LUISS

Dipartimento di Giurisprudenza

Cattedra di Diritto e Procedura Penale degli Enti

LA RESPONSABILITA' DEGLI ENTI NEI REATI INFORMATICI

Chiar.mo Prof.

Antonino Gullo

RELATORE

Chiar.ma Prof.ssa.

Maria Lucia Antonietta Di Bitonto

CORRELATORE

Saro Di Raimondo

CANDIDATO

matricola: 154253

Anno Accademico 2022/2023

SOMMARIO

INTRODUZIONE……...1

CAPITOLO I - IL SISTEMA NORMATIVO DI RESPONSABILITÀ DELL'ENTE NEL D.LGS. 231/2001

1 - La 231/2001: una svolta epocale per la responsabilità dell'ente 3

2 – Natura giuridica della responsabilità..... 13

3 - Criterio di imputazione all'ente: profili oggettivi..... 26

4 -Criterio di imputazione all'ente: profili soggettivi ed autonomia (art.8) 41

5 - Il modello organizzativo come elemento centrale..... 54

CAPITOLO II - IL MODELLO ORGANIZZATIVO E L'ORGANISMO DI VIGILANZA

1. Il ruolo del modello organizzativo e la cooperazione pubblico-privato..... 62

2. I contenuti del modello organizzativo nel d.lgs. 231/2001..... 71

3. Organismo di Vigilanza 86

3.1**(*segue*) Organismo di Vigilanza: i soggetti**..... 87

3.2**(segue) Organismo di Vigilanza: le funzioni** 93

4. La validazione giudiziale del modello.....100

5 - Dal d.lgs. 231/2001 alla responsabilità dell'ente per reati informatici.....103

CAPITOLO III - L'EVOLUZIONE DEL REATO INFORMATICO NEL NOSTRO SISTEMA PENALE

1 - Il crimine informatico 105

2 - la legge 547/1993 109

3 - la Convenzione di Budapest 113

4 – Il secondo protocollo della Convenzione di Budapest. La Convenzione Onu di Palermo. 119

5 - La legge 48/2008 e le modifiche del sistema penale 122

6 - La normativa europea successiva al Trattato di Lisbona. La Direttiva UE 2013/40 ...125

7 – Tipizzazione dei reati informatici e bene giuridico protetto 134

8 - I Reati informatici nel d. lgs. 231/2001 141

8.1 - Art 615-*ter*: accesso abusivo ad un sistema informatico o telematico 144

8.2 - Art.615-*quater*: detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici. 155

8.3 - Art.615-*quinquies*: detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico 157

8.4 - Art 635-*bis*: danneggiamento di informazioni, dati e programmi informatici 158

8.5 - Art.635-*ter:* danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità 163

8.6 - Art. 635-*quater* e *quinquies*: l'applicazione al sistema informatico. 165

8.7 - Art.640-*ter*: frode informatica 167

8.8 – Art.25-*novies*: delitti in materia di violazione del diritto di autore 172

CAPITOLO IV - OLTRE LA 231/2001: GLI ULTERIORI INTERVENTI NORMATIVI

1 - Oltre la 231/2001: gli ulteriori interventi normativi.....182

2 - Il Regolamento Generale sulla Protezione dei Dati (*GDPR*) 183

2.1 - Il sistema 231 ed il GDPR.....189

3 – Direttiva NIS I, NIS II.....193

4 - *Cybersecurity Act*.....196

5 - Il Perimetro di Sicurezza Nazionale Cibernetica.....199

6 - L'Agenzia per la *Cybersecurity* Nazionale.....203

CAPITOLO V - IL MODELLO ORGANIZZATIVO DELL'ENTE COME STRUMENTO PER LA RESISTENZA AL RISCHIO-REATO INFORMATICO

1. Il ruolo del modello organizzativo nei reati informatici 207

2. Il ruolo dell'Organismo di vigilanza nei reati informatici. Il Codice Disciplinare...212

3. La compatibilità dei meccanismi di controllo informatico con il GDPR e con la legge 20 maggio 1970 n. 300 e successive modifiche (*Jobs Act*) 213

4. La compatibilità dei meccanismi di intervento sul software con la violazione del diritto d'autore. 220

5. Rilievi conclusivi sui modelli di prevenzione del reato informatico 225

CONCLUSIONI.....234

INDICE BIBLIOGRAFICO.....236

INDICE GIURISPRUDENZA.....242

INTRODUZIONE

La responsabilità penale degli enti per i reati informatici è un tema complesso e sul quale si è iniziato a prestare particolare attenzione, nel nostro ordinamento, a partire dalla legge n. 48/2008, con la quale alcuni di tali delitti sono entrati a far parte del catalogo dei reati-presupposto di cui al d.lgs. n. 231/2001.

Un simile intervento ha tratto la sua linfa dall'acquisita consapevolezza circa la centralità delle aziende nella dinamica criminologica relativa ai reati informatici: invero, le stesse si possono presentare contemporaneamente come soggetti attivi (si pensi a reati-presupposto commessi a vantaggio dell'ente attraverso un uso improprio delle importanti banche dati di *consumers* presenti nelle proprie memorie), o come soggetti passivi – situazioni sempre più pericolose di *data breach* da parte di *hacker* esterni, particolarmente gravi se rivolte ad aziende che forniscono servizi essenziali in settori strategici (energia, comunicazioni).

Questo costringe continuamente ad operare su due fronti, da un lato quello della *cybersicurezza* basata su sistemi *IT* all'interno delle aziende, coordinati a livello nazionale o sovranazionale con obblighi di comunicazione ben precisi in caso di violazioni; e dall'altro, in termini di protocolli comportamentali e di *education* nei confronti dei dipendenti.

Tema centrale quindi anche a livello internazionale è quello della "sicurezza informatica", definita come "un bene giuridico strumentale alla protezione di un'ampia gamma di beni finali"[1]sottostanti (come la riservatezza, la fede pubblica, i dati personali), che viene messa sempre più in pericolo: il *Rapporto Clusit*[2] 2023 indica il 2022 come l'anno in cui è stato realizzato il maggior numero di attacchi

[1] Per approfondimenti in materia v. GULLO, *I reati informatici*, in LATTANZI - SEVERINO (a cura di), *Responsabilità da Reato degli Enti*, vol. I, Torino, 2020, 381 ss.

[2] Cfr. *Rapporto Clusit* 2022, Associazione Italiana per la Sicurezza Informatica: dal 2012 l'Associazione esamina dati relativi ad attacchi informatici andati a buon fine (quindi denunciati o comunque divenuti di pubblico dominio), *clusit.it.*

informatici, superiore anche alle proiezioni ricavabili da uno sviluppo tendenziale delle serie storiche precedenti.

L'obiettivo del presente elaborato è, dunque, quello di approfondire le tematiche legate alla responsabilità degli enti nei reati informatici, esaminando anche i meccanismi che possono consentire all'azienda di eliminare o attenuare la propria responsabilità, ottimizzando l'organizzazione interna.

A tal fine, l'analisi si svilupperà anzitutto lungo due direttrici: la prima, relativa al sistema 231/2001, come nucleo cardine per l'attribuzione di responsabilità alle persone giuridiche, con attenzione ai modelli organizzativi e all'organismo di vigilanza come strumenti operativi in grado di prevenire la realizzazione dell'illecito o esimere da responsabilità l'ente; la seconda, focalizzata invece sull'evoluzione della normativa dei reati informatici all'interno del nostro sistema, con specifico riguardo a quelli inseriti tra i reati-presupposto all'interno del d.lgs. 231/2001.

Successivamente, si passerà a evidenziare le interazioni fra sistema 231 e reati informatici attraverso l'analisi delle specificità del Modello Organizzativo applicato alla prevenzione dei reati informatici. In particolare, ci si confronterà con le delicate questioni che un modello organizzativo basato sul controllo delle attività informatiche può porre, impattando, se non correttamente calibrato, sia sulla normativa di salvaguardia prevista nello Statuto dei Lavoratori (e successiva modifica del *Job Act)*, sia sulle tematiche *privacy*, sia, infine, sulla stessa violazione del diritto di autore dei titolari del *software* che l'ente utilizza.

CAPITOLO I

IL SISTEMA NORMATIVO DI RESPONSABILITÀ DELL'ENTE NEL D.LGS. 231/2001

SOMMARIO: 1. La 231/2001: una svolta epocale per la responsabilità dell'ente. – 2. Natura giuridica della responsabilità – 3. Criterio di imputazione all'ente: profili oggettivi. - 4. Criterio di imputazione all'ente: profili soggettivi ed autonomia (art.8). – 5. Il modello organizzativo come elemento centrale.

1. La 231/2001: una svolta epocale per la responsabilità dell'ente

Sono passati più di venti anni dall'entrata in vigore del decreto legislativo 231/2001, che ha introdotto la responsabilità degli enti per illeciti dipendenti da reati.

Da quella data è stato sovvertito un principio storico del nostro sistema penale, "*societas delinquere non potest"*, prevedendo al contrario una forma di responsabilità degli enti che ha assunto perimetri sempre più ampi, che, per quanto riguarda la 231/2001 si sono evidenziati con un incremento, nel tempo, dei reati-presupposto.

L'attuale normativa sulla responsabilità degli enti è frutto di un dibattito sorto a partire dagli anni '70. Tale forma di responsabilità tardava, tuttavia, a consolidarsi a livello legislativo, a causa degli ostacoli interpretativi di diritto interno (*in primis* la visione restrittiva dell'art.27 comma 1 Cost., secondo cui "*la responsabilità penale è personale*") e della mancanza di un comune riferimento a livello estero e sovranazionale.

Proprio in quest'ultima sede, iniziava a radicarsi la consapevolezza che, accanto alle persone fisiche, anche le imprese dovessero essere ritenute responsabili per i

reati commessi al loro interno[3]. L'evoluzione tecnologica, i nuovi sistemi di produzione, la complessità delle reti distributive avevano fatto sì che i fattori economici si fossero sviluppati sempre più in forma organizzata, per assumere maggiori dimensioni e migliore efficienza. Allo stesso modo a queste maggiori dimensioni si associavano maggiori impatti sia dal punto di vista sociale che criminale (si pensi ai reati ambientali o alla materia della sicurezza sul lavoro), e rendevano inattuale ed inadeguato un sistema che si limitasse a considerare solo l'individuo come soggetto sanzionabile penalmente[4].

Nei sistemi del *common law*, basati su forte pragmatismo, il criterio del *vicarius liability*[5] aveva consentito già dalla metà del 1800 di affermare la responsabilità di una società ferroviaria[6].

Altri ordinamenti nazionali di *civil law* avevano affrontato e risolto il tema della responsabilità delle persone giuridiche, (Francia, Portogallo, Belgio, Olanda, Danimarca, Finlandia)[7], consapevoli che si stavano creando importanti vuoti di tutela; il d.lgs. 231/2001 emerge quindi sotto la presenza di almeno tre spinte: da un lato un dibattito interno già sviluppato da tempo, poi una normativa internazionale di confronto già ammodernata, a cui ci si doveva armonizzare; ed in

[3] Per una ricostruzione del dibattito storico si veda, *ex plurimis*, DE SIMONE, *Il problema della responsabilità delle persone giuridiche nell'ordinamento italiano*, in LATTANZI - SEVERINO (a cura di), *Responsabilità da Reato degli Enti*, Vol. I, Torino, 2020, 45 ss.

[4] Una ulteriore ricostruzione storica e di contesto è riportata da BERNASCONI– PRESUTTI, *Manuale della responsabilità degli enti*, Milano, 2013, 2: «D'altro canto i singoli sistemi giuridici non mostrano remora alcuna a riconoscere, in ambito civilistico, la responsabilità delle suddette entità collettive. E se un reato commesso da un individuo in esse inserito potesse impegnare, da un punto di vista penalistico, la responsabilità della persona giuridica — rendendola quindi assoggettabile a una sanzione punitiva — era un interrogativo che iniziava ad affacciarsi sempre più di frequente nei paesi interessati dalla prima industrializzazione. I primi disastri ferroviari in Inghilterra portano alla ribalta una nuova forma di criminalità, quella dell'impresa, nella quale il contributo del singolo alla realizzazione dell'evento offensivo non è apprezzabile se non nella misura di una sua contestualizzazione all'interno di una ben più ampia struttura organizzata».

[5] DE SIMONE, *Profili di diritto comparato*, in LATTANZI - SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol. I, Torino, 2020,4. L'autore descrive la *vicarius liability* come un modello vicariale di responsabilità: «il sistema più estensivo e più facile da maneggiare: l'ente può rispondere per la condotta illecita di un qualsiasi agente o dipendente sulla base di semplici criteri ascrittivi: il mero collegamento con l'attività dell'ente, […], oppure l'interesse/vantaggio dell'ente alla commissione del reato». Da rilevare che manca, nel *vicarius liability* un riferimento soggettivo alla colpevolezza.

[6] Le considerazioni sono tratte da BERNASCONI - PRESUTTI, *Manuale della responsabilità*, cit., 4: «grazie alla figura della responsabilità indiretta (*vicarious liability*) le corti inglesi affermano (nel 1842) la responsabilità di una società di gestione ferroviaria in un disastro ferroviario».

[7] A mettere in evidenza le attività solutive in altri Stati europei ANTOLISEI, *Manuale di Diritto Penale*, *Responsabilità degli enti*, parte VI, Milano 2014,747.

ultimo una considerazione di sostanza: l'evidenza che il mantenimento di quell'assetto "limitato" non era più sostenibile.

Vi erano inoltre elementi di indifferibilità: il legislatore doveva recepire una serie di obblighi sovranazionali, in particolare la Convenzione Ocse del 17 dicembre 1997, sulla lotta alla corruzione, e il secondo protocollo del 19 giugno 1997, sulla tutela degli interessi finanziari della Comunità europea, che imponevano agli Stati di prevedere sanzioni anche a carico delle persone giuridiche.[8]

La risposta è arrivata tramite una legge delega, (300/2000) che da un lato ratificava alcuni trattati internazionali, dall'altro forniva le linee guida per la successiva 231/2001. Fino alla data della 231/2001 la responsabilità delle imprese era di tipo civilistico ed a carattere sostanzialmente indiretto, del tutto inadeguata a offrire risposte efficaci sul fronte della criminalità di impresa; con la 231/2001 l'ente diventa "*centro autonomo di imputazione*".[9]

La 231/2001 trovava quindi già del notevole materiale di sottofondo su cui elaborare le proprie regole; in particolare grande evidenza al tema della responsabilità da reato delle persone giuridiche venne dato nel "Progetto preliminare alla riforma del Codice penale", [10](Progetto Grosso), che fece da "battistrada"[11] alla 231/2001.

---

[8] Gli impegni sovranazionali assunti vengono ricordati fra gli altri da ANTOLISEI, *Manuale di Diritto*, cit., 747: «Alla scelta di corresponsabilizzare gli enti per fatti di reato il legislatore è stato obbligato da una serie di convenzioni internazionali firmate dall'Italia. La convenzione OCSE del 17 settembre 1997 per la repressione della corruzione dei pubblici ufficiali stranieri nell'ambito delle transazioni economiche internazionali, all'art. 2, obbliga ciascuna parte contraente ad "adottare le misure necessarie, secondo i propri principi giuridici, per stabilire la responsabilità delle persone giuridiche per la corruzione di pubblico ufficiale straniero"». È da mettere in evidenza che sia questa Convenzione, che quella sulla protezione degli interessi finanziari delle Comunità europee del 26 luglio 1996 (che prevede una responsabilità diretta delle persone giuridiche), vincolano gli Stati a adottare sanzioni, ma non impongono lo schema penale.

[9] In realtà sono già presenti prima del 2001 nel sistema normativo italiano dei casi isolati di illeciti propri dell'impresa: possiamo citare quelli previsti dalla L.287/1990, (c.d. "legge *antitrust*), e le sanzioni previste dal tuf (d.lgs. 58/1998), quest'ultime, non a caso, irrogate da una *Authority*, la Consob.

[10] Ci si riferisce al Progetto preliminare di riforma del Codice penale – parte generale- Commissione Grosso, per la riforma del Codice penale (1° ottobre 1998), Relazione preliminare 12 settembre 2000, in sito ministero della giustizia, *giustizia.it*

[11] L'espressione viene utilizzata da DE SIMONE, *Il problema della responsabilità*, cit., 57. Il modello di disciplina del c.d. Progetto Grosso viene definito dall'autore «all'avanguardia per quei tempi».

Nel Progetto viene dato notevole rilievo al tema della responsabilità *ex crimine* delle persone giuridiche e viene dedicato alla trattazione dell'argomento un intero titolo, il VII, composto da 11 articoli (dal 121 al 131). L'intenzione era dunque quella di andare ad inserire all'interno di un nuovo Codice penale riformato una disciplina organica sulla responsabilità delle persone giuridiche. È da mettere in evidenza che responsabilità e sanzioni previste per le persone giuridiche non vengono etichettate in alcun modo, con lo scopo probabile «di eludere prevedibili e inevitabili obiezioni che sarebbero state sollevate, sul piano dogmatico e anche su quello costituzionale, di fronte ad una responsabilità qualificata *expressis verbis* come penale».[12]

Sono già presenti tutta una serie di elementi che la 231/2001 andrà poi a disciplinare, non sempre in modo sovrapponibile al Progetto Grosso, in quanto sono comunque riscontrabili una serie di scelte che il legislatore sviluppa in modo diverso rispetto a quelle che erano le intuizioni e le regole del progetto di riforma. Ma gli elementi di attenzione restano gli stessi: la definizione dei soggetti coinvolti, i criteri oggettivi di imputazione e le cause di esclusione della punibilità (modello di organizzazione).

La 231/2001 quindi non rappresenta un intervento concettualmente innovativo; quello che la rende invece innovativa è la normazione di queste concettualità che si trasformano in regole legislative e rompono una tradizione che, come accennato in precedenza, escludeva l'ente come possibile centro autonomo di imputazione, di responsabilità e di sanzioni.

Da mettere in evidenza che il lungo dibattito che ha contraddistinto l'inserimento della responsabilità degli enti nel nostro ordinamento è stato oggetto di attenzione e studiato anche a livello internazionale. L'archetipo della normativa italiana sulla responsabilità degli enti ha influenzato in modo significativo altri ordinamenti, in particolare quello spagnolo. Il sistema giuridico spagnolo era fortemente ancorato al principio "*societas delinquere non potest*" ed arriverà ad una disciplina in materia in tempi ben successivi a quelli italiani. *La Ley Organica* n.5 del 2010 rappresenta

[12] Così ancora nella ricostruzione del Progetto Grosso DE SIMONE, *Il problema della responsabilità*, cit., 57.

il momento in cui viene introdotta la responsabilità penale delle persone giuridiche; è da rilevare che «il nucleo centrale del paradigma ascrittivo, […], ricalca, pressoché letteralmente, quella degli art. 6 e 7 d.lgs. n.231 del 2001».[13]

La 231/2001 verrà trattata in questo capitolo solo in alcuni dei suoi aspetti: la natura giuridica della responsabilità, i criteri di imputazione, e degli accenni al modello organizzativo; quest'ultimo verrà analizzato in modo più completo nel secondo e poi nel quinto capitolo, dove verrà collegato ai reati informatici.

Una prima nota relativa ai "modelli organizzativi": la Commissione Grosso, nella Relazione Preliminare per la riforma del Codice penale, riferendosi ai "contenuti del *modello organizzativo idoneo*", a proposito della verifica e valutazione delle situazioni che comportano rischi di violazione della legge penale, fa riferimento al precedente d.lg.626/94 in materia di sicurezza ed igiene del lavoro, dichiarando che viene recepita l'impostazione di base del sistema del d. lg. 626/94 in materia di sicurezza e igiene del lavoro, dove adempimento fondamentale del datore di lavoro è per l'appunto la valutazione dei rischi e la conseguente redazione di un documento che rifletta gli esiti della valutazione e delinei programmi e procedure per il raggiungimento degli obiettivi di sicurezza.[14]

Il sistema del "modello organizzativo" assume nell'ambito della 231/2001 e della responsabilità degli enti per illecito dipendente da reato, un momento centrale, sotto almeno due profili: la mitigazione/esenzione sanzionatoria prevista per l'impresa, che diventa un elemento di fortissimo condizionamento per l'ente a ben ottemperare in modo da evitare provvedimenti penalizzanti a suo carico; e soprattutto assume una carica di prevenzione tale da consentire la stessa interruzione dei meccanismi

[13] In questo senso DE SIMONE, *Profili di diritto,* cit., 17. L'Autore mette in evidenza l'influenza che il modello previsto dal legislatore italiano in tema di responsabilità degli enti ha avuto su un sistema di diritto simile al nostro come quello spagnolo. Viene inoltre sottolineato come nel sistema spagnolo la responsabilità sia stata estesa anche ai partiti politici ed ai sindacati, esclusi invece nel nostro sistema di responsabilità degli enti.

[14] Commissione Grosso, per la riforma del Codice penale (1° ottobre 1998), Relazione preliminare 12 settembre 2000, in *sito ministero della giustizia, giustizia.it,* B. 2. II: «vediamo, brevemente, i contenuti del modello organizzativo idoneo, […]: Questa indicazione recepisce e generalizza l'impostazione di base (non invece i dettagli tecnici) del sistema del d.lgs. 626/94 in materia di sicurezza e igiene del lavoro, dove adempimento fondamentale del datore di lavoro è per l'appunto la valutazione dei rischi, e la conseguente redazione di un documento che rifletta gli esiti della valutazione e delinei programmi e procedure per il raggiungimento degli obiettivi di sicurezza».

che possono portare al reato stesso, in quanto i comportamenti potenzialmente illeciti vengono intercettati e bloccati in una fase antecedente.

Nel mondo dei reati informatici la presenza di un modello organizzativo aziendale in grado di bloccare accessi od utilizzi fraudolenti, con la presenza di una unità interna in grado di coordinarsi con autorità o istituzioni esterne all'azienda, è oggi diventata la regola assoluta (normativa NIS1, NIS2, GDPR); tuttavia la logica è diversa rispetto al sistema 231: l'ente non è chiamato a rispondere solo in quei casi in cui sia ravvisabile un suo interesse od un suo vantaggio, quanto piuttosto ad operare per fronteggiare i rischi derivanti dagli ambiti di intervento che esercita, adottando adeguate misure tecniche ed organizzative che fanno capo a soggetti ben definiti nei confronti dei quali corre anche obbligo di immediata comunicazione in caso di violazione del sistema.[15]

Onde definire il perimetro dei soggetti destinatari della 231/2001, è opportuno un rapido esame dell'art.1 della stessa.

L'art.1 individua, infatti, i destinatari del decreto 231/2001: gli enti forniti di personalità giuridica, le società e associazioni anche prive di personalità giuridica.

Il legislatore si è astenuto da una definizione puntuale delle singole tipologie di enti coinvolti dalla 231/2001, ed ha preferito optare per una forma elastica, che «pone a carico dell'interprete il non agevole compito di fare luce caso per caso sulle zone d'ombra».[16]

È probabile che inizialmente la necessità di approfondire la tematica dei soggetti destinatari della 231/2001 sia stata limitata. La "scarsità" dei reati presupposto riconduceva tendenzialmente sempre a società commerciali, su cui la normativa non dà luogo ad equivoci. Successivamente la maggiore sensibilità alla responsabilità

[15] In questo senso fra gli altri GULLO, *I reati informatici*, cit., 381 ss.
[16] L'espressione utilizzata è di SCAROINA, *Principi generali*, in LATTANZI - SEVERINO (a cura di), *Responsabilità da Reato degli Enti*, vol. I Torino, 2020, 74. Secondo la valutazione dell'autrice, «il sistema punitivo delineato dal d. lgs. 231/2001 intende rivolgersi ad entità dotate di un patrimonio autonomo e di un minimo di organizzazione interna tale da renderne evidente l'alterità rispetto all'imprenditore-persona fisica e giustificare quindi la diversa e cumulativa risposta sanzionatoria».

degli enti, e l'ampliamento del catalogo dei reati presupposto, ha reso necessaria una attività interpretativa. [17]

Un primo requisito comune ai soggetti che sono coinvolti dalla 231/2001 è la presenza di un minimo di organizzazione interna [18], che deve essere quindi rintracciata anche in quelle situazioni dove potrebbe essere incerta l'applicazione del decreto. La presenza di una organizzazione interna è funzionale allo stesso spirito della 231/2001, non ultimo alla alterità fra soggetto persona fisica e soggetto ente.

Per lo stesso motivo alcuni autori sostengono che queste entità devono essere dotate di un patrimonio autonomo[19].

Non è richiesta a questi enti una finalità di profitto. Chi sostiene che esso sia necessario [20] parte dalla considerazione che la struttura della responsabilità tende a colpire il fine di profitto, connaturato alla attività di impresa, e realizzato con mezzi illeciti; la stessa Relazione Ministeriale, si esprime in questo senso: « la scelta dei reati, in uno con ulteriori indizi normativi desumibili soprattutto dalla disciplina civilistica (calibrata sulle società commerciali), consentono di ritenere con

[17] Riporta in questo senso PISTORELLI, *Responsabilità da reato nella giurisprudenza di legittimità, La responsabilità amministrativa delle società e degli enti*, in *Rivis.231*, 2011, 2, 173: «Quello dell'individuazione dei soggetti della responsabilità amministrativa da reato è profilo che nei primi anni dell'applicazione del d.lgs. 8 giugno 2001, n. 231 ha conosciuto scarso approfondimento nelle trattazioni dottrinarie e pressoché nessun riscontro nella produzione giurisprudenziale. Per un verso la definizione normativa della *line up* dei destinatari del nuovo modello di responsabilità era apparsa sufficientemente univoca, per l'altro l'originaria povertà e monotematicità dei cataloghi dei reati presupposto aveva fatto sì che protagonisti dell'illecito da reato fossero più che altro società commerciali, certamente iscrivibili in tale definizione. Il vorticoso ampliamento dei già menzionati cataloghi e la progressiva maggior attenzione riservata dagli uffici giudiziari alla responsabilità degli enti hanno invece pian piano fatto emergere i problemi interpretativi che l'intrinseca genericità delle scelte linguistiche operate dal legislatore per identificare gli autori dell'illecito da reato nascondeva e che nell'ultimo anno alcuni arresti dei giudici di legittimità hanno evidenziato e reso attuali».

[18] Fra gli altri in questo senso anche DI GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo*, in LATTANZI (a cura di), *Reati e responsabilità degli enti, guida al d.lgs. 8 giugno 2001, n.231*, Milano, 2010,35.

[19] Così SCAROINA, *Principi generali,* cit., 74; sul punto vedi anche BERNASCONI – PRESUTTI, *Manuale della responsabilità*, cit., 41, che in termini di patrimonio, riferendosi alla separazione formale fra persone fisiche e persone giuridiche, sostiene invece che lo stesso non rappresenta un criterio discretivo: «L'autonomia patrimoniale dell'ente rispetto alla persona fisica non rappresenta, dunque, il criterio discretivo per attribuire la nuova forma di responsabilità ad una *societa*s piuttosto che all'altra».

[20] La considerazione è di DI GIOVINE, *Lineamenti sostanziali,* cit., 35. Da mettere in evidenza in proposito che nella Relazione al d.lgs. 231/2001 il legislatore delegante «avesse come mira la repressione di comportamenti illeciti nello svolgimento di attività di natura squisitamente economica, e cioè assistite da fini di profitto».

ragionevole certezza che il legislatore delegante avesse di mira la repressione di comportamenti illeciti nello svolgimento di attività di natura squisitamente economica, e cioè assistite da fini di profitto»[21]; tuttavia sono oggetto del decreto anche associazioni dove la finalità di lucro non è presente, ma purtuttavia hanno dimensione importanti e realizzano le loro finalità, che possono anche essere solidaristiche, con ingenti mezzi. Viene inoltre fatta rilevare la presenza di reati per i quali è prevista la responsabilità dell'ente, «quali quelli in materia di sicurezza sul lavoro o terrorismo, non necessariamente assistiti dallo scopo di lucro».[22]

L'applicazione è inoltre prevista anche per gli enti di piccole dimensioni, come si ricava dalla estensibilità del modello organizzativo per queste strutture minori. Qui il superamento della onerosità del modello organizzativo viene risolto dalla facoltatività dello stesso,[23] ed una attenuazione di esso si ha nella norma che stabilisce la possibilità (art.6 comma 4) che le attività previste dall'ODV possono essere svolti anche da un dirigente.

Come è ben chiaro dalla stessa norma, la presenza o meno di personalità giuridica non rappresenta un criterio di differenziazione: «L'obiettivo della normativa non è di incrinare lo schermo formale che consente di separare, agli effetti civili, il patrimonio della persona fisica da quello della persona giuridica, bensì di imputare all'organizzazione pluripersonale, in quanto tale, le conseguenze — per questa vantaggiose — della condotta criminosa realizzata dall'autore che alla medesima appartiene».[24]

Sulle imprese individuali appare preferibile la soluzione negativa, considerato che la disciplina in esame sembra presupporre una distinzione tra ente e persona fisica: le sanzioni finirebbero, infatti, per gravare sullo stesso soggetto, come persona fisica e come impresa individuale, in violazione del *ne bis in idem* sostanziale;

[21] Relazione Ministeriale al d.lgs.231/2001
[22] La valutazione è riportata fra gli altri da SCAROINA, *Principi generali*, cit., 75. Viene anche messo in evidenza che nel testo della normativa non sono rintracciabili riferimenti espliciti allo scopo perseguito nel compimento dell'attività illecita.
[23] Cfr. cap.1, par. 4
[24] Il tema è affrontato e risolto nei termini riportati da BERNASCONI – PRESUTTI, *Manuale della responsabilità*, cit., 42; sul punto vedasi anche la Relazione Ministeriale, che si esprime: «si tratta di soggetti che più agevolmente sottrarsi ai controlli statali sono a maggiore rischio di attività illecite ed attorno alle quali appare dunque ingiustificato creare vere e proprie zone di immunità».

«inoltre, considerato che, come vedremo, la responsabilità dell'ente si fonda sulla colpevolezza di organizzazione per la mancata prevenzione del reato, nel caso di imprese individuali si arriverebbe all'assurdo di fondare la responsabilità di un soggetto per il mancato controllo su se stesso».[25] Tuttavia, sul punto viene citata in senso contrario una sentenza della Cassazione (Cass. 20 aprile 2011, n. 15657)[26]; per quanto poi la stessa Corte si è successivamente espressa in termini di esclusione (23 luglio 2012, n. 3008): «deve rilevarsi, incidentalmente, che la normativa sulla responsabilità delle persone giuridiche non si applica alle imprese individuali, in quanto si riferisce ai soli soggetti collettivi».

In termini di sottoposizione chiara al decreto, senza dubbio giocano un ruolo di primo piano le società di capitali, che rappresentano la "tipologia comune" che aveva in mente il legislatore della 231/2001 (in particolare quelle di dimensioni maggiori): qui si trovano tutti i requisiti citati in precedenza, quali personalità giuridica, autonomia patrimoniale perfetta, finalità di lucro, applicabilità del modello di servizio.

Rientrano senza alcun dubbio le società di persone, e, per quanto detto prima, le associazioni e le fondazioni.[27]

Il decreto dispone successivamente, sempre all'art.1, che il contenuto della 231/2001 non si applica allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale.

---

[25]La considerazione è presa da ANTOLISEI, *Manuale di diritto*, cit., 751. L'autore sostiene che le imprese individuali non sono inseribili fra i soggetti a cui si applica la 231//2001.

[26] Cfr. Cass. pen., Sez. III, 20 aprile 2011, n.15657, La Corte ha sostenuto fra altro che «si creerebbe il rischio di un vero e proprio vuoto normativo, con inevitabili ricadute sul piano costituzionale connesse ad una disparità di trattamento tra coloro che ricorrono a forme semplici di impresa e coloro che, per svolgere l'attività, ricorrono a strutture ben più complesse e articolate».
In senso fortemente critico verso questa sentenza PISTORELLI, *Responsabilità da reato,* cit., 175: «i giudici di legittimità hanno affermato che le norme che regolamentano la materia riguardano anche le imprese individuali, ricorrendo ad una quantomeno discutibile interpretazione estensiva della formula utilizzata dal legislatore nel comma 2 dell'art.1 del menzionato decreto per individuare i destinatari di tali norme», in *onelegale.wolterskluwer.it*

[27] Su basi interpretative rientrano anche società di fatto e irregolari, mentre sono da considerare esclusi i condomini e i fondi patrimoniali; così fra gli altri SCAROINA., *Principi generali,* cit., 79.

Fra i motivi che portano a questa esclusione, la necessità di «evitare l'esigenza del soggetto pubblico che punisce sé stesso, scaricando di fatto sui consociati gli effetti pregiudizievoli derivanti dall'applicazione della sanzione».[28]

Per Stato si intendono tutte le articolazioni amministrative, centrali e periferiche dello Stato (Ministeri, Prefetture), per enti pubblici territoriali si fa riferimento a Regioni, Provincie, Comuni, così come Città Metropolitane, Comunità Montane; gli enti che svolgono funzioni di rilievo costituzionale addensano diverse tipologie associative: sono fra questi istituti che svolgono attività di controllo, come B. Italia, Consob, IVASS, enti che erogano in forma privata un servizio pubblico senza finalità di lucro (Università, Aziende Sanitarie), enti pubblici associativi (come la Croce Rossa o gli ordini professionali), enti che perseguono finalità tipiche dello Stato (Inps, Inail), per quanto riguarda enti che svolgono funzioni di rilievo costituzionale possiamo citare i partiti politici ed i sindacati.[29]

Sono invece da escludere gli enti pubblici economici, che in modo molto sintetico, possono essere definite come imprese che hanno per oggetto esclusivo o principale un'attività commerciale svolta nelle forme private, pur essendo di estrazione pubblicistica[30].

[28] La considerazione è tratta da SCAROINA, *Principi generali,* cit., 80.

[29] BERNASCONI – PRESUTTI, *Manuale della responsabilità* cit., 44. L'autore sviluppa una lista dei soggetti a cui non è applicabile la 231/2001, concludendo poi con l'elenco di altra serie di enti dove «lo statuto di "economicità" dell'ente pubblico — desumibile dalla coesistenza di finalità pubblicistiche con quelle lucrative — preclude l'operatività della clausola di esclusione (*ex* art. 1 comma 3)». L'esempio riportato si rivolge a «realtà a soggettività privata che svolgono un pubblico servizio in regime di concessione ed alle società "miste", cioè quelle partecipate da capitale pubblico e privato. Con riferimento a queste ultime, la giurisprudenza ha puntualizzato — di fronte al caso di un ospedale specializzato interregionale, costituito sia da capitale privato sia da capitale pubblico — che è proprio la finalità lucrativa perseguita a rendere applicabile la normativa del 2001 anche a tale ente (nonostante esso possa dirsi connaturato alla cura di interessi pubblici quali, nella specie, la salute)»; Come evidenziato anche da giurisprudenza (v. Cass.pen., 9 luglio 2010, n. 28699), « non è sufficiente invocare il richiamo delle funzioni di rilievo costituzionale svolte da un istituto ospedaliero specializzato per l'inapplicabilità della disciplina », in quanto la ratio «dell'esenzione è quella di preservare enti rispetto ai quali le misure cautelari e le sanzioni applicabili sortirebbero l'effetto di sospendere funzioni indefettibili negli equilibri costituzionali, il che non accade rispetto a mere attività di impresa. È necessario, infatti, che vi ricorra anche il profilo della non economicità delle funzioni svolte dall'istituto in questione», in *onelegale.wolterskluwer.it*

[30] In questo senso, fra gli altri, SCAROINA, *Principi generali,* cit., 82

2. Natura giuridica della responsabilità

Il dibattito sulla natura della responsabilità dell'ente, con l'introduzione della 231/2001, è senza dubbio di estremo interesse ed importanza, sia dal punto di vista dell'elaborazione giuridica, (di dottrina e di giurisprudenza), sia dal punto di vista delle conseguenze pratiche.

In estrema sintesi la 231/2001 ha creato un meccanismo definito in modo "apparente" di responsabilità amministrativa a carico degli enti per illeciti commessi da soggetti ad essi appartenenti, per attività da ricollegarsi a vantaggio o interesse degli enti stessi.

Ma la lettura della "sostanza" disposta dalla 231/2001 ha evidenziato diversi elementi che più che alla responsabilità amministrativa riportano alla responsabilità penale.

Si sono quindi fronteggiate negli anni importanti argomentazioni nei confronti di entrambe le tesi.[31]

Prima di entrare nel dibattito successivo alla emanazione della 231/2001, può essere opportuno evidenziare il dato *formale* presente nell'intervento legislativo, in uno con quanto ad esso collegato, vale a dire la Relazione Preliminare 12 settembre 2000.

Il decreto legislativo 8 giugno 2001 si esprime formalmente al "*CAPO I*" evidenziando la responsabilità *amministrativa* dell'ente. Successivamente alla Sezione I riporta: principi generali e criteri di attribuzione della responsabilità

[31] Contrari a una etichettatura formale della natura della responsabilità degli enti fra gli altri: RORDORF, *Criteri di attribuzione della responsabilità. I modelli organizzativi e gestionali idonei a prevenire i reati",* in *Soc. 2001*, citato da SANTI, in *Responsabilità da reato degli enti e modelli di esonero*, Milano, 2016,.20: «Lo studio del d.lgs. 8 giugno 2001, n. 231, costituisce un'occasione per riscattarsi dal "mito delle discipline"», ed ancora CENTONZE, *La normalità dei disastri tecnologici. Il problema del congedo dal diritto penale*, Milano, 2004, 1, per il quale l'impostazione metodologica da seguirsi parte dalla «consapevolezza della necessità di abbattere i confini che ancora rigidamente separano le diverse discipline, tutte invece accomunate dalla necessità di risolvere i medesimi problemi presentati dalla società moderna». Secondo DE SIMONE, (che sostiene la presenza di un diritto penale diverso – con categorie sistematiche e criteri d'imputazione suoi propri – ritagliato, ovviamente, sulle specifiche fattezze dei soggetti metaindividuali un "*secundum genus* penalistico") la «soluzione del problema viene a dipendere, in ultima analisi, dal retroterra culturale e ideologico del singolo interprete», in *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi di imputazione*), in *Dir. Pen. Contemp.*, 2012, 19.

amministrativa. L'Art.1, sulla parte relativa ai soggetti, evidenzia che «il presente decreto legislativo disciplina la responsabilità degli enti per gli illeciti *amministrativi* dipendenti da reato […]». All'art 2, principio di legalità che «l'ente non può essere ritenuto responsabile per un fatto costituente reato se la sua responsabilità *amministrativa* […]»; l'art 3, a proposito di successione di leggi, evidenzia che «l'ente non può essere ritenuto responsabile per un fatto che secondo una legge posteriore non costituisce più reato o in relazione al quale non è più prevista la responsabilità *amministrativa* […]». Così ancora si potrebbe citare l'art.9 (sanzioni *amministrative*), e la titolazione della Sezione III e del CAPO III, dove si continua ad usare, nelle sue varie declinazioni, il termine *amministrativo.*

Se ci limitassimo al dato formale, nessun dubbio potrebbe esistere sulla natura della responsabilità dell'ente per illeciti dipendenti da reato: tante volte viene specificato che si tratta di responsabilità amministrativa, anche su punti di estrema importanza come i primi tre articoli.

Il dubbio emerge non appena si toglie la veste nominale della dichiarazione, ed appare una sostanza che negli stessi articoli, capi, sezioni citati assume natura e contenuto penale.

La Relazione Preliminare 12 settembre 2000 stessa assume una posizione più elastica rispetto alla lettera della legge, e chiarisce molti punti, indicandoci un percorso che, spinto dalla necessità e dalla forte volontà di arrivare ad una soluzione, non rifugge da alcuni "chiaroscuri", che vengono considerati secondari rispetto al valore del risultato finale. Sono riportati qui di seguito alcuni punti, particolarmente pertinenti e per certo verso quasi contrastanti la veste formale della 231/2001.

«Fra i punti più innovativi della proposta qui presentata c'è la previsione di un sistema di responsabilità delle persone giuridiche, ancorata al diritto e al processo penale ancorché non qualificata e allo stato non qualificabile come responsabilità penale […]. Nella discussione pro e contro l'introduzione di un sistema di responsabilità penale delle persone giuridiche, pesano fortemente aspetti simbolici. La Commissione ha preferito guardare alla sostanza dei modelli di disciplina, e ai principi che si ritiene di dover seguire. L'etichettatura dell'istituto è stata ritenuta di

secondaria importanza, al punto da poter evitare una esplicita qualificazione entro gli schemi tradizionali [**…]** La maggioranza della Commissione è dell'avviso che le considerazioni sopra menzionate consentirebbero di sostenere la piena legittimità della introduzione nel sistema giuridico italiano di un modello penalistico della responsabilità delle persone giuridiche. Per non forzare una situazione che appare a tutt'oggi oggetto di discussioni aperte anche all'interno della Commissione stessa, ha tuttavia scelto di non utilizzare tale modello. Il sistema delineato, che evita di parlare anche di responsabilità amministrativa, introduce una sorta di "*tertium genus"*, che è sì ancorato a presupposti penalistici (commissione di un reato) e governato dalle garanzie forti del diritto penale, ma che rispetto al diritto penale classico presenta inevitabili diversità, dovute alla diversità dei destinatari».[32]

---

[32] Commissione Grosso per la riforma del Codice penale, 12 settembre 2000, *Ministero della Giustizia, giustizia.it* – a seguire altre parti, estratte dalla relazione, dello stesso tenore: «[…] Il disegno di legge all'esame del Parlamento, nei diversi testi via via approvati, ha optato per un sistema di responsabilità definita amministrativa, affidandone peraltro l'applicazione al giudice penale […].
[…] Uno sguardo comparatistico mostra una sempre più diffusa ammissione della responsabilità penale delle persone giuridiche (così, per restare all'Europa, in Francia, Regno Unito, Olanda, Danimarca, Portogallo, Irlanda, Svezia, Finlandia).
[…] La eventuale responsabilità 'da reato' delle persone giuridiche trova dunque collocazione, sia per i suoi presupposti, che per gli strumenti disponibili, in ambiente penalistico. Per tale ragione, è stata ritenuta una materia di competenza del Codice penale, indipendentemente dalla etichetta ritenuta appropriata, e tale da porre in ogni caso la serie di problemi, soprattutto di garanzia, che la natura penalistica dei presupposti e il contenuto fortemente sanzionatorio traggono con sé.
[…] Le riflessioni della Commissione muovono dai problemi, per i quali la responsabilità delle persone giuridiche viene in discussione. Essi sorgono dentro il terreno penalistico: la questione della responsabilità delle persone giuridiche è direttamente raccordata al presupposto penalistico della commissione di reati. Da ciò l'esigenza di un raccordo coerente fra le diverse risposte che si ritenga opportuno dare alla commissione del reato.
[…] Anche gli strumenti sanzionatori che vengono in predicato, come sanzioni per le persone giuridiche, sono istituti corrispondenti a sanzioni e misure del diritto penale classico. Per tale contenuto pongono problemi 'di garanzia', corrispondenti a quelli cui sono rivolti i principi fondamentali del diritto penale (in questa prospettiva l'art. 124 prevede che "alla responsabilità della persona giuridica si applicano le disposizioni dell'ordinamento penale, in quanto compatibili").
[…] Contro la responsabilità penale delle persone giuridiche, viene invocato da parti non trascurabili della dottrina italiana (e non solo) il principio di personalità della responsabilità, nella dimensione pregnante che esige, quale presupposto indefettibile della responsabilità penale, la colpevolezza del soggetto punibile. Nel corso del dibattito che è seguito alla pubblicazione del documento di base 15 luglio 1999 sono state in effetti numerose le posizioni critiche assunte anche soltanto nei confronti della progettata previsione di una responsabilità (non necessariamente penale) degli enti collettivi (fra queste si colloca sostanzialmente la posizione assunta dalla Commissione della Procura Generale nel parere sul documento; di ben diverso tenore è stata tuttavia la posizione assunta dalla Commissione della Corte di Cassazione, sensibile ai profili positivi di una previsione della responsabilità delle persone giuridiche). Ed anche all'interno della Commissione sono emerse, nelle parole e nei documenti di taluni commissari, le perplessità sopra menzionate.
[…] La maggioranza della Commissione ha condiviso tale indirizzo, ritenendo realistico ipotizzare la sussistenza di condizioni di funzionalità general-preventiva, atte a legittimare un modello di

Fra i vari importanti passaggi citati, sono da sottolinearne in particolare due: il primo, relativo alla volontà di fare prevalere la sostanza sulla forma, nella consapevolezza dell'ampio contrasto che avrebbe generato questa normativa: "*La Commissione ha preferito guardare alla sostanza dei modelli di disciplina, L'etichettatura dell'istituto è stata ritenuta di secondaria importanza, al punto da poter evitare una esplicita qualificazione entro gli schemi tradizionali*" l'altro legato al *tertium genus*: c'è la piena consapevolezza che la disciplina realizzata ha elementi ibridi, in quanto, pur essendo interno al diritto penale, non si sovrappone agli schemi del diritto penale classico.

Ancora la Relazione Grosso del 26 maggio 2001[33], che tiene conto del dibattito successivo alla Relazione del 2000, quando accenna alla responsabilità di impresa fa emergere il contrasto sulla materia, pur senza indietreggiare sulla soluzione ed al contrario ritenendola un indispensabile adeguamento alle legislazioni penali europee: «la previsione della responsabilità delle persone giuridiche, che pur rifiutata da una parte degli studiosi di diritto penale, è stata oggetto di apprezzamento convinto da parte di numerosi commentatori (in primo luogo della Commissione istituita presso la Corte di Cassazione), e che la Commissione Ministeriale, …(omissis)…, ritiene profilo di rilievo in una riforma del sistema penale italiano moderna e coerente con i più recenti orientamenti delle legislazioni penali europee».

Fornito questo quadro, andiamo adesso ad esaminare le posizioni della dottrina e della giurisprudenza sulla natura della responsabilità degli enti per reato, eliminando i riferimenti ai contenuti formali, appena citati e come abbiamo visto frutto più della necessità di confezionare questa normativa in modo da garantire l'inserimento non conflittuale nel nostro sistema giuridico che non di una reale valutazione amministrativa dei contenuti.

disciplina di tipo penalistico, rivolto alla persona giuridica. Questa viene considerata, indipendentemente da schemi di astratta dogmatica giuridica, quale autonomo centro d'interessi e di rapporti giuridici, punto di riferimento di precetti di varia natura, e matrice di decisioni ed attività dei soggetti che operano in nome, per conto o comunque nell'interesse dell'ente».

[33] Commissione Grosso per la riforma del Codice penale, 26 maggio 2001, *Ministero della Giustizia, giustizia.it.*

Per quanto riguarda la "tesi amministrativa" punto base fondamentale è rappresentato dalla incapacità di azione della persona giuridica, in quanto l'azione, nel senso completo, è della persona fisica, soggetto cosciente dotato di volontà psichica. Se la persona giuridica non è un soggetto dotato di volontà, non può essere sottoposto al rimprovero penale; di fatto, quindi, saremmo in presenza di una responsabilità individuata sulla persona fisica e poi trasferita (anche) sulla persona giuridica, andando a violare l'art. 27 Cost comma 1 in quanto la persona giuridica diventa responsabile per "fatto altrui".[34]

La formula a cui si fa riferimento per superare questo ostacolo (teoria della immedesimazione organica)[35] non viene accettata, in quanto l'imputazione di una azione è ben diversa dall'effettuare quella azione; e questo "artificio imputativo" inoltre non può essere utilizzato in un diritto rigoroso, quello penale, che dal compimento dell'azione fa discendere conseguenze particolarmente gravose.

Allo stesso modo è strettamente personale anche il giudizio di rimproverabilità; è arduo riuscire a trovare un motivo per cui giustificare l'imputazione di una colpevolezza altrui; da cui, per inciso, emergerebbe una conseguenza coerente ma non voluta in caso di accettazione della teoria della immedesimazione organica:

[34] ANTOLISEI, *Manuale di diritto penale*, cit.,745, fra gli altri: «il principio di immedesimazione organica tra persona fisica ed ente potrebbe consentire di superare questo primo argomento, perché i fatti commessi dalla persona fisica sono direttamente imputati all'ente. Tuttavia, l'art. 27, co.1, Cost., nella lettura proposta dalla Corte Cost. (sentenze nn. 264 e 1085 del 1988) non si limita a garantire il divieto di responsabilità per fatto altrui, ma richiede una responsabilità per fatto proprio colpevole, ossia assistito da dolo o, quantomeno, da colpa. Così riletto, il principio della responsabilità penale personale richiede una componente soggettiva non ravvisabile in capo all'ente, se non riferendogli l'elemento soggettivo della persona fisica autrice del reato. Per superare l'impasse dell'art. 27, co. 1, Cost. si è allora proposto di prevedere a carico delle persone giuridiche solo misure di sicurezza, dato che queste sanzioni, anch'esse penali, prescindono come noto dall'accertamento della colpevolezza per il fatto, essendo applicate in ragione della pericolosità del soggetto».

[35] BERNASCONI – PRESUTTI, *Manuale della responsabilità* cit.,5, sulla nascita del principio di immedesimazione: «nel Regno Unito, si registra un salto epocale (siamo nel 1944) sul piano dei criteri di imputazione. Compare sulla scena il principio dell'immedesimazione: al cospetto di un reato che richiedeva uno specifico dolo «si decise che gli stati mentali dei funzionari che avevano agito per la società potevano essere attribuiti alla società medesima, la quale si identificava con quei funzionari».

verrebbe esclusa la responsabilità della società in caso di assenza di colpevolezza all'autore del reato.[36]

Per quanto riguarda la "incapacità di pena" essa è legata alla "incapacità" della persona giuridica di avvertire le sofferenze che sono invece percepite dalla persona fisica a seguito della irrogazione della sanzione penale; l'ente è un "soggetto impersonale", la sanzione lascia indifferente lo stesso, la complessità e l'organizzazione fanno sì che la sanzione scivoli senza generare afflizione; allo stesso modo quindi questo "blocco impermeabile" costituito dall'ente non potrebbe trarre alcun beneficio da una pena che abbia funzioni rieducative.(quindi non sarebbe possibile rieducare l'ente, art.27 co.3 Cost.).

Altro elemento sostenuto dagli autori che propendono per una responsabilità amministrativa è relativo alla prescrizione, che viene fatta riferire alla 689/1981, ed è quindi di derivazione amministrativa. In questo senso viene messa in evidenza l'assenza di differenza fra prescrizione dell'illecito e prescrizione della sanzione, che è invece tipica del diritto penale; il termine di prescrizione (5 anni), è inoltre analogo a quanto stabilito dalla 689/1981.[37]

Ancora, sulla trasformazione: l'ente trasformato continua a rispondere dei reati pregressi negli stessi termini in cui ne rispondeva prima[38]

Una ulteriore considerazione riguarda le conseguenze sui soci: chi rigetta la tesi della responsabilità penale, mette in evidenza come la stessa, se irrogata alla *societas*, andrebbe a coinvolgere tutti i soci, e quindi anche quelli innocenti.

---

[36] Così evidenzia DE SIMONE, *Il problema della responsabilità*, cit., 59ss. L'autore mette in evidenza come «il fare pagare unicamente al singolo il prezzo di un illecito collettivo finirebbe col porsi in rotta di collisione con lo stesso principio di responsabilità penale per fatto proprio».

[37] In evidenza le ragioni amministrative in, *Manuale di diritto penale*, sez. VIII, cap. XV.

[38] BERNASCONI – PRESUTTI, *Manuale della responsabilità* cit.,12 in senso critico su questo punto: «è impossibile rispondere alla domanda circa la razionalità di una sanzione, che si assumerebbe penale, quando l'ente » — tra il reato-presupposto e il giudizio — si è « completamente trasformato, naturalmente in termini oggettivi, adeguandosi alle indicazioni prevenzionistiche e 'alleggerendosi' di chi aveva perpetrato o tollerato fatti illeciti e strutture inadeguate »: ciò può verificarsi perché « l'ente non è come la persona fisica, la quale, anche se trasformata, mantiene il ricordo e l'eredità esperienziale del passato».

Per quanto riguarda la giurisprudenza, è citabile la sentenza Gubert 10561/2014[39]: «nell'ordinamento vigente, infatti, è prevista solo una responsabilità amministrativa degli enti e non una responsabilità penale, sicché l'ente non è mai autore del reato».

Il quadro appena descritto si contrappone, sostanzialmente, a tutti quegli autori e alla giurisprudenza che sostiene si sia in presenza di una responsabilità di tipo penale.

Il presupposto assoluto delle teorie "penalistiche" deriva dall'assunto che la persona giuridica ha capacità di imputazione soggettiva. L'assenza di una sfera psichica non impedisce che possano essere individuati criteri di attribuzione della responsabilità che consentano di ritenere i reati della persona fisica espressione di politiche e strategie aziendali.[40]

Come già messo in evidenza in precedenza, è indubbio che la persona giuridica abbia la capacità di esprimersi con forza non solo su comportamenti commerciali od economici, ma anche con finalità criminali, che sono amplificate nelle conseguenze proprio dalla forza organizzativa di un ente. A fronte di un atteggiamento di questo tipo, pericoloso anche in termini di destabilizzazione sociale, (si pensi allo sfruttamento dei lavoratori con mancato rispetto delle misure di sicurezza previste) la reazione normativa non può che essere di tipo penale, rappresentando quest'ultima la risposta più intensa che una comunità può predisporre a propria difesa.[41]

---

[39] Cfr. Cass., Sez. Un., 30 gennaio 2014, n. 10561, "Gubert", così in *Dir. Pen. Contemp., 12, 03, 201,* con nota di T. Trinchera «anzitutto, osservano i giudici di legittimità, il rapporto organico che esiste tra persona fisica e società non è di per sé idoneo a giustificare l'estensione dell'ambito di applicazione della confisca per equivalente. In secondo luogo, proseguono i giudici del Supremo Collegio, non può trovare applicazione il principio per cui a ciascun concorrente devono imputarsi le conseguenze del reato. Nell'ordinamento vigente, infatti, è prevista solo una responsabilità amministrativa degli enti e non una responsabilità penale, sicché l'ente non è mai autore del reato e non può essere considerato concorrente».

