di Stato, sentenza 4-25 novembre 2021, n. 7891 in www.altalex.com

Consiglio di Stato, Sez. VI, Sent. 8 aprile 2019, n. 2270 in medialaws.it

Corte di giustizia dell'Unione Europea

Corte di giustizia dell'Unione europea, Grande sezione, 5 aprile 2022, G.D. c. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General, C-140/20, ECLI:EU:C:2022:258 in curia.europa.eu

Corte di giustizia dell'Unione Europea, Grande sezione, 6 ottobre 2020, La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net c. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées, C-511/18 e C-512/18, ECLI:EU:C:2020:791 in curia.europa.eu

Corte di giustizia dell'Unione Europea, Grande sezione, 16 luglio 2020, Data Protection Commissioner c. Facebook Ireland Ltd, C-311/18, ECLI: EU: C: 2020: 559 in curia.europa.eu

Corte di giustizia dell'Unione Europea, Grande sezione, 21 dicembre 2016, Tele2 Sverige AB (C-203/15) c. Post- och telestyrelsen e Secretary of State for the Home Department (C-698/15) c. Tom Watson, Peter Brice, Geoffrey Lewis, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970 in curia.europa.eu

Corte di giustizia dell'Unione europea, Grande sezione, Sent. 6 ottobre 2016, Maximillian Schrems c. Data Protection Commissioner, C-362/14, ECLI: EU:C: 2015:650 in eur-lex.europa.eu

Corte di giustizia dell'Unione europea, Grande sezione, sent. 13 maggio 2014, Google Spain SL e Google Inc. c. Agencia Espanola de Proteccion de Datos e Mario Costeja González, causa C-131/12, ECLI: EU:C: 2014:317, in curia.europa.eu

Corte di giustizia dell'Unione Europea, Grande sezione, Sent. 8 aprile 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Minister for justice, Equality and Law Reform e Commissioner of Garda Síochána e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a., cause riunite: C-293/12 e C- 594/12, ECLI:EU:C:2014:238 in eur-lex.europa.eu

Corte europea dei diritti dell'uomo

Corte europea dei diritti dell'uomo, Grande camera, 25 maggio 2021, caso *Big Brother watch and others v. The United Kingdom, 58170/13, 62322/14 and 24960/15* in https://hudoc.echr.coe.int/

Corte europea dei diritti dell'uomo, Grande camera, Lopez Ribalda e altri c. Spagna, 17 ottobre 2019 in rivistalabor.it

Corte europea dei diritti dell'uomo, Grande Camera, Barbulescu c. Romania, 5 settembre 2017 in rivistalabor.it

Corte europea dei diritti dell'uomo, Grande camera, 4 dicembre 2015, caso Roman Zakharov v. Russia, 47143/06, in federalismi.it

Corte europea dei diritti dell'uomo, terza sessione, 29 giugno 2006, Caso Weber e Saravia c. Germania 54934/00 in ilsa.org

Americana

Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis, Case no. 2015AP157-CR, 5 *April*-13 July 2016 in caselaw.findlaw.com

Supreme court of Georgia, Pavesich v. New England Life Insurance Company, 3 marzo 1905 in casetext.com

Sitografia

www.academia.edu

www.accademiadellacrusca.it

www.adapt.it

www.aipdp.it

www.altalex.com

www.aodv231.it

www.archiviodpc.dirittopenaleuomo.org

www.astrid-online.it

www.avvocatomandico.it

www.bptmavvocati.it

caselaw.findlaw.com

www.casetext.com

www.contabilita-pubblica.it

www.cortecostituzionale.it

www.costituzionalismo.it

www.curia.europa.eu

www.danilovizzaro.it

www.dirittifondamentali.it

www.diritto.it

www.discrimen.it

www.disf.org

www.dpc-rivista-trimestrale.criminaljusticenetwork.eu

www.dpei.it

www.eius.it

www.eur-lex.europa.eu

www.federalismi.it

www.fglaw.it

www.filodiritto.com

www.flamminiiminuto-chiocci.it

www.fondazionenazionalecommercialisti.it

www.fornariassociati.com

www.foro.it

www.forumcostituzionale.it

www.giurcost.org

www.giurisprudenzapenale.com

www.hbr.org

www.hudoc.echr.coe.int

www.ilpenalista.it

www.informaimpresa.it

www.ilsa.org

www.iusinitinere.it

www.jei.it

www.jstor.org

www.juscivile.it

www.medialaws.eu

www.olympus.uniurb.it

www.osservatoriopenale.it

www.penalecontemporaneo.it

www.privacy.it

www.quotidianogiuridico.it

www.riskcompliance.it

www.rivistalabor.it

www.rivistas.unaerp.br

www.rivista231.it

www.scholarship.law.unc.edu

www.sistemapenale.it

www.sites.les.univr.it

www.studiolegaletosello.it

www.treccani.it

www.unitelma.academia.edu

www.wikilabour.it

Banche dati

HeinOnLine

Ius Explorer

My desk 24

One Legale