[40] DE SIMONE, *Il problema della responsabilità*, cit., 59ss. L'autore sottolinea inoltre che «non bisogna trascurare neppure il particolare significato che assume, sul piano simbolico-espressivo, il ricorso a sanzioni *stricto sensu* penali, la cui applicazione finirebbe con il riflettersi, (in negativo), sull'immagine stessa della *societas*: il che potrebbe contribuire a incrementarne l'efficacia preventiva».

[41] La considerazione è riportata da BERNASCONI – PRESUTTI, *Manuale della responsabilità* cit., 7, che aggiunge «È da tenere presente sin d'ora che *persona fisica e societas* sono ben distinte sul piano della colpevolezza; lo conferma, in termini inconfutabili, il principio dell'autonomia della responsabilità dell'ente (v. art. 8) che consente di perseguire quest'ultimo anche nel caso l'autore materiale dell'illecito non sia stato identificato»

L'art 27 cost. comma 1, è citato sia dai sostenitori della tesi amministrativa che di quella penale. Questi ultimi "ribaltano" le considerazioni sviluppate in precedenza, ed al contrario sostengono che la vera violazione dell'art 27 comma 1 sussisterebbe se non venisse assegnata la responsabilità personale all'ente: il "fatto proprio" è dell'ente[42].

Nella Sentenza delle SSUU Thyssenkrupp[43], che lascia intendere la presenza di un "terzo genere" come soluzione più propria a questa dibattuta vicenda, viene presa posizione in modo molto netto, escludendo sia la violazione del principio di colpevolezza che quello per "fatto proprio", e ribadendo invece l'attribuibilità del fatto, svolto a vantaggio e nell'interesse dell'ente, all'ente stesso.

Sempre a proposito di colpevolezza, viene fatto rilevare da autori che il concetto di colpevolezza in senso psicologico è diverso da quello normativo, e quest'ultimo, essendo più elastico, ricomprende anche l'ente.[44]

Centrale è il concetto di "*colpa in organizzazione*"[45]: il rimprovero che viene mosso alla persona giuridica è di non avere adottato, ed aggiornato, un sistema di misure

[42] Vedasi sul punto fra gli altri, *Manuale della responsabilità* cit., 10: «è la teoria della immedesimazione organica a consentire che il fatto (reato) della persona fisica — inserita nella struttura aziendale — sia imputabile anche all'ente. Non solo. Nel nostro ordinamento il ricorso a questo criterio di ascrizione è indispensabile per non violare il principio di cui all'art. 27 co. 1 Cost., interpretato "nella sua versione minima", come divieto di responsabilità per fatto altrui, o in quella ragionevolmente più ampia di responsabilità necessariamente colpevole».

[43] Cfr. Cass. pen., Sez. Un., 18 settembre 2014, n. 38343, motivazioni della sentenza delle Sezioni Unite nella vicenda relativa al disastro nello stabilimento torinese della ThyssenKrupp: «È senz'altro da escludere che sia violato il principio della responsabilità per fatto proprio. Il reato commesso dal soggetto inserito nella compagine dell'ente, in vista del perseguimento dell'interesse o del vantaggio di questo, è sicuramente qualificabile come "proprio" anche della persona giuridica, e ciò in forza del rapporto di immedesimazione organica che lega il primo alla seconda: la persona fisica che opera nell'ambito delle sue competenze societarie, nell'interesse dell'ente, agisce come organo e non come soggetto da questo distinto; né la degenerazione di tale attività funzionale in illecito penale è di ostacolo all'immedesimazione . Parimenti è da escludere che il sistema violi il principio di colpevolezza. Di certo, però, tale principio deve essere considerato alla stregua delle peculiarità della fattispecie, affatto diversa da quella che si configura quando oggetto dell'indagine sulla riprovevolezza è direttamente una condotta umana. Qui il rimprovero riguarda l'ente e non il soggetto che per esso ha agito: sarebbe dunque vano e fuorviante andare alla ricerca del coefficiente psicologico della condotta invocato dal ricorrente; ciò tanto più quando l'illecito presupposto sia colposo giacché, come si è già avuto occasione di rimarcare, la colpa presenta essa stessa connotati squisitamente normativi che ne segnano il disvalore». In *Giur. Pen., giurisprudenzapenale.com.*

[44] Si esprime in questo senso fra gli altri DI GIOVINE, *Lineamenti sostanziali,* cit., 31; così anche DE SIMONE, *Responsabilità da reato degli enti*, cit., 63, Torino.

[45] BERNASCONI – PRESUTTI, *Manuale della responsabilità* cit., 3, si fa rifermento alla nascita della "colpa in organizzazione" citando una vicenda processuale d'oltremanica dove l'assoluzione nella società è legata al fatto che l'autore del reato non è in una condizione gerarchica sufficientemente elevata da rappresentare la mente e la volontà dell'azienda, con la conseguenza che «le vicende

organizzative in grado di ridurre od eliminare la possibilità che si realizzassero determinati tipi di reati. La responsabilità è diretta, il fatto è dell'organizzazione, l'addebito è di non avere assunto iniziative organizzative stabili per ridurre il rischio di realizzare reati tramite l'esercizio dell'attività tipica.

Altro argomento a favore della tesi penale è la connessione con la commissione di un reato, (come citato dalla stessa Corte nella sentenza appena riferita), e il riferimento della competenza al giudice penale.

Sempre di stampo penale il sistema sanzionatorio, costituito da sanzioni pecuniarie, interdittive, confisca, pubblicazione sentenza di condanna, commisurate in modo proporzionato alla capacità dell'azienda e basato sull'autonomia patrimoniale dell'ente.

Quanto alla capacità afflittiva della pena, essa è indubbia anche nei confronti dell'ente: la confisca, la sanzione pecuniaria, quella interdittiva hanno capacità di incidere profondamente sulla vita societaria, sia in termini economici che di libertà di azione (misure interdittive) e costituiscono un serio deterrente a realizzare comportamenti futuri in linea con le previsioni normative: non è solo la detenzione che ha capacità afflittiva.

I sostenitori della tesi penale evidenziano che è presente anche un comportamento rieducativo, lo stesso "modello organizzativo" che viene inciso al fine di riallineare i futuri comportamenti dell'ente è esplicitazione di capacità educativa.

Di stampo penale sia la previsione del tentativo, che la successione di leggi nel tempo, con applicazione della legge più favorevole, tipica del diritto penale (su quella amministrativa la disciplina è quella della irretroattività (l. 689/1981, art.11).

processuali d'oltremanica, terminate con il proscioglimento delle società alle quali erano stati imputati gli eventi, disvelano che, in assenza di prove di negligenza nei confronti del top management, l'*identification principle* non è applicabile in quanto inidoneo a "fronteggiare eventi disastrosi che, pur non coinvolgendo direttamente i vertici, erano frutto di un assetto organizzativo non adeguato rispetto alle esigenze di protezione". Il focus si sposta così sull'organizzazione dell'impresa; la responsabilità degli enti, avvantaggiati da un reato commesso da un loro "dipendente", può sorgere in presenza di canoni di ascrizione che tengano in debito conto il dato organizzativo: si inizia quindi a utilizzare il concetto di *colpa in organizzazione* per descrivere l'essenza del rimprovero rivolto all'ente».

Significativo ai fini del dibattito dottrinale anche l'articolo 187 *quinquies* Tuf, (responsabilità amministrativa degli enti dipendente da illecito amministrativo). Tale responsabilità viene accertata nell'ambito di un procedimento amministrativo innanzi alla Consob; quindi, evidenzia una separazione fra questa situazione, relativa alla sanzione amministrativa, e la metodologia della 231/2001, che ha caratteristiche ben diverse, sia in termini di garanzie che di procedimento: si pensi alla competenza del giudice penale, lo stesso competente per il reato presupposto.

Per quanto riguarda la giurisprudenza, oltre la prima citata sentenza Thyssen (che, come detto, "apre" al *tertium genus*"), possiamo citare la sentenza della Cassazione penale, sez. II del 30 gennaio 2006 n.3615.[46]

Una ulteriore nota a favore della tesi della responsabilità penale degli enti deriva dalla nota sentenza della Corte Europea dei Diritti dell'Uomo "caso Engel"[47]ed al ricorso Grande Stevens[48]: ci sono tre criteri per definire la natura di una sanzione: la qualificazione nel diritto nazionale, la natura stessa di quest'ultima, il grado di severità della sanzione, e questi criteri sono alternativi.

Vale a significare come che il dato sostanziale prevale sul dato formale. [49]

---

[46] Cfr. Cass. pen., Sez. II, sentenza 30 gennaio 2006 n. 3615 «È noto che il d.lgs. n. 231 del 2001, sanzionando la persona giuridica in via autonoma e diretta con le forme del processo penale si differenzia dalle preesistenti sanzioni irrogabili agli enti, così da sancire la morte del dogma "*societas delinquere non potest"*, e ciò perchè, 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.)». In *onelegale.wolterskluwer.it*

[47] V. Corte EDU, plenaria, 8 giugno 1976, caso n. 5100/71, *Engel and Others* v. *the Netherlands*: «In tale prospettiva, occorre anzitutto sapere se le previsioni che definiscono l'illecito in questione appartengono, secondo il sistema legale dello Stato resistente, alla sfera del diritto penale, disciplinare o entrambi assieme. Ciò, tuttavia, non rappresenta che un punto di partenza. Le indicazioni così fornite hanno solo un valore formale e relativo e vanno esaminate alla luce di un comune denominatore ricavabile dalle legislazioni dei vari stati contraenti. La natura intrinseca dell'illecito è un fattore di maggior importanza».

[48] V. Corte EDU, sez. II, 4 marzo 2014, casi nn. 18640/10, 18647/10, 18663/10, 18668/10 e 18698/10, *Grande Stevens and Others v. Italy:* «La Corte rammenta la sua consolidata giurisprudenza ai sensi della quale, al fine di stabilire la sussistenza di una "accusa in materia penale", occorre tener presente tre criteri: la qualificazione giuridica della misura in causa nel diritto nazionale, la natura stessa di quest'ultima, e la natura e il grado di severità della "sanzione". Questi criteri sono peraltro alternativi e non cumulativi: affinché si possa parlare di accusa in materia penale ai sensi dell'art. 6, 1, è sufficiente che il reato in causa sia di natura penale rispetto alla Convenzione, o abbia esposto l'interessato a una sanzione che, per natura e livello di gravità, rientri in linea generale nell'ambito della materia penale».

[49] Fra gli altri nel senso che i criteri *Engel* portano ad una responsabilità penale MANNA, *Riv. Trim. Dir. Pen. Econ.*, 2018,4,3.

Sulla base delle considerazioni sopra esposte, sembrerebbe che le tesi sostanziali siano favore di una interpretazione "penale" della responsabilità degli enti, anche se mancano una serie di elementi per potere definire questa responsabilità come "penale" in modo completo: manca ad esempio la possibilità di costituirsi parte civile verso l'ente[50], o l'obbligatorietà dell'azione penale verso lo stesso.

In realtà è da mettere in evidenza (e lo fa anche la Cassazione nella stessa sentenza Thyssen), un'altra corrente di pensiero, che sviluppa come un genere ibrido questa responsabilità (terzo genere).[51]

La soluzione del "terzo genere" è già presentata nel Progetto Grosso, nel 2000, ed è forse la soluzione più moderna, e più ricca di sviluppi. Sostiene la contemporanea presenza di elementi del diritto penale e di elementi del diritto amministrativo.

In particolare, sarebbero sicuramente da ricondurre al diritto penale le gravità delle sanzioni, mentre al diritto amministrativo sono da ricondurre una serie di profili di disciplina.

La conseguenza è che, qualora si ci trovi in presenza di una responsabilità dell'ente, e di una disciplina che presenta su di un particolare punto una lacuna, si dovrà fare riferimento alle regole, del diritto penale o del diritto amministrativo, di quel settore a cui quel punto in esame è affine.

Sul "*tertium genus*" si pronuncia anche la Cassazione favorevolmente nella già citata sentenza Thyssen: «il Collegio considera che, senza dubbio, il sistema di cui si discute costituisce un corpus normativo di peculiare impronta, un *tertium genus*,

[50] Cfr. Cass. pen. Sez. VI, 5 ottobre 2010, n. 2251, con note di Pistorelli: La Corte, occupandosi per la prima volta della questione, ha escluso che nel processo instaurato per l'accertamento della responsabilità da reato dell'ente sia ammissibile la costituzione della parte civile, sottolineando come la mancata disciplina dell'istituto nell'ambito del d.lgs. n. 231 del 2001 non costituisca una lacuna, bensì la conseguenza di una consapevole e legittima scelta operata dal legislatore in ragione del fatto che la persona giuridica è chiamata a rispondere non del reato, bensì di un autonomo illecito, inidoneo a fondare una pretesa risarcitoria altrettanto autonoma. In *Dir. Pen. Contemp.*, 2011, 1.

[51] A proposito di un nuovo diritto penale dell'impresa DE SIMONE, *La responsabilità da reato degli enti, natura giuridica e criteri di imputazione*, in *Dir. Pen. Contemp.*, 2012, 10, 9, che cita anche la posizione di Paliero: «Non è difficile scorgere, sullo sfondo di questa singolare qualificazione, le lucide riflessioni di chi (Paliero, ndr), già diverso tempo addietro, aveva preconizzato la nascita di un nuovo "diritto penale dell'impresa" a composizione ibrida, in relazione al quale non avrebbe avuto più molto senso erigere steccati tra il penale criminale e il penale amministrativo». Cfr. sul punto anche PALIERO, *La sanzione amministrativa come moderno strumento di lotta alla criminalità economica*, *Riv. Trim. Dir. Pen. Econ.*, 1993,1043.

se si vuole. Colgono nel segno, del resto le considerazioni della Relazione che accompagna la normativa in esame quando descrivono un sistema che coniuga i tratti dell'ordinamento penale e di quello amministrativo nel tentativo di contemperare le ragioni dell'efficienza preventiva con quelle, ancor più ineludibili, della massima garanzia».[52]

È da mettere in rilievo, alla fine di queste note, che a prescindere dalle considerazioni sul tipo di responsabilità, siamo in presenza di un sistema sanzionatorio indiscutibilmente punitivo, che, come tale, in un sistema come il nostro, deve rispettare le garanzie che la Costituzione e la CEDU impongono.

Sintetizzando, per quanto riguarda la responsabilità per fatto proprio, il criterio di imputazione dell'art.5 della 231/2001 aggancia il reato-presupposto all'ente, e non ne risponde se le persone individuate abbiano agito nell'interesse esclusivo proprio o di terzi. L'immedesimazione organica consente il rispetto dell'art 27 comma 1 Cost.[53]

---

[52] Cfr. Cass. pen., Sez. Un., 18 settembre 2014, n. 38343 - che prosegue: «Parimenti non è dubbio che il complesso normativo in esame sia parte del più ampio e variegato sistema punitivo; e che abbia evidenti ragioni di contiguità con l'ordinamento penale per via, soprattutto, della connessione con la commissione di un reato, che ne costituisce il primo presupposto, della severità dell'apparato sanzionatorio, delle modalità processuali del suo accertamento. Sicchè, quale che sia l'etichetta che si voglia imporre su tale assetto normativo, è dunque doveroso interrogarsi sulla compatibilità della disciplina legale con i principi costituzionali dell'ordinamento penale, seguendo le sollecitazioni difensive»; in *Giur. Pen., giurisprudenzapenale.com*

[53] A seguire, nel senso del rispetto dei principi costituzionali e di un terzo binario ANTOLISEI, *Manuale di diritto*, cit., 745ss: «Crediamo, però, che anche la qualificazione come *tertium genus* di responsabilità di questo nuovo illecito punitivo, un ibrido a metà strada tra illecito penale e illecito amministrativo, invece di risolvere, sposti solo la soluzione dei problemi delle garanzie costituzionali, in quanto dovrà pur essere chiarito quali siano e con quale estensione operino le norme costituzionali di copertura. In questo caso, nessun dubbio che debba essere assicurata alla responsabilità degli enti collettivi la base irrinunciabile di garanzie che devono assistere l'illecito punitivo (le garanzie proprie della "materia penale" *ex* art. 7 CEDU): principio di irretroattività e connesso principio di retroattività della legge più favorevole; criteri di imputazione personale, in modo da garantire il nesso tra reato commesso e organizzazione dell'ente; funzione di prevenzione speciale positiva. In tal senso, la Corte di Cassazione a Sezioni Unite, optando per il modello del *tertium genus*, ha escluso che la disciplina del d.lgs. 231/2001 contrasti con principi costituzionali che presiedono all'illecito punitivo, valorizzandone specifici elementi: «è rispettato il principio di responsabilità per il fatto proprio in forza dell'immedesimazione organica, in quanto l'autore del reato agisce nell'interesse dell'ente "come organo e non come soggetto da questo distinto"; anche il principio di colpevolezza è assicurato, fondando il giudizio di rimprovero sulla colpa di organizzazione; così, anche il principio determinatezza è salvaguardato attraverso la descrizione dei criteri di imputazione del reato all'ente. Si tratta di indicazioni importanti che collocano chiaramente la responsabilità dell'ente da reato nel contesto dell'illecito punitivo con applicazione delle relative garanzie.

Il principio di responsabilità per fatto proprio viene rispettato con le previsioni degli artt. 6 e 7: il giudizio di colpevolezza è fondato sulla colpa in organizzazione[54], per inidoneità del modello a prevenire il rischio commesso. Come messo in evidenza anche dalle Sezioni unite della Cassazione, non si tratta di responsabilità oggettiva, ma di una responsabilità penale fondata sulla violazione "di una aspettativa sociale che l'ente, attraverso meccanismi di controllo interni, avrebbe dovuto attuare, in funzione dei rischi connessi alla propria attività".

Il finalismo rieducativo della pena è conforme all'art. 27 comma 3 Cost.: le sanzioni sono proporzionabili alle condizioni dell'ente, se il modello organizzativo è congruo la pena viene diminuita di conseguenza, il modello organizzativo stesso costituisce un momento preventivo e se "aggiustato" a seguito di una sua mancanza esprime contenuto rieducativo.

Il principio di irretroattività, di legalità sono indicati all'art. 2, quello di determinatezza dalla descrizione dei criteri di imputazione dei reati all'ente.

Pertanto, anche se è assente la espressa qualificazione in termini di responsabilità penale, la 231/2001 si esprime in sintonia con quelle che sono le salvaguardie disposte sia a livello costituzionale che europeo (CEDU) in materia penale.[55]

Seguendo un orientamento linearmente definito, La Corte di Cassazione Sezione IV si è espressa nuovamente in materia anche nel 2022 [56]

Queste riflessioni depongono in termini ancor più marcati in favore della maggiore ragionevolezza della natura sostanzialmente penale della responsabilità degli enti *ex* d. lgs. 231/2001, secondo quella prospettiva che fa delle sanzioni ivi previste un terzo binario del sistema sanzionatorio penale».

[54] DE SIMONE, *La colpevolezza dei soggetti metaindividuali: una questione tuttora aperta*: «la categoria dogmatica più nota e diffusa è senza alcun dubbio quella della colpevolezza di organizzazione (*organisationsverschulden*) che viene ipotizzata da Tiedemann già intorno alla fine degli anni '80 del secolo scorso», in *Cass. Pen.*, Milano, 2017, 2, n.2, 917

[55] Nello stesso senso anche PADOVANI, *Manuale di diritto penale*, *La responsabilità penale delle persone giuridiche*, Milano 2023, riportando sia i criteri Engel che l'interpretazione della Cassazione: «alla luce dei criteri sviluppati dalla giurisprudenza europea (c.d. criteri Engel), la sanzione pecuniaria per quote comminata dal d.lgs. cit., assume natura sostanzialmente penale: ne consegue l'applicazione al sistema di responsabilità "amministrativa" degli enti dei principi che governano la "materia penale", ivi compresa la garanzia di ragionevole prevedibilità dell'ascrizione della responsabilità nei confronti della persona giuridica che costituisce il contenuto più qualificante del principio del *nullum crimen sine lege* nel sistema di tutela convenzionale»

[56] Cfr. Cass. pen. Sez. IV, 15 febbraio 2022 n.18143, che a sua volta riprende Cass. pen. Sez. IV, 8 gennaio 2021 n.32889 e Cass. pen. Sez. VI, 18 febbraio 2010 n.27735, in *onelegale.wolterskluwer.it*.

affermando che «l'ente risponde per un fatto proprio e non per un fatto altrui, ma non pone al riparo da possibili profili di responsabilità meramente oggettiva, sicché il giudice di legittimità ha affermato "la necessità che sussista la c.d. colpa di organizzazione dell'ente, il non avere cioè predisposto un insieme di accorgimenti preventivi idonei ad evitare la commissione di reati del tipo di quello realizzato; il riscontro di un tale deficit organizzativo consente una piana e agevole imputazione all'ente dell'illecito penale realizzato nel suo ambito operativo.
Grava sull'accusa l'onere di dimostrare l'esistenza e l'accertamento dell'illecito penale in capo alla persona fisica inserita nella compagine organizzativa della *societas* e che abbia agito nell'interesse di questa; tale accertata responsabilità si estende per rimbalzo dall'individuo all'ente collettivo, nel senso che vanno individuati precisi canali che colleghino teleologicamente l'azione dell'uno all'interesse dell'altro e, quindi, gli elementi indicativi della colpa di organizzazione dell'ente, che rendono autonoma la responsabilità del medesimo.
Si tratta di un'interpretazione che attribuisce al requisito della "colpa di organizzazione" dell'ente la stessa funzione che la colpa assume nel reato commesso dalla persona fisica, quale elemento costitutivo del fatto tipico, integrato dalla violazione "colpevole" (ovvero rimproverabile) della regola cautelare».

3. Criterio di imputazione all'ente: profili oggettivi

La responsabilità dell'ente è frutto di un collegamento al reato-presupposto; questo legame deve avere caratteristiche ben precise, definite: le conseguenze del collegamento fra reato-presupposto e persona giuridica sono particolarmente gravose, non possono quindi essere frutto di discrezionalità.

La 231/2001 quindi interviene in materia definendo all'art.5 i criteri di imputazione oggettiva; all'art.6 e 7 vengono invece definiti i criteri di imputazione soggettiva.

La Corte ha ricordato che «la Suprema Corte ha recentemente ribadito che la struttura dell'illecito addebitato all'ente risulta incentrata sul reato presupposto, rispetto al quale la relazione funzionale corrente tra reo ed ente e quella teleologica tra reato ed ente hanno unicamente la funzione di irrobustire il rapporto di immedesimazione organica, escludendo che possa essere attribuito alla persona morale un reato commesso sì da un soggettò incardinato nell'organizzazione ma per fini estranei agli scopi di questo».

Il criterio di imputazione oggettiva a sua volta è composto da due elementi: l'esistenza di un rapporto strutturale/funzionale fra la persona fisica che commette il reato e l'ente, e l'esistenza di un vantaggio di tipo "utilitaristico" fra il reato e l'ente.

Secondo l'art. 5, l'ente è infatti responsabile per i reati commessi nel suo interesse o a suo vantaggio 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 (c.d. apicali); nonché da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti precedenti.

L'art.5 dichiara poi che «l'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi».

Il rapporto strutturale/funzionale fra persona fisica ed ente sottintende un ruolo che faccia esprimere una appartenenza reale ed effettiva all'organizzazione aziendale.

Nell'art. 5 questo rapporto è distinto a seconda che si tratti dei soggetti apicali previsti nella prima parte, piuttosto che di sottoposti a direzione o vigilanza, previsti nella parte successiva, ed ha impatti diversi in funzione dei successivi articoli 6 e 7 che, come detto, si riferiscono alla imputazione soggettiva.

Allo stesso tempo l'art. 5 mette in evidenza che l'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio, specificando poi che non ne risponde se le persone indicate nel comma 1 hanno agito nell'esclusivo interesse proprio o di terzi.

Si ricava quindi che entrambe le condizioni devono essere presenti per potere attribuire responsabilità all'ente, e che questo collegamento viene meno se la persona fisica che ha commesso il reato ha agito nell'esclusivo interesse proprio o di terzi.

Come messo in evidenza [57], abbiamo quindi due legami molto forti, ascrivibile il primo al rapporto ente-persona fisica, il secondo al rapporto ente-reato. Entrambi devono essere individuati per potere essere presente la responsabilità dell'ente[58].

Il primo rapporto (ente-persona fisica) riconduce al paragrafo precedente, in particolare al divieto di responsabilità per fatto altrui, divieto rispettato: nel momento in cui la persona fisica appartiene all' organizzazione dell'ente, e realizza il reato nell'ambito di funzioni connesse all'ente, il reato è oggettivamente attribuibile all'ente.

Vale inoltre come considerazione aggiuntiva che il modello organizzativo è disposto in funzione di persone che appartengono all'ente, non in previsione di reati che provengano da soggetti esterni.

Il secondo rapporto (ente-reato) è legato all'interesse/vantaggio che l'ente ricava dalla commissione del reato. É 'richiesto dunque qualcosa in più rispetto al collegamento ente-persona fisica, ed il "qualcosa in più" è rappresentato da una situazione di utilità che, qualora mancasse, non consentirebbe la possibilità di coinvolgere l'impresa.

Questo elemento aggiuntivo è criticato da parte di alcuni autori[59], per almeno due ordini di motivi: non ha senso andare a verificare la responsabilità dell'impresa subordinandola alla presenza di un lucro; inoltre il sistema 231/2001 impegna l'ente

[57] In questo senso anche *Il criterio di imputazione* cit., 174: «il criterio di imputazione oggettiva svolge la funzione di creare un primo legame tra persona fisica ed ente, un legame addirittura molto forte, perché incentrato non solo sul rapporto strutturale fra persona fisica ed ente, ma anche su un collegamento strumentale tra il reato e l'ente».

[58] Così anche SANTI, *Responsabilità da reato degli enti e modello di esonero*, Milano 2016, cap. XIV principio affermato anche da Cass. pen. 5 ottobre 2010, n. 2251, per la quale « il reato che viene realizzato dai vertici dell'ente, ovvero dai suoi dipendenti, è solo uno degli elementi che formano l'illecito da cui deriva la responsabilità dell'ente, che costituisce una fattispecie complessa, in cui il reato rappresenta il presupposto fondamentale, accanto alla qualifica soggettiva della persona fisica e alla sussistenza dell'interesse o del vantaggio che l'ente deve aver conseguito dalla condotta delittuosa posta in essere dal soggetto apicale o subordinato. In altri termini, all'accertamento del reato commesso dalla persona fisica deve necessariamente seguire la verifica sul tipo di inserimento di questa nella compagine societaria e sulla sussistenza dell'interesse ovvero del vantaggio derivato all'ente: solo in presenza di tali elementi la responsabilità si estende dall'individuo all'ente collettivo, in presenza cioè di criteri di collegamento teleologia) dell'azione del primo all'interesse o al vantaggio dell'altro, che risponde autonomamente dell'illecito "amministrativo". Ne deriva che tale illecito non si identifica con il reato commesso dalla persona fisica, ma semplicemente lo presuppone» in *onelegale.wolterskluwer.it*

[59] Così BARTOLI, *Il criterio di imputazione*, cit., 174.

nella "colpa in organizzazione", che prescinde dalla presenza di un "utile" ed è piuttosto legato alla "copertura" del rischio di reato derivante dall'attività aziendale.

Tornando al primo rapporto (persona fisica – ente), il comma 1 dell'art. 5 distingue il c.d. rapporto apicale, dai soggetti sottoposti a direzione o vigilanza.

Fra i soggetti apicali sono individuati coloro che «che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale», oltre che quelli che «esercitano, anche di fatto, la gestione e il controllo dello stesso».

Secondo la Relazione alla 231/2001, [60] mentre la prima parte esplicitava le figure apicali formali, la seconda parte aveva come obiettivo di andare a recuperare le situazioni dell'esercizio di fatto delle funzioni apicali, in linea anche con le disposizioni attuali del Codice civile e della legge fallimentare dove viene disciplinata la figura dell'amministratore di fatto, equiparandola alle figure apicali formali.

Tuttavia, nella interpretazione successiva, si è ritenuto che la prima parte non si limitasse a considerare le qualifiche formali descritte, ma esprimesse un criterio di riconoscimento funzionale-effettivo. Quindi la seconda parte viene di fatto assorbita nella prima nelle modalità descritte dalla relazione, e deve pertanto assumere un significato diverso.[61] Fra queste, la situazione del c.d. "socio sovrano",

---

[60] Relazione alla 231/2001, cit.

[61] Considerazione riportata fra gli altri da SANTI, *Modelli e Responsabilità*, cit., 164; si veda anche Trib. Milano, ordinanza, 20 dicembre 2004, sezione competente in materia di impugnazione di provvedimenti cautelari in *Riv.231*: « È pur vero che, come visto, il fatto che la società appellante sia mera società controllante (o comunque *holding* che gestisce le partecipazioni in altre società) non impedisce di ravvisare il carattere di finalizzazione all'interesse della capogruppo o della *holding* degli atti corruttivi compiuti per fare aggiudicare appalti alla controllata, ma ciò non vuol dire che al fine dell'applicazione della misura cautelare interdittiva nei confronti della controllante i requisiti per la sua applicazione debbano sussistere nei confronti della controllante medesima, senza alcuna possibilità di indebita estensione alla stessa di circostanze verificate solo per la struttura delle controllate.
Infatti, se si hanno elementi per ritenere che l'amministratore della controllante si ingerisca non episodicamente nella direzione operativa della controllata e che gli atti da lui compiuti sistematicamente in quest'ultima siano dovuti al rapporto di fatto che il soggetto instaura con la controllata, allora si deve concludere che questo svolga funzioni di amministratore di fatto di quest'ultima, e la misura interdittiva deve essere richiesta e applicata nei confronti della medesima controllata per l'illecito dipendente da reato commesso da soggetto in posizione apicale in quest'ultima (amministratore di fatto ai sensi dell'art. 5 co. 1 lett. a - persone che esercitano anche di fatto la gestione e il controllo dello stesso ente)»; ed ancora sul punto nello stesso senso BARTOLI, *Il criterio di imputazione*, cit., 180.

cioè quel soggetto che pur senza avere incarichi all'interno della società ne detiene la quasi totalità, condizionandola.

L'art. 5 distingue innanzitutto fra funzione di rappresentanza, di amministrazione e di direzione.

Per quanto spesso ci sia una sovrapposizione fra queste funzioni, esse sono concettualmente diverse.

La rappresentanza indica la capacità ad emettere o ad essere destinatari di dichiarazioni negoziali per conto dell'ente. Deve a sua volta distinta fra rappresentanza organica e volontaria. La prima rappresenta la situazione tipo: si tratta di un potere che viene attribuito, a determinati soggetti, organi della società, di rappresentarla verso l'esterno. Rientra senza alcun dubbio nelle previsioni della lettera a).

La seconda invece è legata ad un negozio giuridico di procura. Questa può essere rilasciata indifferentemente a soggetti interni quanto esterni all'organizzazione aziendale.

Non si ritiene che questi tipi di rappresentanti possano essere annoverati fra i soggetti apicali, in quanto non hanno una posizione di preminenza su altri soggetti, anzi al contrario sono vincolati al compimento di atti o categorie di atti, secondo uno schema mandante -mandatario, sotto la vigilanza dello stesso, nei limiti del mandato e con obbligo di rendiconto. Si tratta dunque di una situazione che ricade nell'ambito dei soggetti sottoposti a direzione o vigilanza.[62]

L'amministrazione indica il potere di gestione e di controllo dell'ente o di parte di esso. La funzione amministrativa si esplica attraverso il potere di iniziativa, quello esecutivo, decisionale e rappresentativo. La figura simbolo è quella dell'amministratore delegato, o degli amministratori delegati, se più di uno, ma deve considerarsi apicale anche il ruolo di consigliere di amministrazione, vale a dire di amministratore non delegato.

[62] Valutazione condivisa da più autori, cfr. nota 61 stesso capitolo.

Nel sistema dualistico ruolo apicale è quello di membri del consiglio di gestione, a cui l'art 2409-*novies* assegna i compiti di gestione dell'impresa e di attuazione dell'oggetto sociale.

L'amministratore dipendente, che rappresenta la situazione in cui l'amministratore ha un contratto di lavoro dipendente, deve essere esaminato secondo il consueto criterio funzionale, e pertanto deve considerarsi apicale.[63]

La "direzione" infine rappresenta una figura da interpretare sempre avendo attenzione non alla definizione formale (che comunque nell'articolo manca), ma a quella sostanziale. La figura tipo è quella del Direttore Generale, dipendente sottoposto alle direttive del consiglio di amministrazione, che deve attuare, con notevoli poteri di gestione, caratterizzati da autonomia nella realizzazione. L'evidenza è di considerare come soggetti apicali i c.d. "*managers*", dipendenti in grado di assumere rilevanti decisioni in ambito aziendale.[64]

L'art. 5 aggiunge alle «funzioni di rappresentanza, di amministrazione o di direzione dell'ente» quelle di «una sua unità organizzativa dotata di autonomia finanziaria e funzionale».

La stessa Relazione ministeriale alla 231/2001[65] spiega che ci si riferisce ad una figura simbolo che è quella del direttore di stabilimento: Soprattutto nelle aziende di dimensioni medio/grandi sono presenti delle unità organizzative, a cui capo sono posti dipendenti con funzioni direttive, in grado di prendere decisioni anche in autonomia gestionale e con un controllo relativo da parte della casa madre.

Tuttavia, nel fare prevalere la sostanza, si dovrà verificare, come ricordato nello stesso art. 5, la presenza di autonomia finanziaria e funzionale, criterio differenziante in tema di imputazione.

A concludere queste note relative alla prima parte dell'art.5 (collegamento persona fisica-ente), resta da esaminare la posizione del collegio sindacale, organo di grande

[63] Così concordemente fra gli altri: PRESUTTI, *Manuale della responsabilità*, cit., 68; SANTI, *Modelli e responsabilità*, cit., *Il criterio di imputazione*, cit., 179.
[64] Valutazione riportata fra gli altri da SANTI, *Modelli e Responsabilità* cit., 166.
[65] Relazione al d.lgs. 8 giugno 2001, n.231, 3.2.

importanza societaria, da rendere compatibile o meno con la prescrizione normativa «esercitano […] gestione e controllo».

È bene sottolineare che l'art. 5 evidenzia la necessità congiunta di due funzioni: quella di gestione e quella di controllo. Questo di suo è già indicativo del fatto che il collegio sindacale non può essere inserito nelle evidenze dell'art. 5.

La stessa Relazione alla 231/2001[66], più volte citata, esclude i sindaci dai soggetti apicali. Anche la riforma societaria del 2003 si è espressa nello stesso modo, e, nell'estendere la responsabilità dell'ente ai reati societari, non ha richiamato i sindaci nell'art.25-*ter*.

A fronte di questa valutazione sono tuttavia presenti posizioni diametralmente opposte: si fa rilevare, ad esempio, la possibilità da parte del sindaco, piuttosto che del collegio sindacale, di realizzare una politica criminale connivente con le attività degli amministratori, e quindi in grado di generare reati per i quali sarebbe presente una responsabilità in capo all'ente.

In realtà il comportamento del sindaco può essere scomposto in due fattispecie: situazioni di reati realizzati dagli amministratori, per i quali i sindaci si muovono "in concorso" per non avere impedito il reato. In questi casi il reato è comunque commesso da soggetti apicali (gli amministratori), e l'ente è quindi coinvolto, senza necessità di sconvolgere il significato letterale dell'art.5 (gestione assente nel collegio sindacale)[67], e altre situazioni, espressioni invece di reati "tipici" dei sindaci, quindi riferite alle attività di gestione degli stessi. I questi casi il dato

[66]Relazione al d.lgs. 8 giugno 2001, n.231,3.2.

[67] BARTOLI, *Il criterio di imputazione*, cit., 181, mette in evidenza che l'uso congiunto dei due termini "gestione e controllo" suggerisce che non possano essere considerati apicali i membri del collegio sindacale. L'autore cita a maggior forza la stessa Relazione ministeriale, (le funzioni di gestione e controllo devono concorrere ed assommarsi nello stesso soggetto), e la stessa riforma societaria del 2003, che nell'estendere la responsabilità dell'ente anche ai reati societari, nell'art.25-*ter* non menziona i sindaci fra gli organi della società. Nel proseguo, lo stesso autore distingue poi le due ipotesi riportate nel testo della tesi: reati che vengono commessi dagli amministratori, rispetto ai quali i sindaci possono rispondere in quanto *in concorso*, per non avere impedito il reato, e situazioni in cui siamo in presenza di reati propri dei sindaci, con intervento penale ritagliato intorno alle specifiche aree gestionali dei sindaci, «con la conseguenza che quantomeno in linea di principio per i reati propri dei sindaci il reato sarà ascritto all'ente secondo il paradigma dei soggetti apicali».

normativo si ripresenta nella sua interezza "gestione e controllo", ed il sindaco sarebbe considerabile soggetto apicale ai sensi dell'art.5.[68]

Venendo alla definizione delle persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali,[69] il discrimine non è di tipo formale, quanto di natura funzionale-oggettiva: si deve dunque osservare la effettiva sottoposizione al controllo degli apicali, senza essere vincolati in modo assoluto dal rapporto formale che lega il soggetto all'ente. Ne deriva che anche in presenza di rapporti temporanei, o di rapporti formalmente non inseriti all'interno dell'organizzazione, si è in presenza di "subordinati" qualora si risponda sotto la direzione e la vigilanza dei soggetti apicali.

Nulla da rilevare se è presente un rapporto di lavoro subordinato, vengono invece in esame altre categorie di lavoratori.

In primo luogo, tutti quei rapporti autonomi dove sono presenti anche caratteristiche del rapporto subordinato: si pensi ad esempio ai collaboratori occasionali, a progetto, gli associati in partecipazione. Si tratta di situazioni che devono sempre essere valutate secondo il criterio funzionale-oggettivo, che mette in evidenza un assoggettamento di questi lavoratori alla direzione ed alla vigilanza degli apicali, sicuramente per ciò che riguarda il risultato finale.

Analoga considerazione vale per una figura sicuramente autonoma dal punto di vista formale (informatori medico-scientifici) che ricoprono una posizione a

[68] Così BARTOLI, *Il criterio di imputazione*, cit., 182. In senso netto, per l'esclusione dei sindaci dalle figure apicali BERNASCONI – PRESUTTI, *Manuale della responsabilità*, cit., 76: « poiché la locuzione "gestione e controllo" (ex comma 1 lett. a) individua un concetto di "dominio, di pilotaggio e di capacità di imprimere all'ente una determinata politica di partecipazione e affermazione sul mercato ", ne consegue che il sostantivo "controllo" non può essere identificato con la funzione di vigilanza (svolta dai sindaci); quindi, i membri del collegio sindacale o di altri organismi di (puro) controllo interno non possono essere considerati alla stregua di soggetti apicali.
[69] Sull'argomento fra gli altri in modo diffuso SANTI, *Modelli e Responsabilità*, cit., cap. XIII, 169. L'autore cita inizialmente le due tendenze interpretative, per la prima l'espressione "sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale" «indicherebbe persone comunque collegate contrattualmente all'organizzazione dell'ente. In questo modo l'ambito di applicazione della norma si allarga fino a comprendere quelle che forniscono prestazioni all'ente, rimanendo tuttavia esterne ad esso. Secondo diversa e più meditata corrente di pensiero l'espressione allude solo le risorse umane interne all'ente o almeno raggiunge quelle che appartengono allo stesso "ambito soggettivo"».

contatto con l'industria farmaceutica nel rapporto con il Sistema Sanitario Nazionale, e che certo sottendono alle disposizioni dell'industria stessa[70].

Più in generale, anche considerando altri soggetti (concessionarie), si cerca un discrimine netto per stabilire se si è in presenza o meno di un rapporto subordinato. Un argomento differenziante può essere rappresentato dal tipo di controllo che la persona giuridica può svolgere nei confronti di questi soggetti, anche considerando il "modello organizzativo", a seconda se sia o meno realizzato nei confronti di questi lavoratori.

Un altro criterio può essere rappresentato dalla verifica delle possibilità di irrogare sanzioni disciplinari.

La distinzione fra "apicali" e "sottoposti" verrà ripresa in seguito per gli impatti sulla imputazione soggettiva.

A questa prima disamina sul rapporto "persona fisica- ente", deve aggiungersi per completare l'analisi dell'art.5, il rapporto "ente-reato", che, come scritto in precedenza, è legato all'interesse/vantaggio che l'ente ricava dalla commissione del reato. È richiesto dunque qualcosa in più rispetto al collegamento ente-persona fisica, ed il "qualcosa in più" è rappresentato da una situazione di utilità che, qualora mancasse, non consentirebbe la possibilità di coinvolgere l'impresa.

Due i punti da mettere in evidenza: L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio; L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi.

La previsione di una utilità, o meglio di una "doppia utilità" (interesse e vantaggio) nel disposto dell'art.5 è oggetto di molteplici interpretazioni.

La Relazione Ministeriale [71] alla 231/2001 commenta: «La formula è stata testualmente riprodotta, e costituisce appunto l'espressione normativa del citato

[70]BERNASCONI - PRESUTTI, *Manuale della responsabilità,* cit., 77, considera in proposito che «più in generale, è un tema aperto quello della collocazione, rispetto all'azienda, dei consulenti, dei collaboratori a vario titolo, dei fornitori: categorie non sussumibili *tout court* tra i subalterni ma nemmeno del tutto estranee alla eventualità di commettere reati che impegnano la responsabilità dell'ente».

[71] Relazione Ministeriale al d.lgs. 231/2001 in Aodv, 7.

rapporto di immedesimazione organica[72]. È appena il caso di aggiungere che il richiamo all'interesse dell'ente caratterizza in senso marcatamente soggettivo la condotta delittuosa della persona fisica e che "si accontenta" di una verifica *ex ante*; viceversa, il vantaggio, che può essere tratto dall'ente anche quando la persona fisica non abbia agito nel suo interesse, richiede sempre una verifica *ex post*».

Seguendo l'impostazione della Relazione Ministeriale, la dottrina ha inizialmente seguito il concetto dell'interesse come utilità caratterizzata in senso soggettivo della persona fisica, verificabile *ex ante*, e del vantaggio come una situazione oggettiva, verificabile *ex post*.

Quindi mentre l'interesse attiene alla finalità perseguita da chi agisce, nel secondo caso prescinde dalla stessa e misura un vantaggio comunque ottenuto. Siamo quindi in presenza di due requisiti autonomi e distinti, come detto uno soggettivo *ex ante*, l'altro oggettivo *ex post*.[73]

Successivamente il criterio dell'interesse si è sempre più oggettivizzato, andandosi a sovrapporre con il criterio del vantaggio. In particolare, è stato messo in evidenza il secondo comma dell'art.5. che afferma che «l'ente non risponde se le persone […] hanno agito nell'interesse esclusivo proprio o di terzi»; in questo articolo viene quindi citato il concetto di interesse ed omesso quello di vantaggio.

Da qui si è ricavato che il vero criterio di collegamento fra reato e persona giuridica è rappresentato dall'interesse: «tale interesse, quale che sia la misura, rappresenta

[72] Relazione Ministeriale al d.lgs. 231/2001, «Ribadito ancora una volta che anche la materia dell'illecito penale-amministrativo è assoggettata al dettato costituzionale dell'art. 27, già la teoria della c.d. immedesimazione organica consente di superare le critiche che un tempo ruotavano attorno alla violazione del principio di personalità della responsabilità penale, ancora nella sua accezione "minima" di divieto di responsabilità per fatto altrui. Vale a dire: se gli effetti civili degli atti compiuti dall'organo si imputano direttamente alla società, non si vede perché altrettanto non possa accadere per le conseguenze del reato».

[73] Fra gli altri: ROSSI, *Responsabilità degli enti: i soggetti responsabili*, in *Rivis. 231*, 1: « l'interesse dell'ente è da intendersi il momento centrale ed imprescindibile, da accertarsi ex ante quale finalizzazione della condotta del reato presupposto , mentre il vantaggio assume connotati più marcatamente oggettivi e richiede sempre una verifica da compiersi ex post: si tratta di una rilevante distinzione, dal momento che non ogni condotta 'interessata' può risultare vantaggiosa, ossia procurare all'ente quel 'beneficio' in vista del conseguimento del quale venne preordinata, per cui la differenziazione normativa tra interesse e vantaggio viene anche a tendere da deterrente per l'impresa, la quale, se diverso fosse il dato normativo sul punto, verrebbe chiamata a rispondere soltanto nel caso in cui l'operazione criminosa fosse andata 'a buon fine', con conseguente ottenuto beneficio economico».

il canale di collegamento realmente indefettibile tra il reato commesso e la persona giuridica, mentre il vantaggio, pur essendo concettualmente ed empiricamente distinto dal primo, giuoca un ruolo sostanzialmente comprimario, ove riscontrabile, e comunque non realmente alternativo».[74]

Si sono quindi delineate due tesi, una c.d. "*monistica*" (viene dato rilievo solo all'interesse), l'altra "*dualistica*" (viene dato rilievo sia all'interesse che al vantaggio), con quest'ultima maggioritaria e sostenuta anche dalla giurisprudenza.

Ai fini di una più completa elaborazione sul punto, ed a sostegno della tesi dualistica, è anche da tenere presente l'art.8, che cita: «la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato».

Da ciò ne deriva, anche ipotizzando che questa mancata identificazione possa essere intesa in termini minimi, ad esempio riferendosi solo e semplicemente all'identità anagrafica dell'autore[75], che non è possibile, in questi casi, dove tuttavia è presente la responsabilità dell'ente, ricostruire la finalità soggettiva dell'autore del reato.

Alla stessa conclusione si arriverebbe, con ancora più evidenza, qualora l'autore del reato non solo non venisse identificato, ma neanche individuato; in questi casi la responsabilità dell'ente sarebbe da ricondurre alla presenza di un difetto organizzativo da cui è scaturita una condotta che ha generato l'illecito: anche qui, a maggiore ragione rispetto all'ipotesi precedente, non è possibile ricostruire la finalità soggettiva della persona fisica. Ecco quindi che per stabilire il criterio di collegamento fra reato ed ente diventa indispensabile utilizzare il criterio del vantaggio.[76]

---

[74] In questo senso DE VERO, *La responsabilità delle persone giuridiche*, Milano, 2008, 158.

[75] BARTOLI, *Il criterio di imputazione oggettiva*, cit., 188. Seguendo lo schema riportato nella trattazione, l'autore individua quattro fasi. In un primo momento l'interesse è valorizzato nella sua componente soggettiva *ex ante*, ed il vantaggio in quella oggettiva *ex post*. In una seconda fase l'interesse si "oggettivizza" ed il vantaggio viene considerato non godere di autentica autonomia. La terza fase viene messa in correlazione al momento in cui la prassi inizia a valorizzare l'applicazione dell'art.8: ne deriva «il definitivo tramonto della concezione soggettiva dell'interesse, dall'altro lato, torna a prendere corpo l'idea che il vantaggio goda di autonomia rispetto all'interesse». La quarta ed ultima fase vede una valutazione oggettiva ed autonoma sia dell'interesse che del vantaggio.

[76] Nel senso che ai fini della configurabilità della responsabilità dell'ente, é sufficiente che venga provato che lo stesso abbia oggettivamente ricavato dal reato un vantaggio, anche quando non é stato possibile determinare l'effettivo interesse vantato "*ex ante*" alla consumazione dell'illecito e purché non sia, contestualmente stato accertato che quest'ultimo sia stato commesso nell'esclusivo interesse

Nel 2014 interviene sul tema la Cassazione, che fornisce una interpretazione che in parte riporta alla Relazione Ministeriale 231/2001: la Corte, nelle sue valutazioni, individua due criteri autonomi, interesse e vantaggio, che devono essere intesi entrambi in modo oggettivo. La sentenza (Thyssenkrupp)[77] mette in evidenza che «[…] di ben maggiore interesse è invece il fatto che l'art. 25-*septies*[78] ha segnato l'ingresso dei delitti colposi nel catalogo dei reati costituenti presupposto della responsabilità degli enti, senza tuttavia modificare il criterio d'imputazione oggettiva di cui si è detto, per adattarlo alla diversa struttura di tale categoria di illeciti. È allora insorto il problema della compatibilità logica tra la non volontà dell'evento che caratterizza gli illeciti colposi ed il finalismo che è sotteso all'idea di interesse».

La Corte afferma che «i concetti di interesse e vantaggio, nei reati colposi di evento, vanno riferiti alla condotta e non all'esito»; la soluzione viene definita logicamente obbligata, adatta l'originario criterio di imputazione (quello evidenziato nella

---

del suo autore persona fisica o di terzi, v. da ultimo Cass. pen., Sez. VI, con provvedimento del 19.01.2021, n. 15543, in *Osserv. 231*.

[77] Cfr. Cass.pen, Sez. Un., 18 settembre 2014, n.38343: «d'altra parte, nei reati colposi di evento sembra ben difficilmente ipotizzabile un caso in cui l'evento lesivo corrisponda ad un interesse o vantaggio dell'ente. Tale singolare situazione ha indotto qualcuno a ritenere che, in mancanza di un esplicito adeguamento normativo, la nuova, estensiva disciplina sia inapplicabile. È la tesi sostenuta dal ricorrente. Tali dubbi e le estreme conseguenze che se ne desumono sono infondati. Essi condurrebbero alla radicale caducazione di un'innovazione normativa di grande rilievo, successivamente confermata dal d.lgs. 7 luglio 2011, n. 121, col quale è stato introdotto nella disciplina legale l'art. 25-*undecies* che ha esteso la responsabilità dell'ente a diversi reati ambientali. Il problema prospettato deve essere allora risolto nella sede propria, che è quella interpretativa. I risultati assurdi, incompatibili con la volontà di un legislatore razionale, cui condurrebbe l'interpretazione letterale della norma accredita senza difficoltà l'unica alternativa, possibile lettura: i concetti di interesse e vantaggio, nei reati colposi d'evento, vanno di necessità riferiti alla condotta e non all'esito antigiuridico. Tale soluzione non determina alcuna difficoltà di carattere logico: è ben possibile che una condotta caratterizzata dalla violazione della disciplina cautelare e quindi colposa sia realizzata nell'interesse dell'ente o determini comunque il conseguimento di un vantaggio. Il processo in esame ne costituisce una conferma. D'altra parte, tale soluzione interpretativa, oltre a essere logicamente obbligata e priva di risvolti intollerabili dal sistema, non ha nulla di realmente creativo, ma si limita ad adattare l'originario criterio d'imputazione al mutato quadro di riferimento, senza che i criteri d'ascrizione ne siano alterati. L'adeguamento riguarda solo l'oggetto della valutazione che, coglie non più l'evento bensì solo la condotta, in conformità alla diversa conformazione dell'illecito; e senza, quindi, alcun *vulnus* ai principi costituzionali dell'ordinamento penale. Tale soluzione non presenta incongruenze: è ben possibile che l'agente violi consapevolmente la cautela, o addirittura preveda l'evento che ne può derivare, pur senza volerlo, per corrispondere ad istanze funzionali a strategie dell'ente. A maggior ragione vi è perfetta compatibilità tra inosservanza della prescrizione cautelare ed esito vantaggioso per l'ente»; in *Giur.Pen., giurisprudenzapenale.com.*

[78] Ci si riferisce al reato di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Relazione Ministeriale), al nuovo quadro di riferimento, e ribadisce che la valutazione deve riguardare la condotta, ed evidenzia che «è ben possibile che l'agente violi consapevolmente la cautela, o addirittura preveda l'evento che ne può derivare, pur senza volerlo, per corrispondere ad istanze funzionali a strategie dell'ente. A maggior ragione vi è perfetta compatibilità tra inosservanza della prescrizione cautelare ed esito vantaggioso per l'ente», favorendo una concezione oggettiva di interesse.[79]

A seguito di quanto riportato, interesse e vantaggio sono quindi due criteri autonomi. L'interesse si riferisce alla persona fisica, non in quanto *psiche* ma nel comportamento realizzato. Il vantaggio invece riferisce maggiormente all'ente, ed in quanto diverso dal criterio di interesse è autonomo da esso.[80]

Entrambi sono da concepire in termini oggettivi, ed entrambi si riferiscono ad utilità ricevute dall'ente. La loro distinzione si basa dunque sul modo in cui devono essere valutati: l'interesse «deve essere valutato in termini potenziali rispetto alla condotta e al momento della realizzazione e quindi in una prospettiva *ex ante*, il vantaggio costituisce invece un evento effettivo da accertare *ex post*».[81]

Entrambi i criteri hanno comunque una nota in comune: l'utilità arrecata all'azienda non è una utilità qualsiasi, quanto piuttosto deve essere presente un contenuto patrimoniale economicamente quantificabile. Questo può esprimersi sia nel senso del risparmio[82] (ad.es. risparmio di costi, di risorse, derivanti dalla non applicazione della normativa di prevenzione), che sotto forma di profitto (aumenti di produttività).

---

[79] Cfr. Cass., Sez. Un, 18 settembre 2014, n.38343, in *Giur. Pen., giurisprudenzapenale.com*

[80] Per considerazioni nello stesso senso della posizione della Corte di Cassazione, una nota proveniente dal settore giudiziario, DE FALCO, Procuratore Repubblica Frosinone, *Interesse e vantaggio dell'ente in tema di salute e sicurezza del lavoro: dal risparmio di costi alle scelte globali di non sicurezza*, *Rivis. 231.*

[81] Nel momento in cui interesse e vantaggio hanno un contenuto quasi sovrapponibile, in quanto entrambi volti al perseguimento di una "utilità" per l'ente, diventa indispensabile mettere a fuoco la distinzione fra i due concetti. Sul punto vedi anche BARTOLI, *Il criterio di imputazione*, cit., 191.

[82] Cfr. Cass. pen. Sez. IV, 16 luglio 2015 n.31003: «interesse e vantaggio vanno letti, nella prospettiva patrimoniale dell'ente, come risparmio di risorse economiche conseguente all'aumento di produttività non ostacolata dal pedissequo rispetto della normativa prevenzionale»; v. anche Cass. pen. Sez. IV, 29 aprile 2015 n. 18073: l'utilità può derivare dal «consistente risparmio di costi per l'ente, in particolare relativi alle consulenze in materia, agli interventi strumentali necessari, nonché alle attività di formazione ed informazione del personale» entrambe in *onelegale.wolterskluwer.it.*

Su questo tema può essere citata la Sentenza 8 giugno 2021 n. 22256 della IV Sezione Penale Cassazione[83] (relativa ad un lavoratore investito da un muletto). Dopo avere riaffermato che i concetti di interesse e vantaggio vanno di necessità riferiti alla condotta e non all'evento e che tali criteri di imputazione oggettiva sono alternativi e concorrenti tra loro, la Corte evidenzia che: «il risparmio in favore dell'impresa, nel quale si concretizzano i criteri di imputazione oggettiva rappresentati dall'interesse e dal vantaggio, può consistere anche nella sola riduzione dei tempi di lavorazione».

La sentenza poi esamina un altro importante aspetto, legato alle situazioni in cui il vantaggio ha una apparenza di esiguità, definendo la necessità che lo stesso, misurato dall'apprezzamento del giudice di merito, non sia irrisorio: «quanto, poi, alla consistenza del vantaggio, deve certamente trattarsi di importo non irrisorio, il cui concreto apprezzamento è rimesso alla valutazione del giudice di merito, che resta insindacabile ove congruamente e adeguatamente motivata».[84]

[83] Cfr. Cass. pen., Sez. IV 8 giugno 2021 n. 22256, in *Giurisp. Pen., giurisprudenzapenale.com*, con note di Fracanzi F.

[84] La Corte stabilisce che il giudice deve valutare in modo completo l'atteggiamento dell'impresa, anche in termini di osservanza generale delle disposizioni in materia di sicurezza del lavoro: « l'esiguità del risparmio di spesa derivante dall'omissione delle cautele dovute, in un contesto di generale osservanza da parte dell'impresa delle disposizioni in materia di sicurezza del lavoro (ed in mancanza di altra prova che la persona fisica, omettendo di adottare tali cautele, abbia agito proprio allo scopo di conseguire un'utilità per la persona giuridica, e - quindi - in una situazione in cui l'omessa adozione delle cautele dovute sia plausibilmente riconducibile anche a una semplice sottovalutazione del rischio o ad un'errata valutazione delle misure di sicurezza necessarie alla salvaguardia della salute dei lavoratori), ai fini del riconoscimento del requisito del vantaggio occorre la prova della oggettiva prevalenza delle esigenze della produzione e del profitto su quella della tutela della salute dei lavoratori quale conseguenza delle cautele omesse: la prova, cioè, dell'effettivo, apprezzabile (cioè non irrisorio) vantaggio (consistente nel risparmio di spesa o nella massimizzazione della produzione, che può derivare, anche, dall'omissione di una singola cautela e anche dalla conseguente mera riduzione dei tempi di lavorazione) non desumibile, *sic et simpliciter*, dall'omessa adozione della misura di prevenzione dovuta. In altri termini laddove non vi sia la prova - desumibile anche dalla sistematica sottovalutazione dei rischi - che l'omessa adozione delle cautele sia il frutto di una scelta finalisticamente orientata a risparmiare sui costi di impresa, (cioè di una specifica politica aziendale volta alla massimizzazione del profitto con un contenimento dei costi in materia di sicurezza, a scapito della tutela della vita e della salute dei lavoratori), e risulti, invece, l'occasionalità della violazione delle norme antinfortunistiche, dovendosi escludere il requisito dell'interesse, deve essere rigorosamente provato quello del vantaggio, che può alternativamente consistere in un apprezzabile risparmio di spesa o in un, sempre apprezzabile, aumento della produttività, e la motivazione della sentenza che riconosca tale vantaggio deve dare adeguatamente conto delle prove, anche per presunzioni, dalle quali lo ha desunto».

Un ulteriore punto di attenzione è relativo alla disposizione dell'art.5 che «l'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi».

Come è evidente, si tratta di una situazione compatibile solo con un comportamento doloso.

La Relazione Ministeriale[85] ha evidenziato come in queste ipotesi si interrompa il rapporto persona fisica-ente, e quindi il reato non è più riconducibile alla persona giuridica, in quanto non realizzato neanche parzialmente nell'interesse di questo.

Come riportato più indietro, la Relazione Ministeriale si esprimeva a favore di una interpretazione dell'interesse in senso soggettivo; ne consegue una sicura coerenza fra questo tipo di interpretazione e l'interruzione del rapporto persona fisica-reato legato alla assenza di interesse prevista nel secondo comma dell'art.5, da cui scaturisce l'assenza di responsabilità della persona giuridica.

In presenza di una interpretazione oggettiva del concetto di interesse diventa più complicato condividere questa posizione: in buona sostanza è ben possibile che il comportamento della persona fisica, pur agendo nell'interesse esclusivo proprio o di terzi, abbia realizzato una condotta che oggettivamente realizzi interesse per l'ente.

In queste situazioni sembra più opportuno distinguere fra i casi in cui non è presente un interesse oggettivo, e la responsabilità dell'ente non sussiste, neanche in caso di vantaggio; ed i casi in cui l'interesse oggettivo è ravvisabile; qui, anche in assenza di un vantaggio, l'ente sarà responsabile.[86]

---

[85] Relazione al d.lgs.8 giugno 2001, n.231, 3.2: «La norma stigmatizza il caso di "rottura" dello schema di immedesimazione organica; si riferisce cioè alle ipotesi in cui il reato della persona fisica non sia in alcun modo riconducibile all'ente perché non realizzato neppure in parte nell'interesse di questo. E si noti che, ove risulti per tal via la manifesta estraneità della persona morale, il giudice non dovrà neanche verificare se la persona morale abbia per caso tratto un vantaggio (la previsione opera, dunque, in deroga al primo comma)».

[86] Così BARTOLI, *Il criterio di imputazione*, cit., 195, che richiama Cass. pen. 5 giugno 2013 n. 24559, «anche la giurisprudenza sembra aderire a questo orientamento, là dove si è ritenuto che anche se la persona ha agito nell'esclusivo interesse proprio, la responsabilità sussiste allorchè la condotta avvantaggi oggettivamente l'ente».

4. Criterio di imputazione all'ente: profili soggettivi ed autonomia (art.8)

Gli articoli 6 e 7 sono centrali nella imputazione soggettiva del reato.

Il legislatore ha distinto normativamente due situazioni diverse, differenziando fra reati commessi da soggetti in posizione apicale (art.6), e da sottoposti all'altrui direzione (art.7).

In entrambe le situazioni viene fatto riferimento alla adozione di un modello organizzativo,[87] che rappresenta, alle condizioni riportate nella norma (e valutate dal giudice), il discrimine fra imputazione e non imputazione soggettiva.[88]

L'imputazione per i reati commessi da soggetti apicali è definita in negativo con una serie di requisiti la cui presenza consente all'ente di "non rispondere". I requisiti, tuttavia, devono essere provati dall'ente stesso; quindi, rispetto agli schemi ordinari del diritto penale, siamo in presenza di una apparente inversione dell'onere della prova.

Di conseguenza l'attenzione degli studiosi si è particolarmente concentrata sull'art. 6, in funzione di questa problematica inversione dell'onere della prova a carico dell'ente; infatti, se un illecito penale sia stato commesso da uno dei soggetti in posizione apicale nel suo interesse o a suo vantaggio , per andare esente da responsabilità, l'ente dovrà dimostrare tutte le circostanze tassativamente elencate nell'articolo stesso: adozione ed efficace attuazione di modelli organizzativi idonei da parte dell'organo dirigente; creazione di un organismo di vigilanza (OdV), con autonomi poteri d'iniziativa e di controllo; elusione fraudolenta dei modelli da parte dell'autore del reato presupposto; non omessa o non insufficiente vigilanza da parte dell'OdV.

---

[87] DE SIMONE, *La colpevolezza dei soggetti metaindividuali*, cit., 917: «Attraverso il richiamo ai modelli organizzativi, di cui si fa menzione nelle anzidette disposizioni, si può ritenere che il legislatore delegato abbia inteso configurare e riempire di contenuto l'*Organisationsverschulden* della persona giuridica».

[88] SALCUNI, *Brevi cenni sull'imputazione soggettiva del reato commesso dagli apicali e ruolo del giudice*, in *Giurisp. Pen.*, 2017, 12 ,1: l'autore mette in evidenza la situazione tipo di "colpevolezza colposa", che rappresenta la regola della 231, distinguendola dalla "colpevolezza dolosa", «difficilmente riscontrabile nella prassi, anche se non del tutto estranea alla 231, laddove all'art.16 si fa riferimento ad un ente che è già stato condannato almeno tre volte negli ultimi sette anni», caratterizzata «da una politica aziendale che veda di buon occhio anche la commissione di illeciti».

Riprendendo la Relazione Ministeriale, per quanto attiene la imputazione soggettiva,[89] la stessa evidenzia innanzitutto che il reato deve essere collegabile all'ente non solo da punto di vista oggettivo, ma anche soggettivo, e specifica che in questo caso è necessario distinguere, come già detto, fra figure apicali e sottoposti.

Prosegue poi, nell'esaminare la responsabilità da reato degli apicali, spiegando che la particolare qualifica degli autori materiali dei reati ha portato a differenziare il sistema rispetto all'ipotesi in cui il reato risulti commesso da un sottoposto; è stato così prevista nel primo caso, una inversione dell'onere probatorio. Di fatto si presume che, quando si è in presenza di un reato commesso da un apicale, il requisito soggettivo è già assunto, in quanto il vertice è in grado di esprimere, ed esprime, la società. Sarà pertanto quest'ultima a dovere dimostrare la propria estraneità.

Per comprendere appieno la logica di questa soluzione, è opportuno ricordare che nella fase storica da cui prende forma la 231/2001 il criterio dominante di collegamento fra persona fisica ed ente era quello della immedesimazione organica[90]; quindi, «come l'amministratore impegna la volontà dell'ente in sede contrattuale senza che altro si richieda, così sarebbe dovuto accadere sul fronte della responsabilità penale».

Tuttavia, la soluzione adottata dalla 231/2001 cerca di assumere caratteri diversi, ed invece di riferirsi in modo pieno al criterio della immedesimazione organica, aderisce a quello della "culpa in vigilando", che diventa "colpa d'organizzazione".

Le valutazioni legislative si erano infatti tarate su modelli aziendali complessi, di notevoli dimensioni, con livelli decisionali fatti non da "un padrone-azienda" o

[89] Relazione Ministeriale d.lgs. 231/2001, in *Aodv231*.: «Ai fini della responsabilità dell'ente occorrerà, dunque, non soltanto che il reato sia ad esso ricollegabile sul piano oggettivo (le condizioni alle quali ciò si verifica, come si è visto, sono disciplinate dall'art. 5); di più, il reato dovrà costituire anche espressione della politica aziendale o quanto meno derivare da una colpa di organizzazione», e, sulla imputazione dell'art.6 «Tanto premesso in generale sulla necessità di costruire un modello puntuale di responsabilità dell'ente, lo schema di decreto legislativo differenzia la disciplina a seconda che il reato sia commesso da un soggetto in posizione apicale ovvero da un semplice sottoposto».

[90] Per una ricostruzione storica delle dottrine e delle tesi preponderanti nella fase di redazione del decreto, v. anche DI GIOVINE, *Il criterio di*, cit., 205

meglio da un amministratore unico di una azienda di piccole dimensioni, quanto piuttosto da un *management* articolato, costituito ad esempio da un nutrito Consiglio di Amministrazione, ed uno o più amministratori delegati.

In una situazione del genere esprimere una normativa basata sul criterio di immedesimazione organica sarebbe stato un errore, perché in strutture di questa complessità l'operato di un amministratore non necessariamente esprimeva quello degli altri.

Si preferì adottare quindi uno schema dove il modello organizzativo veniva applicato ad entrambe le situazioni (apicali e sottoposti), con una inversione della prova per ciò che riguarda l'art.6.

La base partenza, (considerare come modello di riferimento per la legislazione una azienda di notevoli dimensioni, con sistema apicale frazionato), rappresenta una scelta legislativa. L'alternativa sarebbe stata individuare diversi criteri di imputazione soggettiva, in funzione della tipologia giuridica e delle dimensioni aziendali.[91] Si è optato invece per un modello unico.

L' inversione della prova prevista nella 231/2001 è stata notevolmente commentata e criticata in modo diffuso ed importante, rappresentando una deroga notevole ai nostri principi di diritto penale.

Si rileva che di fondo la responsabilità dell'ente sussiste in presenza di un reato commesso nell'interesse dell'ente dagli organi direttivi; considerato poi che la dimostrazione richiesta dall'art. 6, Comma 1, lettera c, impone una "*probatio diabolica*",[92] ne deriva che la responsabilità dell'ente per fatto commesso dai soggetti apicali trova di fatto fondamento nel tradizionale principio di immedesimazione organica.

L'inversione, «altera non poco i criteri di imputazione della responsabilità, tanto più se la responsabilità dell'ente fosse assimilabile ad una responsabilità di tipo

[91] SALCUNI, *Brevi cenni sull'imputazione*, cit. 2017, 12 ,3. L'autore mette in evidenza che per creare un modello di imputazione unica «si è preferito unificare i modelli di imputazione per sottoposti ed apici, anziché prevedere, ad esempio, diversi criteri di imputazione soggettivi a seconda della struttura societaria».

[92] ANTOLISEI, *Manuale di Diritto penale*, cit., vol. 2, 2014, 705. Ci si riferisce al punto c), elusione da parte dei soggetti apicali.

penale, con ciò che ne consegue sulla compatibilità di questo meccanismo con il principio costituzionale della presunzione di non colpevolezza».[93]

Secondo alcuni autori, «la questione, purtuttavia, andrebbe probabilmente sdrammatizzata[94], tenuto conto, in particolare, del fatto che, nel gioco processuale delle parti, sarà l'ente stesso, il più delle volte, a preoccuparsi di portare all'attenzione del giudice la documentazione relativa al modello organizzativo adottato, mentre sarà poi lo stesso giudice a verificarne l'efficienza e l'idoneità».

Sull'importante tema dell'inversione dell'onere della prova è intervenuta la Corte di Cassazione con sentenza 16 luglio 2010, n.27735, ridimensionando il problema dal punto di vista formale[95], ed escludendo che l'accusa sia esonerata dal provare la colpa di organizzazione.

La sentenza della Corte[96] afferma in proposito: «grava certamente sull'accusa l'onere di dimostrare l'esistenza e l'accertamento dell'illecito penale presupposto in capo alla persona fisica inserita nella compagine organizzativa dell'ente e che questa abbia agito nell'interesse o a vantaggio dell'ente stesso. Per converso, è onere dell'ente di provare, per contrastare gli elementi di accusa a suo carico, le condizioni liberatorie di segno contrario di cui all'art. 6 d.lgs. n.231/2001. Per l'effetto, non si realizza neppure alcuna violazione dei principi costituzionali relativi al principio di eguaglianza e all'esercizio del diritto di difesa (art. 3 e 24

---

[93] ANTOLISEI, *Manuale di Diritto penale*, cit., 706, viene anche messo in evidenza che "è necessario tuttavia chiarire che, anche qualora l'ente riesca nella prova liberatoria, non di meno l'ultimo comma dell'art. 6 prevede che sia « comunque disposta la confisca del profitto che l'ente ha tratto dal reato, anche nella forma per equivalente »: questa tipologia di confisca, che si applica anche quando non si accerta la responsabilità dell'ente, non ha un contenuto punitivo, ma di tipo compensativo finalizzato a riequilibrare il trasferimento illecito di ricchezza con la perdita del profitto ingiustamente acquisito dall'ente. Sul punto anche CORDERO, *Procedura penale, processo penale amministrativo*, 2012, Milano, 1328: «da notare come nell'art. 7 manchi un *pendant* al 6 5: parrebbe dunque non confiscabile il profitto derivato dai delitti dei quali non risponda in sede amministrativa; conclusione incongrua, presumibilmente non voluta, ma così` suonano i testi"».

[94] DE SIMONE, *La colpevolezza dei soggetti metaindividuali: una questione tuttora aperta*, in *Cass. Pen.*, 2017, 02, n.2 Milano, 919. L'autore mette anche in evidenza Come, in effetti, non si è mancato di sottolineare, nella prassi applicativa si è verificato «uno spontaneo riequilibrio degli oneri probatori, dovuto alla circostanza che il giudice, per verificare l'efficacia del modello, si serve necessariamente di una perizia, spesso collegiale, con l'effetto che questo mezzo di prova finisce per assorbire e supplire agli oneri probatori dell'ente, ridotti alla sola dimostrazione della tempestiva adozione del modello e della sua astratta idoneità a ridurre il rischio-reato»

[95] L'espressione è tratta da DI GIOVINE, *Il criterio di*, cit., 207

[96] Cfr. Cass. pen. 16 luglio 2010 n.27735, poi confermata in principio da Cass., Sez. Un., 24 aprile 2014 n. 38343, entrambe in *onelegale.wolterskluwer.it*

Cost.), perché non si determina alcuna inaccettabile inversione dell'onere della prova nella disciplina che regola la responsabilità dell'ente: grava comunque sull'accusa l'onere di dimostrare la commissione del reato da parte di persona che rivesta una delle qualità di cui, all'art. 5 del decreto legislativo n. 231/2001 e la carente regolamentazione interna dell'ente, mentre quest'ultimo ha ampia facoltà di fornire prova liberatoria ».[97]

È bene ricordare che quanto l'ente è tenuto a provare per "non rispondere" del reato è indicato nell'art.6 in quattro punti. Si dovrà dimostrare che «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»; poi che «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»; che «le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione» ed infine che non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza.

Dall'esame di questi quattro punti, secondo ricostruzione di parte della dottrina, la previsione del primo comma non determina in assoluto un'inversione dell'onere della prova e quindi una lesione del principio costituzionale della presunzione di innocenza intesa quale regola di giudizio: la prova che l'ente è chiamato a fornire cade infatti sui cosiddetti «fatti impeditivi» e non già sui fatti principali, cosicché il rischio della mancata prova di questi ultimi continuerà a gravare sull'organo di accusa.[98]

È stato anche rilevato che l'elenco dei *facta probanda* «appartiene a due piani ben distinti, forzatamente inseriti in un unico contesto: da un lato, infatti, l'ente deve dimostrare di avere adottato un modello organizzativo e gestionale idoneo a prevenire la commissione di reati della specie di quello verificatosi e di averne demandato l'efficace attuazione ad un organismo autonomo dotato di poteri di iniziativa e di controllo (art. 6 comma 1 lett. a e b del Decreto); dall'altro lato,

[97] In senso critico nei confronti della Sentenza della Corte DE SIMONE, *La colpevolezza dei soggetti metaindividuali: una questione tuttora aperta,* in *Cass. Pen.*, 2017, 2, 919
[98] Si esprime in questo senso CORDERO, *Procedura penale, cit,* 1328

invece, esso deve provare sia la mancanza di *culpa in vigilando* da parte dell'organismo di controllo, sia la condotta fraudolenta dell'autore del reato, cui è addebitabile l'elusione delle norme preventive interne (art. 6 comma 1 lett. c e d del Decreto)».[99]

Il punto di maggiore attrito con i principi costituzionali è rappresentato dalla lettera c) dell'articolo 6, ovvero dai casi di elusione fraudolenta dei modelli di organizzazione e gestione da parte dei soggetti apicali.

Mentre le altre ipotesi sono affrontabili in giudizio in modo quasi automatico, qualora l'ente abbia ben fronteggiato il rischio-reato predisponendo un modello ed una organizzazione interna in grado anche di essere rappresentata cartaceamente (in questo caso al giudice), le ipotesi di elusione possono invece rappresentare un forte innalzamento del livello di difficoltà da parte dell'ente a dimostrare la propria estraneità, in quanto non in grado di provare l'elusione fraudolenta del soggetto apicale.

La Corte di Cassazione nella sentenza 18 dicembre 2013, n.4677[100] mette in evidenza quanto possa essere sofisticata la condotta messa in essere dagli apicali: «L'elusione fraudolenta […] non deve necessariamente coincidere nella mera violazione delle prescrizioni contenute nel modello […]. La *fraus legis facta* di romanistica memoria […] descrive piuttosto una condotta ingannevole, falsificatrice, obliqua, subdola […] una condotta di 'aggiramento' di una norma imperativa, non una semplice e 'frontale' violazione della stessa».

La Corte nella stessa importante sentenza ricorda, che il giudizio di colpa dell'ente si fonda sul terreno dell'adeguatezza del modello: «non si tratta [...] di responsabilità oggettiva, atteso che l'oggetto dell'esame (l'articolato normativo che esplicita un protocollo comportamentale) è comunque conseguenza di un'attività volontaria e consapevole di chi lo ha elaborato, approvato e reso esecutivo, ma si

[99] Così FIORIO, *Presunzione di non colpevolezza ed onere della prova*, in *Aodv231*, 1785, 8, citando AMODIO, *Prevenzione del rischio penale d'impresa e modelli integrati di responsabilità degli enti*, 323.

[100] Cfr. Cass. pen. Sez. V, 18 dicembre 2013, n. 4677, Impregilo, in *Dir. Pen. Contemp*., fra l'altro «l'inganno […] di cui all'art. 6 co. 1 lett. C) d.lgs. 231/2001 è evidentemente diretto verso la struttura aziendale nel cui interesse è stato predisposto il modello organizzativo e gestionale di cui alla lett. a del già menzionato comma primo»

tratta, invece, di un giudizio strettamente normativo». Queste considerazioni, piene di rispondenza se sì ci si riferisce al modello organizzativo piuttosto che all'organismo di vigilanza, valgono sicuramente di meno per il caso di elusione fraudolenta, per di più commessa da un apicale: l'ente si troverebbe nella situazione di una "*probatio diabolica*", in quanto dovrebbe dimostrare gli inganni ed i raggiri messi in opera dai soggetti apicali che hanno commesso un reato nell'interesse o nel vantaggio della *societas*[101], come unica strada per dimostrare che è stato spezzato il nesso di collegamento con l'ente stesso.

Anche dal punto di vista probatorio-documentale, mentre le altre ipotesi previste all'art.6 sono affrontabili dall'ente, come detto in precedenza, con la rappresentazione in giudizio del modello organizzativo di gestione e prevenzione del rischio aziendale, in questo caso l'attività difensiva dell'ente porterebbe ad una attività di indagine svolta dall'ente sull'apicale, relativamente al comportamento realizzato, analoga a quella svolta dal Pubblico Ministero, alla ricerca di prove da parte dell'ente a carico dell'imputato persona fisica.

Una ulteriore criticità è ravvisabile nel combinato con l'art.8, laddove la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato. Se si presumesse che il reato sia stato commesso dal vertice aziendale «il mancato accertamento della colpevolezza rende ancora più scopertamente oggettivo il criterio di imputazione»[102], e sarà ben difficile dimostrare l'elusione fraudolenta da parte di un soggetto sconosciuto.

Come detto in precedenza, l'origine di questa parte dell'art.6 è legata alla volontà di prescindere dalla teoria soggettiva dell'immedesimazione, agganciandosi invece

---

[101] BERNASCONI - PRESUTTI, *Manuale della responsabilità,* cit., 171, la ratio di un problematico requisito:" secondo quanto previsto dall'art.6 co. 1 lett. c sulla persona giuridica incombe-altresì-l'onere di provare che i propri vertici hanno eluso "fraudolentemente" il sistema finalizzato alla prevenzione dei reati: dunque anche laddove l'ente imputato riesca a dimostrare l'adozione di un efficace modello organizzativo interno e l'inesistenza di lacune o inadempienza nel controllo svolto dall'organo di vigilanza, per raggiungere l'esenzione dalla responsabilità esso dovrà allegare questa ulteriore circostanza. iI "carattere congiuntivo" (Amodio) dei fatti da provare ai fini dell'esimente (ex art.6 co. 1 lett.a, b, c e d) si risolve, come noto, in una *probatio diabolica* e il requisito in parola ne rappresenta il passaggio più impervio: infatti, resta 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 vantaggio della *societas* medesima.

[102] Così BERNASCONI - PRESUTTI, *Manuale della responsabilità* cit., 173

a quella più oggettiva della colpa in organizzazione, ma differenziando la stessa fra apicali e sottoposti in funzione di ciò che l'ente deve provare/non deve provare in presenza di reato-presupposto. La differenziazione, tuttavia, genera un recupero di quanto voleva essere evitato, in quanto ci riporta a una figura giuridica al confine fra teoria della immedesimazione organica e colpevolezza in organizzazione, portando alla conclusione che il reato commesso dagli apici è sempre espressione della volontà dell'ente, salvo che non si verifichino determinate condizioni.

È da rilevare che dal punto di vista dell'impianto sostanziale il combinato normativo esaminato è rispettoso del principio di colpevolezza: il modello organizzativo funziona da "esimente", così come l'esclusione del nesso di causalità in caso di condotta fraudolenta dell'apicale. Ciò che potrebbe alterarne il rispetto è questa inversione probatoria di difficilissimo utilizzo da parte dell'ente nel caso di condotta fraudolenta.

Una soluzione potrebbe essere rappresentata dalla considerazione che, dal momento che la società ha adottato ed implementato il modello organizzativo ed ha tenuto le doverose condotte, non dovrebbe rispondere anche se il reato non è stato compiuto eludendo fraudolentemente i modelli[103].

In occasione di un convegno tenuto a Roma nel luglio del 2010, il Ministro della Giustizia presentava un progetto di riforma[104] al d.lgs. 231/2001. Due erano le proposte di modifica di maggior rilievo: in primo luogo, il Progetto eliminava l'inversione dell'onere della prova disposto all'art. 6 d.lgs. 231/2001 per reati commessi da soggetti in posizione "apicale", prevedendo, analogamente a quanto già oggi accade in presenza di reati commessi da un "sottoposto", che sia sempre la Pubblica Accusa a dover dimostrare la mancata adozione di un modello organizzativo, o la sua inefficace attuazione.

---

[103] La considerazione è di DE VERO, *Il progetto di modifica della responsabilità degli enti tra originarie e nuove aporie*, in *Dir. Pen. e Proces.*, 2010,1137ss

[104] Convegno organizzato dall'associazione AREL (*www.arel.it*), e tenutosi a Roma il 7 luglio 2010. Il Ministro della Giustizia presentava un progetto di riforma al d.lgs. 231/2001. Tale progetto, reca la rubrica «schema di disegno di legge di modifica del decreto legislativo 8 giugno 2001, n. 231, Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300», in *Arch. Pen. Contemp.*

In secondo luogo, il Progetto prevedeva l'introduzione di un inedito meccanismo di "certificazione" dell'idoneità del modello organizzativo nel suo complesso o delle singole procedure, collegando al contempo all'ottenuta certificazione a concreti benefici per l'ente indagato/imputato.[105]

In ogni caso, la regola di giudizio secondo la quale il giudice pronuncia sentenza di esclusione della responsabilità dell'ente, prevista nell'art 66 della 231/2001, si riferisce a quando manca, è insufficiente o contraddittoria la prova dell'illecito amministrativo, e trova spazio ove appaia dubbio che il reato-presupposto sia stato commesso dai vertici societari nell'interesse o vantaggio della società: l'onere di dimostrare grava sul pubblico ministero, il che equivale a che quest'ultimo sopporta le situazioni di incertezza probatoria. «In altre parole, il dubbio sul *fatto costitutivo* porta ad una sentenza di assoluzione».

La dimostrazione della adozione e della implementazione degli schemi comportamentali codificati nell'art.6 incombe, invece, sull'ente, e di conseguenza, l'incertezza su queste condizioni ricade sulla difesa: il dubbio sul *fatto impeditivo* conduce quindi alla sentenza di condanna […] in tale ottica, l'unica interpretazione orientata nel solco dell'art.27 comma 2 Cost. sembrerebbe quella di imporre alla pubblica accusa il compito di dimostrare l'inefficacia del modello organizzativo"[106]. Questo corrisponde alla impostazione stabilita dalla Corte di Cassazione, nella citata sentenza[107]dove viene escluso che l'accusa sia esonerata dall'obbligo di provare la c.d. "colpa di organizzazione" dell'ente, e che lo stesso ha un obbligo di mera allegazione.[108]

[105] Nelle note a cura di Vizzari - Santamaria viene evidenziato che il progetto non ha mancato di suscitare immediate reazioni contrastanti: salutato con favore dal mondo delle imprese, ma già guardato apertamente con sospetto dall'Associazione Nazionale Magistrati, e addirittura etichettato come un provvedimento che introdurrebbe uno "scudo" – l'ennesimo – "per aziende e *manager*".
[106] In questo senso BERNASCONI - PRESUTTI, *Manuale della responsabilità* cit., 189,190.
[107] Cfr. Cass. pen., Sez.VI, 16 luglio 2010 n. 27735, in *onelegale.wolterskluwer.it.*
[108] Così DI GIOVINE, *Il criterio di,* cit., 207, mette in evidenza che, sul piano sostanziale, «non può esigersi di più in un settore ad alto tasso di tecnicismo nel quale, anche in presenza di una "normale" ripartizione dell'*onus probandi*, l 'accusato non potrebbe esimersi dal fornire elementi di conoscenza – forse inattingibili dall'accusa- a favore della propri posizione». Il commento dell'Autore è molto netto: «la questione è stata forse troppo enfatizzata (i problemi sono ben altri)».

L’art. 7 è invece dedicato al reato-presupposto commesso dai sottoposti - soggetti sottoposti all’altrui direzione e modelli di organizzazione dell’ente. Tratta inoltre, così come l’art.6, dei modelli di organizzazione dell’ente.

La Relazione Ministeriale mette in evidenza sul tema come [109]”meno problematica si è rivelata l'attuazione della delega in rapporto ai soggetti sottoposti, la commissione dei reati da parte dei quali appare, d'altro canto, statisticamente più rara e comunque suscettibile di determinare un giudizio di minore riprovazione nei confronti del soggetto collettivo (ciò, quanto meno in relazione alla particolare tipologica di delitti contemplata nello schema di decreto).

L’articolo al primo comma prevede la responsabilità dell’ente, qualora si sia in presenza di un reato-presupposto reso possibile dall’inosservanza degli obblighi di direzione o vigilanza. È quindi indispensabile un collegamento causale con l’inottemperanza degli obblighi previsti.

Le restanti parti della norma (commi 2, 3 e 4) disciplinano contenuti ed effetti del modello di organizzazione deputato a prevenire questi reati.

Come riportato precedentemente, il criterio di attribuzione della responsabilità distingue fra figure apicali e sottoposte ad altrui direzione; questo si traduce concretamente nella disciplina della prova. A differenza di quanto previsto nell’art.6, dove siamo in presenza di una inversione dell’onere della prova, se il reato-presupposto è realizzato dalle persone sottoposte indicate all’art. 5 comma 1 lett. b) le regole di accertamento dell’illecito ritornano quelle tradizionali, ed il mancato rispetto degli obblighi di direzione o vigilanza devono essere dimostrati dall’accusa.

Per affermare la colpevolezza della persona giuridica si dovrà quindi provare l’imputazione oggettiva (reato-presupposto commesso nell’interesse o vantaggio della persona giuridica), e quella soggettiva, identificata con il mancato rispetto dei doveri stabiliti (fatto costitutivo).

[109] Relazione Ministeriale 231/2001, cit., in *Aodv231*.

Le situazioni di dubbio seguono la disciplina dell'art. 66 d.lgs. 231/2001 e gravano sempre sul pubblico ministero, e qualora permangano genereranno esclusione della responsabilità dell'ente motivata dall'insufficienza, contraddittorietà o comunque inidoneità della prova dell'illecito amministrativo.[110]

La prima, fondamentale differenza con la disciplina della responsabilità da reato per il fatto degli apicali concerne proprio «l'elemento costitutivo dell'illecito, che viene attribuito all'ente, a fronte di un deficit organizzativo che ha portato come conseguenza all'inosservanza degli obblighi di direzione o vigilanza».

Ciò stabilito, la normativa contempla, anche in questo caso, la funzione esimente del modello organizzativo, che si evidenzia sempre più come elemento centrale della normativa della 231/2001; l'art. 7 commi 2, 3 e 4 si muove in sintonia con alcune previsioni dell'art. 6. Inserisce inoltre una qualità del modello organizzativo non presente nell'art.6: mentre qui si dispone di «modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi», all'art.7 viene inserito il concetto di controllo: quindi «modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi».

L'inserimento della funzione di controllo, in uno con quella di gestione, delinea in modo marcato «la vocazione prevenzionistica di questa figura di *compliance program*, in rapporto al rischio di mancato assolvimento del dovere di direzione e vigilanza, rischio fronteggiabile, per l'appunto, con un modello di organizzazione, gestione e controllo».[111]

Un ulteriore tema da evidenziare in termini di imputazione è la previsione dell'art.8, che afferma nella prima parte che la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato o non è imputabile.

[110] Sul punto BERNASCONI - PRESUTTI, *Manuale della responsabilità* cit., 192: «Se l'ente dimostra che 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 (art. 7 co. 2), nulla gli sarà imputabile (fatto impeditivo); in questo caso, il rischio della mancata prova è nuovamente a carico della difesa; allo stesso modo le situazioni di incertezza probatoria sull'idoneità (ed efficacia) del modello a prevenire i reati ricadranno negativamente sulla *societas*».
[111] In questo senso BERNASCONI – PRESUTTI, *Manuale della responsabilità* cit., 192

Si tratta di una importante ed ulteriore evidenziazione dell'autonomia della responsabilità dell'ente.

La Relazione Ministeriale definisce la disposizione dell'art. 8 "di particolare rilievo" [112] : la norma afferma nuovamente la distinzione fra colpevolezza dell'individuo e responsabilità dell'ente, ed interviene colmando quello che altrimenti sarebbe stato un importante vuoto legislativo: nelle imprese può essere frequente, se non addirittura tipico, il problema della mancata individuazione del soggetto che ha commesso il reato-presupposto, con la conseguenza che, in assenza di una previsione come quella dell'art.8, «si sarebbe infirmata la ratio stessa del provvedimento».[113]

È la stessa Relazione Ministeriale, a dare forza con un esempio all'importanza dell'intervento: si pensi «ai casi di c.d. imputazione soggettivamente alternativa, in cui il reato (perfetto in tutti i suoi elementi) risulti senz'altro riconducibile ai vertici dell'ente e, dunque, a due o più amministratori, ma manchi o sia insufficiente la prova della responsabilità individuale di costoro. L'omessa disciplina di tali evenienze si sarebbe dunque tradotta in una grave lacuna legislativa, suscettibile di infirmare la *ratio* complessiva del provvedimento».

La norma, quindi, prevede che in situazioni dove non viene identificato l'autore del reato-presupposto, (anche per quella che può essere la complessità dell'assetto

[112] Relazione Ministeriale 231/2001, par. 4: «Di particolare rilievo è la disposizione dell'art. 8. Essa chiarisce in modo inequivocabile come quello dell'ente sia un titolo autonomo di responsabilità, anche se presuppone comunque la commissione di un reato. Se infatti il meccanismo punitivo è stato congegnato in modo tale da rendere le vicende (processuali) delle persone fisiche e quelle dell'ente tra loro strettamente correlate (il *simultaneus processus* risponde non soltanto ad esigenze di economia, ma anche alla necessità di far fronte alla complessità dell'accertamento), ciò non toglie che in talune limitate ipotesi' l'inscindibilità tra le due possa venir meno. Una scelta di tal fatta non incontra alcun ostacolo dal punto di vista del sistema. È chiaro, infatti, che [...] ci si trova di fronte ad un reato completo di tutti i suoi elementi (oggettivi e soggettivi) e giudizialmente accertato, sebbene il reo, […]».

[113] La considerazione è inserita nella Relazione, cit.

organizzativo interno), la responsabilità dell'ente permane[114],[115]. Ovviamente, a condizione che all'ente sia imputabile una colpa organizzativa consistente nella mancata adozione ovvero nel carente funzionamento del modello preventivo.

Le conseguenze di questa importante norma di chiusura si traducono innanzitutto in un alleggerimento probatorio dell'onere dimostrativo della pubblica accusa che si accinge a perseguire un *corporate crime*.

Nelle situazioni in cui l'accusa si trovi in presenza di una piattaforma probatoria non adeguata nei confronti della persona fisica sospettata di avere commesso il reato, può contestare l'illecito alla sola persona giuridica. Questo consente al pubblico ministero di avere a disposizione "un'ama tattica"[116] che consenta di

[114] Cfr. Cass. pen., Sez I, 2 luglio 2015- 2 settembre 2015 n. 35818, *Citibank N.A.*, nel commento di AMATO, *Autore ignoto e responsabilità dell'ente*, in *La responsabilità amministrativa delle società e degli enti*, in *Rivis. 231*, 2015, 4, 1: «La Cassazione ha valorizzato il disposto dell'art. 8 d.lgs. n. 231/2001 pervenendo alla conclusione che per l'addebito a carico dell'ente non è necessario pervenire all'individuazione soggettiva di colui il quale, agendo in nome e nell'interesse/vantaggio dell'ente, ha commesso il reato presupposto. È sufficiente, invece, accertare la responsabilità penale presupposto in via incidentale, ai soli fini e per gli effetti dell'addebito a carico dell'ente. Nella specie, ciò che è stato ritenuto relativamente all'illecito di cui all'art. 25-*ter* d.lgs. n. 231/2001, contestato con riferimento al reato presupposto di aggiotaggio previsto dell'art. 2637 c.c., in una vicenda in cui l'autore del reato presupposto era stato assolto, ma era risultata comunque accertata la commissione del reato presupposto da parte di altri soggetti, pur non compiutamente identificati, comunque riconducibili alla società e che, ovviamente, avevano agito nell'interesse o a vantaggio di questa».

[115] V. anche Cass. pen., Sez. V, n. 20060, 9 aprile 2013, in *Riv. Giur. Pen.*, *giurisprudenza penale.com* 13 maggio 2013, che afferma che l'assoluzione della persona fisica imputata del reato presupposto per una causa diversa dalla rilevata insussistenza di quest'ultimo non consegua automaticamente l'esclusione della responsabilità dell'ente per la sua commissione, poiché tale responsabilità, ai sensi dell'art. 8 del d. lgs. n. 231 del 2001, deve essere affermata anche nel caso in cui l'autore del suddetto reato non sia stato identificato.

[116] L'espressione è in BERNASCONI - PRESUTTI, *Manuale della responsabilità* cit., 88. L'autore evidenzia inoltre che: «l'organo giurisdizionale non sarà in grado di stabilire — laddove sia rimasto ignoto l'autore (persona fisica) del reato — quali siano i criteri soggettivi di attribuzione della responsabilità, cioè a dire se il reato sia stato commesso da soggetto in posizione apicale (art. 5 co. 1 lett. a) o da soggetto sottoposto all'altrui direzione (art. 5 co. 1 lett. b), con quel che ne consegue in termini di ripartizione dell'onere probatorio ex artt. — rispettivamente — 6 e 7». La conseguenza è che se il reato per cui si sta procedendo è riferibile necessariamente alle sfere "apicali" perché, come da ipotesi, l'accusa potrebbe argomentare, che un subalterno non avrebbe mai il potere di decidere se corrompere un pubblico funzionario né fruire dell'autonomia necessaria per reperire e gestire le risorse adeguate a commettere il fatto , «il meccanismo dell'art. 8 finirebbe per tradire, fatalmente, l'esistenza di una presunzione: in questo caso, la mancata identificazione dell'autore del reato si ripercuote, in termini di inversione dell'onere probatorio, sull'ente (se si assume che il responsabile sia un soggetto di vertice si applicherà, infatti, la regola prevista dall'art. 6 co.1); l'ente-imputato si troverà quindi nell'impossibilità di dimostrare il requisito della elusione fraudolenta del modello organizzativo previsto dall'art. 6 co. 1 lett. c: quali condotte decettive potrà mai allegare — per provare la "fraudolenza" — se l'autore del reato-presupposto è rimasto ignoto?».

sopravanzare le eventuali difficoltà legate alla presenza di organizzazioni frammentate, in cui è difficile riuscire a risalire all'autore persona fisica del reato.

Viene inoltre messo in evidenza che il pubblico ministero ha di fatto il potere di determinare il grado di effettività del diritto di difesa (art. 24 comma 2 Cost.) e del principio della presunzione di non colpevolezza (art. 27 comma 2 Cost.) nella singola indagine, in funzione del soggetto che viene incolpato (persona fisica od ente); e questo viene riferito in particolare ai reati commessi dai vertici, con riguardo alla responsabilità del *top management*: «la contestazione del (medesimo) reato-presupposto alla persona giuridica fa guadagnare all'accusa — sul terreno della elaborazione dimostrativa — importanti vantaggi, connessi alla inversione dell'onere della prova; in breve: se non è identificato l'autore del reato, all'accusa sarà sufficiente allegare elementi indiziari per fare valere la presunzione che si tratti di un soggetto apicale (per esempio, la decisione e i mezzi per corrompere un pubblico funzionario sono prerogative di amministratori e alti dirigenti, non certo dei subalterni); sarà poi la società stessa a dovere dimostrare di aver adottato in maniera efficace i modelli organizzativi, di avere istituito un autonomo e "sempre vigile" organismo di controllo e, infine, che i vertici aziendali hanno aggirato, con fraudolenza, le suddette regole organizzative»[117].

5. Il modello organizzativo come elemento centrale

Il modello organizzativo verrà ripreso nuovamente ed in modo più esteso nel prossimo capitolo di questa tesi; ci sono tuttavia degli elementi che è opportuno sviluppare già da subito, e che vertono intorno alla centralità del modello organizzativo all'interno della 231/2001.

Il modello organizzativo da un lato rappresenta un elemento condizionante in termini di responsabilità dell'ente: in presenza di un reato-presupposto l'unica possibilità dell'ente per potere non incorrere nella sanzione o subirla in modo attenuato è legato al MOG; per altro verso, ed è un obiettivo di grande importanza, opera su un piano preventivo, o se vogliamo educativo nei confronti dell'ente,

[117] C.sopra

portandolo a predisporre uno schema organizzativo che sia in grado di precedere la realizzazione del reato stesso, evitandolo.

Limitandoci al momento alla componente legata alla responsabilità dell'ente in presenza di un reato presupposto, è pertanto in funzione della presenza e della qualità del modello organizzativo che si potrà rintracciare una colpa di organizzazione; questa sarà ravvisabile sia che ci si trovi davanti ad un reato-presupposto commesso da apicali, piuttosto che da sottoposti, od infine in assenza di una persona fisica a cui il reato è attribuibile, ed avrà conseguenze sulla responsabilità dell'ente o sulle attenuazioni delle conseguenze sanzionatorie.

Il sistema della 231/2001 è quindi" intrinsecamente condizionato dall'adozione e dall'efficace attuazione di un modello organizzativo".[118]

A fronte di una così elevata importanza del modello organizzativo, i quesiti posti in questa fase sono due, e si riferiscono alla sua obbligatorietà giuridica, (quindi se il modello deve essere predisposto obbligatoriamente dall'ente), e alla sua diversificazione, (vale a dire se il modello ipotizzato dalla 231/2001 è unico o cambia in funzione dei soggetti - apicali o sottoposti - a cui è destinato).

[118] L'espressione riportata è tratta da FIORIO, *Presunzione di non colpevolezza ed onere della prova*, in *Aodv, 1785,1*. L'autore oltre a mettere in evidenza la facoltatività del modello riporta tutta una serie di casi dove lo stesso è ormai richiesto obbligatoriamente. Fra queste l'obbligo per le società emittenti che intendano quotarsi nel c.d. STAR (Segmento Titoli con Alti Requisiti), le quali, a far data dal 1° aprile 2008 sono tenute a dotarsi di un modello organizzativo. Sono da aggiungere diverse normative regionali che impongono ai relazionanti l'adozione del modello organizzativo: viene citato l'art. 54 co. 1 L.R. Calabria 13 giugno 2008, n. 15, che prevede che le imprese «che operano in regime di convenzione con la Regione Calabria, sono tenute ad adeguare, entro il 31 dicembre 2008, i propri modelli organizzativi» alle disposizioni di cui al Decreto, «dandone opportuna comunicazione ai competenti uffici regionali». Sempre la Regione Calabria è intervenuta con L.R. 4 dicembre 2012, n. 60, imponendo agli enti pubblici economici dipendenti e strumentali della Regione, con o senza personalità giuridica; alle fondazioni costituite dalla Regione; alle società controllate dalla Regione (art. 2). di adottare «modelli di organizzazione, di gestione e controllo di cui agli articoli 6 e 7 del d. lgs. n. 231/2001, che prevedono, in relazione alla natura de servizi e delle attività svolte e alla dimensione dell'organizzazione, misure idonee a garantire lo svolgimento della propria attività nel rispetto dei princìpi di legalità, eticità e trasparenza». Viene ancora citato l'art. 2 L.R. Abruzzo 27 maggio 2011, n. 15, che impone l'adozione di modelli organizzativi "231" per gli enti dipendenti e strumentali della Regione, con o senza personalità giuridica, i consorzi, le agenzie e le aziende regionali, nonché le società controllate e partecipate dalla Regione Abruzzo ed infine, l'art. 7 co. 5 dello Statuto della Federazione Italiana Giuoco Calcio che prevede che «il Consiglio federale, sentite le Leghe interessate, emana le norme necessarie e vigila affinché le società che partecipano a campionati nazionali adottino modelli di organizzazione, gestione e controllo idonei a prevenire il compimento di atti contrari ai principi di lealtà, correttezza e probità in ogni rapporto.

Secondo l'orientamento più diffuso l'adozione del modello rappresenta un onere, nessun obbligo essendo previsto in tal senso nella 231/2001.

La 231/2001 si esprime all'art.6, disponendo che l'adozione (oltre che l'efficace attuazione) del modello di organizzazione e gestione è di competenza dell'*organo dirigente*.

Da questa formulazione ne sono stati ricavati tre diversi orientamenti, innanzitutto sul soggetto che è tenuto all'adozione del modello: il primo di questi ritiene che la terminologia utilizzata dalla norma è volutamente generica, ed esprime quindi l'ampia autonomia che ha l'ente; il secondo afferma che la competenza spetta ad altro organismo, (che potrebbe essere lo stesso ODV), destinato ad essere inserito nell'ente quale nuovo elemento strutturale. Il terzo orientamento sostiene che la lettera della legge non si presta ad equivoci, il riferimento all' organo dirigente è espressione che indica l'organo a cui spetta l'elaborazione e la gestione della politica dell'ente, in quanto l'adozione del modello, che supporta l'organizzazione dell'ente, è un atto amministrativo.[119]

Dalla formulazione dell'art.6 è stato ricavato anche che l'adozione rappresenta una facoltà, non un obbligo, e che un dovere in questo non è ravvisabile all'interno dell'intera 231/2001, così come nessuna sanzione è prevista in caso di mancata adozione, elemento che fornisce forza all'argomento della facoltatività. Ancora, a favore dell'onere e non dell'obbligo la considerazione che la mancata adozione del modello impedisce all'ente di assumere una prova destinata ad escludere la propria responsabilità (è una scelta) "l'ente non risponde se prova che".

Secondo un'altra corrente di pensiero l'adozione del modello è obbligatoria, e si trovano i fondamenti di questa obbligatorietà già nel Progetto Grosso [120], e

[119] In questo senso SANTI, *Responsabilità da reato degli enti*, cit., cap. 16, p.5. L'autore ritiene la terza ipotesi ben più condivisibile considerando anche che «la decisione dell'organo dirigente dell'ente (nelle società l'amministratore o il consiglio di amministrazione) è espressione del più generale principio di diligenza degli amministratori nel cui ambito rientra il dovere di curare l'adeguatezza dell'organizzazione, in questo caso plasmata sul l'esigenza di gestire il rischio della commissione di reati, presupposto di responsabilità».

[120] Nel senso della obbligatorietà PALIERO – PIERGALLINI, *La colpa di organizzazione*, in *Riv. 231, 172*. Viene citato il Progetto Grosso e la obbligatorietà "testuale" del modello organizzativo. «In prospettiva *de lege ferenda*, particolarmente significativo risulta poi il Progetto Grosso di riforma della parte generale del codice penale, che, nel configurare la nuova disciplina della responsabilità per omissione, sancisce espressamente:

soprattutto negli art. 2381 e 2403 del c.c., attinenti la predisposizione di assetti organizzativi e contabili interni alla società[121].

Il dato testuale sembra tuttavia essere preponderante nella definizione della facoltatività dei modelli, che appare coerente con lo stato della situazione normativa e con l'impianto legislativo[122],[123],[124]

Dal punto di vista sostanziale la facoltatività elimina quella che si sarebbe potuta trasformare in una problematica disciplina operativa per le *societas* potenziali destinatarie dell'obbligo: come noto il tipo di ente che il legislatore ha avuto in mente nella 231/2001 è un ente complesso, organizzato; uno schema che è stato ideato prefigurandosi strutture di dimensioni notevoli, dove, come abbiamo avuto modo di osservare in fase di imputazione, si è preso in considerazione anche il problema del frazionamento delle funzioni apicali.

In una *societas* di questo tipo il modello organizzativo della 231/2001 è sicuramente trasformabile in un obbligo; è anche probabile che in alcune grandi realtà imprenditoriali i modelli 231 siano soltanto una delle forme di compliance attuata, e convivano con altre forme di modelli organizzativi preventivi adottati ad esempio

---

"Le persone giuridiche […] devono adottare e attuare modelli organizzativi idonei ad evitare che vengano commessi reati con inosservanza di disposizioni pertinenti l'attività dell'organizzazione, o comunque nell'interesse dell'organizzazione, da persone agenti per essa"
La disposizione merita di essere segnalata, perché, nel contesto di una riforma che punta dichiaratamente a tipizzare le posizioni di garanzia, fissa immediatamente e autonomamente in capo 'll'ente un dovere di organizzazione, che si salda, nell'economia del Progetto, con un sistema di responsabilità sanzionatoria della *Societas* ».

[121] PIERGALLINI, *Paradigmatica dell'autocontrollo penale*, AAVV, in *Studi in onore di Mario Romano*, Napoli, 382ss, che mette in evidenza nel suo intervento una responsabilità dell'ente per assunzione volontaria di "rischio illecito" in caso di non adozione del modello.

[122] A favore della facoltatività DI GIOVINE, *Il criterio di,* cit., 215. L'autrice mette in evidenza che tuttavia, pur considerando l'adozione del modello come un mero onere, se l'ente ha una struttura complessa resterà difficile andare esente da responsabilità in una situazione di «totale inerzia dal punto di vista organizzativo».

[123] In senso di facoltatività anche SANTI, *Modelli e responsabilità*, cit., cap. XVI, 9, che cita tuttavia alcune deroghe alla facoltatività: ad esempio Consob con delibera 26 marzo 2007 ha stabilito l'obbligatorietà del modello 231/2001 per le aziende del segmento Star, già menzionata in precedenza.

[124] Sempre nel senso della facoltatività anche BERNASCONI, *Manuale della responsabilità*, cit., 93 che riporta a supporto anche Cassazione: si tratta, «piuttosto, di un mero onere— organizzativo ed economico — di cui la società si fa carico vuoi per prevenire i rischi di reato, vuoi per fruire dei benefici qualora incolpata di un illecito (non è consentito al giudice, nel revocare la misura cautelare interdittiva, imporre all'ente l'adozione coattiva di modelli organizzativi: Cass. 23 giugno 2006, n. 32627)», cit., 93.

in armonizzazione con normative di paesi esteri in cui l'azienda ha sedi operative od in cui comunque opera.

Ma su tutta un'altra serie di enti l'imposizione obbligatoria di un modello organizzativo avrebbe pesanti ripercussioni. Ci si riferisce qui a tutta una serie di *societas* di dimensioni medio piccole, che di fatto dominano il panorama italiano, che non hanno in taluni casi neanche la forza economica di andare a generare e mantenere un modello organizzativo come quello ipotizzato nella 231/2001, e dove un sistema di compliance interna potrebbe essere invece realizzato evitando "l'alto tasso di formalizzazione" previsto nella 231/2001.

Il sistema imprenditoriale italiano è prevalentemente composto da *societas* in cui l'articolazione interna è molto semplice, la proprietà aziendale coincide con la gestione, la cultura aziendale si sovrappone con la cultura dei vertici ed allo stesso modo le illegalità commessi da questi coincidono con le illegalità dell'impresa.[125]

Assonime (associazione fra le società italiane per azioni), in una indagine svolta fra i propri associati[126], mette in evidenza, da un lato, i costi elevati di attuazione e gestione del modello, dall'altro lato le strutture organizzative, che quando sono meno complesse come nelle piccole imprese, non giustificano la predisposizione di procedure articolate di controllo. «Si comprende perciò l'opzione delle piccole imprese di non conformarsi a una normativa troppo articolata che implica sforzi eccessivi di organizzazione e di impegno economico (in proporzione ai fini)»[127].

Viene poi messa in evidenza che la mancata considerazione di un diverso trattamento per gli enti di piccole e di grandi dimensioni costituisce un evidente limite della normativa di cui si deve tener conto in sede di applicazione della disciplina, nella valutazione dei presidi organizzativi e delle responsabilità degli enti.

---

[125] La valutazione effettuata dalla dottrina e dall'autore è di sostenere un concetto di esigibilità del modello che guardi alla situazione di fatto dell'ente e diversamente graduabile in funzione delle sue specificità. In questo modo si «eviterebbero gli effetti demotivanti che derivano dalle imposizioni dall'alto di regole non congrue e/o non necessarie» così DI GIOVINE, *Il criterio di*, cit., 215.

[126] Assonime, *Indagine sull'attuazione del decreto legislativo 231/2001*, maggio 2008, *assonime.it*, 37 ss.

[127] Assonime, *Indagine*, cit., 37ss

Altro elemento messo criticamente in evidenza è rappresentato dall'ampliamento dei reati-presupposto, che ha come conseguenza la continua, difficile e costosa predisposizione di modelli organizzativi adeguati perché: «i) un modello organizzativo che pretenda di prevenire un numero elevato di reati eterogenei rischia di essere, nel concreto, meno stringente di uno mirato alla prevenzione di specifiche condotte criminose; ii) i costi che devono essere sopportati dalle società per attuare il sistema 231, oltre ad essere elevati, sono difficilmente valutabili ex ante».[128]

La facoltatività del modello organizzativo diventa quindi un essenziale ed indispensabile strumento di elasticità per evitare una costruzione rigida, onerosa, solo formale; mentre, per altro verso, è indiscutibile che il sistema della 231/2001, coordinato con altre normative dello stesso tenore presenti sia a livello nazionale che internazionale, pur nella sua non obbligatorietà è idoneo ad innescare e sviluppare un meccanismo di graduale innalzamento degli standard di cautela aziendali.[129]

Assodato dunque che la 231/2001 prevede la facoltatività del modello organizzativo, in termini prospettici si potrebbe ipotizzare, come alternativa alla dicotomia facoltatività/obbligatorietà una serie di modelli differenziati in funzione dell'ente a cui si rivolgono, oppure, di esonerare alcune imprese "minori" dall'adottare i modelli organizzativi. Ma appare evidente che fissare una esenzione

[128] Assonime nella sua indagine mette in evidenza che l'ampliamento delle ipotesi di reato pone anche un problema in relazione all'aggiornamento dei modelli organizzativi: «ad oggi, il 91% delle società ha ritenuto opportuno quantomeno integrare l'originario modello e una gran parte di esse ha già approvato un nuovo modello organizzativo per adeguarlo alle nuove previsioni di reato introdotte dalla legge». La relazione sottolinea l'impatto di questi aggiornamenti sotto il profilo dei costi, in particolare per le attività svolte da consulenti esterni all'azienda. Assonime, *Indagine sull'attuazione*, cit., 36.

[129] Prende posizione in modo netto a favore della facoltatività GULLO, *I modelli organizzativi*, in LATTANZI – SEVERINO (a cura di), *Responsabilità da reato degli enti*, vol. I, 2020, Torino, p.248. L'Autore mette in evidenza, fra le varie considerazioni, che la natura obbligatoria del modello avrebbe comportato di conseguenza l'adozione di specifiche sanzioni per l'ente in caso di assenza, sanzioni che non sono presenti. Questo a differenza di quanto avviene nel «contrasto alla corruzione pubblica ove, pur con i dovuti distinguo, alla natura vincolante dell'adozione dei piani triennali anticorruzione corrispondono puntuali obblighi appositamente sanzionati dal responsabile della prevenzione della corruzione e per la trasparenza e degli altri soggetti obbligati. Essa trova altresì conferma nella previsione in taluni settori (nella specie quello della sicurezza cibernetica), adesso attratti nell'obbligo della responsabilità degli enti, di autonomi obblighi di *compliance*, oggetto di elevate sanzioni amministrative, distinti dall'adozione del modello di organizzazione ex artt. 6 e 7 del decreto».

dalla 231/2001 già di suo sembra inopportuno e non sostenibile; si aggiunge inoltre la difficoltà di andare a fissare a livello legislativo il limite della "esenzione", sia individuando numeri (ad esempio: fatturato, dipendenti), che strutture (forma societaria)[130].

Il secondo quesito riguarda la differenziazione del modello organizzativo in funzione delle persone a cui è rivolto: apicali o sottostanti.

La previsione legislativa sembra indirizzare nel senso di contenuti dei modelli distinti a seconda che a realizzare un reato sia un apicale od un sottoposto. Ciò in quanto il coinvolgimento di una figura apicale, dando luogo ad una immediata identificazione con l'ente, darebbe vita ad una presunzione di colpevolezza (con, come abbiamo visto, inversione dell'onere della prova), e necessità di un meccanismo più sofisticato di presidio organizzativo per prevenire i reati[131].

Diversamente, nel caso di soggetto "sottoposto", la responsabilità dell'ente è legata all'inosservanza degli obblighi di direzione e vigilanza; la maggiore distanza dalle figure apicali consentirebbe di adottare un modello organizzativo meno articolato.

Un ulteriore elemento in senso differenziante deriva dalla mancata prescrizione nell'art. 7 dell'istituzione obbligatoria di un "Organismo di Vigilanza con riguardo al Modello penal-preventivo rivolto ai soggetti "sottoposti", diversamente dagli apicali (art. 6) per i quali la coincidenza del ruolo di controllante/controllato impone una vigilanza esterna ed indipendente"[132].

---

[130] A favore di questa soluzione CENTONZE, *La responsabilità degli enti e la piccola e media impresa*, in CENTONZE – MANTOVANI (a cura di), *La responsabilità penale degli enti: dieci proposte di riforma*, Bologna, 2016, 87ss; l'autore propone di escludere l'applicabilità della 231/2001 nei confronti di società dove: l'organo amministrativo sia costituito da soggetti che hanno il controllo dell'ente, ci siano meno di 50 dipendenti a livello nazionale.

[131] Valutazione riportata da GULLO, *I modelli organizzativi* cit., 250. L'autore prende spunto dal dettato legislativo che sembra indirizzare nel senso di prevedere distinti contenuto dei modelli in funzione del soggetto che realizza il reato: apicale o sottoposto. «il coinvolgimento di un soggetto apicale, denotando una immediata identificazione con l'ente avrebbe dato vita ad una presunzione di colpevolezza del soggetto collettivo con correlata inversione dell'onere della prova. Ciò si sarebbe dovuto tradurre nella presenza e dimostrazione da parte dell'ente dell'esistenza di più sofisticati presidi organizzativi per prevenire i reati».

[132] La considerazione è ripresa da BARTOLOMUCCI, *Sulla configurabilità del (fantomatico) modello organizzativo ex d.lgs. 231/2001 dedicato alla PMI*, in *La responsabilità amministrativa delle società e degli enti*, *Rivis. 231*, 2010, 100.

La giurisprudenza e la prassi hanno comunque reso superato questo tema, andando ad evitare considerazioni differenzianti legate alle distinzioni di modelli fra art.6 ed art.7.

Lato prassi, come messo in evidenza dall'indagine Assomine[133], non viene tenuta in conto dalle aziende la differenziazione dei modelli in funzione della figura (apicale o meno) che abbia realizzato il reato -presupposto[134].

[133]Assomine, *Indagine sull'attuazione*, cit., 15: «Nell'adozione del modello viene solo raramente tenuta in considerazione la distinzione tra soggetti apicali e sottoposti e solo in parte si tiene conto del ruolo e della specifica incidenza sulla commissione dei reati d'impresa che possono in concreto avere gli apicali».

[134] Vedi anche BERNASCONI - PRESUTTI, *Manuale della responsabilità*, cit., 192: «non a caso i codici di comportamento redatti dalle associazioni rappresentative degli enti (v. art.6 co. 3) dettagliano metodologia e contenuti dei modelli organizzativi finalizzati a prevenire i reati commessi dai soggetti in posizione apicale, dedicando poco spazio – o addirittura tralasciando ogni riferimento – ai *compliance programs* contemplati dall'art.7 in materia di reati commessi da soggetti sottoposti all'altrui direzione».

CAPITOLO II

IL MODELLO ORGANIZZATIVO E L'ORGANISMO DI VIGILANZA

SOMMARIO**: 1. Il ruolo del modello organizzativo e la cooperazione pubblico-privato. 2. – I contenuti del modello organizzativo nel d.lgs. 231/2001. – 3. L'Organismo di Vigilanza. – 3.1. L'Organismo di Vigilanza: i soggetti. – 3.2. L'Organismo di Vigilanza: le funzioni. – 4. La validazione giudiziale del modello. – 5. Dal d.lgs. 231/2001 alla responsabilità dell'ente per reati informatici**

1. Il ruolo del modello organizzativo e la cooperazione pubblico-privato

Il d.lgs. 231/2001 ha introdotto una inedita forma di controllo sull'assetto organizzativo dell'impresa, al fine di prevenire la commissione di reati economici. Il *simultaneus processus* a carico della persona fisica e di quella giuridica, consente al giudice penale di intervenire non soltanto applicando sanzioni - idonee ad incidere sia sul patrimonio dell'ente, sia sulla sua capacità di stare sul mercato - ma anche di verificare l'adeguatezza della sua struttura organizzativa, sotto il profilo della capacità dell'ente di sviluppare correttamente momenti di controllo interno, idonei ad eliminare o comunque minimizzare il rischio della commissione di reati per i quali è prevista la relativa responsabilità.

Questa capacità dell'ente si esprime attraverso il Modello Organizzativo, che, adottato dagli apicali dell'impresa può essere definito *«come un insieme di procedure volte a disciplinare l'organizzazione, la gestione e il controllo delle attività aziendali al fine di prevenire, o meglio mitigare il rischio di commissione dei reati presupposto previsti dal decreto (c.d. risk mitigation)».* [1]

[1] La definizione è di SCHETTINO – LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. 231/2001*, Milano, 2019, 66.

Punto di origine di questa assoluta novità normativa (e di approccio) è data dai *Compliance Programs*, vale a dire modelli di organizzazione e di gestione idonei a prevenire reati della stessa specie di quelli venuti in essere. L'esperienza dei *compliance programs* deriva dal mondo statunitense[2]; ad essi fa riferimento la stessa Relazione ministeriale accompagnatoria al d. lgs 231/2001, affermando che «si è preferito allora riempire tale dovere di specifici contenuti: a tale scopo, un modello assai utile è stato fornito dal sistema dei *compliance programs* da tempo funzionante negli Stati Uniti. 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 determinati reati. Requisito indispensabile perché dall'adozione del modello derivi l'esenzione da responsabilità dell'ente è che esso venga anche efficacemente attuato: l'effettività rappresenta, dunque, un punto qualificante ed irrinunciabile del nuovo sistema di responsabilità».[3]

A differenza di quanto stabilito nei *compliance programs* statunitensi,[4] il legislatore nazionale non ha limitato la rilevanza degli stessi alla commisurazione della pena

[2] Per interessanti approfondimenti sui *compliance programs* v. anche IELO, *Compliance Programs*: *natura e funzione nel sistema della responsabilità degli enti, modelli organizzativi e d. lgs. 231/2001*, *Responsabilità amministrativa delle società e degli enti*, in *Rivis. 231*, 05, 99 - (Rielaborazione dell'intervento tenuto al CSM, il 7.11.05, sul tema "*La responsabilità amministrativa delle persone giuridiche per reati connessi al rapporto tra criminalità organizzata e pubblica amministrazione: i compliance*"). L'autore mette in evidenza il ritardo con cui si è arrivati nel nostro sistema ad affrontare il tema della responsabilità delle persone giuridiche, in considerazione della "estraneità" alla nostra cultura giuridica dell'istituto, e mettendo a confronto con il sistema anglosassone: «Val qui la pena di ricordare che la Corte Suprema degli *USA* riconosce il primo caso di responsabilità a inizio secolo in *New York Cent. Hudson RR v United Stat*es, 212 U.S. 481, 494-495 (1909). In Gran Bretagna, il primo caso indicato in dottrina è del 1842: *Birmingham and Gloucester Road Railway Co*».

[3] Dalla Relazione ministeriale accompagnatoria della 231/2001, cit., 3.3

[4] Sui *compliances program* vedi anche GULLO, *i modelli organizzativi*, cit., 242, dove viene messo in evidenza che la «valutazione del *compliance*s *program* nel sistema statunitense conduce all'attribuzione all'ente di un determinato *score* avuto riguardo alla sua colpevolezza, secondo le cadenze previste nelle *Federal Sentencing Guilines* del 1991, aggiornabili nel 2018 e visionabili». Approfondisce il tema come riferito in precedenza IELO, *Compliance Programs*: *natura e funzione*, cit., 101: « Le *U.S. Federal Sentencing Guidelines*, corpus di regole elaborato da un'apposita commissione federale, inteso a fornire ai giudici criteri di graduazione della pena da applicare alle organizzazioni in dipendenza dei reati commessi da loro rappresentanti o dipendenti, prevedono fattori di aggravamento della pena e fattori di attenuazione, identificati da un acronimo costituito dalle quattro C di *Comply, Contact, Cooperate, Contrite*, secondo un metodo che è stato definito "*carrot and stick approach to corporate sentencing*". Nell'introduzione al cap. VIII delle *U.S. Federal Sentencing Guidelines*, si legge testualmente: "[...] *this chapter is designed so that the sanctions imposed upon organizations and their agents, taken together, will provide just*

(per quanto ovviamente sia importante questo tema), ma ha assegnato ad essi una posizione decisiva ai fini della stessa presenza della responsabilità dell'ente.[5]

Inoltre, il modello organizzativo assume importante significato anche successivamente alla realizzazione del reato-presupposto: sono infatti previste consistenti riduzioni di pena pecuniaria qualora l'ente si faccia carico di adottare e rendere operativo un modello idoneo a prevenire reati della specie di quelli verificatesi.[6]

Sintetizzando, il modello organizzativo, per un verso interviene come leva preventiva, alzando le "barriere" di protezione aziendali e implementando misure di legalità nella gestione societaria. Trattasi di misure caratterizzate dalla introduzione di vincoli di natura procedimentale/decisionale, oltre che da specifiche attività di formazione del personale coinvolto in processi a rischio di reato. Per altro verso interviene come criterio di esenzione di responsabilità, tutte le volte in cui sia presente la commissione di un reato, da parte di soggetti titolari di posizioni apicali o di persone che alla direzione o vigilanza di detti apicali siano sottoposti e si realizzi una posizione di interesse o vantaggio per l'ente; infine l'esistenza di un efficace modello di servizio è criterio di attenuazione delle conseguenze giuridiche ed economiche conseguenti alla responsabilità dell'ente, anche *post factum,* con comportamenti ravveditivi che indichino la volontà concreta dell'ente di

punishment, adequate deterrence, and incentives for organisations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct».

[5] Con queste considerazioni v. GULLO, *i modelli organizzativi*, cit., 242. L'autore sottolinea come il modello organizzativo «rappresenta il supporto materiale della colpa di organizzazione, essendo la trama normativa su cui si innesta l'eventuale rimprovero all'ente per il difetto di organizzazione, ma è altresì il perno dei meccanismi premiali sparsi nel decreto 231».

[6] V. art. 12 co. 2 del d.lgs.: la sanzione è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado: a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; b) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi. Art.17: 1.ferma l'applicazione delle sanzioni pecuniarie, le sanzioni interdittive non si applicano quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrono le seguenti condizioni: a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; b) l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi; c) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca (segue 1-*bis*).

intraprendere una strada conforme alla minimizzazione del rischio di realizzazione di reati.

In un quadro come quello appena abbozzato, possiamo individuare due prospettive diverse per giustificare l'adozione del modello, a seconda che si abbia un approccio giuridico od aziendalistico.[7]

La ragione giuridica prende in considerazione che è presente una disciplina sanzionatoria stabilita normativamente, e che in presenza di determinati accadimenti ne deriverà una conseguenziale responsabilità, ed è incentrata sul rischio legale.

La ragione aziendalistica si incentra sulla convenienza/vantaggio ad adottare il modello previsto dalla 231/2001, che può discendere anche da una analisi costi/benefici di tipo economico. È infatti da tenere presente che le aziende di dimensioni medio-grandi e con una organizzazione complessa adottano in ogni caso uno o più Sistemi di Controllo Interni (SCI), indispensabili al buon funzionamento delle attività, prevedendo misure organizzative e di controllo che vanno anche a prevenire rischi-reato, con forme differenziate in funzione di diverse variabili, fra le quali l'oggetto sociale piuttosto che dei sistemi-paese in cui operano.

L'adozione di modelli organizzativi inoltre non è ormai solo un fatto interno all'azienda, ma è atto a consentire l'assunzione e il presidio di regole *compliance*, migliorando l'organizzazione e la gestione delle attività, ed è anche diventato un elemento distintivo della qualità della *governance*, ed è oggetto di promozione dell'azienda stessa. [8] Rimanendo in ambito 231/2001, si pensi al *rating* di legalità

[7] Per un approfondimento sul modello organizzativo, sia in termini di *compliance programs* che di diversità di approccio giuridico/aziendale, v. anche SANTI, *responsabilità da reato*, cit., 196. A proposito dei due "punti di vista" giustificativi all'adozione del MOG, l'autore nette in evidenza che «Non si tratta tuttavia di due visioni alternative, in quanto da entrambe possono essere ricavati elementi utili per formulare un'argomentazione " convincente ", adatta a creare nel probabile interlocutore (chiunque esso sia, amministratore, membro di un organo di controllo, consulente o giudice) che il modello da adottare (concretamente o adottato) discende da un procedimento di elaborazione affidabile, che ha portato alla creazione di un prodotto valido, adeguato e idoneo allo scopo per il quale esso è stato concepito».

[8] SANTI, *La responsabilità da reato*, cit., 196, fa riferimento ad una prospettiva di promozione della governance aziendale in termini di *New Institutional Theory*, nel rapporto con gli s*takeholdes.* Volendo fornire una estrema sintesi su questa corrente di pensiero ci si riferisce a una prospettiva teorica secondo la quale *le istituzioni* in senso ampio vengono analizzate come strutture cognitive, normative e di regolazione che fanno sì che il comportamento *individuale* risulti più come il riflesso

attribuito alle imprese da parte dell'Autorità per la concorrenza ed il mercato. Previsto tra i contenuti di carattere non finanziario che alcuni enti sono tenuti a presentare, su base volontaristica può anche essere depositato presso la Consob nell'ambito delle politiche e delle attività volte ad incrementare la *corporate social responsability* dell'azienda.

Il modello 231/2001 si colloca nell'ambito degli SCI, ed a fronte del quadro premiale prima sinteticamente rappresentato, è evidente che anche per l'azienda c'è grande convenienza ad adottare e realizzare uno schema organizzativo (o se si preferisce dei *compliance programs)* in grado di arrecare i benefici evidenziati.[9]

La "convenienza" dell'ente ad operare in un sistema di regole che lo formalizzano concretamente come *compliant* consente di utilizzare la stessa impresa come alleato nel perseguimento dell'obiettivo, «avvalendosi dell'accurata capacità di diagnosi della propria struttura interna, della conoscenza analitica dei meccanismi di funzionamento, dell'attitudine a indirizzare i comportamenti dei membri e a forgiare "meccanismi di autorinforzo" volti a mitigare il rischio di realizzazioni di reati».[10]

Si sostanzia quindi un percorso di collaborazione fra pubblico e privato dove l'ente non è più un soggetto da contrastare con sanzioni sempre più crescenti, contando sull'effetto dissuasivo delle stesse, e dotato di una organizzazione

---

di pressioni esterne che lo definiscono e lo condizionano che come il riflesso di scelte intenzionali. Le scelte organizzative aziendali sono limitate da un insieme di pressioni esogene cui le Organizzazioni devono rispondere ed adattarsi per poter sopravvivere e le pressioni del contesto istituzionale tendono a produrre una convergenza nei modelli organizzativi tale da adattarsi al contesto, assecondandone le aspettative in termini di modello organizzativo appropriato *(Hinings e Greenwood, 1988).*

[9] SCHETTINO– LUCARIELLO, *La difesa degli enti e dagli enti nel d.lgs. 231/2001*, Milano, 2019, 64, mette in evidenza fra gli altri come «la via scelta del legislatore per incoraggiare la creazione di una cultura della prevenzione dei reati sia stata quella del c.d. *carrot-stick approach*, vale a dire la politica del bastone e della carota. In altre parole, è indubbia la prospettiva premiale dei modelli organizzativi: l'ente introduce al proprio interno un modello idoneo a prevenire i reati presupposto e ne garantisce una efficace attuazione sotto la verifica vigile e continua dell'Organismo di Vigilanza, sarà esonerato dalla responsabilità. In caso contrario, subirà le gravi conseguenze della propria mancata organizzazione».

[10] La considerazione riportata è di GULLO, *i modelli organizzativi*, cit., 245. L'autore definisce il modello organizzativo come «espressione di una compliance preventiva, ispirata alla gestione del rischio-reato e animata da logiche ipercautelari; il fenomeno che si intende scongiurare ha talora contorni più sfumati del reato in senso tecnico-giuridico e l'obiettivo realistico cui mirare è la minimizzazione, e non già l'eliminazione del rischio».

pregiudizialmente «ritenuta fattore di dispersione di responsabilità»[11], ma un potenziale cooperante, che nel perseguire propri interessi si avvale di modalità e percorsi organizzativi interni *compliance* che coincidono con le finalità cautelari dell'autorità pubblica.

Questa cooperazione può essere esaminata anche da un ulteriore punto di vista, che è quella della *Corporate Social Responsability*.

La Responsabilità Sociale d'Impresa parte da un dato ormai ampiamente assodato e non più in discussione: le vicende di una azienda hanno impatto non solo sul conto economico, ma coinvolgono un numero di soggetti molto ampio e variegato, che non è limitato ai soli dipendenti.[12]

Gli esempi possono essere vastissimi: si pensi alle alterazioni dell'ecosistema, all'impatto sui consumatori, alla costruzione di un ambiente di lavoro sano che non generi complicazioni fisiche o psichiche nei dipendenti. Questi soggetti a vario titolo sono tutti "portatori d'interesse" (*stakeholders*), rispetto all'attività di impresa.

L'impresa può dunque scegliere se nel proprio procedere vuole interessarsi di queste conseguenze, ed in quale modo gestirle, avendo cura degli *stakeholders*, o "limitarsi" ad un percorso tradizionale, dove il confronto avviene con il conto economico interno e con il rispetto formale della normativa stabilita.

La *CSR* ha un ruolo rilevante nelle politiche della Comunità Europea la quale, a partire dal *Green Paper* per promuovere un quadro europeo per la responsabilità del 2001[13], ed attraverso altri importanti documenti quali la Comunicazione della

[11] L'espressione è di Gullo, *i modelli organizzativi*, cit., 245

[12] Un approfondimento in materia è tratto da , *Modello organizzativo e corporate social responsability: la via etica alla 231*, *Rivis. 231, 2009, 2, 124.*

[13] Commissione delle Comunità Europee, Bruxelles, 18.7.2001, *Libro Verde: Promuovere un quadro europeo per la responsabilità sociale delle imprese*, che riporta al punto 6« L'Unione europea si preoccupa della responsabilità sociale delle imprese, poiché essa potrebbe recare un contributo positivo all'obiettivo strategico definito a Lisbona: "divenire l'economia della conoscenza più competitiva e più dinamica del mondo, capace di una crescita economica sostenibile accompagnata da un miglioramento quantitativo e qualitativo dell'occupazione e da una maggiore coesione sociale». Ed al successivo punto 8: «Il concetto di responsabilità sociale delle imprese significa essenzialmente che esse decidono di propria iniziativa di contribuire a migliorare la società e rendere più pulito l'ambiente. Nel momento in cui l'Unione europea si sforza di identificare valori comuni adottando una Carta dei diritti fondamentali, un numero sempre maggiore di imprese riconosce in modo sempre più chiaro la propria responsabilità e la considera come una delle

Commissione del 2 luglio 2002, relativa alla "*Responsabilità sociale delle imprese, un contributo allo sviluppo sostenibile*", si è fortemente spesa ed orientata affinchè il concetto di responsabilità etica si diffonda fra le imprese comunitarie.

Si dichiara nelle prime righe di questa comunicazione che "*il successo economico delle imprese non dipende più unicamente dalle strategie di massimizzazione dei profitti a breve termine, bensì dal perseguimento di obiettivi sociali e ambientali, anche nell'interesse dei consumatori*".

Questo insieme di preoccupazioni, di carattere preminentemente etico, è quindi quello che si può riassumere nel concetto di Responsabilità Sociale d'Impresa, o *Corporate Social Responsability* ("CSR").

L'oggetto di attenzione dell'ente non è più solo il proprio patrimonio; si aggiunge la salvaguardia dell'interesse degli *stakeholders*; l'ente impronta in modo volontario la propria attività al non commettere fatti costituenti reato: risulta evidente che ci si trova di fronte ad un salto culturale, ove il Modello Organizzativo diventa anche un facilitatore del modo in cui l'ente può organizzarsi per perseguire le scelte aziendali in modo *compliance* tutelando l'impresa e di salvaguardia per gli *stakeholders*.

A chiusura è tuttavia necessaria una precisazione. Tutte le evidenze sopra riportate descrivono un meccanismo virtuoso ed un percorso che gradualmente sarà sicuramente sempre più implementato e strutturato; i punti di riferimento sono tuttavia soggetti giuridici di dimensioni importanti, con strutture amministrative consolidate; gli stessi precedenti dei *compliances program* statunitensi fanno riferimento a strutture societarie fatte di grandi imprese, multinazionali, *public companies*. Il nostro contesto nazionale è al contrario permeato da strutture di dimensioni medio-piccole. Come può conciliarsi la cooperazione pubblico-privata su strutture che, anche per un solo fatto economico, non sono in grado di realizzare un apparato organizzativo interno in grado di avere le caratteristiche del modello tipo previsto dalla 231/2001?

componenti della propria identità. Tale responsabilità si esprime nei confronti dei dipendenti e, più in generale, di tutte le parti interessate all'attività dell'impresa ma che possono a loro volta influire sulla sua riuscita».

Il tema è stato affrontato in precedenza [14] , a proposito della facoltatività/obbligatorietà del modello 231. Fra i vari argomenti a favore della facoltatività nella adozione del modello si era riportata l'opportunità, soprattutto per le aziende più piccole, di non essere gravate da un fardello aggiuntivo di costi che avrebbe funzionato come disincentivo economico alla stessa prosecuzione dell'attività aziendale, al punto da ipotizzare, da parte di vari autori, l'inserimento di limiti dimensionali al di sotto dei quali lo schema 231 non dovrebbe essere più previsto.

Questa soluzione come detto non è normativamente quella praticata, e comunque non sarebbe priva di rischi: la realtà evidenzia che proprio nelle strutture che hanno una debole, se non inesistente proceduralizzazione delle attività è difficile realizzare una cultura del controllo; si tratta inoltre di strutture dove spesso l'imprenditore è figura di riferimento assoluta; e mentre negli enti complessi vi è una costante dissociazione fra la posizione della persona fisica e quella della persona giuridica, per cui da un lato è possibile che la prima abbia agito in maniera delittuosa solo per soddisfare un proprio interesse, e dall'altro è altrettanto possibile affermare che l'azione del singolo sia stata realizzata mediante una elusione fraudolenta del modello preventivo, queste affermazioni sono assai meno credibili qualora siano rese con riferimento ad enti di piccole dimensioni. «In queste realtà, infatti, la compenetrazione tra la persona giuridica e la persona fisica che ha agito in maniera criminosa (spesso lo stesso imprenditore) è così forte che diventa difficile, anche se non impossibile, escludere la responsabilità dell'ente — che ontologicamente si identifica con chi ha agito materialmente — quando si verifichi uno dei reati considerati nel d.lgs. n. 231/2001».[15]

Al momento la soluzione di "differenziazione" adottata dal legislatore è all'art. 6 comma 4 del decreto 231/2001: si consente infatti agli enti di piccole dimensioni di

[14] *Supra*, cap.1, par.5

[15] Sul punto v. anche SCHETTINO – LUCARIELLO, *La difesa degli enti, cit.*, 89, che mette in evidenza che «tuttavia questo profilo è scarsamente considerato dalle linee guida di Confindustria, che prima evidenziano questo tema e poi affermano che alle piccole imprese è comunque richiesto uno sforzo organizzativo e di prevenzione minore»; viene inoltre sottolineato che l'esperienza giudiziaria ha dimostrato che sono proprio le piccole e medie imprese gli enti potenzialmente target della responsabilità ex d.lgs. n. 231/2001, verificandosi con maggiore frequenza proprio al loro interno quelle carenze di organizzazione che favoriscono il verificarsi di reati presupposto.

attribuire le funzioni di Organismo di Vigilanza direttamente all'organo dirigente, consentendo quindi una diminuzione dei costi rispetto alla soluzione ordinaria.[16]

Tuttavia ci si chiede se il Modello Organizzativo in chiave interpretativa possa in qualche modo essere ridimensionato nelle aziende di dimensioni minori.

Secondo la valutazione di alcuni autori[17] la risposta può essere positiva, e si può assumere un punto di vista che porti a soluzione diversa, semplificando il modello di servizio, riguardando sia alla tipologia di reati che si intende prevenire, che le effettive dimensioni dell'ente considerato. Con riferimento al primo profilo, si deve distinguere fra reati dolosi e colposi. Qualora il modello organizzativo sia destinato a prevenire i reati colposi, le dimensioni dell'impresa non hanno alcun rilievo, e pertanto il MOG adottato non può differenziarsi dallo schema tipo previsto dalla 231/2001.

Diversamente, per quanto riguarda i reati dolosi; qui le dimensioni e le caratteristiche dell'ente potrebbero assumere rilevanza. Nelle imprese di dimensioni minori tendenzialmente le attività di decisioni sono nelle mani di un solo soggetto, che utilizza schemi societari diversi (società di capitale piuttosto che di persone), ma mantiene nella sostanza la piena titolarità delle decisioni. In situazioni del genere qualora il titolare dell'impresa volesse delinquere, un modello organizzativo difficilmente sarebbe idoneo a prevenire una sua determinazione personale.

Di conseguenza, si potrebbero ipotizzare, nelle imprese più piccole, modelli di organizzazione diversi in funzione della differenza fra apicali e sottoposti. Si è però visto che la prassi ha decisamente preso una strada diversa, riferendosi ad un modello unico, privo di differenziazione in funzione delle figure coinvolte.

In altra valutazione viene messa in evidenza che l'aspetto dimensionale potrà influire sul processo di gestione dei rischi, potendo l'imprenditore limitare la

[16] Tale possibilità ovviamente rende più problematica la terzietà dell'*OdV* rispetto alla dirigenza aziendale, e verrà esaminata più compiutamente al paragrafo 4.

[17] La soluzione descritta è riportata da SCHETTINO – LUCARIELLO, *la difesa degli enti*, cit., 90. Viene riferita «alle c.d. microimprese (con un numero di dipendenti inferiore a dieci e il cui fatturato o totale di bilancio annuo non superi 2 milioni di euro) in cui il processo decisionale si concentra tendenzialmente tutto in capo ad un solo soggetto»

relativa analisi alle sole funzioni aziendali particolarmente soggette al rischio di attività illecite o alla prevenzione solo di alcuni fra i reati considerati nel d.lgs. n. 231/2001, e adottare di conseguenza protocolli e procedure meno onerose;[18]tuttavia, il tema della semplificazione del MOG per le imprese minori rimane normativamente non risolto.

2. **I contenuti del modello organizzativo nel d.lgs. 231/2001**

La fonte normativa dei modelli di organizzazione, gestione e controllo previsti nel d.lgs. 231/2001 è rappresentata dagli articoli 6 e 7.

Come messo già in evidenza, sembrava intenzione del legislatore differenziare i modelli in funzione dei soggetti a cui veniva applicato (apicali piuttosto che sottoposti), ma sia la prassi che la giurisprudenza e la dottrina hanno invece semplificato questo aspetto, evidenziando l'unicità del MOG.

Gli articoli 6 e 7 devono pertanto essere esaminati in modo unico e coordinato, con lo scopo di mettere in evidenza contenuti e caratteristiche del modello stesso.

Secondo la lettura fornita da unanime dottrina, gli articoli non definiscono in modo compiuto il modello organizzativo, piuttosto inseriscono elementi relativi sia alla funzione che al contenuto dello stesso, limitandoli al minimo; indicano, inoltre, in maniera ritenuta insufficiente, le fasi della procedura che devono portare all'adozione del modello idoneo.

Di fatto quindi si è creata una doppia incertezza, innanzitutto quella degli enti che, pur volendo aderire alla compliance 231, dal punto di vista operativo non sanno esattamente come procedere; per altro verso, gli stessi giudici nelle loro attività di

[18] In un intervento di BARTOLOMUCCI, *sulla configurabilità del*, cit., 102, è presente un ulteriore approfondimento, sempre legato alla possibilità di individuare un modello semplificato a cui fare riferimento nelle realtà più piccole. L'autore mette in evidenza innanzitutto le difficoltà a definire quali sarebbero le "imprese più piccole"; propone poi una soluzione che partendo dalla considerazione che è data per definita «la co-essenzialità dei componenti del Modello, quali Codice etico, Matrici di mappatura dei rischi-reato, Protocolli comportamentali (generali o speciali), Sistema disciplinare interno, istituzione dell'OdV», si possono indicare per ciascuno di essi alcuni « lineamenti e segnalare talune opzioni e soluzioni applicative aderenti alle prerogative di un ente minore», che sono sostanzialmente delle attività di limatura su ogni singolo punto attenzionato.

valutazione non hanno strumenti oggettivi per la misurazione del modello, per cui il giudizio può restare esposto all'utilizzo di criteri soggettivi.

È stato quindi necessario negli anni un lavoro importante di elaborazione, che è stato effettuato non solo grazie al lavoro della dottrina e della giurisprudenza, ma che ha preso sostanza dalle stesse Linee Guida stabilite dalle associazioni di categoria[19] e da quelle che sono state le migliori pratiche realizzative del modello stesso.

È bene ricordare che se il modello di organizzazione dovesse essere assente od inadeguato, per l'ente, in presenza di un reato-presupposto, ne scaturirebbero importanti conseguenze, in temini di imputazione dell'illecito all'ente; l'azienda deve svolgere quindi in modo accurato le proprie attività di realizzazione del MOG.[20]

---

[19] Si possono citare, senza esaurire il numero, le Linee Guida per la costruzione dei Modelli di organizzazione, gestione e controllo ai sensi del Decreto Legislativo 8 giugno 2001, n. 231di Confindustria, approvate nel 2002 e aggiornate periodicamente, quelle di Confagricoltura per le imprese del settore agricolo; dell'ABI per le banche; dell'ANIA per le società assicuratrici. Rilevante evidenziare le caratteristiche delle Linee Guida. Lo spunto viene fornito da SCHETTINO – LUCARIELLO, *la difesa degli enti,* cit., 66, dove si sottolinea che le linee guida assumono un valore di "punto di riferimento" autorevole, con elevato standard di qualità, definendo i passaggi fondamentali per una corretta formazione del sistema di controllo, ma che le indicazioni devono necessariamente essere adattate alle singolarità dei vari enti, alle particolarità organizzative, in quanto prevedono una serie di destinatari non sempre omogenei fra di loro. Per questo motivo nelle linee guida è prevista una parte generale, divisa in sezioni, «dedicate alla forma societaria dell'ente (e dell'eventuale gruppo), alla sua storia giudiziaria, al sistema di governance, di deleghe e procure, ai principi contenuti nel codice etico, alle scelte effettuate in ordine alla composizione e alla disciplina dell'Organismo di Vigilanza e ai flussi informativi tra questo e gli organi dell'ente; all'attività di formazione e informazione del personale sul funzionamento del modello e il sistema disciplinare previsto nel caso di una sua violazione»; ed una parte speciale, calibrata sulle caratteristiche specifiche dell'ente a seguito di una specifica mappatura, saranno individuate le attività sensibili al rischio, cioè più esposte al verificarsi di reati-presupposto nonché i protocolli e le procedure atti a prevenirlo. Al modello organizzativo dovranno, poi, essere allegati il testo del codice etico e il regolamento dell'Organismo di Vigilanza.

[20] SANTI, *La responsabilità da reato* , cit., 212, mette in atto una ricostruzione che si riferisce allo "spettro della valutazione giudiziale": si parte dalla richiesta del PM di applicazione di una misura cautelare all'ente, a cui il giudice replica in funzione di tre elementi: «1) gravi indizi per ritenere la responsabilità dell'ente, 2) l'esistenza di elementi sul piano oggettivo per l'imputabilità dell'illecito all'ente, 3) l'inesistenza, sul piano soggettivo, di elementi che comportino l'esonero della responsabilità dell'ente, nonostante il reato commesso, fra i quali è il fatto che l'organo dirigente abbia adottato ed efficacemente attuato modelli di organizzazione e gestione idonei a prevenire reati della stessa specie di quello verificatosi». Per quanto riguarda quest'ultimo punto, il giudice nella valutazione del modello si avvale solitamente di un esperto tecnico, nomina quindi un consulente di ufficio che esamina non solo il contenuto del MOG ma anche la metodologia usata per la sua costruzione e che sarà il vero contraddittore dei consulenti di parte; « si comprende allora che la procedura di costruzione del modello organizzativo deve essere animata dalla prospettiva del risultato da raggiungere: il modello deve essere "adeguato" alla realtà dell'ente e, per costituire

Le concettualità espresse dal legislatore nel definire il modello sono diverse. Innanzitutto, il modello deve essere considerato *idoneo*[21]. L'idoneità viene abbinata alla capacità del modello a prevenire reati della specie di quello verificatesi, e viene pertanto definita da alcuni autori[22] *"idoneità in concreto*", in quanto rappresenta l'obiettivo finale dell'intero modello di organizzazione: essere in grado di prevenire la realizzazione del reato.

Per potere essere considerato *idoneo in concreto* un modello di servizio deve essere innanzitutto *adeguato* alla realtà aziendale su cui opera; questo comporta una personalizzazione del modello teorico in funzione delle caratteristiche specifiche dell'ente, ed esclude di conseguenza gli schemi di modelli standardizzati utilizzabili in modo indifferenziato per ogni tipo di azienda.

Il modello deve poi essere *effettivo*, con ciò intendendosi che deve realmente calarsi nella realtà aziendale, e non restare un mero esercizio teorico. Alla effettività viene abbinata la implementazione del modello stesso, vale a dire l'attuazione continua dello stesso.

Infine il modello deve avere caratteristiche di efficienza, e deve quindi essere in grado di adeguarsi alle eventuali variazioni organizzative dell'ente, senza mai perdere dunque le sue caratteristiche di attualità.

Se queste sono le caratteristiche del modello, e la finalità abbiamo evidenziato essere l'idoneità in concreto a prevenire i reati-presupposto, viene da stabilire in che modo questo può costruirsi.

Dal punto di vista dell'impostazione organizzativa, è indispensabile fare riferimento all'attività svolta nel tempo dalle Linee Guida. Dall'esame degli esempi più significativi il modello organizzativo può definirsi un "documento contenitore"

---

elemento di esonero della responsabilità da reato, deve essere suscettibile di una "valutazione positiva" da parte del giudice sulla sua idoneità, misurata in correlazione all'esigenza di prevenire il "rischio reato"».

[21] Per approfondite analisi in materia vedasi Gullo, *i modelli organizzativi*, cit., 252. L'autore valuta che il requisito dell'i*doneità in concreto* rappresenta il carattere in grado di stabilire il giudizio di esclusione della responsabilità dell'ente. L'Autore distingue fra idoneità in astratto ed idoneità in concreto; alla prima viene fatto risalire il criterio dell'adeguatezza, che rappresenta l'idoneità (astratta) del disegno del modello, in grado poi di trasformarsi in idoneità concreta se accompagnata dai caratteri dell'implementazione e dell'efficienza.

[22] L'espressione è di Gullo, *i modelli organizzativi*, cit., 252.

costituito da "componenti documenti"[23]. Sono individuabili a) una parte generale - che rappresenta una sorta di carta d'identità dell'ente, b) una parte speciale - che è il territorio applicativo specifico, c) il Codice Etico, d) il sistema disciplinare. Nessuna di queste sezioni, per quanto possa essere raccomandata dalle varie associazioni, è prevista normativamente; quindi il modello potrebbe validamente assumere forma diversa da quella rappresentata. Inoltre, anche qualora il modello ricalcasse quanto stabilito dalle associazioni, non impegnerebbe in alcun modo il giudice, che resta assolutamente libero di formare il proprio convincimento.

Per quanto riguarda i contenuti, l'art. 6 comma 2 individua diversi *step*: una prima fase è rappresentata dalla mappatura del rischio; segue poi la procedimentalizzazione, la gestione dei flussi finanziari e di quelli informativi; inoltre deve essere introdotto un sistema disciplinare in caso di mancato rispetto delle misure del modello.

La mappatura del rischio (*risk assessment*) prende inizio dall'analisi di diverse variabili, in primo luogo legate al tipo di attività svolta dall'azienda, alla tipologia dell'ente, alla presenza o meno di un gruppo societario, piuttosto che allo svolgimento di attività in più nazioni, caratterizzate da omogeneità (o meno) di legislazione. Si tratta, come detto, di indentificare il rischio approfondendone anche

[23] La definizione virgolettata è di SANTI, *Modelli e responsabilità*, cit., 218ss; fra i vari approfondimenti viene riportato il percorso svolto dalle associazioni di categorie per validare le proprie linee guida. Si fa riferimento in proposito al decreto del Ministro della giustizia 26 giugno 2003, n. 201 (regolamento recante disposizioni regolamentari relative al procedimento di accertamento dell'illecito amministrativo delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, ai sensi dell'articolo 85 del dec.reto legislativo 8 giugno 2001, n. 231). Secondo l'art. 5 di tale decreto ministeriale, le associazioni rappresentative degli enti comunicano al Ministero della giustizia, presso la Direzione generale della giustizia penale, i codici di comportamento contenenti indicazioni specifiche (e concrete) di settore per l'adozione e per l'attuazione dei modelli; a seguire, secondo l'art. 6, il Direttore generale della giustizia penale esamina detti codici di comportamento assumendo quale schema di riferimento l'art. 6 d.lgs. 8 giugno 2001, n. 231; se passati trenta giorni dalla data del ricevimento il Direttore generale della giustizia penale non comunica all'associazione eventuali osservazioni in merito alla idoneità delle suddette "linee guida", il singolo codice di comportamento acquista efficacia. Tuttavia, come messo in evidenza anche in chiaro nel testo, «1) l'adeguamento dei modelli ai codici di comportamento non determina di per sé l'automatica esclusione della responsabilità degli enti; 2) la mancata conformità del Modello alle indicazioni specifiche delle Linee guida non ne inficia di per sé la validità. Tali Linee Guida costituiscono "prescrizioni di carattere generale" per garantire una uniformità problematica. L'eventuale valutazione ministeriale dei codici di comportamento "non negativa" non è vincolante per il giudice che deve giudicare dell'idoneità concreta del singolo modello. In altri termini le linee guida elaborate dalle associazioni di categoria hanno esclusivamente una funzione di indirizzo, per quanto fondamentale».

la potenziale intensità. Pertanto, non si potrà fare a meno di prendere in considerazione la dimensione dell'ente, il volume di affari, il numero di dipendenti, i mercati di riferimento; la tipologia di attività svolta poi può parecchio aiutare a definire il rischio potenziale: fa parecchia differenza in termini di orientamento del modello organizzativo esercitare una attività di estrazione petrolifera piuttosto che essere in presenza di una catena di supermercati.

La definizione di questo primo quadro deve avvenire con strumenti formali (atto costitutivo, statuto, presenza di certificazioni), e con attività di implementazione svolte sul campo, raccogliendo documenti aziendali o verificando sul posto la presenza dei presidi di controllo previsti dalle procedure, e porterà in sintesi a definire quelle che sono le attività a maggior rischio dell'ente.

Seguirà a questo punto lo studio e l'individuazione del quadro normativo con lo scopo di andare a definire i reati-presupposto e quali di essi possono intersecarsi con il business dell'ente.

Un esempio può venire dalla rappresentazione di un ente che svolge la propria attività economica interagendo con la Pubblica Amministrazione, da cui riceve appalti. In una situazione del genere grande cautela è indispensabile nel prevenire i fattori corruttivi, che rappresentano quindi l'area di rischio su cui l'ente deve intervenire. I comportamenti corruttivi necessitano della presenza di denaro per generare fondi occulti, (ad esempio con sovrafatturazioni) per cui diventa conseguente obiettivo dell'ente mettere sotto stretto controllo i dati relativi alla generazione ed al trasferimento di denaro, quindi verranno definiti *iter* e controlli molto accurati per quanto riguarda il processo degli acquisti e dei pagamenti, piuttosto che dei finanziamenti e del bilancio; ma è da evidenziare che l'identificazione dei reati-presupposto che possono intersecarsi con l'ente non è sempre agevole, anche per la intervenuta implementazione dei reati-presupposto effettuata nel corso degli anni, e alla natura eterogenea dei beni protetti: da questo discende la necessità di una attività continua di mappatura del rischio, a cui è delegato, come vedremo, l'OdV.

Dall'incrocio fra i primi due passaggi verrà definito il livello di rischio tollerabile a cui l'ente può esporsi, nella considerazione reale che non è possibile andare ad

azzerare completamente il rischio-reato, e pertanto l'obiettivo concreto a cui l'ente deve aspirare è di minimizzarlo, nella consapevolezza di non poterlo eliminare.[24] Questo controllo dovrà essere effettuato dal giudice, verificando la presenza di un assetto organizzativo che abbia adoperato in tal senso.

Qualora diversamente si ritenesse che il modello idoneo è solo quello che azzera il rischio reato-presupposto, si arriverebbe paradossalmente alla conclusione che la realizzazione di un qualunque reato-presupposto escluderebbe l'idoneità del modello; così come è indispensabile che il giudice arrivi a definire la responsabilità dell'ente attraverso il modello organizzativo adottato, e non sulla base del reato commesso dalla persona fisica.[25]

Il rischio accettabile (*risk tolerance*), allo stato della normativa attuale, è determinato in modo autonomo dall'ente, ed è frutto di valutazioni dove la componente economica ha il suo sicuro peso.[26] Viene individuato in funzione della capacità dell'azienda di "generare rischio" (*risk apetite*) e del *risk target* che intende

---

[24] Sul punto GULLO, *i modelli organizzativi*, cit., 255 ricorda come il legislatore spagnolo abbia ragionevolmente affermato, nell'art.31-*bis*, che l'obiettivo è la neutralizzazione o la riduzione in modo molto significativa. L'autore cita anche le Linee Guida di Confindustria, dove si suggerisce per i reati dolosi una definizione parametrata sul requisito dell'elusione fraudolenta, con ciò intendendosi la costruzione di «un sistema preventivo tale da non potere essere aggirato se non fraudolentemente»

[25] V. Cass. pen., sez. VI 24 settembre 2019, n. 43656, con nota di BELLOMI, GENTILE, *La Cassazione rileva la diversa natura del Piano Operativo per la Sicurezza ("P.O.S.") e del Modello di Organizzazione, Gestione e Controllo ("M.O.C.G.") e statuisce che la violazione della normativa sulla sicurezza nei luoghi di lavoro non comporta in automatico la sanzione ex d.lgs. n. 231/2001 a carico dell'ente,* in *Giurisp. Pen.,* 2020, 2. La vicenda processuale trae origine dal un decesso di un operaio in un cantiere durante l'utilizzo di un pesante macchinario. Sia in primo grado che in appello i giudici avevano ritenuto responsabili sia le persone fisiche che il capo-cantiere responsabile della sicurezza, che il datore di lavoro, ed inoltre anche l'ente ai sensi dell'art.25-*septies* 231/2001 (omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla salute e sicurezza sul lavoro). La Corte di Cassazione ha ritenuto che omettendo la valutazione relativa al contenuto e all'idoneità del modello organizzativo, le Corti di merito sono di fatto giunte alla condanna dell'ente sulla base del mero accertamento della responsabilità penale della persona fisica. Secondo la Cassazione un automatismo di tal genere non può che essere censurato, in quanto si pone in contrasto con l'articolata disciplina posta dal Decreto Legislativo 231/2001. La normativa in esame, e in particolare l'art. 6, infatti, esplicitamente ricollega la responsabilità della persona giuridica alla sussistenza della c.d. colpa di organizzazione, ovvero di un deficit organizzativo che si configura quando la stessa non abbia provveduto ad adottare ed efficacemente attuare un modello di organizzazione e di gestione conforme alle norme e idoneo a prevenire la commissione di reati della specie di quello verificatosi.

[26] In termini meramente economici la valutazione del "rischio accettabile" viene legato al costo della protezione del rischio: se questo costo è superiore al valore della risorsa che si vuole proteggere, il rischio può divenire accettabile. Non può trascurarsi, tuttavia, l'incidenza del costo reputazionale a cui l'ente si espone in presenza di determinati tipi di reato.

raggiungere, tutti processi che nelle realtà aziendali di dimensioni medio-grandi sono frutto di analisi da parte degli SCI (Sistemi Controllo Interni).

Nella attività di copertura dal rischio da reato-presupposto da cui l'ente intende proteggersi, al termine di questa attività, da un lato verranno esclusi quei reati (e quindi le coperture organizzative del relativo rischio), incompatibili con le attività dell'ente, e quelli dove non sia rintracciabile un suo coinvolgimento in termini di interesse o vantaggio, (che rappresenta il criterio di collegamento ai fini della responsabilità), dall'altro si porrà particolare cura nei confronti dei reati ritenuti invece rilevanti.[27]

In questo caso l'ente dovrà definire in modo approfondito le modalità in cui l'illecito può realizzarsi all'interno del contesto societario, ed in particolare se ci sono apparati più esposti a questo rischio, (quindi, dove il rischio è allocato e su quali funzioni); dovrà inoltre verificare se sono o meno già presenti sistemi di prevenzione, per poi stabilire, in funzione del grado di rischio (più o meno alto), se stabilire dettagliate e prescrittive modalità di comportamento, che dovranno come già detto essere ben comunicate ai soggetti destinatari, coinvolgendoli in attività formative, o adottare una disciplina più blanda, legata ad esempio a forma di controllo periodiche dell'Organo di Vigilanza.

Conclusa la fase di valutazione del rischio, l'ente deve procedere a definire un processo, realizzando una organizzazione interna funzionale, dotata di elementi di controllo, centri di imputazione intermedi delle responsabilità, prevedendo anche, viste le finalità del modello, autonomia, definizione di poteri, segregazioni delle funzioni.

La 231/2001 non cita il termine processo, in quanto usa quello di "*protocollo*". Il protocollo rappresenta un insieme di regole applicative di carattere generale, dirette

[27] Il percorso appena delineato rappresenta una costruzione del modello, (siamo nella parte speciale), effettuata per *fattispecie criminose*. In questo caso si muove dalle singole figure di reato per definire la specifica possibilità che gli stessi vengano realizzati. A questa metodologia può sostituirsene un'altra, che prende spunto dai *process*i presi in considerazione (ad esempio, formazione del bilancio), per analizzare quali reati possono interagire con il processo stesso. Secondo la valutazione di GULLO, *i modelli organizzativi*, cit., 266, «la prima eventualità assicura maggiore linearità nella costruzione della parte speciale», la seconda «tuttavia, è quella che tende ad imporsi, in quanto armonica con l'approccio seguito dalle imprese, inclini a ragionare per processi».

a programmare e definire la formazione delle decisioni e dei comportamenti dell'ente in modo conforme alle valutazioni effettuate in fase di analisi del rischio. Definisce il modo in cui le precedenti attività svolte trovano un percorso per trasformarsi in comportamenti concreti disciplinati.

Ad essi si affiancano all'interno dell'azienda le procedure, che rappresentano la disciplina esecutiva ed operativa di dettaglio, che regola in modo minuzioso il modo in cui determinate attività devono essere realizzate, prevedendo una serie di sequenze precise di comportamenti, dove viene definito ad esempio chi decide, cosa deve fare per decidere, fino a che punto può decidere, chi controlla la decisione. La non corretta applicazione di una procedura rappresenta un campanello d'allarme sulla presenza di una violazione interna, ed i controlli sulla corretta applicazione della stessa svolgono la funzione di prevenzione di un ipotetico reato.

Protocolli e procedure sono entrambi rivolti all'applicazione del modello organizzativo, ma operano su livelli diversi: viene anche fatto notare come il protocollo abbia caratteristiche trasversali, potendosi rivolgere a più procedure o meccanismi di controllo, mentre la procedura applica quella parte di protocollo che la coinvolge.[28]

[28] Per fornire un esempio della differenza possiamo riferirci al processo aziendale relativo alla partecipazione alle gare di appalto: il protocollo conterrà disposizioni che vietino nella maniera più assoluta di richiedere e concedere indebiti favori a funzionari pubblici, a prescindere dall'opportunità o dal vantaggio; la procedura invece descriverà in concreto chi dovrà fare che cosa, quando e con quali poteri, in un'ottica di separazione di compiti tra chi autorizza un'operazione, chi la esegue, chi la contabilizza e chi la controlla; così, SCHETTINO – LUCARIELLO, *La difesa degli enti*, cit., 70. Gli autori riportano anche una valutazione sul Codice Etico, definito il "protocollo dei protocolli", ritenendolo un elemento indispensabile del modello organizzativo. Secondo le già citate Linee Guida di Confindustria, il Codice Etico può essere definito come un documento ufficiale dell'ente, «voluto e approvato dal massimo vertice, che contiene l'insieme dei suoi diritti, doveri e responsabilità nei confronti dei c.d. "portatori d'interesse" (ovvero, i dipendenti, i fornitori, i clienti, la Pubblica Amministrazione, gli azionisti, il mercato finanziario, e così via) e costituisce un elemento essenziale del sistema di controllo preventivo. Esso deve mirare a raccomandare, promuovere o vietare determinati comportamenti, indipendentemente da quanto previsto a livello normativo e, a tal fine, può prevedere sanzioni proporzionate alla gravità delle eventuali infrazioni commesse, siano esse o meno, reati, illeciti di altra natura o semplici violazioni di regole organizzative interne». In questo modo il codice etico assolve anche ad una importante funzione integrativa nelle attività di applicazione ed interpretazione dei protocolli e delle procedure contenute nel modello organizzativo. Nella prassi applicativa il codice etico è solitamente diviso in tre parti: a) principi generali; b) principi di condotta per i dipendenti; c) sistema sanzionatorio, previsto per la violazione dei primi. Ferma restando la indispensabilità del Codice Etico, la sua valutazione all'interno del sistema 231 non è unitaria. Secondo un orientamento dottrinale, Modelli Organizzativi e Codici Etici sono entità distinte, per natura, contenuto ed efficacia giuridica. In questo senso v. SANTI, *Responsabilità da reato,* cit., 224 ss. Secondo altro orientamento, si ritiene

I flussi finanziari rivestono grande importanza in quanto una attenta analisi degli stessi può consentire di prevenire il reato; è necessario quindi sia definire in modo adeguato i poteri decisionali di spesa, i processi con cui vengono prese le relative decisioni, il sistema delle deleghe, gli eventuali step autorizzativi, i momenti di controllo e la presenza di linee guida su determinate operazioni, tutto in modo che i flussi finanziari possano sempre essere tracciati e controllati.

Questa attività può essere particolarmente valida ad esempio nei reati di corruzione, che trovano presupposto in reati-spia quale falso in bilancio, riciclaggio, che a loro volta possono essere anticipati da un attento controllo dei flussi finanziari.

Si cita in materia l' Ordinanza del Tribunale di Milano del 20 dicembre 2004,[29] relativa a vicenda che ha per oggetto un caso di corruzione aggravata nell'ambito di aggiudicazione di appalti, e dove viene di conseguenza valutata l'idoneità del modello organizzativo dell'ente a prevenire il relativo rischio, al fine di definirne la responsabilità; in particolare viene esaminata la modalità di gestione ed individuazione delle risorse finanziarie, verificandone la idoneità ad impedire la commissione del reato, attribuendo alla stessa grande importanza.[30]

I flussi informativi all'interno di un modello dinamico come quello previsto nel d. lgs. 231/2001 sono assolutamente indispensabili per la costanza di attivazione. Si tratta di una comunicazione che deve operare in modo trasversale alle varie aree di

---

che «pur riconoscendo che il Codice Etico ben potrebbe esistere in via autonoma a prescindere dall'adozione di un Modello Organizzativo» esso ne costituisce il «nocciolo duro». Vedasi in proposito SALVATORE, *Il "Codice Etico": rapporti con il Modello Organizzativo nell'ottica della responsabilità sociale dell'impresa*, in *La responsabilità amministrativa delle società e degli enti, Rivis. 231, 2008, 4, 71*.

[29] Ordinanza del Tribunale di Milano del 20 dicembre 2004, con nota di CARDANI, *Spunti di riflessione applicativi,* in *Riv. 231*. fra le considerazioni: «Nel caso in esame particolare attenzione dovrà essere rivolta ai meccanismi di creazione di fondi extracontabili, alle modalità di redazione dei bilanci, ai meccanismi di fatturazione infragruppo, agli spostamenti di liquidità da una società all'altra del gruppo, alle modalità di esecuzione degli appalti ed ai controlli relativi».

[30] Nel caso specifico il Tribunale si esprime valutando che: «deve altresì essere considerata la totale opacità nella gestione delle risorse finanziarie della società: la commissione dei reati di corruzione ha evidenziato che la gestione dei flussi finanziari rappresenta una delle aree maggiormente a rischio nelle società X e Y. La gestione amministrativa delle società "del gruppo" è dominata da una grave assenza di trasparenza: anche, e soprattutto sotto questo profilo, si manifesta l'inadeguatezza dei *compliance programs* che non affrontano il punto e non dettano regole che, rendendo controllabile la gestione delle risorse finanziarie, possano diminuire il rischio del verificarsi di eventi della stessa indole di quelli già verificatisi».

operatività dell'ente, prevedendo scambi con il vertice e con le varie funzioni aziendali.

La presenza di flussi informativi e formativi continui, come fatto rilevare,[31] è alla base della creazione di una vera cultura etica. È innanzitutto indispensabile la concreta e attiva partecipazione del *top management*, e di tutti i soggetti apicali, nella divulgazione e diffusione dei valori aziendali; questi soggetti devono diventare ambasciatori della compliance interna, innescando un meccanismo di emulazione positiva nei confronti dei propri comportamenti da parte di tutta la gerarchia aziendale.

L'azienda deve inoltre predisporre, su istruzioni dell'organo dirigente, una accurata attività di comunicazione delle regole di condotte interna, organizzata in modo tale da potere essere definita capillare; allo stesso modo, queste regole devono essere messe a disposizione di destinatari sia interni che esterni; devono ad esempio trovarsi pubblicate sul sito *internet* o sull'*intranet aziendale*, in modo da potere esser consultate in modo agevole sia dai dipendenti che da soggetti terzi, e si avrà ovviamente cura che lo stesso venga regolarmente aggiornato.

La comunicazione deve riguardare tutti gli aspetti legati all'operatività "*compliance*" dell'azienda: saranno presenti il codice etico, le procedure, i poteri autorizzativi, ed anche il sistema disciplinare che l'ente prevede in caso di inosservanza delle regole interne, in modo trasparente.

È inoltre da adottare un atto formale di comunicazione nei confronti di tutti i destinatari interni affinchè obbligatoriamente prendano visione dell'adozione del Modello 231, ritirando una dichiarazione, almeno dai soggetti apicali, «nella quale si attesti la conoscenza dei principi contenuti nel modello, nonché l'impegno ad osservarne le prescrizioni e a non tenere condotte che possano esporre l'ente alla responsabilità del reato».[32]

Nella corretta logica della diffusione dei comportamenti *compliance* e della convinta adesione ai valori dichiarati, l'ente ha la possibilità di riferire verso

[31] Fra gli altri, SCHETTINO – LUCARIELLO, *la difesa degli enti,* cit.,84
[32] Come sopra.

l'esterno il proprio modello, prevedendo nelle stipule contrattuali verso clienti, fornitori, partner, consulenti la obbligatoria adesione allo stesso ed al codice etico previsto, stabilendo che la violazione di tale clausola comporta inadempimento contrattuale.

Coesistente con questa attività informativa e di comunicazione, deve inoltre essere prevista una attività di formazione, con *recall* periodici, attinente sempre la *compliance* interna, i contenuti del modello organizzativo, le regole di condotta, il sistema disciplinare, il meccanismo anonimo di segnalazioni *whistleblowing*, avendo cura di diversificare i livelli formativi in funzione dei destinatari e assicurando la presenza di una formazione effettiva, in presenza od a distanza (*e-learning*), composta con moduli sistematicamente aggiornati e risposta alla formazione misurabile tramite test finali.[33]

Seguendo sempre l'art. 6 comma 2, al punto e) viene stabilita l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Le sanzioni svolgono una funzione autonoma rispetto alla realizzazione o meno del reato-presupposto: sono conseguenziali alla violazione del modello, a prescindere dalla chiamata in giudizio dell'ente.

Devono rispettare le prescrizioni dello Statuto dei Lavoratori, e ottemperare ai principi generali di proporzione, (commisurando la sanzione irrogata alla violazione commessa, assicurando il contraddittorio), e di tipicità e specificità,

[33] Di sicuro interesse a proposito di formazione l'Ordinanza 9 novembre 2004 Tribunale di Milano, *Esame dell'idoneità dei modelli di organizzazione, gestione e controllo ex art.t 6 e 7 d.lg. 231/2001*, in *Olympus, osservatorio per il monitoraggio permanente della legislazione e della giurisprudenza sulla sicurezza del lavoro*, *olympus.uniurb.it*: «In ordine alla formazione - il cui compito è quello di assicurare una adeguata conoscenza, comprensione ed applicazione del modello da parte dei dipendenti e dei dirigenti - le contenute nel modello VCM sono assolutamente generiche: non si differenzia la formazione a seconda che la stessa si rivolga ai dipendenti nella loro generalità, ai dipendenti che operino in specifiche aree di rischio, all'organo di vigilanza ed ai preposti al controllo interno; non si prevede il contenuto dei corsi, la loro frequenza, l'obbligatorietà della partecipazione ai programmi di formazione; non si prevedono controlli di frequenza e di qualità sul contenuto dei programmi di formazione.
Per quanto concerne il sistema disciplinare non è espressamente prevista la comminazione di sanzione disciplinare nei confronti degli amministratori, direttori generali e *compliance officers* che — per negligenza ovvero imperizia — non abbiano saputo individuare, e conseguentemente eliminare, violazioni del modello e, nei casi più gravi, perpetrazione di reati».

prevedendo fra l'altro un meccanismo trasparente preventivo, ben comunicato dove vengono indicate le fattispecie punibili e la graduazione delle sanzioni, ed il ruolo dell'Organismo di Vigilanza.

Il sistema disciplinare può riguardare anche i collaboratori esterni all'ente, a questo vincolati da un rapporto contrattuale di vario tipo, come può essere un rapporto di lavoro autonomo, piuttosto che di appalto, o di fornitura di beni o di servizi.

Il motivo di questa estensione sta nell'interesse protetto dal d.lgs. n. 231/2001, consistente nell'evitare che l'ente si avvalga dello strumento reato per la propria "politica di impresa" o comunque per la propria operatività in concreto.[34]

Ovviamente in questo caso la responsabilità non potrà che essere di tipo contrattuale; sarà pertanto necessario che nel momento in cui venga instaurato il rapporto contrattuale, la controparte abbia conoscenza di questa volontà e dei contenuti relativi.

Dovranno pertanto essere contenute delle clausole che prevedano, al verificarsi di determinate condizioni, funzionali al rispetto del modello organizzativo, il recesso dell'ente, piuttosto che l'irrogazione di penali, salvo in ogni caso l'eventuale risarcimento del danno che l'ente possa subire nel caso di applicazione delle sanzioni; o la risoluzione del rapporto contrattuale.

Con legge 179 del 2017 è stato inoltre inserito nell'impianto dell'art. 6 del d.lgs. 231/2001 l'istituto del *whistleblowing*. Così come i *compliances program,* anche questo strumento trova origine dalla normativa statunitense, dove indicativamente negli anni '80 del secolo scorso venne introdotta una importante normativa che disciplina ed incentiva la rivelazione da parte dei membri di un'organizzazione, di pratiche illegali, illegittime o anche soltanto immorali, prevedendo la tutela, l'anonimato od anche la premialità dei soggetti informatori, e prescindendo dalle

[34] Sul punto v. SANTI, *Modelli e responsabilità,* cit., 218 ss, che affermando la responsabilità di collaboratori esterni, fa presente, che l'ente può pretendere che tale collaboratore rispetti e si adegui alle regole di condotta che rispecchiano i valori contenuti nel Codice Etico.

motivazioni delle stesse, che possono essere di natura etica, od anche meramente economica.[35]

Il *whistleblowing* entra nel nostro ordinamento nel 2012 con la legge 190, (c.d. Legge Anticorruzione o Legge Severino), contenente «Disposizioni per la prevenzione e la repressione della corruzione dell'illegalità nella pubblica amministrazione», che ha introdotto nel d.lgs. 165/2001 (c.d. «TU Pubblico Impiego») il nuovo art. 54 *bis* ("Tutela del dipendente pubblico che segnala illeciti").

La nuova disciplina si inseriva all'interno di una strategia coordinata a livello europeo per la prevenzione di un reato, la corruzione, ad alto impatto destabilizzante sia dal punto di vista sociale che economico, sempre più radicato anche a livello internazionale, importando dei meccanismi che contribuissero ad innalzare il senso civico e la tutela di chi denunciasse fenomeni corruttivi.

Nel nostro sistema la legge 190/2012 inserisce questi meccanismi di tutela ed incentivazione limitandosi alla sola Pubblica Amministrazione, prevedendo il divieto di sottoporre a sanzione, licenziamento o a misura discriminatoria il dipendente pubblico che denuncia all'Autorità Giudiziaria, alla Corte dei conti o all'Autorità Nazionale Anticorruzione (ANAC), ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, con esclusione delle ipotesi di segnalazione integranti calunnia o diffamazione. La norma, inoltre, a maggiore cautela, contemplava il tendenziale divieto di rivelazione del nome del segnalante nei procedimenti disciplinari, assicurandone l'anonimato,[36] e prevedeva la segnalazione di eventuali misure

[35] Per approfondimenti in materia di *whistleblowing*, fra gli altri BORSARI – FALAVIGNA, *Whistleblowing, obbligo di segreto e "giusta causa" di rivelazione*, *Rivis. 231, 2018, 02, 41ss.*

[36] L'identità del segnalante non può essere rivelata ed è coperta da segreto, nei modi e nei limiti indicati dalla legge; in particolare, per quanto riguarda il procedimento penale eventualmente scaturito dalla segnalazione l'identità è coperta dal segreto seguendo i contenuti dell'art. 329 c.p.p.; pertanto, incontra il limite imposto dal diritto di difesa. In proposito può essere citata la sentenza della Cass. pen., Sez. VI, 31 gennaio 2018, n. 9047. La Corte ha precisato che, anche nella nuova formulazione dell'art. 54-*bis*, d.lgs. 165/2001, «la tutela della riservatezza del segnalante è prevista solo e a determinate condizioni in sede disciplinare, ma non qualora la segnalazione sia utilizzata nel procedimento penale», in *onelegale.wolterskluwer.it*

discriminatorie al Dipartimento della funzione pubblica, per i provvedimenti tutelanti di competenza.

Con l'art. 2 della legge 179 del 2017 la disciplina del *whistleblowing* viene estesa al settore privato, con l'inserimento dell'istituto all'interno dell'art. 6 della legge 231/2001. Sono soggetti segnalanti sia i soggetti apicali che i sottoposti, che presentano «a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del […] decreto e fondate su elementi di fatto precisi e concordanti», ma anche di «violazione del modello di organizzazione e gestione dell'ente». Viene precisato dall'articolo che i fatti sono venuti a conoscenza «in ragione delle funzioni svolte».

Inoltre vengono confermate una serie di tutele, previste dalla disciplina del settore pubblico, per garantire innanzitutto la riservatezza del soggetto segnalante, poi la presenza di un canale di comunicazione alternativo, anche di tipo informatico, in grado anche questo di tutelare la riservatezza [37]; il divieto di atti ritorsivi o discriminatori, e la specifica della presenza, all'interno del sistema disciplinare, sia di sanzioni nei confronti di chi viola le misure di sicurezza del segnalante, che nei confronti del segnalante stesso che con dolo o colpa grave effettua segnalazioni che poi si rivelano infondate.

Di rilievo l'art. 3 della nuova legge che stabilisce un'opportuna disciplina di coordinamento con l'obbligo di segreto d'ufficio, professionale, scientifico, industriale e aziendale, mettendo al riparo il *whistleblower* da eventuali responsabilità di carattere penale o civile in caso di violazione di tale obbligo, stabilendo una "giusta causa di rivelazione", considerato il preponderante interesse all'integrità delle amministrazioni pubbliche e private.

[37] Sul punto GULLO, *i modelli organizzativi*, cit., 260, mette in evidenza che a differenza della disciplina del settore pubblico, dove sono individuati i destinatari della segnalazione (ANAC, Corte dei Conti, Autorità Giudiziaria), nulla viene detto dalla normativa. L'autore ritiene che «l'interlocutore naturale sembrerebbe essere l'Organismo di Vigilanza, tanto più se sia garante del Codice Etico. In linea di principio si potrebbe però istituire una differenza tra segnalazioni riguardanti condotte illecite integrati reati presupposto (di competenza dell'ODV) e quelle concernenti violazioni del modello, che potrebbero vedere un'istruttoria avviata dalle funzioni interne dell'ente (es. compliance o risorse umane).

In termini critici viene rilevato da alcuni autori[38] che la scelta del legislatore di utilizzare la normativa 231/2001 non appare convincente, «in quanto il d.lgs. 231/2001 configura un apparato di norme funzionalmente orientato alla prevenzione di reati e non alla segnalazione di illeciti o mere irregolarità per giunta già verificatisi. Va peraltro considerato che la nuova disciplina non si rivolge a tutti gli enti, ma solo a quelli destinatari del "Decreto 231" che abbiano scelto di adottare un Modello Organizzativo, con l'ulteriore conseguenza che, rappresentando l'adozione del MOG una facoltà e non un obbligo, la tutela del w*histleblower* non può che ritenersi, a propria volta, meramente facoltativa»; da sottolineare che, pur in presenza della riportata considerazione, l'inserimento del *whistleblowing* all'interno del settore privato viene valutato con estremo favore.[39]

Una volta conclusa l'elaborazione del modello, le norme di autoregolamentazione in esso contenute devono diventare regola operativa per l'ente. Sarà quindi necessaria una delibera dell'organo dirigente, che deve avere caratteristiche formali evidenti, anche in termini di certezza di data e pubblicizzazione. Si ricordi in proposito che l'esimente prevista all'art.6 si riferisce a modelli di organizzazione e gestione idonei adottati *prima* della commissione del fatto. Inoltre che il modello può sortire effetti benefici sull'ente anche se adottato dopo il reato, ma prima dell'apertura del dibattimento. La presenza di una data certa, oltre ad essere argomento di trasparenza, anche in termini reputazionali e dichiaratori dell'atteggiamento *compliance* dell'ente, può quindi assumere particolare importanza in singoli casi concreti.

[38] BORSARI – FALAVIGNA, *Whistleblowing, obbligo di segreto,* cit.,46, 59.

[39] Da segnalare il recente d.lgs. 24/2023, che recepisce la Direttiva UE n. 1937/2019 – c.d. "Direttiva *Whistleblowing*". Il Decreto, ampliando la portata oggettiva (gli illeciti e le violazioni che possono essere oggetto di segnalazioni) e soggettiva (coloro che sono legittimati a realizzare la segnalazione, i c.d. *whistleblowers*), mira a colpire eventuali condotte illegittime, assicurando il buon andamento dell'ente pubblico o privato. Allo stesso tempo, nella convinzione di incentivare le segnalazioni, la nuova normativa prevede una lunga serie di tutele per il *whistleblower*, fra queste la tutela della riservatezza. Per approfondimenti sull'argomenti v. fra gli altri SINGH, *Whistleblowing e riservatezza nel d.lgs. n. 24/2023, in Altalex,* 2023,07

3. **Organismo di Vigilanza**

La presenza del Modello Organizzativo è stata più volte citata come centrale all'interno dell'apparato del d.lgs. 231/2001; analoga importanza è da attribuire all' Organismo di Vigilanza, che presidia e vigila sul funzionamento e sull'osservanza del Modello stesso.

Anche per quanto riguarda l'OdV la normativa di definizione è estremamente scarna[40].

Il punto di riferimento principale è rappresentato dall'art.6 del d.lgs. 231/2001, dove al comma 1, ai fini della esimente di responsabilità, viene richiesto, alla lettera b), che sia presente un «organismo dell'ente dotato di autonomi poteri di iniziativa e controllo» con «il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento », e alla lettera d) dove, sempre ai fini della esimente, viene richiesto che «non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)».

Ancora, sono presenti disposizioni normative dirette all'Organismo nell'art.6, 4 e 4-*bis*[41], dove si fa presente che negli enti di piccole dimensioni i compiti dell'OdV «possono essere svolti direttamente dall'organo dirigente» (art.4) e 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 vigilanza di cui al comma 1, lettera b)».

---

[40] GULLO, *i modelli organizzativi*, cit., 275 parla di «laconicità del dato normativo», citando a sua volta ABRIANI-GIUNTA, *L'Organismo di Vigilanza previsto dal d.lgs. 231/2001. Compiti e funzioni*, in *Responsabilità amministrativa delle società e degli enti*, *Rivis. 231, 2012, 3, 192,* che definiscono la normativa sull'OdV come uno dei punti più oscuri della normativa 231 e così si esprimono sul punto: « Ad ogni modo, la mancanza di una disciplina dettagliata spiega la ragione per la quale le articolazioni del tema in esame (funzionamento, modalità di nomina, requisiti dei membri, ecc.) saranno affrontate essenzialmente alla luce della dottrina di settore (penalistica e commercialistica), di alcune (sul punto, peraltro, sporadiche) decisioni giurisprudenziali e delle Linee Guida elaborate dalle associazioni di categoria. Ciò nella consapevolezza che l'OdV resta uno dei punti più oscuri della disciplina delineata dal d.lgs. 231/2001, anche in ragione del fatto che si tratta di un *unicum* nel panorama comparatistico, con la conseguenza che l'interprete non può giovarsi di indicazioni tratte dell'esperienza straniera».

[41] Art.6, 4-*bis,* introdotto con l'art.14 co. 12 della legge n.183 del 2011.

Non essendoci altri riferimenti all'OdV all'interno della 231/2001, oltre quelli già citati[42]; i contenuti relativi ai suoi poteri, alla qualificazione dei suoi componenti, alla sua concreta operatività sono frutto di una elaborazione proveniente innanzitutto dalle associazioni di categoria, espresso dalle Linee Guida, poi la prassi delle singole aziende, con l'individuazione delle *best practies*, oltre il lavoro della dottrina e della giurisprudenza.[43]

Da segnalare che secondo una parte della dottrina, l'assenza di più analitiche indicazioni legislative sarebbe frutto di una scelta consapevole, onde consentire che l'OdV possa essere liberamente modellato in relazione al grado di complessità aziendale di ogni singolo ente[44].

In termini sistematici, possiamo dividere le attività di approfondimento sull'OdV in due blocchi, il primo legato ai soggetti che dell'organismo fanno parte, l'altro legato ai contenuti; sarà inoltre di sicuro interesse relazionare sull'indagine svolta nel 2021 da Assonime, focalizzata sulla presenza e sul funzionamento dell'OdV, in un campione selezionato di società di dimensioni medio-grandi.

3.1 **(*segue*) Organismo di Vigilanza: i soggetti**

La prima considerazione legata all'OdV è che esso può esistere sia come organo a composizione plurima[45] che monocratico. La scelta è frutto di una valutazione ponderata, affidata all'organo dirigente, in funzione della complessità aziendale ed in particolare avendo riguardo agli assetti organizzativi e alle conclusioni della fase

[42] Neanche per ciò che riguarda l'istituto del *whistleblowing*, dove l'OdV è stato riferito come soggetto destinatario delle comunicazioni (cfr. cap.4, par.3)

[43] Nel 2021 Assonime ha svolto una ulteriore indagine in materia di 231/2001, focalizzato sull' OdV, al titolo *L'Organismo di Vigilanza nella prassi delle imprese a vent'anni dal d.lgs. 231/2001*, presente sul sito istituzionale *assonime.it*. L'indagine, particolarmente interessante, ha riguardato i comportamenti concreti realizzati dalle imprese sulla realizzazione ed il funzionamento dell'OdV.

[44] In questo senso ABRIANI -GIUNTA, *L'Organismo di Vigilanza previsto*, cit., 192.

[45] Secondo SANTI, *Modelli e responsabilità*, cit., 241 si deve parlare di una composizione collegiale imperfetta: «Nelle discipline giuridiche i collegi vengono qualificati: come perfetti (o reali) quali sono quelli che possono deliberare solo con la presenza di tutti i membri che li compongono; come collegio imperfetto, che può assumere deliberazioni anche con la presenza di alcuni membri sempreché sia raggiunto il numero legale previsto dalle norme che ne regolano il funzionamento. Nel diritto commerciale gli organi, le cui funzioni si avvicinano maggiormente a quelle di un Organismo di Vigilanza, sono l'organo di revisione, se collegiale e il collegio sindacale. Poiché entrambi non sono qualificati come collegi perfetti, si deve ritenere che questa conclusione debba essere confermata anche per l'Organismo di Vigilanza pluripersonale».

di *risk assesment*: qualora emerga una predisposizione contenuta alla realizzazione di un reato-presupposto, si potrebbe optare per un organismo di vigilanza monocratico, diversamente si dovrà preferire una vigilanza più articolata. Confindustria in proposito nelle Linee Guida fa riferimento alle *dimensioni* dell'ente nella scelta fra OdV monocratico o collegiale. In ogni caso dovrà essere tenuta ben presente, nelle decisioni, la necessità di un presidio effettivo ed aggiornato nei controlli da effettuare.

Secondo diversi autori è inoltre preferibile che si definisca un organismo autonomo ulteriore rispetto a quelli già esistenti. Questa valutazione è effettuata sulla base di un dato formale: la espressa previsione fatta all'art.6 comma 4 e 4-*bis* della 231/2001 dal legislatore di consentire l'identificazione dell'OdV con l'organo dirigente o con il collegio sindacale deve essere intesa come eccezione; ed inoltre sulla base di una necessità sostanziale: la presenza di una struttura autonoma consente un più specifico ed accurato controllo. Viene inoltre messo in evidenza[46] che anche la struttura di *internal audit*, teoricamente la più accreditata a svolgere le funzioni di OdV, ha un piano annuale che deve essere approvato dal CdA, mentre il Piano annuale di Vigilanza, disposto dall'OdV, deve solo essere comunicato al CdA, con evidenza di maggiore indipendenza.[47]

Prima di passare alle caratteristiche della composizione soggettiva dell'OdV, devono essere citati i due comma. 4 e 4-*bis*, dove vengono presi in considerazione due situazioni ben diverse: il comma 4 si riferisce agli enti di piccole dimensioni, e rappresenta uno dei pochi casi dove il legislatore evidenzia la differenza di dimensioni aziendali ai fini della legge 231/2001, (tema che abbiamo già sviluppato in precedenza). In questo caso la soluzione proposta dalla norma è che i compiti indicati nella lettera b) possono essere svolti dall'organo dirigente; questo ovviamente nella considerazione che siamo in presenza da un lato di una struttura meno complessa, dall'altro che c'è probabilmente una minore disponibilità organizzativa e finanziaria a generare un OdV con caratteristiche "ordinarie". Per

[46] Fra gli altri GULLO, *i modelli organizzativi*, cit., 279; BERNASCONI – PRESUTTI, *Manuale della responsabilità*, cit., 158

[47] A favore di una struttura autonoma che deve essere costituita all'interno dell'azienda e sia specificamente preposta a quei compiti, anche la Relazione al decreto 231, cit.

quanto la soluzione generi una corretta semplificazione, crea tuttavia un a situazione di potenziale sovrapposizione fra controllore e controllante.

L'art. 6 comma 4-*bis* è invece introdotto dalla legge 12 novembre 2011 n.183 mette in evidenza 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 vigilanza di cui al comma 1, lettera b)». La soluzione, funzionale anche in questo caso ad una semplificazione, come vedremo a breve è stata adottata solo da un limitatissimo numero di aziende intervistate nel 2021 da Assonime, ed è stata oggetto di considerazioni critiche: si ritiene fra l'altro che le funzioni del collegio sindacale, stabilite per legge, non prevedano quei poteri di iniziativa e controllo che devono essere caratteristica dell'OdV, così come è assente la continuità di azione richiesta invece all'Organismo. [48]

[48] In questo senso, le Linee Guida Abi osservano che: «Attesa la configurazione e le funzioni che il decreto attribuisce a tale organismo, non appare coerente una sua identificazione con il collegio sindacale, le cui funzioni sono stabilite dalla legge e che non è fornito, in materia, di quei poteri autonomi di iniziativa e di controllo di cui il decreto fa, come visto, espresso riferimento», mentre le Linee Guida di Confindustria recitano che in capo al Collegio Sindacale appare arduo:« riscontrare la necessaria continuità di azione che il legislatore ha inteso attribuire all'Organismo. Va inoltre, tenuto presente che in molte realtà societarie di dimensioni minori quest'obbligo non è obbligatorio per legge, e ancora, che l'attività di esso può essere soggetto di controllo (in particolare con riferimento al delitto di false comunicazioni sociali) ai sensi del d.lgs: n.231/2001». Altri approfondimenti in questo senso sono su AODV, (*Associazione dei Componenti degli Organismi di Vigilanza*), *La modifica dell'art.6 del d.lgs.231/2001: critica ragionata all'attribuzione al collegio sindacale della funzione di organismo di vigilanza*, 2012,3, 1ss. Sul punto inoltre anche BERNASCONI – PRESUTTI, *Manuale della responsabilità*, cit., 161; l'autore da un lato evidenzia da un lato che è «indubbio che il problema della proliferazione degli organi di controllo endosocietari vada affrontato perseguendo il duplice obiettivo di razionalizzare un quadro quanto mai composito riducendo il numero dei controllori armonizzandone le competenze — e di diminuire i costi (economici, di tempi e di risorse) connessi alle attività di vigilanza», ma che tuttavia «la scelta operata dal legislatore del 2011 si rivela un rimedio peggiore del male da contrastare, al punto tale che essa si presta ad essere disapplicata.» Fra i punti critici messi in luce: a) l'incompatibilità di funzioni tra i due organi; la legislazione societaria ha progressivamente caricato i sindaci di una pluralità di compiti di controllo sull'amministrazione della società, ritagliando per tali figure un ruolo, per non pochi aspetti, contraddittorio; la vigilanza sull'operato dell'organo gestorio si snoda infatti attraverso una molteplicità di "momenti di condivisione" delle decisioni degli apicali, ovvero situazioni nelle quali il sindaco (controllore) appare in rapporto "osmotico" con l'amministratore (controllato); in altre parole, l'attuale sistema di controllo *intramoenia* sembra spingere il titolare dell'obbligo di vigilanza ad affiancare il *top management*, quasi a corresponsabilizzarlo in scelte che — resta fermo — non possono non rimanere di stretta prerogativa dell'amministratore » questa situazione viene ritenuta incompatibile con la necessaria previsione di alterità stabilità invece per l'OdV; b) la già segnalata «coincidenza tra controllore e controllato palesata, in maniera plastica, dalla responsabilità dei sindaci per taluni reati societari quali le false comunicazioni sociali (art. 2621 c.c.)», poi ancora c) «la posizione di garanzia ricoperta dal sindaco si sostanzia nell'obbligo di impedimento del reato altrui e nella responsabilità penale del primo per mancato esercizio della funzione di controllo; trattasi di un profilo inconciliabile con l'attività e il ruolo dell'organismo di vigilanza che, per sua natura, non è destinatario di un obbligo di impedire l'evento, non ricopre

La provenienza dei soggetti che faranno parte dell'OdV, deve essere distinta fra nominativi interni all'azienda, possibilmente inseriti in funzioni che hanno dimestichezza con attività di controllo e compliance, e nominativi esterni, in grado di assicurare un tema di indipendenza in linea di principio superiore.

Nel caso sia stato istituito un organismo a struttura monocratica, si impone la scelta per un componente esterno all'ente.[49] Qualora invece l'organo dirigente abbia optato per un organismo collegiale, è condivisibile la preferenza per situazioni miste, dove la presenza di una risorsa interna può rappresentare un elemento di notevole valore per l'approfondita conoscenza dell'azienda e dei suoi processi, favorendo anche la velocità di interazione. Nella scelta di questo elemento interno è opportuno che provenga da filiere che abbiano competenza sui processi e le normative di controllo e compliance, quindi il Responsabile *Internal Audit* potrebbe essere un candidato ideale per l'OdV.

Le figure professionali adibite all'OdV devono inoltre possedere dei requisiti ben definiti, sintetizzabili nella indipendenza, autonomia professionalità, onorabilità. Si tratta di caratteristiche individuali, non solo dell'Organismo nel suo complesso (quindi non deve ritenersi compensabile all'interno dell'OdV una eventuale situazione di carenza).

L'indipendenza e l'autonomia discendono dalla stessa dicitura dell'art. 6, comma 1, lettera b), dove si afferma la necessità per l'OdV di «autonomi poteri di iniziativa e di controllo».

L'indipendenza si riferisce alla esclusione di qualunque tipo di conflitto di interessi in grado di incidere sullo svolgimento dell'attività, condizionandola. Deve quindi

posizioni di garanzia e — dunque — non può considerarsi, nelle figure dei suoi componenti, penalmente responsabile; ed infine d) «le competenze tecniche del collegio sindacale non coincidono con quelle dell'organismo di vigilanza; la composizione paradigmatica del primo annovera un ragioniere (o un perito commerciale, o un consulente del lavoro), addetto al controllo contabile delle poste di bilancio, affiancato da un dottore commercialista, chiamato a vagliare la metodologia seguita nel redigere la contabilità, nonché da un avvocato (civilista), per la verifica degli atti; ben diversa, in quanto riflette natura e funzioni dell'oggetto del controllo, cioè il modello organizzativo, la struttura "ideale" — secondo le *best practice* formatesi nel primo decennio di applicazione del d.lgs. n. 231 del 2001 — dell'organismo di vigilanza, nel quale le professionalità di natura giuridico-penale ed organizzativo-aziendale esercitano un ruolo preminente e non certo surrogabile da quelle di matrice contabile».

[49] In questo senso in modo categorico SANTI, *Modelli e responsabilità,* cit., 248, scelta che appare sicuramente preferibile per un tema di terzietà.

essere evitata con grande cura qualunque forma di situazione possa generarlo, con ciò intendendo a titolo di esempio rapporti di sottoposizione gerarchica al *management*, ma anche rapporti di tipo economico, prestazioni di consulenze alla società; deve inoltre essere assicurata la separazione dagli organi di gestione.

L' autonomia riguarda invece la capacità dell'organismo di svolgere effettivamente i suoi poteri di ispezione e controllo, e quindi di potere assumere d'iniziativa attività di accesso ai dati pertinenti dell'impresa, alla capacità di svolgere verifiche, all'organizzazione autonoma della propria struttura, alla nomina di eventuali consulenti esterni (si pensi agli esperti informatici) ed ovviamente ad avere capacità finanziaria, con l'assegnazione di un *budget* congruo e con livelli retributivi adeguati al ruolo, sia che si tratti di soggetti interni che esterni.

La professionalità, secondo le linee guida di Confindustria è riferibile a due ipotesi nelle quali sono attribuite queste qualità: la competenza tipica nelle funzioni di *internal auditing* riferibili a conoscenza e dimestichezza con metodologie proprie delle attività ispettive o di controllo dedicate alla individuazione e valutazione dei rischi, non escludendo la capacità di individuare possibili frodi; la competenza di tipo giuridico nella prospettiva del diritto di impresa che vede in quello legale il rischio da gestire. A tale riguardo, la conoscenza del diritto penale deve necessariamente integrata da quelle che attengono ad altri profili normativi che riguardano la dinamica dell'ente nella sua concretezza

Ulteriore componente legata alla individualità dei componenti dell'organo è l'onorabilità. Pur non essendo esplicitamente prevista, è desumibile dall'ordinamento, in funzione delle normative che richiedono infatti la sussistenza dell'onorabilità in capo agli amministratori di società e ai sindaci. Pertanto dovranno essere assenti sentenze di condanna, anche non definitive, ovviamente su reati pertinenti la funzione che si sta esaminando.

Infine, requisito concordemente richiesto all'Organismo, è quello della continuità di azione. Si sostanzia in una serie di attività di impulso, che possono essere rappresentate da un articolato calendario dei lavori, nella presenza di regolari riunioni, nella verbalizzazione e tracciabilità dei contenuti delle stesse, nella presenza di adeguati e completi flussi informativi verso l'amministratore delegato,

il consiglio di amministrazione, il collegio sindacale, incontri con la funzione responsabile delle risorse umane per la formazione del personale, controllo delle informazioni ricevute dalle aree sensibili, verifiche da eseguire in conformità al piano annuale, ispezioni mirate, segnalazioni delle riscontrate violazioni del modello, aggiornamento di quest'ultimo: l'attività dell'Organismo deve essere continua, non può svolgersi in modo episodico o saltuario.

Può essere molto interessante riportare in modo sintetico una serie di considerazioni e dati tratti dal nuovo rapporto Assonime del 2021 dedicato all'OdV.

La precedente indagine era stata svolta dall'associazione a pochi anni dall'avvento della 231/2001 (il primo rapporto è del 2008), ed era riferito ad un campione di 300 società di capitali.[50] Il nuovo rapporto a vent'anni di distanza dalla nascita del d.lgs. opera in un contesto molto più maturo rispetto al precedente. Si riferisce inoltre ad aziende quotate in borsa, (226 aziende) quindi decisamente strutturate dal punto di vista organizzativo, con strutture di controllo interno multiple e particolare attenzione alla *compliance* aziendale[51]; ne è testimonianza che il 98% delle società intervistate ha un Organismo di Vigilanza attivo, ed il residuo 2% non ha OdV esclusivamente perché si tratta di holding dove è stato valutato assente il rischio reato.

Riprendendo in considerazione i punti precedentemente evidenziati, risulta innanzitutto che la nomina dell'OdV e la scelta della sua composizione «configurano un atto organizzativo rimesso alla discrezionalità del consiglio di amministrazione». La nomina viene quindi attribuita all'organo di gestione. Sono segnalati solo due casi in cui la nomina è stata rimessa alla competenza assembleare, ed in queste due situazioni l'OdV è stato fatto coincidere con il collegio sindacale.

---

[50] Rapporto Assonime "*Indagine sull'attuazione del decreto legislativo 231/2001" sul sito istituzionale, assonime.it. 2008*

[51] Come riportato dal sito istituzionale, «L'indagine Assonime è stata condotta sulle società emittenti titoli quotati sul mercato regolamentato di Borsa Italiana. Si tratta di imprese di dimensioni medio-grandi, articolate in organizzazioni di gruppo, che operano in settori eterogenei, sensibili al profilo reputazionale e che investono in sistemi di compliance e controllo avanzati, allineati alle migliori prassi nazionali e internazionali. Questo campione rappresenta il destinatario fisiologico delle finalità di prevenzione della disciplina 231 e delle specificità dei modelli di organizzazione previsti dalla L'Organismo di Vigilanza nella prassi delle imprese a vent'anni dal d.lgs. 231/2001", *Rapporto Assonime*, "*L'Organismo di Vigilanza nella prassi delle imprese a vent'anni dal d.lgs. 231/2001*", assonime.it, 2021,10 0

In quasi tutte le altre situazioni, come detto prevalenti in modo pressochè assoluto, l'OdV è un organismo autonomo, a composizione plurima, composto nella maggior parte dei casi da tre elementi di cui uno interno all'azienda, mentre il ruolo di Presidente viene fatto assumere quasi sempre ad uno dei nominativi esterni (nominativo interno solo nel 25% dei casi).

Come correttamente messo in evidenza, «la composizione dell'organismo che emerge dalla prassi riflette l'evoluzione nel tempo sia della giurisprudenza sia dell'autodisciplina. Spetta agli amministratori dare all'OdV la fisionomia più adatta all'impresa, sulla base dell'organizzazione, dimensione, tipo di attività esercitata, specifici profili di rischio, purché sia sempre assicurato un adeguato coordinamento dell'OdV nel sistema dei controlli societari».

I requisiti di indipendenza, autonomia, onorabilità professionalità vengono dichiarati nell'intervista come rispettati, non solo nominalmente, ma con la predisposizione di strumenti specifici, quali possono essere ad esempio regole dettagliate in tema di ineleggibilità e decadenza e un regolamento interno con previsione delle situazioni di giusta causa di revoca; allo stesso modo le società assicurano la previsione di autonomia finanziaria attraverso la predisposizione di un *budget*.

Da una prima analisi dei dati qui riportati in sintesi sui "soggetti" (ma vedremo che le stesse considerazioni saranno possibili quando tratteremo la parte relativa alle "funzioni") si delinea quello che è stato definito da Assonime come un «quadro omogeneo in cui le scelte organizzative delle imprese appaiono sostanzialmente allineate e sembrano rispondere alle principali questioni interpretative sorte nell'applicazione della disciplina».

3.2 **(segue) Organismo di Vigilanza: le funzioni**

Prendendo nuovamente spunto dall'art. 6 comma 1 b), il compito fondamentale dell'OdV è quello di «vigilare sul funzionamento e l'osservanza del modello»; alla lettera d) viene poi riportato che ai fini della esenzione di responsabilità, non vi deve essere stata «omessa od insufficiente vigilanza da parte dell'OdV». La

normativa si limita a queste prescrizioni, pertanto anche in tema di compiti e funzioni, fondamentale, nello sviluppo dei contenuti è stata l'attività delle associazioni con le Linee Guida, della prassi, della giurisprudenza e della dottrina.

Una prima considerazione che viene ricavata in modo condiviso è legata all'assenza di attività "gestionale": l'OdV non ha compiti gestionali, ha esclusivamente compiti di sorveglianza, non interviene con poteri impeditivi e con facoltà di sostituirsi ad altri soggetti non ottemperanti; piuttosto, in situazioni dove si prefigura una operazione a rischio-reato, deve riferire al vertice aziendale.[52]

Nella definizione del compito di vigilanza sul funzionamento e l'osservanza del Modello Organizzativo, possono individuarsi una serie di attività a cui l'OdV deve dedicarsi. Innanzitutto è necessario che venga esaminata la struttura del Modello per verificarne la conformità con quanto previsto dalle disposizioni di legge e con le eventuali linee guida, se presenti, delle associazioni di categoria specifiche per il settore a cui appartiene l'ente. Si verificherà anche la presenza di un Codice Etico, che abbiamo detto fare parte del MOG.

Si entrerà nel merito del modello, verificando che la parte generale corrisponda alle caratteristiche reali dell'ente, e che allo stesso modo nella parte speciale siano presenti i protocolli destinati a programmare il modo in cui l'ente forma e crea decisioni in relazione alle aree di rischio dove sono presenti reati da prevenire.

Curerà la verifica sulle attività formative (quindi se è stata fatta ed il modo in cui è stata erogata la formazione sul Modello), e l'accettazione dell'obbligazione di osservanza del modello; verificherà altresì la presenza di un sistema disciplinare, che come detto in precedenza è sganciato dalla ipotesi di realizzazione del reato-

[52] In questo senso, in modo comune, fra gli altri, GULLO, *i modelli organizzativi,* cit., 282; SANTI, *Modelli e responsabilità,* cit.*;* BERNASCONI – PRESUTTI, *Manuale della responsabilità,* cit., 173; ne viene ricavata la non configurabilità della responsabilità penale dei componenti dell'organismo per non avere impedito l'evento. Gullo in specifico afferma «non è in dubbio la possibilità di ammettere una responsabilità penale dei suoi membri in relazione ad una condotta attiva»(ad esempio concorso attivo ex art.110 in accordo con il *management*), piuttosto è da escludere una posizione di garanzia, in quanto «l'intera attività e l'insieme delle sue prerogative sono proiettate sul funzionamento del modello (…), i suoi doveri hanno come parametro di riferimento il modello»: gli obblighi dell'Organismo hanno oggetto l'organizzazione preventiva dell'ente e si riferiscono a ipotesi astratte.

presupposto, in quanto legato al rispetto del modello stesso, controllandone la pubblicizzazione.

Dovrà inoltre realizzare un sistema di comunicazione interno che garantisca il flusso di informazioni verso l'OdV, assicurandosi anche in questo caso una capillare informazione sulla presenza di questo meccanismo e sugli strumenti da utilizzare per realizzarlo.

Considerata la delicatezza della materia trattata, e gli impatti anche giudiziari, l'OdV si preoccuperà di verbalizzare le attività in cui viene coinvolto, comprese le proprie riunioni, la trasparenza di ogni decisione, e che siano tracciabili le operazioni e i soggetti che hanno dato luogo o sono destinatari delle operazioni svolte, con possibilità di ricostruire *ex post* in modo documentale quanto è avvenuto nei processi aziendali, archiviando in modo verificabile e inalterabile le attività che si sono realizzate.

Inoltre l'Organismo deve procedere a pianificare il programma delle verifiche, fermo restando che la vigilanza sulla funzione e l'osservanza del modello può supporre anche la sorpresa dell'attività di controllo.

L'attività dell'OdV è certamente di tipo dinamico: affinchè possa vigilare sull'osservanza del modello sarà necessaria continuità d'azione; così come continua dovrà essere l'attività di interazione con gli organi di amministrazione.

Fra i compiti di tipo dinamico l'art, 6 comma 1 lett. b) afferma che l'Organismo cura l'aggiornamento del modello organizzativo. Deve essere quindi prestata attenzione a mutamenti che possono essere intervenuti sia nella normativa esterna (si pensi all'inserimento di nuovi reati-presupposto che vadano generare situazioni di rischio per l'ente), piuttosto che variazioni nelle interpretazioni della giurisprudenza che richiedano interventi interni di aggiornamento, così come grande attenzione deve essere prestata alle dinamiche aziendali: la variazione di forma sociale, piuttosto che l'apertura a nuovi mercati, od ancora l'espansione verso nuove attività o una ipotetica acquisizione aziendale rappresentano tutte situazioni che non possono lasciare indifferente l'OdV, che, a fronte di rischi legati alla commissione di reati-presupposto, piuttosto che ad impatti negativi reputazionali,

preparerà e presenterà all'organo dirigente delle proprie note; quest'ultimo poi curerà che le stesse vengano realizzate.

Fra le attività che ingaggiano di continuo l'OdV sono inoltre da ascrivere sia i flussi informativi verso l'Organismo, che quelli che dall'OdV si sviluppano verso terzi.

Sul primo aspetto l'art. 6, comma 2, lett. d) del decreto dispone che i modelli devono prevedere obblighi di informazione nei confronti dell'organismo di vigilanza. È quindi *in primis* necessario che sia stata predisposta ed attuata una capillare attività di informazione sulla possibilità o il dovere di contattare, anche in forma anonima l'OdV, creando anche dei canali di accesso diretti (ad esempio di tipo informatico), e mettendo questi mezzi a disposizione di soggetti apicali e sottoposti, senza distinzioni.

Le notizie potranno riguardare, ad esempio, intervenuti segnali di allarme relativi alla commissione di un reato-presupposto, ma più in generale, tutto ciò da cui potrebbe derivare una responsabilità dell'ente ai sensi della normativa 231/2001; riguarderanno l'avvio di un procedimento giudiziario a carico di soggetti apicali o di sottoposti o le violazioni del Codice Etico piuttosto che del Modello Organizzativo, ed anche la segnalazioni di modifiche interne all'ente in grado di aumentare il livello di rischio.

In presenza di informative come quelle riportate, l'OdV deve svolgere una attività di attenta analisi delle stesse, sia per non disperdere il contributo prezioso fornito, che per evitare al contrario di dare rilevanza ad informazioni priva di contenuti o che diano luogo a sospetti non fondati.

In funzione dei principi generali di trasparenza e tracciabilità, l'OdV sicuramente deve tenere traccia anche di tutte le segnalazioni ricevute; dovrà poi selezionare quanto sia riferibile alla violazione del Modello o al rischio di realizzazione di reati-presupposto, distinguendo a questo punto la propria attività: potrebbe archiviare la notizia, in quanto priva di rilevanza, piuttosto che istruirla, arrivando anche a valutare una sanzione se prevista.

Per quanto riguarda il secondo aspetto, vale a dire verso chi comunica l'OdV, viene rilevato possano essere individuati tre destinatari: l'organo dirigente, l'autorità giudiziaria, l'assemblea dei soci[53].

L'organo dirigente rappresenta senza dubbio il destinatario istituzionale dei flussi informativi provenienti dall'Organismo di Vigilanza, trattandosi anche del soggetto che adotta il Modello e che ha la capacità e la responsabilità di aggiornarlo, anche e proprio sulla base dei pareri forniti dall'OdV.

L'informativa pertanto deve essere periodica, pianificata, e qualora l'organo dirigente si dimostri insensibile alle attività richiesta dall'OdV, lo stesso potrebbe rivolgersi ad altri organi di controllo aziendali.

L'autorità giudiziaria viene considerata interlocutore eventuale: il membro dell'OdV viene sottoposto ad audizione qualora avvenga la contestazione dell'illecito amministrativo all'ente ex art. 59 del d.lgs. 231/2001.

Infine l'assemblea dei soci non viene considerata destinataria dei flussi informativi dell'OdV. Incide su questa valutazione anche la considerazione della necessaria riservatezza delle attività svolte, che diversamente verrebbero pubblicizzate come verrebbero pubblicizzati processi e valutazioni interne. Ci sarebbe anche il rischio che le notizie assunte potrebbero essere maliziosamente strumentalizzate, creando all'azienda seri danni.

Anche sul tema delle funzioni e dei compiti dell'OdV il questionario Assonime ha fornito le seguenti importanti indicazioni. Per quanto riguarda l'adozione/creazione di un Regolamento, nel 74% dei casi l'OdV adotta un proprio regolamento nel quale generalmente vengono disciplinate la cadenza delle riunioni, i criteri di votazione, la verbalizzazione, i flussi informativi con gli altri attori del sistema dei controlli.

Da tenere sempre presente che il Regolamento può costituire un utile strumento per il giudice per valutare in sede di accertamento della responsabilità dell'impresa l'effettività della vigilanza e l'efficacia dei controlli svolti, nella prospettiva di un adeguato assetto organizzativo.

[53] La distinzione viene effettuata da BERNASCONI – PRESUTTI, *Manuale della responsabilità*, cit.

Il 75,6% delle società del campione assicura all'OdV una piena autonomia di spesa attraverso l'attribuzione di un *budget* dedicato all'assolvimento dei propri compiti, gestito in modo indipendente.

La presenza di una programmazione dell'attività di vigilanza, effettuata tramite un "piano di vigilanza", è presente nel 64% dei casi; viene anche considerato in proposito come il piano di vigilanza sia un elemento centrale in sede di valutazione giudiziale dell'operato dell'OdV. Altro elemento giudizialmente di significato è rappresentato dalla presenza di una attività stabilmente verbalizzata, indicatrice di attivazione e in grado di ricostruire l'operato dell'Organismo. Nel 75% dei casi la risposta è stata positiva.

L'80% delle società prevede espressamente nel modello organizzativo il potere dell'OdV di accedere liberamente a tutta la documentazione che ritiene possa essere rilevante ai fini della propria attività di vigilanza sul modello organizzativo e sul rispetto dei principi 231. Non si tratta generalmente del generico potere di chiedere atti e documenti, ma del potere di avere accesso diretto alla documentazione ritenuta utile, senza il consenso o la previa informazione di organi e funzioni aziendali.

Per quanto riguarda i flussi informativi, con riguardo a quelli che vanno dalla struttura verso l'OdV si distingue tra i flussi ad evento (in caso di criticità o rischio) e i flussi periodici. I flussi periodici – che sono comunicati dai responsabili delle diverse funzioni sulla base delle indicazioni pervenute dall'OdV – sono definiti dall'84% delle società del campione. Inoltre, in linea con la lettura della giurisprudenza che attribuisce un ruolo di controllo all'OdV non formalistico e cartolare, emerge dall'indagine che nel 68% delle società del campione l'oggetto dei flussi e la conseguente attività di vigilanza svolta dall'organismo, riguarda sia il complesso di informazioni e documenti che possono avere rilevanza ai fini 231, valutati in autonomia dall'organismo; sia i report che sintetizzano l'esito di controlli svolti sulle attività a rischio reati, per le proprie competenze, dalle funzioni interne.

Per quanto riguarda invece i flussi dall'OdV ai vertici societari, vengono distinti in diverse categorie. La prassi evidenzia che intercorrono: flussi continuativi, in genere con l'amministratore delegato e con il Presidente del consiglio di amministrazione, mentre per quanto riguarda i flussi periodici emerge dall'indagine

che in tutte le società l'OdV riferisce dell'attività svolta al consiglio di amministrazione con cadenza principalmente semestrale.

Due ulteriori aspetti. Il primo legato ai gruppi di imprese. Qui l'analisi mette in evidenza una serie di complessità legate all'attuazione della 231 nei gruppi, non facilmente risolvibili. I dati disponibili non sono molti e la maggior parte delle società intervistate che appartengono a gruppi ha dichiarato che è difficile ancora assicurare un'adeguata compliance 231 a livello di gruppo, soprattutto nelle multinazionali con sedi estere in ordinamenti in cui non è prevista una disciplina analoga a quella prevista dal decreto 231.

Viene tuttavia rilevato come i principi generali in tema di direzione e coordinamento introdotti dalla riforma del diritto societario del 2003, producano rilevanti effetti anche nella disciplina 231, in quanto è dovere della capogruppo verificare l'adeguatezza degli assetti organizzativi delle società del gruppo, da un lato, sollecitando l'adozione di modelli organizzativi omogenei e coerenti con le procedure della controllante, seppur adattandoli alle specificità della singola impresa; e dall'altro, garantendo un coordinamento tra gli OdV del gruppo attraverso adeguati flussi informativi.

Il secondo legato al *whistleblowing*, dove l'OdV viene considerato "naturale" deputato alle segnalazioni. Dall'indagine risulta che il 67% delle società affida all'Organismo di Vigilanza la tutela *whistleblowing*. Il 13% ha optato, invece, per altri soggetti, tra cui in particolare l'*internal audit* o funzioni responsabili appositamente istituite. Per il 20% delle società il dato non è disponibile.

Anche su questa parte di indagine, pur tenendo ben presente che ci si è riferiti a società particolarmente strutturate, quotate in Borsa [54], con obblighi quindi particolarmente penetranti legati alle attività di tutela del risparmio, sicuramente attente ai profili reputazionali, emerge un livello di attenzione molto elevato alle

[54] Il campione è composto per la maggior parte (52%) da imprese con una capitalizzazione di mercato compresa tra 463 e 2 milioni di euro. Seguono le imprese con una capitalizzazione media di circa 1,5 miliardi di euro13 (26%). Il 15% è rappresentato dalle imprese di maggiori dimensioni con una capitalizzazione media di 11miliardi di euro

prescrizioni della normativa 231/2001, che è stata adottata in base ad autodisciplina, linee guida, evoluzione giurisprudenziale.

4. La validazione giudiziale del modello

Uno dei problemi più attuali della disciplina della responsabilità dell'ente ex d.lgs. 231/2001 è rappresentato dalla scarsa validazione nelle aule giudiziarie del Modello Organizzativo, momento che al contrario doveva rappresentare il banco di prova conclusivo di tutta la normativa 231. Dall'approfondimento nel merito circa l'idoneità dello stesso modello da parte dei giudici, ne poteva infatti scaturire, in caso di valutazione positiva, l'esclusione della responsabilità dell'ente, sugellando e certificando l'efficacia del nuovo sistema normativo, e fornendo allo stesso tempo stimolo alle aziende ad implementare e migliorare i propri MOG in chiave premiale oltre che *compliance*.

La presenza di una elevata casistica avrebbe inoltre consentito la creazione di una spessa interpretazione giurisprudenziale, che avrebbe contribuito a migliorare i modelli organizzativi, consentirne l'evoluzione, così come avrebbe potuto mettere in evidenza le caratteristiche dei modelli che avessero invece "resistito" alle valutazioni del giudice, esprimendone l'idoneità giudiziale, e incentivando l'ente ad affrontarne i costi di realizzazione e mantenimento.[55]

Diversi i motivi che portano a valutazioni critiche. Innanzitutto, come prima riferito, un numero limitato di casi in materia, tale da non potere consentire, soprattutto sui punti più controversi, la creazione di una interpretazione giurisprudenziale del giudice di merito, ed una conseguente presenza limitata di sentenze di legittimità della Corte di Cassazione.

Poi, la generale tendenza ad escludere in sede giudiziaria l'idoneità del modello senza realmente effettuare uno sforzo di verifica sia di quella che è la carenza organizzativa, che della singola cautela che è mancata; oppure, la presenza di

[55] Sul punto sono presenti gli approfondimenti di GULLO, *i modelli organizzativi,* cit.; l'autore sostiene come «senza una concreta chance di andare esente da responsabilità l'ente difficilmente si mostrerà pronto a sostenere i significativi oneri, anche economici, legati all'adozione preventiva del modello». Viene inoltre riconosciuto complessivamente «il fallimento della 231 nella prassi giurisprudenziale».

valutazioni che *bypassano* direttamente l'esame del modello, attribuendo semplicemente sulla base dell'avverarsi del reato-presupposto la responsabilità all'ente. Si possono citare ulteriormente le situazioni in cui l'esame del modello non viene effettuato *ex ante*, come logico, ma *ex post*, a reato consumato, sancendo quindi l'equivalenza fra reato-presupposto commesso e l'inadeguatezza del modello.

La posizione dell'ente è quindi particolarmente delicata. Come è stato fatto notare, le imprese che si dotano del modello, di fatto, sottoscrivono una sorta di cambiale in bianco, in quanto pur affrontando un consistente impegno, sia dal punto di vista finanziario che organizzativo, non sono in grado di immaginare in anticipo come questo impegno sarà valutato a livello giudiziale.[56]

Il quadro appena descritto deve essere tuttavia aggiornato con decisioni più recenti riferite alla Corte di Cassazione, che esprimono un orientamento in linea con la logica 231.

La prima decisione è riferibile alla sentenza della Corte Penale, sez. VI, 24 settembre 2019, n. 43656, già citata[57] , che sinteticamente riportiamo nel principio espresso: la Corte di Cassazione ha ritenuto che omettendo la valutazione relativa al contenuto e all'idoneità del modello organizzativo, le Corti di merito sono di fatto giunte alla condanna dell'ente sulla base del mero accertamento della responsabilità penale della persona fisica. Secondo la Cassazione un automatismo di tal genere non può che essere censurato, in quanto si pone in contrasto con l'articolata disciplina posta dal Decreto Legislativo 231/2001. La normativa in esame, e in particolare l'art. 6, infatti, esplicitamente ricollega la responsabilità della persona giuridica alla sussistenza della c.d. colpa di organizzazione, ovvero di un *deficit* organizzativo che si configura quando la stessa non abbia provveduto ad adottare ed efficacemente attuare un modello di organizzazione e di gestione conforme alle norme e idoneo a prevenire la commissione di reati della specie di quello verificatosi.

[56] Le valutazioni sono, fra gli altri di SALVATORE, *La validazione giudiziale del modello organizzativo*, in *Rivis. 231, 2023, 3, 234*.
[57] Cfr. cap.4, par.2

La seconda decisione si riferisce alla Corte Penale, Sez. IV, 11 gennaio 2023, n.570[58], e riveste anche questa particolare importanza nell'orientare la lettura del modello di organizzazione da parte dei giudici di merito nel senso voluto dalla 231/2001.

Nel caso specifico sia il Tribunale che la Corte d'Appello condannavano una società al pagamento della sanzione pecuniaria, ai sensi dell'art. 25-septies, comma 3, d.lgs. 231/2001, per reato presupposto di omicidio colposo, dovuto all'inosservanza di norme sulla prevenzione degli infortuni sul lavoro, da cui l'azienda aveva tratto vantaggio (fra gli altri, risparmio di costi legati alla mancata predisposizione di mezzi di protezione individuale idonei).[59]La Corte di Cassazione ha ritenuto il ricorso fondato, annullando la sentenza impugnata, con rinvio ad altra Corte d'Appello, affermando che il giudice d'appello non ha motivato sulla «concreta configurabilità di una colpa in organizzazione dell'ente, né ha stabilito se tale elemento abbia avuto incidenza causale rispetto alla verificazione del reato-presupposto. I giudici di merito, invece, avrebbero dovuto approfondire anche e soprattutto l'aspetto relativo al concreto assetto organizzativo adottato dall'impresa in tema di prevenzione dei reati della specie di quello di cui ci si occupa, in maniera tale da evidenziare la sussistenza di eventuali deficit di cautela propri di tale assetto, causalmente collegati con il reato-presupposto».

---

[58] Cfr. Cass. pen., Sez. IV, 11 gennaio 2023, n.570, con nota di SALVATORE, *La validazione giudiziale,* cit., *234,* ed anche *Red. Giur. Pen., Responsabilità degli enti ex d. lgs. 231/2001 e infortuni sul lavoro,* in *Giurisp. Pen.,* 2023, 01. Nella sentenza la Corte ha affermato anche che la responsabilità deve emergere avendo riguardo ai modelli di organizzazione e gestione previsti dagli artt. 6 e 7 del d. lgs. 231/2001, «la cui efficace adozione consente all'ente di non rispondere dell'illecito, ma la cui mancanza, di per sé, non può implicare un automatico addebito di responsabilità».

[59] La società presentava ricorso, premettendo innanzitutto di essere un ente di dimensioni significative, dotato di articolata struttura societaria con specifico conferimento di deleghe in materia di sicurezza e salute dei lavoratori, di un Modello organizzativo adottato in epoca antecedente all'evento e periodicamente aggiornato, nonché sottoposto al controllo di un Organismo di Vigilanza.
Fra i motivi di ricorso l'ente rilevava la violazione di legge per «avere i giudici di merito erroneamente disapplicato gli artt. 6 e 7, co. 2, d.lgs. 231/2001, in ordine alla valutazione di idoneità *ex ante* e in concreto del Modello organizzativo adottato dalla società Alfa prima della verificazione dell'infortunio e manifesta illogicità e mancanza (mera apparenza) e contraddittorietà intrinseca ed estrinseca della motivazione nella parte in cui si era ritenuto non idoneo il Modello organizzativo ai fini della esclusione della responsabilità dell'ente. La Corte di appello avrebbe operato, sulla base del *post hoc propter hoc,* una indebita e automatica logica induttiva sulla scorta della quale la mera verificazione dell'evento *ex post* proverebbe la inidoneità del Modello organizzativo *ex ante*»

La sentenza ha quindi espresso in modo chiaro che solo un esame degli assetti organizzativi, e la presenza di eventuali carenze, tali da determinare le condizioni di verificazione del reato-presupposto, giustifica il rimprovero e l'imputazione dell'illecito, oltre a sorreggere la costruzione giuridica per cui l'ente risponde dell'illecito per fatto proprio, e non per fatto altrui. Il giudice di merito non può esimersi da una valutazione approfondita prima di affermare il collegamento fra reato presupposto e responsabilità dell'ente, e lo stesso non può essere stabilito sulla base del *post hoc propter hoc*, ma sulla base di una idoneità *ex ante.*

Nel pieno rispetto della formazione del libero convincimento del giudice, c'è quindi una crescente convergenza anche giudiziale su quelle che sono le logiche della 231/2001 e su quelli che sono i meccanismi che ne stanno alla base, i *compliance programs* precedentemente ricordati. Più in generale, anche guardando altri interventi, quali possono essere il GDPR, le attività delle *Autority,* NIS, è evidente la ricerca della cooperazione aziendale nello sviluppo di salvaguardie dalla commissione di illeciti o nella protezione del buon funzionamento dei sistemi. Questa evoluzione avviene nell'ambito di una indispensabile integrazione internazionale, in funzione di fenomeni societari che hanno ben superato i confini tradizionali.

5. Dal d.lgs. 231/2001 alla responsabilità dell'ente per reati informatici

A seguito dell'entrata in vigore della Legge 48/2008, vari reati informatici sono stati inseriti nell'elenco dei reati presupposto ex d.lgs.231/01; si è aperta quindi la possibilità per gli enti destinatari del decreto, di vedersi coinvolgere in termini di responsabilità in caso di commissione di tali reati da parte di loro apicali e/o dipendenti, ovviamente in presenza di interesse o vantaggio dell'ente stesso.

Considerata la enorme e sempre maggiore diffusione degli strumenti informatici, presenti in modo condizionante anche nel mondo lavorativo (la stessa gestione organizzativa interna di una azienda è ormai affidata anche nelle imprese più piccole a sistemi informatici), è evidente che il rischio di commissione di reati informatici è altissimo.

Per l'ente diventa in pratica obbligatorio (e non più facoltativo) attrezzarsi in modo conveniente per prevenire la commissione di questi reati od attenuarne le conseguenze. L'applicazione del MOG previsto dalla 231/2001 diventa lato ente condizione essenziale, non solo e non tanto ai fini dei "benefici legislativi" previsti in termini di responsabilità, ma anche in termini di convenienza economica e produttiva ad operare con un meccanismo organizzativo/procedurale sano, in grado di prevenire anomalie e che contribuisca a formare i dipendenti sulle componenti di rischio implicite alle attività quotidiane.

A questi reati, commessi all'interesse o vantaggio dell'azienda, e di provenienza endo-aziendale, si aggiungono poi i rischi di compromissione dall'esterno dei sistemi informatici, con enormi conseguenze in termini di violazione di dati sensibili tutelati da altre normative (GDPR), o di compromissioni di reti di importanza strategica (NIS I, NIS II), a cui si accennerà brevemente. Anche qui sono indispensabili per l'ente predisposizioni di modelli organizzativi in grado di fronteggiare il rischio implicito.

Come riportato sopra, i reati informatici entrano nel d.lgs. 231/2001 con la legge 48/2008. Successivi interventi legislativi estenderanno il numero dei reati presupposto. I prossimi due capitoli saranno pertanto destinati ad un breve *excursus* sull'evoluzione del reato informatico nel nostro sistema, e ad un approfondimento su singoli reati informatici, mentre nel capitolo conclusivo approfondiremo in che modo il modello organizzativo possa essere predisposto al fine di prevenire la commissione di reati-presupposto informatici.

CAPITOLO III

L'EVOLUZIONE DEL REATO INFORMATICO NEL NOSTRO SISTEMA PENALE

SOMMARIO: 1. Il crimine informatico. – 2. La legge 547/93. – 3. La Convenzione di Budapest. - 4. Il secondo protocollo della Convenzione di Budapest. – 5. La legge 48/2008 e le modifiche del sistema penale 231. - 6. La normativa europea successiva al trattato di Lisbona. – 7. Tipizzazione dei reati informatici e il bene giuridico protetto. – 8. I reati informatici nel d.lgs. 231/2001. – 8.1. Art.615-*ter*: accesso abusivo ad un sistema telematico od informatico. - 8.2. Art.615-*quater*: detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici. - 8.3. Art.615-*quinquies*: detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. - 8.4. Art.635-*bis*: danneggiamento di informazioni, dati e programmi informatici. - 8.5. Art.635-*ter*: danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità. - 8.6. Art. 635-*quater* e *quinquies*: l'applicazione al sistema informatico. - 8.7. Art.640-*ter*: frode informatica. - 8.8. Art. 25-*novies*: delitti in materia di violazione del diritto di autore.

1 - Il crimine informatico

Sotto l'aspetto tecnico-giuridico, il reato informatico o *computer crime* è definito dall'art. 1 della Convenzione di Budapest del Consiglio d'Europa del 2001, ratificata in Italia con la l. 48/2008. Si tratta di «ogni tipo di violazione penale commessa per mezzo o con l'ausilio di un sistema o programma informatico e/o avente ad oggetto lo stesso sistema o programma informatico».

Con i reati informatici il Diritto Penale tradizionale viene messo alla prova ed utilizzato su un territorio completamente nuovo[1], dove qualsiasi riferimento spaziale, o fisico, viene sostituito da un universo privo di regole, se non quelle tecniche indispensabili al proprio funzionamento, e dove emerge una criminalità dematerializzata, priva di confini geografici, che non può essere accertata all'interno di confini nazionali, o di un luogo fisico ben preciso: un *personal computer* è facilmente trasportabile in qualunque parte del mondo, fa rete con qualunque altro *pc*, ovunque posizionato, non soffre problemi linguistici o dialettali[2].

Inoltre, con l'avvento delle *cryptovalute*, il *cybercriminale* non ha neanche necessità di interfacciarsi con il "mondo reale" per approvvigionarsi di denaro od effettuare pagamenti: le transazioni monetarie vengono svolte in modo dematerializzato su piattaforme che non subiscono controlli delle Istituzioni.

Le peculiarità del crimine in esame possono quindi essere individuate nei seguenti elementi: la a-territorialità del contesto di riferimento, la prossimità con la vittima senza la dinamica del contatto fisico e l'anonimità dell'autore del reato; caratteristiche che determinano conseguenze sia a livello repressivo sia a livello investigativo.[3]

I comportamenti lesivi di interessi penalmente rilevanti sono molteplici, e sono adoperati con schemi che possono essere flessibili e mutevoli. Sul piano del Diritto Penale possiamo distinguere fra fattispecie "comuni" che rappresentano fatti non tipici dei *cyber-reati* ma commessi con mezzi informatici (*cybercrime*[4] o reati informatici in senso lato), e fatti tipici strettamente commessi al mondo informatico

[1] In questo senso MATTARELLA, *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Riv. Pen., Dir. Pen. e Proc.*, 2022, 6, 809 ss

[2] MATTARELLA, che evidenzia una «*quarta dimensione, destinata a diventare la nuova frontiera della sovranità statale* dopo la terra, il mare, il cielo e lo spazio, per la quale gli Stati dovranno concorrere nel futuro», in *La futura convenzione Onu sul cybercrime e il contrasto alle nuove forme di criminalità informatic*a, in *Sist. Pen.*, 2022, 3.

[3] Sul punto v. PICCINNI, *Il reato di danneggiamento di sistemi informatici e telematici disciplinato quale reato presupposto dall'art.24-bis, d.lgs.231/2001 per l'applicazione delle sanzioni in materia di responsabilità amministrativa delle società e degli enti*, in *Responsabilità amministrativa delle società e degli enti*, *Rivis. 231, 2017, 4, 2*.

[4] Distinzione riportata fra gli altri da GULLO, *I reati informatici*, in LATTANZI – SEVERINO, (a cura di), *Responsabilità da reato degli enti*, vol. I, Torino2020, 384

(ad.es. procedimenti di automazione di dati), che danno luogo a reati informatici in senso stretto[5] .

Parte della dottrina ritiene inoltre che il *cybercrime* comprenda almeno tre categorie: reati in cui il sistema informatico è l'obiettivo dell'attività criminale; reati in cui la tecnologia informatica rappresenta lo strumento per commettere o preparare un reato (la tecnologia è indispensabile per la realizzazione del reato); reati in cui il sistema informatico costituisce un "aspetto incidentale" con ciò intendendo che siamo in presenza di "vecchi reati" commessi con nuove tecnologie (la tecnologia non è indispensabile per la realizzazione di quel tipo di reato).

Altro elemento che caratterizza il reato informatico è la percezione dello stesso, sia da parte dell'agente che di chi lo subisce.

La vittima non ha talvolta percezione che nel momento in cui collega un *pc* ad *internet* di fatto apre la porta di casa (o dell'ufficio) a qualunque tipo di intrusione; ne consegue che la soglia di attenzione della vittima spesso non è in linea con il rischio potenziale espresso da questa modalità.

Allo stesso tempo il disvalore percepito nel realizzare un reato informatico non è pieno, soprattutto se messo a confronto con reati penali "tradizionali".

Seguendo l'indicazione dell'elaborato del Quadro Strategico annuale per la sicurezza nello spazio cibernetico della Presidenza del Consiglio del 2013 [6], possiamo distinguere quattro categorie di comportamenti criminali informatici:

Cyber crime: attività con finalità criminali che vanno dalla frode telematica al furto di identità, alla sottrazione di informazioni, creazioni o proprietà intellettuali.

Cyber spionage: acquisizione indebita di informazioni sensibili o classificate.

Cyber terrorismo: attività ideologicamente motivate, volte a condizionare uno Stato od una Organizzazione criminale.

Cyber warfare: operazioni pianificate e condotte all'interno dell'ambiente militare.

[5] Nello stesso senso MATTARELLA, *IL cybercrime nell'ordinamento italiano*, cit., 809 ss
[6] Per la consultazione del *Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico, Presidenza del Consiglio dei Ministr*i, 2013, visionato nel sito istituzionale *Agid.gov.it*

Vengono poi aggiunte le attività di *intelligence*, grazie alle quali ci si infiltra stabilmente in un sistema informatico

Per quanto ci riguarda, concentreremo la nostra attenzione sulla prima categoria di comportamenti, con attenzione al tema degli enti/aziende

Una ulteriore considerazione: per quanto il diritto penale svolga un ruolo centrale nella regolazione dei crimini informatici, le caratteristiche dello spazio digitale potrebbero diminuire fortemente, se non addirittura annullare, la capacità general-preventiva e la capacità di deterrenza tipica del diritto penale e della sanzione; questo rende ancora più importante il passaggio dalla "*rule of law"* alla "*rule of code*": nel mondo informatico è consentito tutto ciò che è tecnicamente possibile, quindi se si volesse impedire un utilizzo per scopi criminosi si dovrebbe trovare l'espediente tecnico più efficace, anziché concentrarsi sullo stigma penale di determinate condotte.

La prevenzione del rischio diventa quindi fattore centrale, ancora di più nel mondo degli enti e delle imprese, e si aggancia ad almeno tre temi: l'individuazione di sistemi informatici sicuri, protetti, ed in grado di evolvere continuamente questa protezione; costruire filiere interne all'azienda in grado di monitorare, prevenire, reagire al rischio informatico, che può provenire sia dall'interno (dipendenti) che dall'esterno; realizzare attività strutturate di formazione del personale (è da mettere in evidenza che la formazione del personale dipendente sulle tematiche *del cyber risk* consente un innalzamento della consapevolezza che viene trasferito dal dipendente anche nei suoi comportamenti fuori dall'azienda; da questo punto di vista si ha quindi una estensione positiva della formazione assimilata).

Nelle aziende più digitalizzate il tema "*IT"* è ormai centrale, sia come acceleratore di efficienza e di business, sia nella protezione dell'importante patrimonio di dati interni, relativi a banche dati od a brevetti, progetti, modelli degni di protezione.

Come messo in evidenza, nei crimini informatici l'azienda si può trovare spesso nella situazione di essere soggetto passivo del *cybercrim*e. Questa rappresenta una situazione diversa rispetto alla responsabilità prevista nella 231/2001, dove siamo

in presenza di un reato-presupposto collegato all'azienda e ad un interesse/vantaggio della stessa.

2 - la legge 547/1993

La legge 547/1993 "*modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica*", rappresenta il primo ingresso organico della nostra legislazione nel mondo dei crimini informatici. Introduce disposizioni specifiche relative a cinque categorie di reati: frode informatica, accesso abusivo a sistemi informatici e telematici, detenzione e diffusione abusiva di codici di accesso, diffusione di hardware e *software* diretti a danneggiare sistemi, intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.[7]

L'attenzione della dottrina penalistica ai fenomeni di criminalità informatica era ben precedente, e risale agli anni '70 del secolo scorso, localizzata prevalentemente negli *States* quando vennero pubblicati degli studi che mettevano in evidenza la possibilità di comportamenti illeciti, realizzati tramite tecnologie informatiche.

Negli anni '80 fu poi il diritto penale ad interessarsi della materia, perché iniziarono effettivamente ad emergere tutta una serie di pratiche illecite legate alla tecnologia informatica, ed a quegli anni risale la prima condanna in materia informatica (1983, Milwaukee – sei adolescenti fecero irruzione in importanti sistemi informatici, con conseguente condanna a due anni di libertà vigilata).

Sempre in quegli anni, a livello internazionale, nel 1983 l'OCSE condusse uno studio volto a verificare la possibilità di generare ed armonizzare a livello internazionale leggi penali per contrastare i reati informatici, e nel 1986 pubblica la

[7] Per un approfondimento in materia fra gli altri FLOR., *Cyber Criminality: le fonti internazionali ed europee,* in CADOPPI – CANESTRARI – MANNA – PAPA (diretto da), *Cybercrime,* Torino 2023,108 ss. L'autore evidenzia come prima della data del 1993 ci siano stati comunque singoli interventi sporadici da parte del legislatore. Viene citato in proposito la L. n. 191/1978, che aveva introdotto nel Codice penale l'art. 420 che, nel sanzionare l'attentato ad impianti di pubblica utilità, menzionava espressamente anche gli impianti di elaborazione di dati. Questa disposizione è stata integralmente sostituita dall'art. 2, L. n. 547/1993 e, successivamente, in parte abrogata dall'art. 6, L. n. 48/2008, di attuazione della CoC.
Altro "episodio" è rappresentato dall'art. 12, L. n. 197/1991, che puniva l'uso indebito di carte di credito o di pagamento.

relazione *"Computer-Related Crime: Analysis of Legal Policy"*, in cui analizza le normative esistenti e le proposte di riforma elaborate da alcuni Stati membri, raccomandando una serie di strumenti di natura penale nel contrasto ai crimini informatici.

Nel 1992, la medesima organizzazione esorta gli Stati membri a adottare mezzi di tutela per la sicurezza dei sistemi d'informazione.

In Europa un ruolo fondamentale nell'evidenziare questi nuovi fenomeni criminali e proporre una adeguata normativa è stato il Consiglio d'Europa, che il 13 settembre 1989, quattro anni prima della legge 547/1993, emanava una Raccomandazione sulla Criminalità informatica dove venivano discusse le condotte informatiche abusive.

Venivano definiti due macrogruppi di reati, quelli della c.d. "lista minima", cioè reati che gli Stati venivano invitati a perseguire penalmente, e un'altra lista, di cui facevano parte comportamenti da incriminare "eventualmente".[8]

I reati previsti nella lista minima erano: la frode informatica, il falso in documenti informatici, il danneggiamento di dati e programmi, il sabotaggio informatico, l'accesso abusivo, associato alla violazione delle misure di sicurezza del sistema, l'intercettazione non autorizzata, la riproduzione non autorizzata di programmi protetti, la riproduzione non autorizzata di topografie di prodotti a semiconduttore.

Venivano inseriti invece nella lista facoltativa i seguenti reati: alterazione di informazioni o programmi non autorizzata sempre che non costituisca un danneggiamento, lo spionaggio informatico, inteso come la divulgazione di informazioni legate al segreto industriale o commerciale, l'utilizzo non autorizzato di un elaboratore o di una rete di elaboratori, l'utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto.

A pochi mesi di distanza, in occasione del XV Congresso dell'Associazione Internazionale di Diritto Penale del 1990, emergeva la necessità di perseguire non

[8] Per una ricostruzione sul punto v. anche CONCAS, *Il crimine informatico*, *Diritto.it*, 2021,8

esclusivamente i reati previsti dalla lista minima ma anche i comportamenti descritti nella lista facoltativa.

Lo scenario dinamico degli anni '80 aveva infatti evidenziato una rapidissima migrazione sulle reti telematiche di attività lavorative e sociali, delle comunicazioni via *web*, del commercio elettronico; a queste migrazioni si era affiancata la presenza crescente di reati legati all'informatica.

La legge 547/1993 inserisce nuove figure criminose nel codice penale: l'art.615-*ter*, 615-*quater* e 615-*quinquies*, destinati a tutelare l'accesso abusivo ad un sistema informatico o telematico, la detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici, e la detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; gli art. 617-*quater*, 617-*quinquies* e 617-*sexties*,che si occupano di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, e di falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche; l'art. 635-*bis*, danneggiamento di informazioni, dati e programmi informatici, e 640-*ter*, frode informatica; inoltre modifica, riadattandoli, articoli già esistenti: art.392 esercizio arbitrario delle proprie ragioni con violenza sulle cose , art. 420 attentato a impianti di pubblica utilità, art. 491-*bis* documenti informatici, art. 616 violazione, sottrazione e soppressione di corrispondenza, art. 621 rivelazione del contenuto di documenti segreti ed art. 623-*bis* rivelazione di segreti scientifici o industriali.

Caratteristica della legge del 1993 è di prevedere nuovi illeciti, in funzione di tutela di beni già penalmente rilevanti, ma aggrediti con nuove forme; quindi, una estensione del codice esistente a nuove figure [9]; in questo una parte della dottrina assunse rilievo critico, ipotizzando la necessità della creazione di una nuova

[9] Cfr. Camera dei Deputati, presentazione del disegno di legge a cura del Min. Grazia e Giustizia

Sezione all'interno del Codice Penale, dedicata solo ai reati informatici e telematici.[10]

Assegnando un ordine ai nuovi delitti previsti nella 547/1993, possiamo evidenziare che all'interno del libro secondo del Codice penale gli art. 615-*ter-quater-quinquies* sono stati inseriti al Titolo XII, fra i delitti contro la persona, al Capo III (libertà individuale), nella Sez. IV legata all'inviolabilità del domicilio. Gli art. 617-*quater-quinquies-sexties* sempre al Titolo XII Capo III, ma nella Sez. V (inviolabilità dei segreti). L'art.635-*bis* è inserito fra i delitti contro il patrimonio, mediante violenza a cose o persone, mentre il 640-*ter* fa parte sempre dei delitti contro il patrimonio, ma realizzati mediante frode.

Gli articoli modificati ed integrati sono invece l'art.392, al Titolo III (delitti contro l'amministrazione della giustizia), Capo III, rivolto alla tutela arbitraria delle proprie ragioni; l'art. 420 è fra i delitti contro l'ordine pubblico, l'art. 491-*bis* fra i delitti contro la fede pubblica, mentre l'art. 616, 621 e 623-*bis* sono tutti inseriti al Titolo XII fra i delitti contro la persona, al Capo III (libertà individuale), Sez. V inviolabilità segreti.

La legge del 1993 ha sicuramente una importanza rilevante dal punto di vista della storia della legislazione e di ciò che ne consegue dal punto di vista sociale: c'è la presa di coscienza formale di una nuova realtà (quella digitale), che non è più marginale o di nicchia, ma impattante sotto ogni punto di vista, e che deve essere necessariamente disciplinata dal legislatore. L'evoluzione normativa in materia ovviamente non si è arrestata, ed ha trovato sempre grande impulso in particolare nelle iniziative sovranazionali che avevano lo scopo non solo di introdurre nuove aggiornate discipline, ma di armonizzare le stesse coordinando ed uniformando le regole a livello internazionale; di grande rilievo è la successiva Convenzione di Budapest del 2001.

[10] Era stata valutata anche durante l'iter legislativo l'opportunità di andare ad inserire nel Codice penale un nuovo titolo, destinato ai reati informatici, e presentato un disegno di legge per l'inserimento di una nuova sezione rubricata "dei delitti in materia informatica e telematica". L'argomento viene ripreso in successivo paragrafo.

3 - la Convenzione di Budapest

Alla normativa nazionale del 1993 succede un importante legislazione, che prende avvio con la Convenzione di Budapest del 2001. Questa convenzione rappresenta uno dei primi documenti normativi sul crimine informatico a carattere internazionale.

Aderiscono 66 paesi, non solo dell'Unione Europea, ma anche esterni ad essa (fra questi Stati Uniti e Giappone)[11];

La Convenzione, che merita particolare attenzione, verrà poi ratificata in Italia con la legge 48/2008.

La Convenzione si occupa dei crimini commessi attraverso internet o altre reti informatiche. L'obiettivo è di realizzare una politica comune fra gli Stati membri, attraverso l'adozione di una legislazione che consenta di combattere il crimine informatico in maniera coordinata, e mira principalmente ad armonizzare i sistemi penali nazionali e le disposizioni connesse nel settore della criminalità informatica, intensificando la cooperazione internazionale[12].

Gli Stati prendono formalmente atto che le variazioni realizzate dalla rivoluzione informatica hanno interferito, modificandolo, su quasi ogni aspetto delle attività umane.

«La Convenzione di Budapest si basa quindi sulla consapevolezza che le nuove tecnologie mettono in discussione i concetti legali esistenti. Le informazioni e le comunicazioni fluiscono più facilmente in tutto il mondo e i criminali riescono ad agire localizzati in luoghi diversi da quelli in cui i loro atti producono i loro effetti. Di fronte a questo, le leggi nazionali, tradizionalmente limitate a un territorio specifico, non sono sufficienti. Pertanto, gli Stati hanno preso consapevolezza che

[11] Numero considerato ancora esiguo: così MATTARELLA, *La futura convenzione ONU*, cit., 3, 53. «tuttavia, nonostante la Convenzione abbia prodotto molteplici risultati positivi, solo 66 Stati hanno proceduto alla ratifica: è un numero notevolmente superiore a quello degli Stati membri del Consiglio d'Europa, ma assai inferiore a quello dei membri delle Nazioni Unite».

le soluzioni alle problematiche descritte devono essere rintracciate nel diritto internazionale, sempre nel rispetto dei diritti umani».[13]

Le note del Consiglio d'Europa relative alla Convenzione sulla criminalità informatica di Budapest riportano[14]una serie di considerazioni preliminari; fra esse «La Convenzione sulla criminalità informatica è l'unico strumento internazionale vincolante in tale ambito. Rappresenta una guida per ciascun paese che desideri elaborare una legislazione completa per combattere la criminalità informatica, nonché un quadro per la cooperazione tra i suoi Stati parti. La Convenzione stabilisce la condotta anziché la tecnologia, garantendo che le norme e le procedure rimangano valide con l'evolvere della tecnologia».

Sempre nelle proprie considerazioni, il Consiglio d'Europa precisa gli obiettivi: «criminalizzare le infrazioni contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici, le infrazioni associate all'informatica, le infrazioni associate ai contenuti (ovvero pedopornografia, razzismo e xenofobia) e le infrazioni legate alla violazione del diritto d'autore e dei diritti correlati. Stabilire procedure per aumentare l'efficienza delle indagini. Fornire una base giuridica per la cooperazione internazionale tra gli Stati parti alla Convenzione, compresi gli scambi di informazioni su base spontanea, l'estradizione e l'assistenza reciproca a livello internazionale e punti di contatto disponibili 24 ore su 24, 7 giorni su 7, ed individua dei risultati. Fra questi, "utilizzo della Convenzione sulla criminalità informatica come guida o "normativa modello" in molti paesi per il potenziamento della legislazione nazionale, miglioramento della cooperazione tra le parti interessate, compresa la cooperazione pubblico-privato, Linee guida volte a migliorare la cooperazione tra le autorità preposte all'applicazione della legge e i provider di servizi Internet nell'indagine sulla criminalità informatica».

Da sottolineare che: "*La Convenzione stabilisce la condotta anziché la tecnologia, garantendo che le norme e le procedure rimangano valide con l'evolvere della tecnologia*". L'approccio è assolutamente generalizzato e rappresenta l'unico

[13] Per un approfondimento sulla Convenzione ONU di Palermo v. MATTARELLA, *La futura convenzione ONU*, cit., 12.
[14] Consiglio d'Europa, *Convenzione sulla criminalità informatica di Bucarest*, in sito istituzionale coe.int

modus operandi in presenza di una tecnologia che ha una velocità di sviluppo insostenibile per qualsiasi sistema normativo dove la norma abbia bisogno di un minimo di ponderazione temporale prima di essere generata.

Il meccanismo è alla base anche dei sistemi normativi preventivi, dove la responsabilità dei contenuti tecnologici viene lasciato alle imprese, che hanno una capacità di adattamento alla velocità della tecnologia di certo superiore rispetto a un sistema giuridico che pretendesse di imporre protocolli non finalizzati al risultato quanto piuttosto alla forma tecnica da utilizzare. La stessa nascita delle *Autority* specializzate (in particolare ENISA ed ACN), con funzioni tecniche di supporto e vigilanza è coerente con questo schema operativo.

La Convenzione si compone di 48 articoli, divisi in quattro capitoli [15]. Ci soffermeremo sul primo capitolo e sulla parte iniziale del secondo (sezione 1: diritto penale sostanziale)

Nel primo capitolo (art.1: uso dei termini), la Convenzione si preoccupa di definire tre "termini concetto":[16]

Innanzitutto, viene chiarito che per *sistema informatico* si indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate; diversamente, per *dati informatici* ci si riferisce a qualunque fatto, informazione, concetto suscettibile di essere utilizzata in un sistema informatico; per *service*

[15] I quattro capitoli sono elencabili come di seguito: capitolo 1: uso dei termini, capitolo 2: provvedimenti da adottare a livello nazionale, capitolo 3: cooperazione internazionale, capitolo 4: disposizioni finali.

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

provider, infine si considera qualunque attività pubblica o privata che fornisce la possibilità di comunicare, archiviare, rielaborare, processare dati.

Viene quindi preso in considerazione sia il mondo dell'*hardware*, del *software*, dei processi di trasmissione ed elaborazione/archiviazione dei dati.

La definizione fornita dalla Convenzione mette in evidenza la differenza fra "dato informatico" e "sistema informatico". Lo stesso schema verrà ripreso e confermato anche nella legge 48/2008 che "porterà" con qualche modifica la Convenzione nel nostro sistema legislativo (*cfr. paragrafi successivi*).

Di fatto siamo in presenza di un "sistema informatico" quando ci si riferisce ad una apparecchiatura, un dispositivo, un gruppo di apparecchiature o dispositivi, interconnesse o collegate, che eseguono, anche individualmente, elaborazione automatica dei dati. La "generalità" della definizione consente di includere qualunque strumento elettronico, informatico, telematico, sia inoltre che "lavori in autonomia", sia che sia "in rete". Qualunque dispositivo abbia un *software* rientra in questa definizione.

Il "dato informatico" invece è dato da qualunque rappresentazione di fatti, informazioni, concetti in forma idonea per potere essere elaborato da un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione. [17]

Quindi sia il singolo file, sia il "programma", cioè il *software*, inteso in modo esteso (ciò che consente ad un pc di operare, ma anche un programma che prenda singoli file e li elabori, li ordini, li sviluppi).

[17] Sul tema, aggiunge DEZZANI, *La criminalità informatica*, in *Diritto.it*, 2017, 2: «L'art. 1 della Convenzione riveste un'importanza rilevante in quanto per la prima volta viene chiarita, in modo univoco ed accettato da tutti i Paesi europei che hanno ratificato il trattato, la definizione di un sistema informatico o telematico, di dato e di programma. Per schematizzare la struttura, il sistema informatico è un dispositivo *hardware* che "contiene" uno o più programmi – tra cui obbligatoriamente un sistema operativo – con cui si possono gestire i dati. Da questa espressione generale si comprende la ragione del diverso trattamento sanzionatorio: colpire un dato informatico non significa impedire il funzionamento del sistema, colpire quest'ultimo significa impedire l'uso dell'intera struttura e di quanto in essa memorizzato. Di conseguenza deriva la necessità di differenziare, negli articoli del Codice penale, gli illeciti che hanno come oggetto la struttura *hardware* rispetto a quelli relativi ai *files* (che siano questi contenitori di dati o di programmi)».

L'architettura dei reati sviluppati distingue queste due situazioni, chiarirle e rendere questo termine con lo stesso significato per almeno tutti i firmatari dell'accordo consente un linguaggio comune su un tema dibattuto[18].

Le conseguenze sono ovvie: compromettere un singolo file non impedisce il funzionamento di un sistema, colpire o rallentare un sistema ha impatti su tutta la struttura informatica, gli illeciti conseguenti hanno quindi disvalore (e maccanismi sanzionatori) giustamente differenziati.

Il secondo capitolo è particolarmente congruo alle nostre finalità, che sono quelle di individuare l'attuale stato delle "*rule of law*" del nostro sistema; è intestato: provvedimenti da adottare a livello nazionale; la sezione 1: diritto penale sostanziale, è divisa in cinque titoli, di cui i primi quattro destinati a "blocchi di reati". In particolare, il Titolo 1 tratta dei reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici. Sono previsti i seguenti reati: art 2: accesso illegale ad un sistema informatico; art 3: intercettazione abusiva; art 4: attentato all'integrità dei dati; art 5: attentato all'integrità di un sistema; art 6: abuso di apparecchiature.

Al Titolo 2 sono elencati i "reati informatici": art 7: falsificazione informatica; art 8: frode informatica. Al Titolo 3: reati relativi ai contenuti, relativi alla pornografia infantile (art.9). Nel Titolo 4 sono contenuti i reati contro la proprietà intellettuale e diritti collegati, esposti all'art.10.

In tutti gli articoli citati viene disposto che «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».

Al Titolo 5 (altre forme di responsabilità sanzioni), si trova poi l'art 12[19], che si riferisce alla responsabilità delle persone giuridiche coinvolgendoli in pieno come

[18] DEZZANI, *la criminalità informatica*, cit., 2: «L'art. 1 della Convenzione riveste un'importanza rilevante in quanto per la prima volta viene chiarita, in modo univoco ed accettato da tutti i Paesi europei che hanno ratificato il trattato, la definizione di un sistema informatico o telematico, di dato e di programma».

[19]Cfr. art. 12 - Responsabilità delle Persone Giuridiche:

1. Ogni Parte deve adottare le misure legislative e 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

soggetti nei reati informatici, sia per le condotte commissive: «[..]ogni parte deve adottare le misure legislative e 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», che omissive: «[…] ogni parte deve adottare le misure necessarie affinché una persona giuridica possa essere ritenuta responsabile se la mancata sorveglianza o controllo di una persona fisica di cui al par.1 ha reso possibile la commissione di reati previsti al par.1 per conto della persona giuridica da parte di una persona fisica che agisca sotto la sua autorità».

È da tenere presente che la normativa italiana in proposito aveva già avuto una positiva importante evoluzione con la legge 231/2001, che come noto prevede la responsabilità della persona giuridica per reato; la Convenzione amplia il catalogo dei reati imputabili agli enti, coprendo crimini prima previsti solo per le persone fisiche.

Viene poi aggiunto che, secondo i principi giuridici della Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa; ed inoltre che questa responsabilità è stabilita senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso il reato.

Infine, l'ultimo articolo di questa "sezione 1" della Convenzione (art. 13) dispone che le sanzioni da adottare dalle parti siano effettive, proporzionate e dissuasive, includano la privazione della libertà per le persone fisiche, mentre per le persone giuridiche le sanzioni, siano esse penali o non penali, oltre a mantenere le caratteristiche di effettività, proporzione, dissuasione, (o ad altre misure), includano le sanzioni pecuniarie.

---

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.

.

4 – Il secondo protocollo della Convenzione di Budapest. La Convenzione Onu di Palermo.

Al primo protocollo del 2001 della Convenzione di Budapest si aggiungerà successivamente un secondo protocollo, deliberato nel novembre 2021 dal Consiglio d'Europa e sottoscritto dall'Italia il 17 maggio 2022.

Il secondo protocollo interviene su un altro argomento molto delicato, il rafforzamento della cooperazione e della divulgazione delle prove elettroniche.

Nel discorso del Segretario Generale alla Conferenza di apertura alla firma del secondo protocollo, viene messa in evidenza l'urgenza e la preoccupazione che generano i *cybercrime*.[20]

Tema di fondo è attenuare «la disomogeneità dei quadri normativi fra le nazioni, (che) in assenza di una base giuridica comune, non consente alle Forze di Polizia e alla Magistratura di operare rapidamente e con efficacia al di fuori delle proprie giurisdizioni, con il serio rischio di ulteriore perpetrazione e di reiterazione dei reati e, soprattutto, di dispersione, distruzione o di mancato ottenimento delle prove».[21]

Il protocollo costruisce una "base comune" giuridica sulla condivisione di informazioni relative alla registrazione dei nomi di dominio e acquisizione di informazioni su nomi abbonati e traffico; strumenti di assistenza reciproca, garanzie di protezione dei dati personali.

È previsto che, in caso di procedimento penale, le autorità procedenti di un paese possano intervenire direttamente su fornitori di servizi, enti regolatori dei nomi di dominio, richiedano specifiche informazioni su utente e traffico dati di altri paesi firmatari della Convenzione, anche "in urgenza".

---

[20] Il *Discorso del Segretario Generale* alla Conferenza di apertura alla firma del secondo protocollo aggiuntivo alla Convenzione sulla Criminalità Informatica è stato tratto dal sito istituzionale del Consiglio d'Europa, *coe.int/fr/web/secretary-general/speeches-and-op-ed*s: «[…] perché la criminalità informatica continua ad aumentare e a mutare sempre più velocemente. Oggi provoca danni per miliardi di euro ogni anno. Sta distruggendo tutto, dalle aziende agli ospedali fino alle infrastrutture critiche da cui tutti dipendiamo. Viene utilizzato per estorcere riscatti alle organizzazioni, per indebolire le elezioni e altre istituzioni democratiche e per violare i diritti e la *privacy* delle persone ovunque. Molto recentemente, abbiamo visto criminali sfruttare la pandemia di *Covid-19* attraverso la tecnologia e *Internet* – le truffe e la vendita online di forniture mediche contraffatte sono i primi esempi».

[21] In questo senso CARTISANO, *Reati informatici, più facile cooperare e condividere le prove: le novità dopo la firma del protocollo della Convenzione di Budapest*, in *Agenda Dig.*, 2022, 5.

Si supera quindi il meccanismo della rogatoria, che allunga la filiera procedurale generando ritardi, intervenendo direttamente sul soggetto fornitore di risposte.
Ovviamente ci sono dei meccanismi di salvaguardia (il Paese destinatario può chiedere al fornitore che ha ricevuto l'ordine, di notificare allo stesso prima della trasmissione all'autorità straniera, per valutare se la risposta stessa possa pregiudicare, ad esempio una indagine penale).
Nella proposta di decisione [22] del Consiglio, che autorizza gli Stati membri a ratificare, viene messo in evidenza che: la Convenzione contiene disposizioni che armonizzano gli elementi del diritto penale sostanziale interno e le disposizioni collegate nel settore della criminalità informatica; fornisce le competenze di diritto procedurale penale a livello interno necessarie per le indagini e l'esercizio dell'azione penale in relazione a tali reati, così come in relazione ad altri reati commessi per mezzo di un sistema informatico o laddove le prove siano in formato elettronico ed è volta a istituire un rapido ed efficiente regime di cooperazione internazionale.
L'articolo 2 definisce il campo di applicazione del protocollo, in linea con quello della Convenzione: il protocollo si applica a indagini o procedimenti penali specifici relativi a reati connessi a sistemi e dati informatici, e all'acquisizione di prove di reato in formato elettronico.
Grande attenzione viene posta alla tutela dei diritti fondamentali: l'articolo 13 del protocollo impone alle Parti di assicurare che i poteri e le procedure siano soggetti a un adeguato livello di tutela dei diritti fondamentali che garantisca, in linea con l'articolo 15 della Convenzione, l'applicazione del principio di proporzionalità; e, in coerenza, l'articolo 14 del protocollo prevede la protezione dei dati personali, quali definiti all'articolo 3 in linea con il protocollo che modifica la Convenzione sulla protezione delle persone rispetto al trattamento di dati a carattere personale e con il diritto dell'Unione.
Come messo in evidenza in precedenza, la Convenzione di Budapest è stata particolarmente importante nella definizione della disciplina italiana della

[22] Proposta del Consiglio che autorizza gli Stati membri a ratificare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche (Bruxelles, 25.11.2021 COM 2021), 719

successiva Legge 48/2008, e nella armonizzazione a livello soprattutto europeo. Ma il numero di aderenti (66) è rimasto limitato. È bene dunque completare il quadro di quegli anni citando la Convenzione Onu contro il crimine organizzato transnazionale, firmata a Palermo nel 2000.

Quest'ultima costituisce il principale strumento internazionale di riferimento contro tutte le forme di criminalità, in quanto vede la partecipazione di oltre 190 Stati e contiene soprattutto norme innovative in materia di indagini, sorveglianza elettronica, cooperazione giudiziaria e responsabilità da reato degli enti, ivi compresi gli intermediari di internet, assumendo quindi un ruolo suppletivo rispetto alla Convenzione di Budapest.[23]

La Convenzione Onu si caratterizza per definire in modo ampio sia il concetto di "gruppo criminale organizzato", che quello di "reato transnazionale grave". L'accorgimento è indispensabile per consentire una definizione che potesse essere recepita da tutti i singoli Stati firmatari, ed allo stesso tempo riuscisse a ricomprendere in modo dinamico un fenomeno, come quello del crimine organizzato transnazionale.

Questa "notevole ampiezza e flessibilità", che caratterizza la Convenzione di Palermo, ha permesso di includere negli anni anche le diverse forme di criminalità informatica, supplendo alla relativamente limitata adesione ricevuta dalla Convenzione di Budapest contro il *cybercrime.*

La Convenzione Onu di Palermo ha inoltre previsto la responsabilità delle persone giuridiche e in particolare dei soggetti che, a vario titolo, operano nel complesso universo di *internet*, nella consapevolezza che i reati commessi *online* sono proprio tra le forme di criminalità transnazionale più frequenti.

La convenzione impone infatti agli Stati firmatari di introdurre nei propri ordinamenti norme che stabiliscano la responsabilità delle persone giuridiche per i

[23] In termini sicuramente positivi relativamente all'iniziativa ed ai risultati: MATTARELLA., *La futura Convenzione Onu,* cit., 52

reati commessi al proprio interno, da amministratori, dirigenti, dipendenti [24],[25]

5 - La legge 48/2008 e le modifiche del sistema penale

Con la Legge 48/2008 "Il Presidente della Repubblica è autorizzato a ratificare la Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, di seguito denominata «Convenzione»" (art.1).

Nella Relazione di Ratifica, viene riportato: "preliminarmente, deve essere sottolineato come l'Italia sia stato uno dei primi paesi europei a varare una legge organica, la n. 547 del 23 dicembre 1993, in tema di delitti informatici. […]. Peraltro, si è, comunque, ritenuto opportuno procedere all'integrazione o alla modifica di alcune disposizioni del Codice penale, per considerazioni legate, da un lato, alla esigenza di una migliore collocazione sistematica, dall'altro, all'insorgere di nuove problematiche che avevano determinato l'inadeguatezza delle originarie forme di tutela[26].

Dagli articoli 1 e 2 della legge si rileva l'intenzione di dare piena ed intera esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica; tuttavia, la convenzione non viene recepita integralmente.[27]

---

[24] Cfr. Art.10: Responsabilità delle persone giuridiche: 1. Ogni Stato Parte adotta misure necessarie, conformemente ai suoi princìpi giuridici, per determinare la responsabilità delle persone giuridiche che partecipano a reati gravi che coinvolgono un gruppo criminale organizzato e per i reati di cui agli artt. 5, 6, 8 e 23 della presente Convenzione. 2. Fatti salvi i princìpi giuridici dello Stato Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa. 3. Tale responsabilità è senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso i reati. 4. Ogni Stato Parte si assicura, in particolare, che le persone giuridiche ritenute responsabili ai sensi del presente articolo siano soggette a sanzioni efficaci, proporzionate e dissuasive, di natura penale o non penale, comprese sanzioni pecuniarie. Dal sito *Uif.bancad'italia.it*

[25] Sul punto ARMONE, pur in presenza di una valutazione di fondo positiva, già citata, a seguire una considerazione critica dell'autore: «rispetto ai modelli successivamente affermatisi, soprattutto in seno all'Unione europea, l'art. 10 della convenzione appare tuttavia caratterizzato da una certa debolezza prescrittiva. […]. Si allude piuttosto alla mancata specificazione dei criteri di imputazione, posto che l'art. 10 non consente di distinguere tra i reati commessi dai vertici dell'ente e quelli commessi dai sottoposti; sicché l'obbligo imposto dalla norma potrà dirsi assolto dagli Stati anche attraverso l'introduzione di criteri di collegamento assai elastici, che esonerino, nella maggior parte dei casi, l'ente dalla responsabilità», *La convenzione di Palermo sul crimine organizzato transnazionale e la responsabilità degli enti: spunti di riflessione*, in *Rivis. 231*.

[26] Relazione di Ratifica "DDL - Ratifica della Convenzione d'Europa sulla criminalità informatica (Budapest, 3/11/2001)" in sito *Ministero della Giustizia, giustizia.it*

[27] Per un approfondimento sul tema v. CUNIBERTI, BATTISTA, MICOZZI, ATERNO, *La legge di ratifica della Convenzione di Budapest del 23 novembre 2001*, in *Altalex*, 2014, 3.

La legge non ne ratifica, ad esempio, l'art. 1 relativo alle definizioni tecniche (sistema informatico); dalla Relazione al DDL, sembra evidente che tale omissione sia consapevole e voluta, in quanto vi si trovano i riferimenti alle normative speciali contenenti tali definizioni, nonché alle elaborazioni terminologiche dottrinali e giurisprudenziali.

La Convezione parla espressamente solo di sistema informatico (non di sistema telematico), così definendo "qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati".

Diversamente, la 48/2008 ha preferito non fornire una definizione. La scelta è probabilmente legata alla volontà consapevole di non rischiare di creare un limite rigido dichiarativo, vincolando poi le interpretazioni, in una materia dove l'evoluzione tecnologica potrebbe rischiare di rendere superata la definizione prevista nella Convenzione, e lasciando invece una maggiore elasticità alla giurisprudenza (che magari potrà far propria la definizione di cui alla stessa convenzione).

Ovviamente, come sempre in queste situazioni, si crea una minore certezza del diritto, lasciando totalmente al magistrato la responsabilità, (e la libertà) di decidere se, nel caso concreto, si sia o meno in presenza di un sistema informatico o telematico.

Con la legge 48/2008, vengono dunque introdotte significative modifiche alle disposizioni penali in tema di reati informatici ed alla disciplina processuale inerente alle indagini relative a tali crimini, integrando e modificando la normativa già introdotta in materia dalla legge 23 dicembre 1993, n. 547, costituente, come è noto, il primo, organico intervento in materia di criminalità informatica nel nostro sistema legislativo.

La legge è divisa in quattro Capi: il primo è dedicato alle dichiarazioni di ratifica ed esecuzione, il secondo alle modifiche al Codice penale ed al decreto legislativo 8 giugno 2001, il terzo è intestato "modifiche al codice di procedura penale ed al

codice di cui al decreto legislativo 30 giugno 2003 n. 196", ed il quarto è composto dalle disposizioni finali.

Quello che dunque ha maggiore rilevanza ai fini della nostra trattazione è il Capo II, composto di 5 articoli; di questi, gli artt. 3-6 sono dedicati alla modifica, sostituzione, inserimento di reati informatici all'interno del nostro sistema penale, mentre l'art. 7 introduce l'art. 24-*bis* nel d.lgs. 231/2001, definendo quindi una parte dei reati informatici come reati presupposto della responsabilità dell'ente.[28]

Più in specifico, l'art. 3 prevede modifiche all'art.491-*bis* (documenti informatici), ed inserisce inoltre il nuovo art. 495-*bis* (falsa dichiarazione od attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri); l'art.4 sostituisce l'art 615-*quinquies* (detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico); l'art. 5 sostituisce l'art.635-*bis* (danneggiamento di informazioni, dati e programmi informatici), ed inserisce gli art. 635-*ter* (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), 635-*quater* (danneggiamento di sistemi informatici o telematici), 635-*quinquies* (danneggiamento di sistemi informatici o telematici di pubblica utilità), ed ancora inserisce l'art.640-*quinquies* (frode informatica del soggetto che presta servizi di certificazione di firma elettronica); infine, ,art. 6 abroga secondo e terzo comma dell'art.420 (attentato ad impianti di pubblica utilità), ritenendosi tali previsioni assorbite dal nuovo art. 635-*quinquies* c.p.11. [29]

L'importante articolo 7 inserisce dopo l'art. 24 del d.lgs. 231/2001 il nuovo art. 24-*bis*, nei cui contenuti si trovano: gli artt. 615-*ter*, 615-*quater*, 615-*quinquies* (relativi a riservatezza dei dati e delle comunicazioni informatiche e telematiche); gli artt. 617-*quater*, 617-*quinquies* (che si occupano di intercettazione o impedimento di comunicazioni informatiche e telematiche); gli artt. 635-*bis*, 635-*ter*, 635-*quater*,

[28] V. art.24-*bis*: delitti informatici e trattamento illecito dati.
[29] Per approfondimenti in materia v. fra gli altri anche SANTORIELLO, *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti*, in *Rivis. 231, 2011, 1, 211ss*.

635-*quinquies* (che si riferiscono all'integrità dei dati informatici e telematici); l'art 491-*bis* e l'art. 640-*quinquies*, (già citati poco sopra).[30]

Relativamente alla disciplina di rito, invece, la legge 48/2008 ha modificato il codice di procedura penale nella sezione relativa ai mezzi di ricerca della prova ed alle indagini di polizia giudiziaria attraverso l'indicazione di specifiche modalità di esecuzione di ispezioni, perquisizioni e sequestri con la prescrizione di apposite regole di conservazione, di intangibilità degli originali dati informatici e di conformità delle copie.

6 - La normativa europea successiva al Trattato di Lisbona. La Direttiva UE 2013/40

L'Unione Europea ha rappresentato negli anni un soggetto attivo che è intervenuto più volte in tema di criminalità informatica. Riprendendo solo alcune delle attività realizzate, in modo molto sintetico, possono citarsi il Consiglio dei ministri GAI dell'Unione europea del 19.3.1998, che ha approvato la formulazione in dieci principi relativi alla lotta contro la criminalità ad alta tecnologia, adottati dal G8, ed ha esortato gli Stati membri dell'UE non partecipanti al G8 a aderire alla suddetta rete.[31]

Nel giugno del 2000, il Consiglio Europeo approvava un piano d'azione globale per l'Europa telematica ("*eEurope Action Plan*"), sollecitandone l'attuazione entro la fine del 2002. Il piano d'azione dava particolare rilievo all'importanza della sicurezza delle reti e della lotta alla c.d. criminalità telematica., mettendo in evidenza la criticità potenziale delle infrastrutture dell'informazione e delle comunicazioni, in presenza dei nuovi comportamenti criminali multiformi e di portata transnazionale. Veniva messo in evidenza come i reati informatici rappresentino non solo una minaccia di tipo economico, ma incidano anche sulla sicurezza e sulla fiducia nella società dell'informazione.

[30] Come noto, l'elenco dei reati presupposto è stato aumentato da successivi innesti, vedremo in seguito in modo più dettagliato quali sono i reati presupposto di tipo informatico.
[31] FLOR, *Cyber Criminality*, cit., 120 mette in evidenza che «tali principi sono stati elaborati tenendo conto che le Nazioni Unite avevano pubblicato un manuale completo (*Manual on the prevention and control of computer-related crime*) nel 1994».

Più in generale, sono ricordabili una serie importanti di decisioni quadro riferibili al mondo del crimine informatico, alcune delle quali, le più importanti, sono poi state sostituite con Direttive dopo il Trattato di Lisbona.[32]

Fra queste possiamo citare la Decisione quadro 2001/413/GAI del Consiglio del 28.5.2001 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dal contante, la Decisione quadro 2004/68/GAI del 22.12.2003 relativa ad attività di coordinamento delle disposizioni legislative e regolamentari degli Stati membri per quanto riguarda la cooperazione giudiziaria e di polizia in materia penale per combattere lo sfruttamento sessuale dei minori e la pornografia infantile, con particolare attenzione alle condotte di distribuzione, divulgazione o trasmissione di materiali pedopornografici, offerti o messi a disposizione, nonché il loro acquisto e la loro detenzione, la Decisione quadro 2005/222/GAI del Consiglio del 24.2.2005, relativa agli attacchi contro i sistemi di informazione, che prevedeva che ciascuno Stato membro adottasse le misure necessarie affinché l'accesso intenzionale, senza diritto, ad un sistema informatico o ad una parte dello stesso fosse punito come reato, almeno per i casi gravi, salvo stabilire che tali condotte fossero punibili solo quando il reato fosse commesso violando una misura di sicurezza (art. 2).

Allo stesso tempo veniva chiesto che fosse punito come reato anche «l'atto intenzionale di ostacolare gravemente o interrompere il funzionamento di un sistema informatico mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili» , ed allo stesso modo per gli atti di cancellazione,

[32] FLOR , *Cyber Criminality*, cit., 120, ricorda che « prima dell'entrata in vigore del Trattato di Lisbona non sussisteva un chiaro ed esplicito assetto di competenze e di fonti giuridiche europee concernenti il settore penale, in quanto le fonti vincolanti del diritto comunitario in senso stretto (c.d. primo pilastro: regolamenti, direttive) non si adattavano ad una competenza penale controversa, oltre che limitata ai soli settori che ricadevano nelle materie di competenza della Comunità, come ad esempio l'ambiente, i trasporti o gli interessi finanziari comunitari. Gli strumenti del terzo pilastro (convenzioni, decisioni quadro, posizioni comuni) erano finalizzate soprattutto alla "cooperazione giudiziaria e di polizia in materia penale" e riguardavano singoli gruppi di fenomeni criminosi. Sul piano del diritto penale sostanziale si è assistito ad un ampio uso dello strumento della decisione quadro […], alcuni dei quali sostituiti, dopo l'entrata in vigore del Trattato di Lisbona, con nuove direttive».

danneggiamento, deterioramento, alterazione, soppressione o resa inaccessibilità di dati informatici in un sistema di informazione (art.4).

All'art. 8 inoltre veniva chiesta l'introduzione della responsabilità degli enti per i reati previsti nell'articolato.

Possiamo ulteriormente citare la Decisione quadro 2008/919/GAI del 28.11.2008 che ha modificato le precedenti Decisioni quadro 2002/475/GAI e 2005/671/GAI sulla lotta contro il terrorismo e lo scambio di informazioni e la cooperazione in materia di reati terroristici, nella considerazione, per quanto riguarda i reati informatici, che le cellule terroristiche ricorrono alle nuove tecnologie per mantenere un legame non facilmente individuabile e che di fatto Internet è utilizzato per ispirare e mobilitare reti terroristiche locali e singoli individui in Europa e fornisce una importante serie di informazioni, fungendo da «campo di addestramento virtuale.

Con la firma e la successiva entrata in vigore (1dicembre 2009) del Trattato di Lisbona il nucleo centrale delle competenze in materia di diritto penale sostanziale risiede nell'art. 83.1 del TFEU. Questo dispone che «Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni».

Le sfere di criminalità "particolarmente gravi" indicate al comma successivo sono rappresentate da terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, ed a concludere è inserita la criminalità informatica (oltre che la criminalità organizzata).

L'intervento tramite Direttiva consente di mantenere la competenza penale europea indiretta, ma obbliga gli Stati membri a dare attuazione alle disposizioni in cui essa

si esprime, con la minaccia di un ricorso per inadempimento e di una condanna da parte della Corte di Giustizia.

Fra le prime Direttive che riguardano il mondo informatico possiamo evidenziare la Dir. 2011/93/UE del 13.12.2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile; la Direttiva ha sostituito la decisione quadro 2004/68/GAI, ed interviene, per la parte relativa ai reati informatici, sull'uso delle nuove tecnologie e di *internet* come strumenti di diffusione di immagini piuttosto che di adescamento, prevedendo anche la rimozione o il blocco di pagine *web* legate al mondo della pedopornografia.

Particolarmente significativa ai nostri fini è la Direttiva 2013/40/UE del 12.8.2013 relativa agli attacchi contro i sistemi di informazione, che ha sostituito la decisione quadro 2005/222/GAI, e che costituisce uno strumento che si inserisce in una coordinata politica criminale europea diretta a sviluppare la strategia di rafforzamento della *cybersecurity*.[33]

Gli obiettivi della Direttiva sono rappresentati innanzitutto dalla necessità di riavvicinare il diritto penale sostanziale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime relative alla definizione dei reati e delle sanzioni.

Al punto (4) della Direttiva viene messo in evidenza con preoccupazione che «vi sono nell'Unione infrastrutture critiche la cui distruzione o il cui danneggiamento avrebbe un significativo impatto transfrontaliero. Dalla necessità di rafforzare la capacità di protezione delle infrastrutture critiche nell'Unione risulta evidente che le misure contro gli attacchi informatici dovrebbero essere integrate con sanzioni penali rigorose che rispecchino la gravità di tali attacchi». [34]

Sono previsti gli elementi minimi delle fattispecie di reato di "Accesso illecito a sistemi di informazione", "Interferenza illecita relativamente ai sistemi",

[33] Per approfondimenti in materia v. anche altri FLOR, *Cyber Criminality*, cit., 128ss

[34] Viene specificato che «per infrastrutture critiche si potrebbe intendere un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico o sociale delle persone, come gli impianti energetici, le reti di trasporto o le reti governative, e il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni».

"Interferenza illecita relativamente ai dati", "Intercettazione illecita", "Strumenti utilizzati per commettere i reati", nonché relativamente ad "Istigazione, favoreggiamento, concorso e tentativo",[35] con la specifica all'art.8 che gli Stati membri garantiscono che l'istigazione o il favoreggiamento e il concorso nella commissione di un reato di cui agli articoli da 3 a 7 (vale a dire quelli appena citati) siano punibili come reato e che il tentativo di commettere un reato di cui agli articoli 4 e 5 sia allo stesso modo punibile come tale.[36]

Da rilevare che la legge n. 238/2021 "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2019-2020" è intervenuta, apportando modifiche al Codice penale italiano a seguito

[35] V. art. 3 - accesso illecito a sistemi di informazione: gli Stati membri adottano le misure necessarie per garantire che, se intenzionale, l'accesso senza diritto a un sistema di informazione o a una parte dello stesso, sia punibile come reato qualora sia commesso in violazione di una misura di sicurezza, almeno per i casi che non sono di minore gravità.
V. art. 4 - interferenza illecita relativamente ai sistemi: Gli Stati membri adottano le misure necessarie a garantire che l'atto di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione di dati informatici, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di tali dati o rendendo tali dati inaccessibili, compiuto intenzionalmente e senza diritto, sia punito come reato almeno per i casi che non sono di minore gravità.
V. art. 5 - interferenza illecita relativamente ai dati: gli Stati membri adottano le misure necessarie a garantire che l'atto di cancellare, danneggiare, deteriorare, alterare, sopprimere dati informatici in un sistema di informazione, o di rendere tali dati inaccessibili, compiuto intenzionalmente e senza diritto, sia punibile come reato, almeno per i casi che non sono di minore gravità.
V. art. 6 - intercettazione illecita: 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.
49 art.7 – strumenti utilizzati per commettere i reati: 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 artt. 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.

[36] Per un approfondimento fra gli altri CIVELLO, *Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. Pen. Contemp., 2013, 10*. L'autore afferma che il lavoro fatto negli anni dal legislatore nazionale ha consentito la presenza di una normativa già attuale rispetto alla Direttiva: « anche l'Italia, dotatasi già nel 1993 di una legge organica per la protezione dei sistemi informatici , ha recepito la Convenzione di Budapest con L. 18 marzo 2008, n. 48, apportando modifiche ai titoli XII e XIII del libro II del codice penale, nonché al decreto legislativo 8 giugno 2001, n. 231, e ciò ridimensiona decisamente il valore aggiunto della direttiva. Quello che da circa vent'anni ci si è abituati a chiamare "diritto penale dell'informatica" non subirà, sostanzialmente, grandi cambiamenti, se non una ridefinizione, in certi casi, del quadro sanzionatorio».

della procedura di infrazione n. 2019/2033, che ha imposto al legislatore di adeguare alcune disposizioni alla Direttiva 2013/40/UE.

Le fattispecie incriminatrici che hanno subito modifiche nel nostro Codice penale sono gli artt. 615-*quater*, 615-*quinquies*, 617, 617-*bis*, 617-*quater* e 617-*quinquies*; nel caso degli articoli 617 e 617-*quater* l'intervento ha riguardato i limiti edittali. Nelle altre ipotesi, invece, gli interventi hanno avuto ad oggetto la rubrica, le condotte tipiche o altri elementi strutturali delle fattispecie «che, però, non hanno portata tale da riconfigurare i limiti o i contenuti dell'oggettività giuridica».[37]

L'art. 10 è interamente dedicato alla responsabilità delle persone giuridiche. Viene chiesto agli Stati membri di adottare 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». La Direttiva specifica, inoltre, su cosa deve essere basata la posizione dominante, definendo tre criteri: il potere di rappresentanza della persona giuridica; il potere di prendere decisioni per conto della persona giuridica; il potere di esercitare il controllo in seno alla persona giuridica.

Viene inoltre affermato che le misure adottate dovranno prevedere che le persone giuridiche possano essere ritenute responsabili qualora la mancata sorveglianza o il mancato controllo da parte di una persona di cui al paragrafo 1 (posizione dominante) 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. Si tratta di uno schema ben noto all'interno del sistema legislativo nazionale.

Allo stesso modo viene inoltre affermato che la responsabilità delle persone giuridiche a norma dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali

[37] Così FLOR, *Cyber Criminality*, cit., 129

contro le persone fisiche che siano autori o istigatori o abbiano concorso in uno dei reati di cui agli articoli da 3 a 8.[38]

La Direttiva ha anche definito i concetti di "sistema di informazione"(art.2, a), che corrispondono ad «un'apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione», di "dati informatici"(art.2, b) «una rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata in un sistema di informazione, compreso un programma atto a far svolgere una funzione a un sistema di informazione», di "persona giuridica" (art.2, c) «un'entità che ha lo status di persona giuridica in forza del diritto applicabile; la definizione non include gli Stati o gli organismi pubblici che agiscono nell'esercizio dell'autorità statale o le organizzazioni pubbliche internazionali» ed il requisito di "illiceità speciale"(art.2, c) «senza diritto» (una condotta, prevista dalla direttiva, ivi inclusi l'accesso, l'interferenza o l'intercettazione, che non è autorizzata da parte del proprietario o da un altro titolare di diritti sul sistema o su una sua parte, ovvero non consentiti a norma del diritto nazionale)

La Direttiva opera poi nelle attività di cooperazione fra le autorità competenti, compresa la polizia e gli altri servizi specializzati degli Stati membri, nonché le agenzie e gli organismi specializzati dell'Unione, come Eurojust, Europol e il Centro europeo per la criminalità informatica, e l'Agenzia europea per la sicurezza delle reti e dell'informazione.

Fra gli ulteriori obiettivi della Direttiva, la volontà di affrontare alcune criticità sorte a livello europeo relative alle notevoli differenze nel diritto e nelle procedure penali

[38] Sul punto v. anche CIVELLO, *Una prima lettura*, cit., «Identiche a quelle della vecchia decisione quadro sono poi le previsioni relative alla responsabilità delle persone giuridiche, che rispondono dei reati informatici commessi a loro vantaggio. L'art. 24-*bis* introdotto nel 2008 al decreto legislativo 8 giugno 2001, n. 231, recependo una norma che prevede la punibilità delle condotte commesse "per conto" dell'impresa, include tanto quelle commesse nell'interesse dell'ente quanto quelle commesse nell'interesse (anche esclusivo) di altri, che però abbiano procurato vantaggio all'ente medesimo. Non sarà dunque necessario, sul punto, alcun adeguamento».

degli Stati membri nel settore degli attacchi contro i sistemi di informazione, che possono ostacolare la lotta contro gravi forme di criminalità, come il crimine organizzato e il terrorismo, e possono complicare un'efficace cooperazione di polizia e giudiziaria.

Infine, l'attuazione e l'applicazione adeguata della Decisione quadro 2009/948/GAI del Consiglio, del 30.11.2009, sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali, dovrebbe agevolare il coordinamento dell'azione penale nei casi di attacchi contro i sistemi di informazione.

Gli Stati membri, in collaborazione con l'Unione, dovrebbero altresì cercare di migliorare la cooperazione internazionale relativamente alla sicurezza dei sistemi di informazione, delle reti informatiche e dei dati informatici. Qualsiasi accordo internazionale riguardante lo scambio di dati dovrebbe tenere debito conto della sicurezza del trasferimento e della archiviazione dei dati stessi.

Nei preamboli il legislatore europeo al punto (23) esplicita la necessaria cooperazione tra le autorità pubbliche, da un lato, e il settore privato e la società civile, dall'altro, sia di grande importanza per prevenire e combattere gli attacchi contro i sistemi di informazione. In sintesi, sarebbe necessario promuovere e migliorare la cooperazione tra fornitori di servizi, produttori, organismi preposti all'applicazione della legge e autorità giudiziarie, nel pieno rispetto dello stato di diritto.[39]

Seguendo uno schema abituale, improntato al garantismo ed al grande rispetto dei diritti individuali, in due punti (23) e (30)[40] la Direttiva fa riferimento al rispetto dei

[39] Prosegue la Direttiva al punto (23) affermando che «tale cooperazione potrebbe includere, ad esempio, l'assistenza da parte dei fornitori di servizi al fine di conservare possibili prove, fornire elementi che aiutino a identificare gli autori dei reati e, in ultima istanza, disattivare totalmente o parzialmente, conformemente al diritto e alla prassi nazionali, i sistemi di informazione o le funzioni che siano stati compromessi o utilizzati a fini illegali. Gli Stati membri dovrebbero altresì prendere in considerazione la creazione di reti di cooperazione e di partenariato con fornitori di servizi e produttori per lo scambio di informazioni relativamente almeno ai reati che rientrano nell'ambito di applicazione della direttiva».

[40] Al punto (30) viene specificato che «la presente direttiva rispetta i diritti umani e le libertà fondamentali e osserva i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea e dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, inclusi la protezione dei dati personali, il diritto alla riservatezza, la libertà di espressione e d'informazione, il diritto a un processo equo, la presunzione di innocenza e i diritti

diritti umani e le libertà fondamentali, alla Carta dei diritti fondamentali dell'Unione europea ed alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, includendo la protezione dei dati personali, il diritto alla riservatezza, la libertà di espressione e d'informazione, il diritto a un processo equo, la presunzione di innocenza e i diritti della difesa così come i principi della legalità e della proporzionalità dei reati e delle pene.

Merita attenzione, inoltre, la 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 Direttiva. 2013/40/UE. Tale 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 dall'*Europol* figurano 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 conclude che la direttiva ha determinato progressi sostanziali in termini di criminalizzazione degli attacchi informatici, facilitando la cooperazione transfrontaliera fra le autorità competenti. La Commissione, pur riconoscendo gli sforzi compiuti dagli Stati membri per dare attuazione alla direttiva, individua fra i miglioramenti, *in primis*, l'uso delle definizioni (art. 2), che incidono 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).[41]

della difesa così come i principi della legalità e della proporzionalità dei reati e delle pene. In particolare, la presente direttiva è volta a garantire il pieno rispetto di tali diritti e principi e deve essere attuata di conseguenza. La protezione dei dati personali costituisce un diritto fondamentale conformemente all'articolo 16, paragrafo 1, TFUE e all'art. 8 della Carta dei diritti fondamentali. Pertanto, qualsiasi trattamento di dati personali nell'ambito dell'attuazione della presente direttiva dovrebbe avvenire nel pieno rispetto del pertinente diritto dell'Unione in materia di protezione dei dati.

[41] Riferimenti in materia presenti fra gli altri su FLOR, *Cyber Criminality*, cit., 129

Ancora, fra gli ulteriori interventi menzionabili merita rilievo la Direttiva antiterrorismo 2017/541/UE del 15.3.2017, che sostituisce la precedente decisione quadro 2002/475/GAI.

La Direttiva evidenzia l'opportunità di una definizione comune, a livello europeo, dei reati di terrorismo, dei reati riconducibili a un gruppo terroristico e dei reati connessi ad attività terroristiche, nonché che le condotte siano punibili se messe in atto anche attraverso *Internet*, inclusi i social *networks*. I fenomeni di particolare criticità messi in rilievo e relativi ad *Internet* sono l'auto-apprendimento e l'auto-addestramento, finalizzati al terrorismo, che dovrebbero pertanto assumere rilevanza penale se si traducono in "ricevere addestramento a fini terroristici", qualora siano effettuati con l'intento di commettere o di contribuire a commettere un reato di terrorismo.

Viene messa in evidenza la necessità di rimuovere alla fonte i contenuti online, grazie alla cooperazione con Paesi terzi; ed in ogni caso dovrebbero essere individuati meccanismi volti a bloccare l'accesso a questi siti nei Paesi dell'Unione.

In tema di reati informatici sono inoltre menzionabili la Direttiva 2018/843 del Parlamento Europeo e del Consiglio, del 30.5.2018, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, nonché la Direttiva 2013/36/UE, che prevede specifiche disposizioni relativamente alla definizione di valuta virtuale e alle attività di cambio con le valute legali, perseguendo l'obiettivo di coprire tutti i possibili usi al fine di prevenire il riciclaggio ed il finanziamento al terrorismo.

7 – Tipizzazione dei reati informatici e bene giuridico protetto

Come già riportato[42], il legislatore nella normativa del 1993 ha individuato e definito nuove fattispecie di reato, ma ha anche scelto, nel caratterizzarle e posizionarle, di non discostarsi eccessivamente da fattispecie legali tradizionali contigue. In quella sede abbiamo messo in evidenza che una parte della dottrina

[42] *Supra*, stesso capitolo, par.2

assunse rilievo critico nei confronti di questa soluzione, ipotizzando invece la necessità della creazione di una nuova Sezione all'interno del Codice penale, dedicata solo ai reati informatici e telematici.

Anche gli interventi legislativi successivi hanno rispettato l'impostazione appena ricordata: denominazione, collocazione sistematica, anche sanzioni, fanno rimando ad altri reati percepiti come vicini[43]. Così, a titolo di esempio, la frode informatica (art.640-*ter*), è stata collocata accanto alla truffa comune (art. 640); il delitto di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*), insieme con i reati di cui agli artt. 615-*quater* e *quinquies* (c.d. prodromici), è stato posizionato subito dopo la violazione di domicilio (art.614); accanto al danneggiamento comune di cose (art. 635), sono stati posizionati i delitti di danneggiamento a dati e sistemi informatici (artt. 635-*bis*, *ter*, *quater* e *quinquies*).

In questo modo si è reso più evidente per ognuna delle fattispecie inserite quale era la *ratio* di tutela; ma per altro verso si è ingenerato un possibile rischio, rappresentato dall' equivoco di utilizzare schemi ed orientamenti interpretativi formatisi sulle "fattispecie tradizionali", anche per questi nuovi reati, perdendo di vista la portata innovativa, anche in termini di sviluppi interpretativi, dei nuovi inserimenti.

Possono essere individuate innanzitutto, alcune fattispecie appositamente create dal legislatore delineando, in autonomi articoli, condotte nuove o, meglio, "fatti tipici" inediti, costitutivi di nuovi reati, che fanno riferimento a "reati tradizionali" con i quali differiscono tuttavia in modo consistente.

La prima di queste fattispecie può essere rappresentata dal delitto di frode informatica, previsto all'art.640-*ter*; riprenderemo in seguito in dettaglio l'art.640-*ter*; quello che adesso vuole essere messo in evidenza è che esso è affiancato all'art.640, dedicato alla truffa, al quale viene accomunato da analogo disvalore penale, limiti di pena, ed eventi consumativi, quali il danno altrui ed il profitto ingiusto per sé od altri, realizzati attraverso condotte manipolatorie.

[43] Per un ampio approfondimento in materia v. PICOTTI, *Il diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme, in* CADOPPI - CANESTRARI – MANNA – PAPA, (diretto da), *Cybercrime,* Torino, 2023, 5.1

Tuttavia mentre nella truffa comune le attività manipolative si sviluppano in artifici e raggiri rivolti verso la persona, tali da portarlo alla "cooperazione" della vittima nel dare luogo alla disposizione patrimoniale, qui abbiamo una attività indirizzata direttamente sul sistema informatico: «la sostituzione dell'uomo in carne ed ossa, quale vittima dell'inganno (c.d. soggetto passivo della condotta), con il sistema informatico, porta ad una profonda riconfigurazione della struttura stessa del "fatto" delittuoso, spostandone il perno dall'induzione in errore all'"abuso" delle procedure tecniche o dei dati ad esse inerenti […] restando in ogni caso esclusa la necessità di una disposizione patrimoniale voluta concretamente dalla vittima».[44]

Altro esempio può essere tratto da un delitto informatico di grandissima diffusione, rappresentato dall'accesso abusivo previsto all'art.615-*ter*, e le fattispecie prodromiche previste agli artt. 615-*quater* e *quinquies* (anche questo verrà sviluppato in modo più analitico in seguito); il legislatore ha posizionato gli articoli in prossimità dell'art.614 (violazione di domicilio), bene giuridico sottoposto anche alla tutela dell'art.14 della Costituzione, sulla base di una analogia fra domicilio fisico e domicilio informatico.

Tuttavia la diversità strutturale di queste due ipotesi è ben presto emersa, ed ha portato ad una serie di complessità nel definire la condotta di "introduzione" informatica nel sistema, (concetto diverso dall'introduzione in un domicilio fisico), con non poca difficoltà di fissare il correlativo *tempus* e soprattutto il *locus*

[44] Così PICOTTI, *Il diritto penale*, Torino, 2023, cit., 62. L'autore evidenzia che in uno degli schemi più frequenti di frode informatica viene utilizzato il meccanismo del c.d. *phishing*, in cui il reo induce la vittima (ad es. inviando una falsa e-mail che appare provenire dall'istituto bancario presso cui è appoggiato un suo conto corrente gestibile on line) a fornire i propri dati riservati d'accesso ai servizi *home banking* , poi utilizzati per operare trasferimenti od operazioni a danno del titolare, a sua insaputa, con ingiusto profitto degli autori o di terzi. In questo schema «l'utilizzazione "senza diritto" delle credenziali fraudolentemente carpite integra oggi la fattispecie aggravata, introdotta dalla L. 15.10.2013, n. 119, di conversione del d.l. 14.8.2013, n. 93, che ha aggiunto un nuovo co. 3 all'art. 640-*ter* c.p., per superare le incertezze insorte al riguardo e rafforzare la tutela penale contro questi fatti illeciti, prevedendo un elemento specializzante così formulato: "se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti"». L'autore valuta positivamente la novella legislativa, che ricorrendo ad un elemento specificamente riferibile alla tecnologia informatica, dà espressa rilevanza penale anche ad un nuovo interesse, se non diritto della persona, vale a dire l'"identità digitale", che, sostiene «si sostituisce, quale bene giuridico indirettamente protetto, alla libertà di disposizione patrimoniale, tradizionalmente considerata offesa in seconda battuta dalla truffa comune, giustificando il più severo trattamento sanzionatorio rispetto a quello delle due ipotesi base. La notazione critica da esprimere è che tale bene giuridico non rileva soltanto nel campo dei delitti contro il patrimonio, oggetto dell'intervento d'urgenza del legislatore, ma si correla strettamente alla ben più ampia sfera dei diritti della personalità»

commissi delicti; e ugualmente per quanto riguarda la condotta di "mantenimento informatico", che dovrebbe essere associato ad un accesso lecito, in quanto in caso contrario verrebbe assorbito come reato nell'accesso abusivo. Il "mantenimento" rappresenta poi una tipizzazione della nostra legislazione, assente a livello internazionale.

Un ultimo esempio può essere fornito riferendoci all'art. 392 comma 3, "violenza informatica", dovuto alla legge 547/1993.[45]In questo caso il legislatore ha utilizzato come contenitore l'art.392 comma 2, legato alla "violenza sulle cose", per riferirsi ad una realtà delittuosa, quella informatica, descritta così al terzo comma "si ha altresì violenza sulle cose allorché' un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico".

Ci si trova quindi ad equiparare una violenza che genera danneggiamento su un oggetto dotato di fisicità, con un intervento manipolativo del *software* di un sistema informatici o telematici, che ne determina un'alterazione o un "turbamento" nel funzionamento, facendo venire meno la distinzione fra mezzo "violento" e mezzo "fraudolento".

Riprendendo e seguendo la collocazione stabilita dal legislatore all'interno del codice, che, come abbiamo prima scritto, è stata determinata in funzione della vicinanza rispetto alle fattispecie normative comuni preesistenti, e della prossimità teorica del bene giuridico tutelato, possiamo provare a raggruppare i diversi reati informatici seguendo uno schema che prende avvio dai Titoli, Capi e Sezioni in cui il reato è inserito. [46]

La maggior parte dei reati informatici si colloca nel Titolo XII fra i "delitti contro la persona", ed in particolare nel Capo III, dedicato ai "delitti contro la libertà individuale", ripartiti fra le diverse Sezioni.

[45] Vedasi anche sul punto in temini critici PICOTTI, *Il diritto penale,* Torino, 2023, cit., 67, «in altri casi, il legislatore è ricorso ad una tecnica legislativa ancor più criticabile, perché ha semplicemente dilatato concetti tradizionali – come quello di "violenza sulle cose", di cui all'art. 392, co. 2»
[46] Per un ampio approfondimento in materia v. PICOTTI, *Il diritto penale,* Torino, 2023, cit., 5.2.

Nella prima, che riguarda i "delitti contro la personalità individuale", si trovano quelli a tutela dei minori, dunque tutti i delitti di pedopornografia (artt. 600-*ter*, *quater*, *quinquies*.1); nella Sezione II, che riguarda i "delitti contro la libertà personale", è collocato il delitto di adescamento di minorenni (artt. 609-undecies), che prevede fra i suoi reati-fine, oltre a molti delitti sessuali collocati nella medesima sezione, anche quelli di prostituzione minorile, di schiavitù, di pedopornografia, ecc.,

Nella sezione III, fra i "delitti contro la libertà morale", si colloca il delitto di atti persecutori aggravato dall'uso di "strumenti informatici o telematici" (art. 612-*bis*, comma 2). e quello di "detenzione illecita di immagini o video sessualmente espliciti" (art. 612-*ter*, il c.d. *revenge porn*); nella Sezione IV, dedicata all'"inviolabilità del domicilio", si collocano, come già riferito in precedenza, i delitti di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* ed i relativi reati prodromici artt. 615-*quater* e 615-*quinquies*), che per inciso appartengono alla categoria dei reati informatici in senso stretto.

Infine, nella sezione V, che raccoglie i "delitti contro l'inviolabilità dei segreti", vi sono le fattispecie poste a tutela sia della corrispondenza, anche "informatica" o "telematica" (art. 616), sia delle altre comunicazioni, anche "informatiche o telematiche", contro le intercettazioni illecite (artt. 617-*quater*, 617-*quinquies* e 617-sexies).

Fra i reati modificati od integrati dalla l.547/1993 è da evidenziare anche l'art. 621 che punisce la rivelazione del contenuto di "documenti segreti", il cui comma 2, è stato aggiunto proprio dall'intervento legislativo appena citato.[47]

Sempre nella Sezione V, si trova l'art.623-*bis*, norma di chiusura, anche questo modificato dalla l.547/1993. La formulazione iniziale dell'articolo risale al 1974, e

[47] Viene messo in evidenza da PICOTTI, *Il diritto penale*, cit., 5.2, che il secondo comma dell'articolo 621 c.p., quando afferma "include anche qualunque supporto informatico contenente dati, informazioni o programmi", riproduce « l'infelice espressione che era stata usata dal legislatore per definire la nozione di "documento informatico" nella formulazione originaria dell'art. 491-*bis* c.p. Ma mentre questa è poi stata opportunamente soppressa nel 2008, in conformità all'evoluzione tecnologica della rete, sopra richiamata, non è stata modificata anche la disposizione in commento, che continua ad imperniare la nozione di "documento" – seppur non ai fini di tutela della fede pubblica – sull'obsoleto collegamento con un "supporto informatico"».

si riferiva alla intrusione nelle comunicazioni telefoniche e telegrafiche; l'intervento del 1993 ha aggiornato ed esteso l'ambito di pertinenza, inserendo le comunicazioni informatiche o telematiche.[48]

Il Titolo XIII riporta diversi reati che troveremo richiamati come reati-presupposto all'interno della 231/2001. Si tratta di "delitti contro il patrimonio"; al Capo I (delitti commessi mediante violenza) abbiamo quelli relativi al danneggiamento informatico (artt. 635-*bis*-*quater*-*quinquies*, introdotti con la l.547/1993), compresi quelli relativi a dati e sistemi "di pubblica utilità", nei quali l'aspetto della tutela del patrimonio è quantomeno secondario, ed il bene giuridico realmente tutelato è l'ordine pubblico[49]. Nel Capo II, dedicato ai delitti "mediante frode", si colloca l'importante art. 640-*ter* c.p., che punisce la frode informatica, anche questo richiamato dall'art.24 della 231/2001, ma prevedendo la responsabilità dell'ente solo ove la frode informatica venga realizzata a carico dello Stato o di un ente pubblico o dell'Unione Europea; si aggiunge inoltre l'art. 640-*quinquies*, fattispecie rubricata: "frode informatica del soggetto che presta servizi di firma elettronica", che è tuttavia non correttamente collocata fra i delitti contro il patrimonio "mediante frode". Infatti, la condotta punibile del certificatore si realizza con la mera "violazione" di tutti i richiamati obblighi incombenti sul soggetto qualificato, «per cui siamo in presenza di un reato proprio che non richiede alcun connotato di fraudolenza, né alcun evento di danno, essendo sufficiente il dolo specifico di arrecarlo, in alternativa a quello di "procurare a sé o ad altri un ingiusto profitto". Conseguentemente il bene giuridico protetto non è il patrimonio, ma la fede pubblica nello specifico campo delle firme elettroniche e dei documenti informatici».[50]

Proseguendo nella elencazione, nel Titolo I del Libro II, fra i "delitti contro la personalità dello Stato", si trovano nel Capo I, che tutela la "personalità internazionale", alcuni delitti contro il terrorismo, introdotti a partire dagli attentati

[48] Viene rilevato da PICOTTI, *Il diritto penale*, cit.,5.2. che «tutte tali disposizioni si applichino altresì "a qualunque altra trasmissione a distanza di suoni, immagini od altri dati", operando una discutibile apertura a possibili estensioni analogiche, in quanto risulta difficile delimitare a priori i caratteri identificativi della categoria».
[49] In questo senso fra gli altri ATERNO, *Sistema penale, cit.55;* PICOTTI, Il diritto penale, cit., 5.2
[50] La considerazione è di PICOTTI, *Il diritto penale*, cit., 5.2

dell'11.9.2001 alle torri gemelle, che vanno a colpire la parte "preparatoria" del crimine nella dimensione globale del *Cyberspace*. Quindi, assistenza agli associati (art. 270-*ter*), che prevede fra le varie condotte consumative anche quella di "fornire [...] strumenti di comunicazione" (fra i quali possono ovviamente essere compresi anche quelli informatici o telematici), nonché l'addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinquies*), che prevede al comma 2 l'ipotesi aggravata della commissione "attraverso strumenti informatici o telematici" (reato da considerare questo "in senso stretto").

Nel Titolo III, fra i "delitti contro l'amministrazione della giustizia" si colloca invece nel capo III, che sanziona la "tutela arbitraria delle proprie ragioni", la norma definitoria di cui al nuovo comma 3 dell'art. 392, inserita dalla l. 547/1993 modificando l'originario articolo, contenente la nozione generale di violenza c.d. informatica, equiparata a quella "sulle cose".

Il Titolo VII, infine, raccoglie i "delitti contro la fede pubblica"; al Capo III sono presenti le "falsità in atti", fra le quali si trova l'art. 491-*bis*, anche questo modificato dalla l. 547/1993, con cui vengono punite le falsità informatiche, e gli artt. 493-*ter* e 493-*quater*, che riguardano le frodi in strumenti di pagamento diversi dai contanti. Nel capo IV, dedicato alla "falsità personale", è collocato il nuovo art. 495-*bis* c.p., che punisce le "false dichiarazioni al certificatore di firme elettroniche" concernenti "l'identità o lo stato o altre qualità della propria o dell'altrui persona" rilevanti per ottenere i servizi di certificazione.

Come è evidente, rispetto alle previsioni di reati informatici riportate dalla l.547/1993 c'è stata una notevole espansione di fattispecie tutelate, che riguardano in molti casi beni giuridici variegati e di particolare importanza, sia pubblici che privati, ed in particolare inseriti nel Titolo XII relativo ai delitti contro la persona.

A queste tutele si devono inoltre aggiungere quella penale prevista dalla legislazione sul diritto d'autore.

8 - I Reati informatici nel d. lgs. 231/2001

Abbiamo esaminato nelle pagine precedenti una serie di interventi normativi che a più riprese hanno inserito all'interno del nostro sistema penale una serie di delitti informatici. In quelle occasioni è stato evidenziato anche la sistematica organizzativa stabilita all'interno del codice (Titoli, Capitoli), e i vari bene giuridici tutelati. Finalizzando il nostro lavoro alla 231/2001, è da mettere in evidenza che non tutti i reati che sono stati richiamati rientrano nel corpo normativo in esame.

É ancora da rilevare che la stessa dinamica implementativa temporale che ha riguardato l'ingresso dei vari reati informatici nel nostro sistema penale, si è avuta con la 231/2001. Al primo intervento realizzato con l'inserimento dell'art. 24-*bis*, per statuizione della l. 48/2008, si sono succedute altre normative, che hanno distribuito fattispecie delittuose in vari articoli del d.lgs. 231/2001. Obiettivo del presente paragrafo è mettere in evidenza i reati informatici presupposto dai quali scaturisce responsabilità dell'ente.

L'art. 24-*bis* riporta una serie di reati che hanno come caratteristica comune quella di potere essere commessi esclusivamente con il mezzo informatico[51]. Come già messo in evidenza in precedenza, ad essi si assomma, come "reato informatico in senso stretto" l'art.640-*ter*, contenuto nell'art.24.

I reati informatici in senso stretto contenuti nel 24-*bis* sono raggruppabili in tre gruppi diversi in funzione della materia disciplinata: la "*riservatezza"* dei dati e delle comunicazioni informatiche e telematiche, poi l'*"integrità*" dei dati informatici e telematici, ed infine la *fede pubblica* (che fa riferimento anche alle disposizioni contenute all'art 24).

Nel primo gruppo (riservatezza dei dati e delle comunicazioni informatiche e telematiche), sono ascrivibili[52]:gli artt. 615-*ter*, *quater*, *quinquies*, e gli artt. 617-

[51] Distinzione riportata fra gli altri da GULLO, *I reati informatici*, cit., 384, nello stesso senso MATTARELLA, *IL cybercrime nell'ordinamento italiano*, cit., 809 ss (*supra,* cap.3 par.1)

[52] Art.615-*ter*: accesso abusivo ad un sistema informatico o telematico; art.615-*quater*: detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici; art.615-*quinquies*: detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.
A seguire, l'art.617-*quater*: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche. L'articolo al secondo comma prevede anche la "rivelazione", mediante

quarter e 617 *quinquies*. Nel secondo gruppo (integrità dei dati informatici e telematici), sono da riportare [53] l'art.635-*bis*, l'art. 635-*ter*, l'art.635-*quater* e *quinquies*); il terzo gruppo integra l'art. 491-*bis* e 640-*quinquies*[54].

L'art.640-*ter*, riportato invece all'art.24 ma sempre ascrivibile ai reati informatici in senso stretto, è titolato "frode informatica", ed è una figura che attiva la responsabilità dell'ente ove realizzata a carico dello Stato o di un ente pubblico o dell'Unione europea.

Nell'ambito del 24-*bis* è stata inoltre di recente aggiunta una ulteriore fattispecie, introdotta in sede di conversione dall'art. 11-*bis* del d.l.105/2019, poi convertito in legge 133/2019, che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC). [55] L'art.11-*bis* rimanda nella definizione delle figure delittuose inserite all'art. 11 che sanziona la falsa, ovvero l'omessa comunicazione entro i termini prescritti di informazioni, dati o elementi di fatto, rilevanti per la predisposizione o l'aggiornamento degli elenchi dei sistemi informativi e dei servizi informatici impiegati o per lo svolgimento di altre attività indicate dal decreto, allo scopo di ostacolare o condizionare l'espletamento di specifici procedimenti o delle attività ispettive e di vigilanza attribuite alla Presidenza del Consiglio dei Ministri e al Ministero dello Sviluppo Economico.

É possibile aggiungere inoltre i delitti di pornografia minorile (art. 25-*quinquies*, in specie comma 1, lettere b) e c), le violazioni del diritto d'autore, relative anche a programmi informatici, banche dati, opere digitali (artt. 171, primo comma, lettera

qualsiasi mezzo di informazione al pubblico, in tutto o in parte, delle comunicazioni di cui al primo comma e l'art.617 *quinquies*: detenzione, diffusione e installazione abusive di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

[53] l'art.635-*bis*, l'art. 635-*ter*, l'art.635-*quater* e *quinquies*, che si riferiscono: l'art. 635-*bis* al danneggiamento di informazioni, dati e programmi informatici; l art. 635-*ter*: danneggiamento di informazioni, dati e programmi informatici utilizzato dallo Stato o da altro ente di pubblica utilità; l'art. 635-*quater*: danneggiamento di sistemi informatici o telematici (l'art. 635-*bis* si riferisce alle informazioni, qui ai sistemi informatici. Rappresenta quindi una ipotesi autonoma di reato); l'art. 635-*quinquies*: danneggiamento di sistemi informatici o telematici di pubblica utilità (l'art. "completa" il 635-*ter*, prevedendo il danneggiamento di un sistema informatico).

[54] l'art. 491-*bis* si occupa di falsità in documenti informatici pubblici aventi efficacia probatoria, mentre l'art. 640-*quinquies* è riferito alla frode informatica del certificatore di firma elettronica. Si tratta di una autonoma figura di truffa, realizzata dal soggetto certificatore, al fine di procurare ingiusto vantaggio per sé od altri e rappresenta una nuova ipotesi di reato

[55] V. art. 24-*bis*, comma "[…] e dei delitti di cui all'art.1, comma 11, del decreto legge 21 settembre 2019, n.105, si applica all'ente la sanzione pecuniaria fino a 400 quote"

a-*bis*), e terzo comma, 171-*bis*, 171-*ter*, 171-*septies* e 171-*octies* della legge 22 aprile 1941, n. 633 e successive modifiche), richiamati nell'art. 25-*novies* d.lgs. n. 231/2001.

Come messo in evidenza[56], prendendo in considerazione quei reati che sono realizzabili con tecnologie informatiche, (anche se non esclusivamente con tecnologie informatiche), l'elenco può estendersi a diversi delitti, fra i quali le falsità in monete e strumenti o segni di riconoscimento (art. 25-*bis*), piuttosto che quelli con finalità di terrorismo (art. 25-*quater*), il riciclaggio, l'impiego di capitali di illecita provenienza, l'autoriciclaggio (art. 25-*octies*), la diffusione di contenuti razzisti e xenofobi (art. 25-*terdecies*), i reati in materia di giochi e scommesse (art. 25-*quaterdecies*, introdotto dall'art. 5 legge 3 maggio 2019, n. 37 con riferimento anche ai delitti di giochi e scommesse *on line* non autorizzati, puniti ex art. 4, comma 4-*ter* legge 13 dicembre 1989, n. 401, aggiunto dall'art. 37, comma 5, della legge 23 dicembre 2000, n. 388).

Nelle pagine successive tratteremo alcuni dei principali reati informatici in senso stretto, aggiungendo ad essi l'art.25-*novies*, che è un reato realizzabile non necessariamente/esclusivamente con mezzi informatici, che si occupa di un tema particolarmente delicato quale la violazione del diritto d'autore; l'argomento impatta anche sulla tutela della proprietà di programmi informatici, settore di ampissima diffusione.

[56] Sul punto si veda per un approfondimento PICOTTI, *Cybercrime,* cit., 23. L'autore non manca di mettere in evidenza una tematica già sviluppata in questa tesi, relativa al mancato inserimento di "*reati-privacy*" all'interno della 231/2001. Cita inoltre una serie di reati informatici inseriti nel codice penale ma non riportati nella 231/2001. Fra questi: «né altri delitti che possono ricondursi alla categoria dei reati informatici, presenti nel codice penale (ad es. ex artt. 617-sexies, 621 co. 2, 616 co. 4 e 623 c.p. in materia di corrispondenza informatica o telematica nonché commessi con altre modalità di trasmissione a distanza), oltre che in leggi speciali (ad es. in materia di abusivismo finanziario mediante tecniche di comunicazione a distanza ovvero servizi di comunicazione di dati *ex* art. 166 co. 1 lettere c) e c-*bis*) d.lgs. 24 febbraio 1998, n. 58 e succ. modifiche, c.d. TUF)».

8.1 - Art 615-*ter*: accesso abusivo ad un sistema informatico o telematico

L'art 615-*ter* trova origine nella già citata legge 547/93. La sua stessa collocazione, prossima all'art.614 c.p. (violazione di domicilio), dà il senso e fa intuire come si sia rappresentata una violazione di "domicilio informatico"[57], equivalente alla violazione del domicilio fisico. Il testo «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», costruisce il "domicilio informatico" che è rappresentato dai sistemi informatici intesi come espansione ideale del bene protetto all'art.14 della Costituzione.

Il reato di accesso o trattenimento abusivo in un sistema informatico e telematico può dare luogo a responsabilità dell'ente collettivo, quando commesso da uno dei soggetti indicati negli artt. 5 e 6, d.lgs. 231/2001 e sempre che la condotta delittuosa sia stata assunta nell'interesse o a vantaggio della persona giuridica coinvolta. La sanzione prevista è quella pecuniaria da cento a cinquecento quote ed è inoltre prevista anche l'applicazione - in ricorrenza delle condizioni di cui agli artt. 9, 12 e 13, d.lgs. 231/231 - delle sanzioni dell'interdizione dall'esercizio dell'attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

Nella Convenzione *Cybercrime* del 2001, l'accesso illegale compare al primo posto dei reati da punire (art. 2); sottende la considerazione che la gran parte dei reati informatici, non solo in senso stretto, ma anche cibernetici in senso lato, si commettono "da remoto" e l'accesso abusivo rappresenta spesso il primo passo essenziale per la realizzazione di altri delitti anche più gravi.

L' incriminazione dell'accesso abusivo eleva la riservatezza informatica, protetta in via diretta, a bene giuridico meritevole di tutela penale. Il titolare di questi beni ha esclusività sugli stessi, ovunque si trovino ed a prescindere dal supporto utilizzato; il titolare ha il diritto di tutelare questi dati ed escludere terzi, comprese le autorità pubbliche, dall'accesso, salvi i casi espressamente previsti dalla legge e con le

[57] Per un approfondimento sull'art. 615-*ter* v. fra gli altri PIETROPAOLI, *informatica criminale: diritto e sicurezza nell'era digitale,* Torino, 2022, 1.2.1

garanzie del controllo giudiziario, come emerge dalle fonti sovranazionali (art. 8 CEDU e art. 7 CDFUE).[58],[59]

Si tratta di un reato di mera condotta, che può esprimersi in due modalità differenti: l'accesso abusivo ad un sistema automatico protetto, e lo "stazionamento" che avvenga senza l'autorizzazione dell'avente diritto.

Nel primo caso l'ipotesi tipo è quella di un *hacker*, o di un soggetto che riesce a "copiare" od a "sbirciare" la *password* di ingresso.

In sede interpretativa un punto di attenzione è rappresentato dalla dicitura "introduzione" utilizzata dal nostro legislatore, differente dal termine "accesso" utilizzata dalla Convenzione del 2001. Si ritiene che l'introduzione rappresenti un momento successivo a quello dell'accesso, ma la norma non fornisce elementi differenzianti.

L'accesso deve essere in qualche modo ostacolato da "misure di protezione", che vengono violate: per la configurabilità del reato il sistema informatico o telematico deve essere protetto da "misure di sicurezza", «non essendo sufficiente che si sia verificata una qualsivoglia connessione fisica o logica *on line* tra *computers* ed operatore, laddove non si sia determinato il superamento di specifiche misure di protezione nel cui ambito rientrano anche mere misure di carattere organizzativo che si limitano a disciplinare le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo, come la sistemazione dell'impianto all'interno di un locale munito di serrature, la prescrizione di un codice di accesso e l'esclusione al personale impiegatizio, attraverso la rete interna del

[58] La considerazione, condivisa dalla dottrina, è di MONTI- LUPARIA: *Cybercrime e responsabilità da reato degli enti: prevenzione, modello organizzativo ed indagini preliminari*, Milano, 2012.

[59] In termini di estensione del concetto di domicilio informatico anche Cass. pen., Sez. VI, 14 dicembre 1999 n.3067 in *Massimario-24356, avvocato.it*:: «Tuttavia l'art. 615-*ter* c.p. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello jus *excludendi alios,* quale che sia il contenuto dei dati racchiusi in esso, purché attinenti alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati sia che titolare dello *jus excludendi* sia persona fisica, sia giuridica, privata o pubblica».

sistema, dall'accesso ai comandi centrali per intervenire sui dati, ed altri simili accorgimenti». [60]

Ai fini dell'applicazione della norma, è sufficiente una qualsiasi forma di "sbarramento" atta ad impedire il libero accesso di terzi, che possono essere rappresentate anche da protezioni esterne, (ad es., la custodia degli impianti); non è inoltre previsto un apprezzamento in concreto della qualità e idoneità di queste misure di sicurezza, né è necessario che siano attive: è sufficiente la predisposizione.[61]

È inoltre irrilevante la finalità dell'autore: viene punito il comportamento che ha generato l'introduzione, non è indispensabile una violazione dei dati del soggetto passivo.[62]

La seconda condotta prevista dall'articolo prevede invece la "permanenza" all'interno di un sistema informatico protetto, con accesso anche legittimo, ma utilizzo non autorizzato dal titolare: il soggetto si è mantenuto all'interno del sistema con finalità diverse da quelle per cui l'accesso era consentito. È il caso di situazioni emerse in giurisprudenza con riferimento ad accessi a sistemi pubblici da parte di pubblici ufficiali.

---

[60] SANTORIELLO - DEZZANI*: Il reato di accesso e trattenimento "abusivi" nel sistema informatico e la responsabilità amministrativa delle persone giuridiche*, in *la responsabilità amministrativa delle società e degli enti, Rivis. 231, 2012, 1, 57ss*. Gli autori sostengono si sia in presenza di un reato plurioffensivo: «In realtà ci pare possa più propriamente parlarsi di un reato plurioffensivo, posto che mediante la protezione del "domicilio informatico" vengono a tutelarsi un insieme di interessi eterogenei che possono fare capo al titolare del sistema e ricevere pregiudizio dalla condotta aggressiva: si pensi all'interesse squisitamente personale di non subire intrusioni nella propria sfera di riservatezza, all'interesse patrimoniale correlato alla apprensione dei dati riservati ovvero pregiudicato dall'avvenuto "danneggiamento" del sistema (cfr. l'aggravante di cui al comma 2, n. 3, dell'art. 615-*ter* c.p.), agli interessi militari o sanitari correlati alle specifiche qualità del titolare del sistema (cfr. l'aggravante di cui al comma 3 dell'art. 615-*ter* c.p.)» .

[61] Nel senso riportato nel testo: SANTORIELLO - DEZZANI, *Il reato di accesso e trattenimento "abusivi",* cit., 59.

[62] V. Cass. pen., Sez. V, 6 febbraio 2007 n.11689, in Mass. Uff. 236221, per la quale il reato si consuma con la violazione del domicilio informatico, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa: proprio da queste premesse, pur non essendovi stata alcuna cognizione di dati riservati, il reato è stato ravvisato in una fattispecie in cui gli imputati si erano abusivamente introdotti in una centrale telefonica, non appunto per acquisire dati riservati, ma solo per fini strettamente patrimoniali, avendo provveduto abusivamente ad allacciarsi a numerose linee di utenti privati, dalle quali avevano effettuate delle telefonate ad utenze caratterizzate dal codice "899", con conseguente notevole addebito di denaro in danno degli inconsapevoli titolari di dette utenze, in *massimario-2349, avvocato.it.*

Il concetto di "mantenimento" (abusivo) previsto dall'art.615-*ter* ha scarso riscontro a livello internazionale, e segue lo stesso schema della violazione di domicilio prevista all'art.614, dove viene punito sia chi si introduce che chi si "mantiene" (contro la volontà) nel domicilio altrui. Questa "differenza" è stata valorizzata dalla nostra giurisprudenza, «perché in grado di colpire i soggetti cosiddetti "intranei", che sono legittimati ad introdursi con le loro credenziali nel sistema informatico protetto, ma abusano poi di detta facoltà e vi si "mantengono" per compiere attività non consentite rispetto alle direttive del titolare od ai loro compiti d'ufficio"»[63];[64]

Sul punto si sono contrapposte interpretazioni giurisprudenziali che hanno dato un significato opposto al "mantenimento" all'interno di un sistema informatico di un soggetto autorizzato, che utilizzi le proprie credenziali per perseguire finalità diverse, (se non illecite), da quelle strettamente legate alle finalità per le quali tali credenziali sono state fornite.

La diversa interpretazione si riferisce, come detto, ad un soggetto legittimato all'accesso. Dispone dunque di *password* o "chiavi" che gli consentono di introdursi all'interno del sistema. Il soggetto può permanere all'interno del sistema in modo altrettanto legittimo, perseguendo finalità ed obiettivi del soggetto autorizzante (si pensi ad un ipotetico datore di lavoro); potrebbe invece "deviare" la propria finalità di utilizzo, come nel caso in cui durante la permanenza autorizzata nel sistema vengano acquisiti dati riservati che vengono utilizzati in modo illecito trasmettendoli a terzi.

---

[63] Fra gli altri, si esprimono in questo senso MONTI - LUPARIA, *Cybercrime e responsabilità da reato*, cit., cap.2,5I

[64] Cfr. Cass. pen., Sez. Un., 8 settembre 2017, n. 41210. La questione sottoposta alle Sezioni Unite era la seguente: «se il delitto previsto dall'art. 615-*ter* co. 2 n. 1 c.p. sia integrato anche nella ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio che, 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». Le Sezioni Unite hanno risposto affermando il seguente principio di diritto: «Integra il delitto previsto dall'art. 615-*ter* co. 2 n. 1 c.p. la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un servizio informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita», in *Giurisp. Pen.*, 2017, 9.

In una prima sentenza (Cassazione Penale, Sez. V, 6 dicembre 2000 n. 12732 "Zara"[65]), il reato di cui al primo comma dell'art.615-*ter* c.p. può essere integrato da chi, pur essendo abilitato ad accedere al servizio telematico, lo utilizzi per finalità diverse da quelle consentite.

La vicenda è relativa a un soggetto autorizzato solo all'accesso per funzioni di controllo della funzionalità del programma informatico, che in maniera indebita si avvale di tale autorizzazione per copiare i dati inseriti nel programma. L'interpretazione prende in considerazione che il reato è una "espansione" al domicilio informatico dell'art.614 (inviolabilità del domicilio, tutelato costituzionalmente); da ciò ne discende che si deve seguire una interpretazione in linea (analoga) a quella accolta per la violazione del domicilio ex art.614, che si realizza sicuramente quando il soggetto che è in possesso della chiave dell'abitazione altrui per realizzare, ad esempio, interventi di pulizia, e dopo essere entrato nell'abitazione, vi si mantenga per altre ragioni. Il perseguimento di una finalità diversa da quella stabilita equivale dunque al mantenimento non autorizzato.

Questo orientamento è stato ribadito in successive altre occasioni. Fra queste le sentenze della Corte di Cassazione Penale, Sez. V, 10 dicembre 2009, n. 2987[66], e Corte Cassazione Penale, Sez. V, 22 settembre 2010, n. 39620.[67]

Di diverso avviso altra giurisprudenza di legittimità, che afferma che il reato del 615-*ter* non viene integrato nel caso ci si avvalga delle *password* a cui si ha titolo,

---

[65] Cfr. Cass. pen., Sez. V, 6 dicembre 2000 n.12732 "Zara", "La sentenza Zara del 2000, che aderisce all'orientamento estensivo, afferma che l'analogia con la 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» in commento di SCIRÈ, *Abuso del titolo di legittimazione all'accesso ad un sistema informatico: alle SS.UU. la questione della configurabilità del delitto di cui all'art.615-ter c.p.*, in *Dir. Pen. Contemp.*, 2011, 9.

[66] Cfr. Cass. pen., sez. V, 10 dicembre 2009 n.2987, riferita alla copiatura da parte di dipendenti di files presenti nella memoria del computer della azienda di cui erano dipendenti, in *onelegale.wolterskluwer.it*

[67] Cfr. Cass. pen., sez. V, 22 settembre 2010 n.39620, riferita alla «condotta di colui che, in qualità di agente della Polstrada, addetto al terminale del centro operativo sezionale, effettui una interrogazione al CED banca dati del Ministero dell'Interno, relativa ad una autovettura, usando la sua *password* e l'artifizio della richiesta ad un organo di Polizia in realtà inesistente, necessaria per accedere a tale informazione», in *onelegale.wolterskluwer.it*

per finalità estranee a quelle di ufficio. Resta ferma, per quanto ovvio, la responsabilità per i diversi reati che dovessero configurarsi a seguito di queste "diverse finalità".

Fra i principali argomenti portati a sostegno di questa interpretazione riduttiva vi è la considerazione che in situazioni di questo tipo, ai fini della configurabilità del reato, la volontà contraria dell'autorizzante deve essere verificata solo ed esclusivamente con riguardo al «risultato immediato della condotta posta in essere dall'agente con l'accesso al sistema informatico e con il mantenersi al suo interno e non con riferimento a fatti successivi che, anche se già previsti dall'agente al momento dell'ingresso, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione».[68];[69]

Le Sezioni Unite sono state pertanto chiamate a dirimere il contrasto giurisprudenziale una prima volta con l'intervento del 27 ottobre 2011 [70], sostenendo quest'ultima interpretazione

Il caso è rappresentato da un maresciallo dei carabinieri in servizio presso una stazione dei Carabinieri di Roma che aveva titolo ad accedere a un sistema informatico in dotazione alle forze di polizia e contenente dati di indagine coperti da riservatezza; il maresciallo, nonostante fosse fuori dal servizio, e, pur non essendo stato incaricato di accertamenti sul loro conto, aveva acquisito notizie

[68] In questo senso SANTORIELLO - DEZZANI, *Il reato di accesso e trattenimento "abusivi"*, cit., 61

[69] Così Cass. pen., Sez V, 20 dicembre 2007 n.2534, «non integra il reato di accesso abusivo ad un sistema informatico la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all'Arma dei Carabinieri, si introducano nel sistema denominato S.D.I. (banca data interforze degli organi di polizia), considerato che si tratta di soggetti autorizzati all'accesso e, in virtù del medesimo titolo, a prendere cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi ad una agenzia investigativa, condotta quest'ultima ipoteticamente sanzionabile per altro e diverso titolo di reato (rivelazione di segreto d'ufficio, ex art. 326 c.p., ndr)", ed anche Cass. pen. Sez., 21 ottobre 2008 n. 39290, in *Altal., altalex.com*, 2011,12.: "Non commette il reato di accesso abusivo ad un sistema informatico o telematico il soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga per acquisire informazioni per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente configurabili, ove le suddette finalità vengano poi effettivamente realizzate. (Fattispecie in cui è stato contestato il concorso nel delitto di abusiva introduzione nel sistema informatico del C.E.D. della Corte di Cassazione da parte di ignoti pubblici ufficiali, i quali avrebbero fornito all'indagato, addetto alla cancelleria della Corte, informazioni riservate sullo stato di alcuni procedimenti pendenti, al fine di avvantaggiare la posizione processuale o detentiva di taluni imputati».

[70] V. Cass. pen., Sez. Un., 27 ottobre 2011, n.4694, in *Arch. Pen.*, con nota di ROMEO, «*Le Sezioni Unite sull'accesso abusivo ad un sistema informatico o telematico*».

riguardanti la sfera privata e le vicende giudiziarie di svariate persone e successivamente aveva rivelato le informazioni così apprese a una delle persone interessate e a un terzo.

Le Sezioni Unite hanno deciso in quell'occasione ritenendo che la questione di diritto controversa non deve essere esaminata mettendo in rilievo le finalità perseguite da chi accede o si mantiene nel sistema: la volontà del titolare del diritto di "escludere" si connette soltanto al dato oggettivo della permanenza dell'agente in esso: il che significa che la volontà contraria dell'avente diritto deve essere verificata solo con riferimento al risultato immediato della condotta posta in essere, non considerando i fatti successivi.

Ciò che rileva è solo il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che non può considerarsi autorizzato ad accedervi e a permanervi sia quando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro), sia quando ponga in essere operazioni di natura diversa da quelle di cui egli è incaricato e in relazione alle quali l'accesso gli è consentito.

Quindi in una situazione dove l'agente ha l'autorizzazione ad accedere, e la stessa prevede delle abilitazioni operative che non sono superate nei limiti e nelle forme definite dal titolare autorizzante (nel caso specifico sono rappresentate dalle autorizzazioni ricevute ad accedere al sistema informatico interforze degli organi di polizia), non viene commesso il reato in esame, in quanto lo scopo perseguito non rileva ai fini del 615-*ter*.

Afferma la Corte che «il giudizio circa l'esistenza del dissenso del *dominus loci* deve assumere come parametro la sussistenza o meno di un'obiettiva violazione, da parte dell'agente, delle prescrizioni impartite dal *dominus* stesso circa l'uso del sistema e non può essere formulato unicamente in base alla direzione finalistica della condotta, soggettivamente intesa. Vengono in rilievo, al riguardo, quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, da prendere necessariamente in

considerazione, mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati».[71]

Successivamente a questa pronuncia della Corte, una parte della giurisprudenza si è in toto conformata; sono tuttavia presenti sentenze che giungono a soluzioni opposte a quelle proposte dalle SS.UU, pur prendendo le mosse dallo stesso principio di diritto.

La sentenza Cassazione Penale, Sez. V, n. 22024/2013 afferma diversamente che integra il reato di accesso abusivo al sistema informatico la condotta del pubblico dipendente, impiegato della Agenzia delle entrate, che effettui interrogazioni sul sistema centrale dell'anagrafe tributaria sulla posizione di contribuenti non rientranti, in ragione del loro domicilio fiscale, nella competenza del proprio ufficio.[72]

Le ragioni di fondo della decisione sono legate alla posizione di pubblico dipendente. La Cassazione sostiene che «quando l'agente è un pubblico dipendente, non può non trovare applicazione il principio di cui alla l.241/1990, in base alla quale l'attività amministrativa persegue fini determinati dalla legge ed è retta da criteri di economicità, efficacia, imparzialità, pubblicità, trasparenza, […]. L'esercizio del potere pubblico può certamente essere connotato da discrezionalità ma mai da arbitrio».[73] La Corte ricorda come l'esercizio dei poteri debba avvenire in conformità della "*legalità sostanziale*", della "*legalità indirizzo*" e della "*legalità garanzia*".

Secondo la Corte l'assegnazione del potere di accesso al sistema informatico è compatibile solo con un utilizzo dello stesso all'interno di quei limiti che la PA e i suoi dipendenti devono rispettare; la individuazione del fine per il quale il soggetto ha agito non riveste valore in sé (come stabilito nella sentenza del 4694/2011 viene in rilievo il fatto oggettivo dell'accesso), ma può contribuire a chiarire se il soggetto abbia agito o meno nell'ambito o al di fuori dei suoi poteri istituzionali, e nel caso rileva l'applicabilità del 615-*ter*.

[71]Cfr. Cass. pen., Sez. Un., 27 ottobre 2011, n. 4694, in *Arch.Pen.*
[72] Cfr. Cass. pen., Sez V, 24 aprile 2013 n.22024, *onelegale.wolterskluwer.it*
[73] Cfr. Cass. pen., Sez. V, aprile 2013 n. 22024, ivi.

Le Sezioni Unite si pronunciano quindi nuovamente sull'importante argomento, con conclusioni diverse rispetto al precedente orientamento.

L'ordinanza di rimessione si riferisce ai soggetti di pubblico ufficiale ed incaricato di pubblico servizio (comma 2, n.1 615-*ter*), sostenendo che le finalità per le quali tali soggetti accedono o si trattengono in un sistema informatico o telematico, in funzione della disciplina a cui sottostanno, non possono essere considerate ininfluenti ai fini della configurazione del delitto in esame. Ciò in quanto nell'autorizzazione all'accesso ed al mantenimento, (così come nel loro *status*) è "incorporato" il fine istituzionale che sovraintende l'attività, e sono "incorporate" le norme (legali, regolamentari, deontologiche), che ne regolano lo svolgimento.

La Corte si esprime nella sentenza 41210/2017, affermando che «integra il delitto previsto dall'art. 615-*ter* comma 2 n. 1 c.p. la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un servizio informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita»[74]

Il caso riguardava un cancelliere in servizio presso la Procura della Repubblica di Busto Arsizio; l'imputata accedeva, tramite le proprie credenziali, a notizie riservate attinenti a un procedimento penale a carico di un suo conoscente, su cui non aveva nessun interesse d'ufficio. La stessa era stata assolta dal Tribunale, in quanto aveva usato le sue credenziali per operazioni il cui accesso era consentito, e condannata in appello, in quanto l'uso (autorizzato) delle credenziali aveva consentito l'accesso a visione di atti per i quali l'imputata non aveva alcuna necessità di ufficio, realizzando una operazione "ontologicamente diversa" da quelle autorizzate.

La Corte nella sua decisione ha quindi modificato il proprio precedente orientamento, riconducendo entro l'ambito del 615-*ter* c.p. il caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, seppure a seguito di utilizzo di proprie

[74] V. Cass. pen., Sez. Un., 8 settembre 2017 , n. 41210, cfr *supra*, nota 54 cap.

legittime credenziali, ed in assenza di ulteriori espressi divieti in ordine all'accesso ai dati, acceda o si mantenga nel sistema informatico dell'ufficio con abuso delle proprie funzioni.

Tuttavia la Corte specifica che «il pubblico ufficiale, l'incaricato di pubblico servizio, l'investigatore privato e l'operatore del sistema possono rispondere del reato solo in forza della previsione del secondo comma»; quest'ultimo prevede un incremento di pena se il fatto è commesso da un pubblico ufficiale, o da un incaricato di pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio. Pertanto, se l'agente è un soggetto pubblico, ai fini del 615-*ter* non può non rilevare la soggezione ai principi generali dell'attività amministrativa disposti nella 241/90 e fondati sugli articoli 54, 97 e 98 della Costituzione: l'attività deve essere indirizzata a finalità istituzionali, basate sul rapporto funzionale, incorrendosi altrimenti nella figura dell'eccesso di potere.

Per chiudere questa lunga trattazione giurisprudenziale, è opportuno citare una ulteriore sentenza della Cassazione Penale, sez. V 34296/2020[75].

La Quinta Sezione si è occupata della vicenda di un professionista - socio sia di uno studio professionale associato che di una società tra professionisti, che aveva effettuato il *backup* dei dati dei clienti per avviare un'attività autonoma e diversa rispetto a quella per cui i dati stessi erano stati raccolti. Querelato per il reato di cui all'art. 615-*ter* c. p., l'imputato veniva condannato in entrambi i gradi di merito, ricorrendo, infine, in Cassazione.

In sede di legittimità, quindi, veniva lamentata dal ricorrente la erronea applicazione dell'art. 615-*ter* c.p., in quanto l'accesso al sistema informatico era stato eseguito utilizzando le chiavi d'accesso di cui era legittimamente in possesso e sottolineando come nessuna normativa interna all'associazione o alla società vietasse in alcun modo l'utilizzo delle stesse per le finalità con cui erano state impiegate.

La Corte ha respinto il ricorso, ripercorrendo gli argomenti proposti da alcune pronunce precedenti, ed affermando – nuovamente – il principio per cui vi è accesso abusivo a sistema informatico ogni qualvolta l'agente entri o si trattenga nel sistema

[75]Cfr. Cass. pen., Sez. V, sentenza 2 dicembre 2020 n. 34296, in *onelegale.wolterskluwer.it*

stesso per finalità diverse da quelle "istituzionalmente" previste per l'accesso al sistema stesso.

La sentenza in esame fornisce lo spunto per una rilettura ulteriore dell'artr.615-*ter*.[76] I criteri stabiliti dalla Suprema Corte nella sentenza del 2017, limitati ai soggetti destinatari del comma 2 art.1 615-*ter* vengono estesi anche alle ipotesi del primo comma. In particolare la Corte ha affermato che «decisiva, per giudicare della liceità dell'accesso effettuato da chi sia abilitato ad entrare in un sistema informatico, è, per la giurisprudenza di legittimità, la finalità perseguita dall'agente, che deve essere confacente alla *ratio* sottesa al potere di accesso, il quale mai può essere esercitato in contrasto con gli scopi che sono a base dell'attribuzione del potere, nonché in contrasto con le regole dettate dal titolare o dall'amministratore del sistema».

La Corte nelle sue motivazioni riprende la sentenza 41210/2017, ricordando che «le Sezioni Unite sono tornate sul tema dell'accesso operato da chi sia munito di apposite chiavi e sia abilitato a farlo, ma lo faccia in violazione delle norme pubblicistiche che disciplinano l'operato dei pubblici dipendenti e che indirizzano verso finalità di pubblico interesse attività della pubblica amministrazione. Ebbene, richiamato il principio di cui all'art.1 della legge n.241/1990, 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", le Sezioni Unite sopra richiamate hanno ribadito l'illeceità e l'abusività di qualsiasi comportamento si ponga in contrasto, manifestandosi in tal modo la "ontologica incompatibilità" dell'accesso al sistema informatico, connaturata ad un utilizzo dello stesso estranea alla ratio del conferimento del relativo potere».[77]

[76] In questo senso ritiene BORGOBELLO, *Il reato di accesso abusivo a sistema informatico di cui all'art. 615-ter c.p. alla luce della giurisprudenza più recente*, in *Giurisp. Pen.*, 2021, 2.

[77] Cfr. Cass. pen., sez. V, 2 dicembre 2020 n.34296, cit. Per un approfondimento possono essere considerate anche le considerazioni della Corte riportate a seguire: «Decisiva, quindi, per giudicare della liceità dell'accesso effettuato da chi sia abilitato ad entrare in un sistema informatico è, per la giurisprudenza di legittimità, la finalità perseguita dall'agente, che deve essere confacente alla ratio sottesa al potere di accesso, il quale mai può essere esercitato in contrasto con gli scopi che sono a base dell'attribuzione del potere, nonché, come è stato già rimarcato, in contrasto con regole dettate

Viene quindi superata la concezione esclusivamente oggettiva del requisito del mantenimento abusivo, per inserire l'elemento soggettivo della finalità dell'agente. Diventa inoltre decisiva quindi, sulla base di questa pronuncia della Corte, verificare la finalità perseguita dall'agente, prescindendo dalla qualifica pubblica o privata e dai doveri legati al codice della pubblica amministrazione: il potere di accesso non può mai essere esercitato in contrasto con le regole o gli scopi dettati dall'autorizzante.

Il reato prevede il dolo generico, e la querela di parte nella formulazione del primo comma. Nel secondo comma sono invece previste ipotesi più gravi, per le quali si procede d'ufficio.[78]

8.2 - Art.615-*quater*: detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici.

All'art.615-*ter* seguono due "reati prodromici", il 615-*quater* e *quinquies*.

dal titolare o dall'amministratore del sistema. Tanto vale per i pubblici dipendenti, ma, stante l'identità di ratio, anche per i privati, allorchè operino in un contesto associativo da cui derivino obblighi e limiti strumentali alla comune fruizione dei dati contenuti nei sistemi informatici. In tal caso la limitazione deriva non già da norme pubblicistiche, che non esistono, ma dai principi della collaborazione associativa, che hanno, come base necessaria, il conferimento di ben, utilità, diritti e quant'altro funzionali al perseguimento dello scopo comune, ed impongono l'utilizzo degli stessi in conformità allo scopo suddetto. Anche l'accesso ai sistemi informatici predisposti a servizio dell'attività comune deve avvenire, quindi, in conformità alla ratio attributiva del potere, configurandosi come abusivo, ai sensi dell'art.615-*ter*, ogni accesso che risulti con esso incompatibile», in *onelegale.wolterskluwer.it*

[78] Cfr. art. 615-*ter*, co. 2: «la pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio».

Se il 615-*ter* persegue l'accesso non autorizzato ad un sistema informatico, il 615-*quater* si occupa di chi ha "favorito" questo accesso procurando, producendo o realizzando tutta un'altra serie di condotte in grado di rendere idonei l'accesso ad un sistema informatico protetto. [79]

Viene punita la condotta, non è necessario il realizzarsi dell'evento. Siamo in presenza di un reato di pericolo, accompagnato da dolo specifico: procurare a sé o altri un profitto, o arrecare ad altri un danno, prescindendo, come detto, che questo danno si realizzi.

La condotta può inoltre assumere due tipologie: la prima è di tipo operativo[80] , e consiste nel "procurarsi, riprodurre, diffondere, comunicare o consegnare" una serie di possibili strumenti (codici, parole chiave o altri mezzi) "idonei" all'accesso; la seconda tipologia di condotte, che potremmo definire 'informativa', consiste invece nel "fornire indicazioni o istruzioni idonee al predetto scopo"

I due reati non possono concorrere fra di loro se contestati nel medesimo riferimento spazio-temporale e in danno di uno stesso soggetto.[81].[82]

---

[79] Cfr. art 615-*quater*: «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.
La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) al quarto comma dell'articolo 617-*quater*»

[80] Per un approfondimento sul 615-*quater* v. anche MONTI - LUPARIA, *Cybercrime e responsabilità da reato*, cit., cap.2, 7.

[81] Così PIETROPAOLI, *informatica criminale*, cit., 1.2.2, citando anche Cass. pen., sez. II, n.21987/2019.

[82] Cfr. Cass. pen., sez. II, 20 maggio 2019 n.21987, in *Giur.Pen.*, con note di Borgobello M.: «Utilizzando queste coordinate ermeneutiche in ordine ai reati in esame, la Corte di Cassazione ha, in primo luogo, affermato la possibilità di concorso tra l'art. 640-*ter* Cod. pen. e l'art. 615-*ter* Cod. pen. da un lato e, in secondo luogo, la possibilità di concorso tra l'art. 640-*ter* Cod. pen. e l'art. 615-*quater* Cod. pen. per poi affrontare compiutamente la questione dell'assorbimento del reato di cui all'art. 615-*quater* Cod. pen. in quello di cui all'art. 615-*ter* Cod. pen.
Ferma restando l'applicazione dell'art. 15 Cod. pen., la Seconda Sezione ha fatto ricorso alla categoria dell'assorbimento ed individuato due elementi distintivi, affinché il detto fenomeno si possa verificare, ossia il trattamento sanzionatorio più lieve della fattispecie assorbita rispetto a quella assorbente e l'identità di bene giuridico tutelato tra le due norme incriminatrici», *giurisprudenzapenale.com*, 2020, 1.

8.3 - Art.615-*quinquies*: detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

Se il 615-*quater* è volto a prevenire l'intrusione, il 615-*quinquies* si preoccupa invece di prevenire il danneggiamento. Anche qui siamo in presenza di un reato di pericolo, accompagnato dal dolo specifico di danneggiare, "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". [83]

L'articolo è una evoluzione di una fattispecie già disciplinata nella 547/93, dove si puniva la diffusione di prodotti informatici dannosi. Nella attuale formulazione viene punita la creazione, detenzione, diffusione e installazione sia di componenti *hardware* in grado di danneggiare sistemi informatici e telematici, sia di programmi rientranti nella categoria dei malware, dove si trovano i diversi tipi di *virus* informatici.[84]

Viene messo in evidenza[85] che la formulazione della fattispecie si discosta dalla previsione della Convenzione *Cybercrime* che all'art. 6 fa riferimento a programmi o dispositivi concepiti o adattati "primariamente" allo scopo di commettere reati informatici, «richiedendo così una loro connotazione oggettiva già sul piano tecnico ed escludendo dalla sfera di punibilità altri programmi o dispositivi, che invece siano tecnicamente "neutri" o solo eccezionalmente destinabili a scopi illeciti».

La norma attuale invece tratta di programmi tecnicamente "neutri" in grado di assumere valenza penale sulla base di un solo elemento che è il dolo specifico di danneggiamento. La necessità di distinguere fra un utilizzo "lecito" ed un utilizzo "illecito" viene quindi affidata ad un elemento di non facile prova.

---

[83] Art.615-*quinquies*: «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 o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329»

[84] La ricostruzione è di PIETROPAOLI, *informatica criminale* cit., 1.2.3.

[85] In questo senso MONTI - LUPARIA, *Cybercrime e responsabilità da reato*, cit., cap.2, 9.

Entrambe le forme prodromiche (615-*quater* e *quinquies*) sono procedibili d'ufficio. È stato fatto notare che l'accesso abusivo nella sua ipotesi base, ex art. 615-*ter* comma 1, ed il delitto di danneggiamento di dati "privati", ex art. 635-*bis*, comma 1 c.p. sono invece procedibili a querela, determinando disarmonie in sede processuale.[86]

8.4 - Art 635-*bis*: danneggiamento di informazioni, dati e programmi informatici

Del secondo gruppo di reati inseriti nell'art. 24-*bis*[87] fa parte l'art.635-*bis* che si occupa assieme al 635-*ter*, 635-*quater* e *quinquies* della integrità dei dati e dei sistemi informatici.

La norma viene inserita nel Codice penale con la legge 547/1993,[88] e rappresenta un primo intervento specialistico di tutela legislativa di dati informatici. In precedenza, in assenza di un vuoto legislativo da un lato, ed in presenza di un sempre maggiore numero di reati informatici, la giurisprudenza tendeva ad utilizzare l'art.635 c.p. (danneggiamento).

L'utilizzo del 635 c.p. non creava particolari problemi nelle situazioni in cui oggetto del reato fosse l'*hardware*; si tendeva inoltre ad utilizzare con ben maggiori difficoltà lo stesso articolo anche quando ad essere danneggiato era il *software*, con una interpretazione che, ritenendo "indivisibile" *hardware* e *software*, trasformasse il danneggiamento di quest'ultimo in una lesione del primo. I limiti di una lettura di questo genere erano evidenti e permanevano inoltre delle situazioni non risolvibili con l'interpretazione citata, come nelle ipotesi in cui i dati erano "viaggianti" da un sistema ad un altro.

L'art. 5 della legge 18 marzo 2008 n. 48, di ratifica ed esecuzione della Convenzione di Budapest, modifica l'art.635-*bis* rispetto alla originaria formulazione, ed amplia l'elenco delle fattispecie incriminatrici in materia di danneggiamento informatico e

[86] MONTI – LUPARIA, *Cybercrime e responsabilità da reato*, cit., 22.
[87] *supra* cap.III, par.8.
[88] Per un approfondito *excursus* storico sulla evoluzione dei reati di danneggiamento informatici v. ATERNO, *Le fattispecie di danneggiamento informatico*, in LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, cap. 2, 35ss

telematico, inserendo nel tessuto codicistico altri tre articoli, con i quali l'art. 635-*bis* crea un "microsistema" normativo, composto quindi dal già citato 635-*bis*, che si occupa del danneggiamento di *dati* informatici, il 635-*quater* che tutela i *sistemi* informatici*,* il 635-*ter* che riguarda i *dati* di *pubblica utilità*, ed il *quinquies* riferito ai *sistemi* di *pubblica utilità*.

A questi si aggiungono il 640-*ter* c.p. (frode informatica), ed il 615-*quinquies* (diffusione di programmi diretti a danneggiare un sistema informatico), in modo tale da ottenere un complesso normativo destinato a tutelare l'integrità dei dati e dei sistemi informatici.

La distinzione fra "*dati informatici*" e "*sistemi*", trae origine dalla stessa Convenzione sul *Cybercrime*, che disponeva in modo separato agli articoli 4 (attentato all'integrità dei dati), e 5 (attentato all'integrità di un sistema), dopo avere fornito all'art.1 definizione differenziata fra "*dato* e *sistema*"[89] : per dati informatici si intende «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione».

Viene inoltre aggiunta dal legislatore italiano una ulteriore distinzione, non presente nella Convenzione, che distingue fra dato o sistema *"privato"* e dato o sistema *"utilizzato dallo Stato o da altro ente pubblico o comunque di pubblica utilità";* questa distinzione viene normativizzata agli articoli 635-*ter* e *quater*.

L'art.635-*bis* tutela, sotto il profilo dell'oggetto materiale, programmi, informazioni e dati informatici di privata utilità. Sono ricompresi in questa definizione il *software*, e tutte quelle informazioni codificate in forma non percepibile visivamente. La dicitura "programmi", inserita nell'articolo, è ritenuta pleonastica: si tratta di un insieme coordinato di dati, di per sé ascrivibili alle definizioni precedenti.

Si tratta di un reato a forma libera, non è richiesto che l'azione si sviluppi con particolari modalità o mezzi.

[89] *Supra,* cap.III par.3

Per quanto riguarda il soggetto attivo, si deve considerare che stiamo parlando di un bene privo di materialità, che può anche essere concesso a terzi senza apprensione materiale. Ci si chiede se sia possibile che il proprietario del bene dato in godimento possa commettere questo reato[90]. L'opinione prevalente ritiene che il proprietario non possa essere soggetto attivo di questo reato, che invece è configurabile in capo al titolare del delitto di godimento.

Una certa attenzione richiede la definizione di programma informatico "*altrui*". Anche qui la immaterialità del bene oggetto di tutela rende complesso definire il concetto di altruità, considerata la non possibile apprensione esclusiva da parte di un soggetto.

Viene suggerito che la definizione dei soggetti interessati deve essere estesa a tutti i soggetti che abbiano un legittimo interesse a che i dati od i programmi possano funzionare ed essere correttamente utilizzati, non limitandosi al solo proprietario o concedente.

La definizione del soggetto che può essere offeso dal reato rappresenta un problema che dovrebbe risolversi in concreto, attraverso, ad esempio, l'analisi della detenzione dei dati; ma come accennato in precedenza in ambito informatico non è sicuramente agevole stabilire questo elemento; un criterio che potrebbe portare a dei risultati è quello di desumere «dall'insieme di interessi giuridicamente rilevanti che ruotano intorno ad essi. È agevole pensare alla sostanziale differenza che vi potrebbe essere rispetto all'integrità di un file che un soggetto invia in copia, trasmette, duplica a favore di un altro soggetto, il quale però subisce in epoca successiva il danneggiamento del file in questione. L'esistenza a monte di un file originale ridurrà di molto il tenore del danno subito. Mentre, di contro, il

[90] Sul punto ATERNO, *Sistema penale*, cit.,2, 44; l'autore cita una sentenza (per la verità non recentissima): Trib. Torino, 12 dicembre 1983: «non integra gli estremi del reato di danneggiamento la condotta di chi riduce la funzionalità di un programma informatico da lui creato e concesso in godimento a terzi. Nella specie, è stato ritenuto che il tecnico di una ditta di programmazione di *computer* che aveva parzialmente cancellato il programma presso una società che aveva richiesto il servizio, non è responsabile del reato di danneggiamento».

danneggiamento dell'unico file esistente nella Rete, potrebbe aumentare di molto la gravità del danno».[91]

A questo proposito, appare esaustiva e completa l'individuazione di persone offese dal reato come il concessionario di programmi *software*, l'utilizzatore legittimo, il concedente e il proprietario/licenziatario.

Sotto il profilo dell'elemento oggettivo, le condotte che generano il reato sono quelle della distruzione, deterioramento, cancellazione, alterazione, soppressione. Rispetto alle condotte descritte nell'art. 635 c.p. del danneggiamento semplice non è presente la condotta relativa alla "dispersione", che avrebbe avuto difficile collocazione all'interno di un reato quale è quello di cui all'art.635-*bis*.

Per "distruzione" deve intendersi il completo annientamento del dato o del sistema, l'eliminazione totale o parziale non solo nel suo aspetto materiale ma anche nella sua funzione strumentale di soddisfacimento del bisogno; rientra sicuramente anche la rottura fisica. La distruzione può avvenire anche attraverso un'infezione irrimediabile del dato o del programma realizzata tramite dei virus, in grado di provocare l'impossibilità di utilizzare il dato informatico. In questo caso è da sottolineare che il dato non viene cancellato (altrimenti varrebbe la successiva previsione di cancellazione): quindi nella memoria del supporto il dato è comunque presente, per quanto non più utilizzabile.

Il deterioramento va inteso come una diminuzione apprezzabile del funzionamento del dato o del programma; questi restano quindi nella disponibilità del soggetto, ma perdono la possibilità di essere pienamente utilizzati e valore. Anche in questo caso il deterioramento può avvenire tramite *virus*.

La cancellazione rappresenta forse l'ipotesi più frequente, ed è generata da una eliminazione dei dati non in senso fisico, ma con strumenti che possono essere rappresentati da virus, comandi, piuttosto che da fenomeni in grado di eliminare il dato (magneti). La cancellazione di un file potrebbe anche non rappresentare una situazione definitiva, in quanto sono presenti sofisticati programmi informatici in

[91] Così ancora ATERNO, *Sistema penale.* L'autore pone anche un interrogativo nel caso in cui su di un *computer* vi sia un programma realizzato da un terzo: quest'ultimo, quale pretesa potrà vantare se quel file o quel programma dovesse andare distrutto? cit., 2, 45.

grado di recuperare il dato oggetto di cancellazione. Sul punto ha preso posizione la Corte di Cassazione[92], chiamata a intervenire sul caso di un dipendente di una ditta aveva cancellato un cospicuo numero di dati dall' *hard disk* del proprio pc aziendale ed aveva sottratto diversi *cd-rom* contenenti il back up dei medesimi contenuti.

La Corte ha affermato che il termine "cancellazione" deve essere interpretato nella accezione informatica, non semantica del termine, ossia come «rimozione da un certo ambiente di determinati dati, in via provvisoria attraverso il loro spostamento nell'apposito cestino o in via 'definitiva' mediante il successivo svuotamento dello stesso».

Diventa del tutto irrilevante, ai fini della sussistenza del reato, il fatto che i *files* cancellati possano essere recuperati successivamente attraverso una specifica procedura tecnico-informatica. La configurabilità del reato di danneggiamento informatico non viene dunque preclusa dall'eventuale reversibilità del danno, ritenendosi sufficiente che il bene sia stato - anche se temporaneamente - oggetto di manomissione o alterazione «rimediabili solamente attraverso un postumo intervento riparatorio, e comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro».

L'alterazione è una figura che tende a completare le ipotesi di danneggiamento dei dati o dei programmi, e comprende la modifica dei contenuti del dato, effettuata con manipolazioni, sovrascritture, tali da alterare la funzionalità e la fruibilità originaria. Diverse le ipotesi immaginabili: si pensi ad un virus che non consente più di modificare o andare in stampa un testo, o all'inserimento materiale di una password, da parte di terzi, sconosciuta all'utente legittimo, che rende il file non utilizzabile.[93]

La soppressione, infine, è una figura residuale, non è agevole individuarne la portata applicativa, considerate le possibili sovrapposizioni con le figure della distruzione e della cancellazione.

---

[92] V. Cass. pen., sez. V, 18 novembre 2011 n.8555, in *Dir. Pen. Cont.*, con nota di PUSATERI, *"Sussiste il reato di danneggiamento informatico anche quando i file cancellati possono essere recuperati*", in A*rchiviodpc,* 2012, 4

[93] In questo senso ATERNO, *Sistema penale,* l'autore precisa che in queste situazioni il file esiste nella sua immaterialità, ma non è più in grado di svolgere le sue normali funzioni, cit., 2, 49.

Nella descrizione del reato è da mettere in evidenza che lo stesso, nella formulazione base, (che è quella del primo comma), è perseguibile solo a querela di parte. Si differenzia quindi dal secondo comma, che rappresenta il reato nella forma aggravata, qualora lo stesso venga commesso "con violenza o minaccia, oppure con abuso della qualità di operatore di sistema": in questi casi è previsto l'intervento d'ufficio.

La figura dell'*operatore di sistema* inserita nel secondo comma come soggetto che può dare luogo alla forma aggravata del reato, è stata oggetto di interpretazione. Si discute in proposito se debba essere configurata questa qualifica in modo restrittivo od estensivo. Si tratta sicuramente di una figura che possiede una qualifica professionale o conoscenze informatiche particolari; è da definire se ci si debba riferire esclusivamente al tecnico o al supervisore del sistema (interpretazione restrittiva) o ad ogni operatore che acceda al sistema (interpretazione estensiva)[94].

La ratio dell'aggravante speciale va ricercata nel fatto che chi opera nell'ambito di un sistema ha una 'speciale opportunità' nella commissione del reato, e quindi è facilitato rispetto ad un estraneo. Inoltre, poiché l'operatore di sistema riveste un ruolo di vigilante del bene informatico e che contro le condotte offensive di quest'ultimo spesso le difese tecniche opponibili risultano inefficaci, il legislatore ha voluto optare per un aumento della pena (e quindi statuire la condotta come aggravante).

8.5 - Art.635-*ter*: danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

L'art.635-*ter* riferisce alle medesime fattispecie previste all'art 635-*bis*, differenziandosi dallo stesso per ritenere sufficiente un "*fatto diretto"* (a

[94] Sul punto v. PICCINNI, *Il reato di danneggiamento di sistemi informatici e telematici disciplinato quale reato presupposto dall'art.24-bis, d.lgs.231/2001 per l'applicazione delle sanzioni in materia di responsabilità amministrativa delle società e degli enti, in Rivis. 231, 2017, 4, 9.*

distruggere, deteriorare, cancellare, alterare o sopprimere) e definire come utilizzatore dei dati, delle informazioni e dei programmi "lo Stato, altro ente pubblico o comunque di pubblica utilità".

In sede di esame dei lavori effettuati durante la Commissione parlamentare[95]era emersa l'intenzione di inserire una circostanza aggravante dell'art.635-*bis*, che contemplasse le ipotesi di utilizzo da parte dello Stato, di altro ente pubblico o comunque un utilizzo di pubblica utilità; tuttavia, venne poi preferita l'istituzione di un autonomo titolo di reato probabilmente per assicurare maggiore tutela al bene garantito dal 635-*ter*.

La formulazione dell'articolo *"chiunque commette un fatto diretto*", evidenzia un delitto a consumazione anticipata: il solo attuare una condotta volta a ledere il bene oggetto di tutela realizzerà il reato, con pena reclusiva da uno a quattro anni.

In via interpretativa la soglia di punibilità deve assimilarsi al tentativo di danneggiamento ipotizzabile all'art. 635-*bis*, comma 1, e deve basarsi sulla prognosi postuma (ex ante), rilevando atti che risultino oggettivamente idonei e diretti in modo non equivoco a creare un concreto pericolo per il bene giuridico tutelato.

La realizzazione dell'evento è prevista nel secondo comma, con conseguente inasprimento della pena (delitto aggravato dalla realizzazione dell'evento).

Necessita un approfondimento il concetto di "*dati utilizzati dallo Stato*". Come più volte messo in evidenza, il dato informatico ha caratteristiche di immaterialità che rendono difficile una interpretazione realizzata con criteri ordinari. I dati in esame sono stati formati, realizzati dallo Stato, oppure sono stati creati da altri soggetti e poi trasmessi allo Stato, o ancora si tratta di dati di terzi recepiti ed inseriti in procedimenti della Pubblica Amministrazione? «Il fatto che lo Stato utilizzi un dato o un'informazione da lui non creata o a lui non riconducibile a livello di volontà formativa non significa per ciò solo che tale dato debba godere di una tutela

[95] L'attività di approfondimento è svolta da ATERNO, *Sistema penale,* cit., 2, 50. L'autore riferisce dei resoconti parlamentari e alla discussione in aula, cfr. *I resoconti parlamentari e della discussione in aula del 19 e 20 febbraio 2008: http://legxv.camera.it/resoconti,* evidenziando che la decisione presa in aula modificò la valutazione della Commissione, intenzionata ad inserire la fattispecie come aggravante dell'art.635-*bis.*

maggiore solo perché è memorizzato all'interno dei suoi sistemi informatici e ad esempio non vi è un reale utilizzo concreto di quel dato o di quella informazione».[96]

Il requisito della «pubblica utilità» deve intendersi in senso ampio comprensivo delle informazioni, dati o programmi, che pur se non appartenenti allo Stato sono destinati a soddisfare interessi pubblico-collettivi per la indeterminatezza del numero dei soggetti fautori (ad.es.: i dati di *computer* di ospedali).

8.6 - Art. 635-*quater* e *quinquies*: l'applicazione al sistema informatico.

Gli articoli 635-*quater* e *quinquies* si distinguono dai due articoli che li precedono in particolare per prevedere, come bene tutelato, non il dato, l'informazione od il programma, ma il sistema informatico o telematico.

Come già messo in evidenza[97] la nozione unitaria di sistema informatico è frutto della Convenzione di Budapest, che riporta definisce all'art.1: «sistema informatico: indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati».

L'art.635-*quater* si presenta come un reato a forma vincolata, differentemente dall'art.635-*bis* da cui prende spunto che è a forma libera. Il reato si realizza mediante le condotte previste nell'art. 635-*bis* ovvero «attraverso l'introduzione o la trasmissione di dati, informazioni o programmi»; queste ultime rappresentano una delle ipotesi più diffusa di danneggiamento, realizzata tramite virus informatici, in particolare *malware*[98].

---

[96] In senso critico ATERNO, *Sistema penale,* « Se vogliamo, mentre tale concetto di "utilizzazione" e`, con alcuni limiti, concepibile e giustificabile per i programmi informatici che sono strumentali alla vita e allo sviluppo della pubblica amministrazione, meno si spiega per i dati e le informazioni di atti e documenti non riconducibili allo Stato o alla volontà della PA e che, essendo di terzi oppure endoprocedimentali o addirittura del tutto estranei agli interessi dell'ente pubblico, non trovano giustificazione in una norma come l'art. 635-*ter* c.p.». L'autore aggiunge che il concetto di utilizzazione, quando riguarda un ambito informatico, assume rilievi non sempre facili da spiegare. cit., 54.

[97] *Supra,* cap.III, par 3

[98] A seguire un breve approfondimento sui più comuni virus utilizzati, riportando DEZZANI, *reati informatici,* in *diritto.it,* 2017,2, che dedica alcune considerazioni al tema dei reati informatici e descrive tre tipologie di *software* utilizzati in ambito di criminalità informatica: «In particolare, negli

Le condotte devono generare danneggiamento (quindi diminuzione della funzionalità, situazione corrispondente al deterioramento ipotizzato all'arti 635-*bis*), ovvero inservibilità totale o parziale (non idoneità, senza che ci sia danneggiamento o distruzione), ovvero grave ostacolo al funzionamento (corrispondente ad una alterazione solo temporanea).

L'art.635- *quinquies* al primo comma segue l'impronta del 615-*ter* primo comma, e si riferisce a situazioni in cui il sistema informatico o telematico viene aggredito da fatti previsti all'art.635-*quater*, "*diretti"* a distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità, o ad ostacolarne gravemente il funzionamento. Si tratta quindi nella formulazione del primo comma di un delitto a consumazione anticipata, in cui la realizzazione dell'evento è poi prevista con aggravio di pena al secondo comma.

---

ultimi anni si è assistito all'ascesa di tre tipologie di *software* utilizzati in ambito di criminalità informatica: *ransomware, trojan bancari e keylogger*. I primi sono diventati una delle minacce più diffuse su *computer* di privati, enti pubblici, studi professionali, ospedali e aziende dal 2014, in contemporanea con l'ascesa della moneta matematica nota come *Bitcoin* che ne ha tristemente aumentato il potenziale. I ransomware sono infatti *software* diffusi in diverse maniere, nascosti in: allegati di posta elettronica mascherati da finte fatture, note di credito, bollette di operatori telefonici o elettrici o all'interno di siti web compromessi in modo da attivare in automatico il download e l'avvio del *malware* da parte degli ignari visitatori.

L'effetto di un'infezione di un *ransomware* è devastante: i dati presenti sul proprio *PC* sono cifrati cancellando perennemente gli originali e proteggendoli con una chiave di cifratura (in pratica una sorta di "*password*") che l'utente non conosce e che quindi non potrà utilizzare per ripristinare i propri documenti. I delinquenti che hanno creato o diffuso il *ransomware* richiedono il pagamento di un riscatto da versarsi in *Bitcoin* entro alcuni giorni, pena il raddoppio del riscatto o persino la cancellazione permanente della chiave, il che implica l'impossibilità di riottenere i propri documenti. (…) L'unico aspetto fino a questo punto certo è che in presenza di una condotta estorsiva il soggetto passivo si configura quale vittima. Per questa ragione, anche in caso di pagamento del riscatto, non si configura un comportamento illecito.

Il secondo tipo di *software* spesso coinvolto nei reati informatici è identificato dai cosiddetti "*trojan* bancari", programmi il cui unico scopo è quello di monitorare l'utilizzo del computer al fine di intromettersi nelle operazioni dispositive su portali di *web banking* per deviare i bonifici verso altre destinazioni rispetto a quelle intese dalle vittime. Ignari imprenditori si ritrovano così con estratti conto che riportano bonifici verso località estere inoltrati in momenti nei quali essi avevano effettivamente inviato disposizioni ma non ovviamente verso i beneficiari che hanno ricevuto il denaro.

Terzo tipo di programmi che rientrano nella categoria degli "*spyware*" sono i *keylogger, software* di monitoraggio che ormai oltre ad acquisire la pressione dei tasti (e quindi "leggere" ciò che la vittima digita, *password* incluse) intercetta qualunque tipo d'informazione anche visiva o uditiva del *PC* o dall'ambiente della vittima. Il tutto per gli utilizzi più disparati, tra i quali la truffa del cosiddetto "*man in the mail*", che prevede l'intromissione dei criminali nella mail aziendale al fine di ingannare clienti o fornitori deviando così pagamenti anche d'ingenti somme verso conti dai quali i fondi spariranno poi nel nulla in breve tempo. O ancora, può ritornare il fine estorsivo, che si realizza quando i delinquenti acquisiscono informazioni riservate e chiedono un riscatto per impedirne la diffusione».

Da parte di alcuni Autori[99] viene criticato l'inserimento di questo reato fra i delitti contro il patrimonio: i sistemi di pubblica utilità cui fa riferimento l'art. 635-*quinquies* c.p. sono soprattutto quelli tipici delle c.d. "infrastrutture critiche" gestite spesso da grandi società private ed oggetto di attenzione anche tramite altre normative (NIS). Il bene giuridico tutelato, strategico al fine del buon funzionamento del sistema atterrebbe quindi all'ordine pubblico.[100]

8.7 - Art.640-*ter*: frode informatica

Del terzo gruppo di reati informatici in senso stretto[101] fa parte l'art.640-*ter*, titolato *frode informatica*, che è situato non nell'art.24-*bis*, quanto piuttosto nell'art.24, e prevede la responsabilità dell'ente solo ove la frode informatica venga realizzata a carico dello Stato o di un ente pubblico o dell'Unione Europea.[102]

---

[99] In questo senso Aterno, *Sistema penale*, cit., 55

[100] Sul punto v. pure DE SIMONE, *La rilevanza dei delitti contro l'integrità dei dati dei programmi e dei sistemi informatici al tempo della guerra russo-ucraina*, in *Diritto Penale*. L'Autrice evidenza come «l'ambito codicistico è quello dei reati contro il patrimonio, ma rispetto al bene giuridico non tutti concordano e trova sempre più consenso l'orientamento secondo cui proprio l'integrità dei dati, programmi e sistemi informatici costituisca essa stessa il bene giuridico tutelato». In questo senso viene sostenuta la necessità di raggruppare tutta la categoria dei reati informatici in un unico corpus normativo, che permetterebbe di graduare meglio il trattamento sanzionatorio, superando anche le obiezioni mosse in termini di sproporzione delle sanzioni.

[101] *Supra*, cap. III par.8

[102] L'art. 24, titolato «disciplina della responsabilità amministrativa delle persone giuridiche» dispone al comma 1 «in relazione alla commissione dei delitti di cui agli articoli 316-*bis*, 316-*ter*, 353, 353-*bis*, 356,640, co. 2, n.1, 640-*bis* e *640-ter se commesso in danno dello Stato o di altro ente pubblico o dell'Unione europea*, del Codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote». In senso critico MONTI, *Cybercrime e responsabilità da reato degli enti*, Milano, 2022, ss. L'autore ritiene un errore il mancato inserimento dell'articolo 640-*ter* nell'art.24-*bis* fra i reati informatici. A seguire alcune sue considerazioni sul punto: « Accanto a tale grave incongruenza, che solo in parte può spiegarsi con il fatto che la frode informatica non è considerata fra i reati oggetto della direttiva 2013/40/Ue relativa agli attacchi contro i sistemi di informazione (come non lo era fra quelli oggetto della precedente decisione quadro 2005/222/GAI), stupisce il fatto che il legislatore italiano, con la legge n. 48/2008 di ratifica della Convenzione *Cyber-crime*, abbia invece incluso l'art. 640-*quinquies* c.p. che punisce la "frode informatica" del certificatore fra i reati contenuti nell'elenco dei delitti informatici di cui al menzionato art. 24-*bis* d.lgs. n. 231/2001. […], quest'ultima norma è in effetti posta a tutela del sistema delle firme elettroniche certificate, e dunque della fede pubblica. E del resto punisce — nonostante la rubrica menzioni una condotta di "frode" — la mera violazione degli "obblighi previsti dalla legge per il rilascio di un certificato qualificato" da parte del "soggetto che presta servizi di certificazione di firma elettronica". Si tratta, quindi, di un reato proprio, commissibile solo da parte del soggetto così qualificato, che rimanda necessariamente […] alla citata disciplina delle firme elettroniche contenuta nel Codice dell'amministrazione digitale (d.lgs. n. 82/2005 e succ. modifiche), che poco ha a che vedere con la tutela del patrimonio in quanto tale».

A detta di alcuni autori, si tratta di uno dei reati, fra quelli inseriti con la 547/1993 o con la 48/2008 che riveste maggiore interesse, sia dal punto di vista dottrinario che operativo[103]. Preliminarmente è opportuno mettere in evidenza che non sempre le condotte fraudolente poste in essere tramite l'uso di tecnologie informatiche devono scriversi al novero delle frodi informatiche in quanto riferibili più correttamente alle truffe tradizionali previste all'art.640 c.p.

Un esempio può chiarire la differenza: acquistare un prodotto on-line per vedersi poi recapitare un pacco con un contenuto assente o diverso dal prodotto scelto ravvisa le ipotesi della truffa tradizionale, a nulla rilevando che l'acquisto sia stato fatto tramite internet; diversamente invece, nel caso un soggetto che tramite un *malware* inserito a sua insaputa nel suo dispositivo, invece di accedere al sito della propria banca, viene indirizzato ad un sito clonato, e dispone senza volerlo di un bonifico a favore di un terzo prenditore: questa ipotesi rappresenta un caso-scuola di una frode informatica.

Tra le altre condotte tipiche con cui viene commesso il reato possiamo ancora citare le condotte legate all'utilizzo di *dialer* e di *phishing*, ormai abituali frequenze delle cronache quotidiane. Il *dialer* è un *software*, inserito all'interno del *device* della vittima tramite un *link*, in grado di dirottare le chiamate verso numeri telefonici internazionali a pagamento; il *phishing* realizza un tipo di frode che consente di ottenere dati personali (compresi anche codici di accesso o *password*), dall'ignaro utente, che risponde in modo non sufficientemente accorto a *e-mail* o *sms* ingannevoli.

Il reato rientra comunque, pur con le differenze che andremo a rilevare, nello schema della truffa di cui all'art.640 c.p.; in questo senso rileva anche la Corte di Cassazione, che sul punto si è espressa nel seguente modo: «per la giurisprudenza di questa Corte, il reato di frode informatica - che postula necessariamente la manipolazione del sistema - presenta la medesima struttura e gli stessi elementi costituivi della truffa, con l'unica differenza che non viene indotto in errore la persona del soggetto

[103] In questo senso PIETROPAOLI, *informatica criminale* cit., 1,5,1ss. L'Autore mette anche in evidenza l'aumento enorme di denunce di riferibili a condotte fraudolente, messe in essere in rete o tramite la rete.

passivo, ma l'attività fraudolenta dell'agente investe il sistema informatico riferibile al suddetto».[104]

È bene precisare che la presenza di uno schema condiviso in parte con il reato di truffa non toglie autonomia al 640-*ter*, considerate le caratteristiche peculiari dello stesso. La valutazione è realizzata anche dalla Corte di Cassazione, Sez. I Penale, con la sentenza 15 aprile 2011 n. 17748, che afferma: «è quindi indubbio, anzitutto, che la fattispecie di cui all'art. 640- *ter* integri senz'altro una autonoma figura di reato, a differenza di quanto si è invece ritenuto in giurisprudenza a proposito della ipotesi di truffa aggravata per il conseguimento di erogazioni pubbliche, prevista dall'art. 640-*bis* cod. penale, ormai pacificamente ricondotta nel novero delle circostanze aggravanti rispetto al reato "base" di truffa ex art 640 c. p.». [105]

L'art.640-*ter* sviluppa due condotte alternative. Il reato può realizzarsi *alterando* il funzionamento di un sistema informatico o telematico, (ipotesi riconducibile per esempio ad un virus), oppure *intervenendo* con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico. In questo caso, viene specificato che l'intervento deve essere effettuato *senza diritto.*

Stabilito che l'assenza di diritto si ha certamente nell'ipotesi in cui si opera in assenza totale di legittimazione, ma deve essere individuata anche qualora l'agente usi impropriamente, o abusi, di un diritto di cui è titolare, [106] merita considerazione la definizione delle due condotte previste.

La prima, consiste nell'alterazione, in qualsiasi modo, (quindi siamo in presenza di un reato a forma libera), del "funzionamento di un sistema informatico o telematico": in tale fattispecie vanno fatte rientrare tutte le ipotesi in cui viene alterato, in qualsiasi modo, il regolare svolgimento di un sistema informatico o telematico. Seguendo l'indicazione della Corte di Cassazione[107], per sistema

[104] Così si esprime Cass. pen., Sezione V, 24 novembre 2003 n.4576, citando anche Cass. pen., Sez. VI, 14 dicembre 1999 n.3065, in *onelegale.wolterskluwer.it*
[105] Cfr. Cass. pen. Sez. I, 15 aprile 2011, n.17748, in *onelegale.wolterskluwer.it*
[106] Si esprime con questa valutazione VITALE, *Brevi riflessioni sul reato di "frode informatica": i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cybercrime,* aggiungendo: «Nella frode informatica, infatti, l'agire "senza diritto" è un elemento del fatto tipico, perciò colui che agisce nell'esercizio di un diritto, correttamente esercitato, pone in essere un fatto che è diverso da quello descritto dalla fattispecie astratta», *Arch. Pen.,* 2015, 1, 9.
[107] Cfr. Cass. pen, Sez. II, 24 febbraio 2011 n. 9891, in *onelegale.wolterskluwer.it*

informatico o telematico deve intendersi «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", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente» , mentre per alterazione deve intendersi «ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul *software*. In altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato».

La Corte successivamente alle considerazioni e alle definizioni appena riportate prosegue differenziando la frode informatica dai delitti di danneggiamento informatico (artt. 635-*bis*, *ter*, *quater* e *quinquies* c.p.), mettendo in evidenza non solo che in quest'ultimi è assente ogni riferimento all'ingiusto profitto ma anche perché «l'elemento materiale dei suddetti reati è costituito dal mero danneggiamento dei sistemi informatici o telematici e, quindi, da una condotta finalizzata ad impedire che il sistema funzioni o perché il medesimo è reso inservibile (attraverso la distruzione o danneggiamento) o perché se ne ostacola gravemente il funzionamento».

La seconda condotta prevista dall'art. 640-*ter* c.p. è costituita dall'intervento «senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico [...]»: si tratta quindi anche qui di un reato a forma libera che, finalizzato pur sempre all'ottenimento di un ingiusto profitto con altrui danno, si concretizza in una illecita condotta intensiva ma non alterativa del sistema informatico o telematico.

Ulteriore elemento necessario alla realizzazione del reato è un ingiusto profitto con altrui danno.

È stato messo in evidenza che l'ingiusto profitto genera il danno patrimoniale sulla sfera giuridica del soggetto passivo del reato, ed il rapporto è tale da far assumere al danno il carattere di un vero e proprio "secondo evento". Se ne deduce che, considerando tale reato come posto a presidio del patrimonio e del regolare funzionamento dei sistemi informatici, il danno patrimoniale subito dal soggetto passivo del reato è il *quid pluris* che differenzia la frode dagli altri reati informatici, il cui danno si potrebbe anche dire è *in re ipsa.*[108]

Il reato è punibile a querela della persona offesa, salvo che non ricorrano talune delle circostanze di cui al secondo e terzo comma (fra le quali viene riportata quella di avere commesso il reato con abuso della qualità di operatore del sistema).

Come accennato in precedenza, l'art. 24 stabilisce che il reato di frode informatica coinvolga la responsabilità dell'ente solo ove venga realizzata carico dello Stato o di un ente pubblico o dell'Unione europea.[109]

Ne deriva che l'ente, in termini cautelativi, seguendo le linee guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ex d.lgs. 231/2001 emesse da Confindustria il 7 marzo 2002, dovrebbe andare a mappare le attività e i processi aziendali a rischio reato, per individuare le aree di rischio dove sia possibile andare a realizzare, fra i vari eventi pregiudizievoli previsti dal d.lgs.231/2001, anche i reati indicati all'art.640-*ter*.

Sulla base di questa considerazione sono individuabili almeno tre aree di rischio che vedono in contatto la persona giuridica con lo Stato o con un ente pubblico: una prima area di rischio riguarda sicuramente i flussi informativi obbligatori verso la Pubblica Amministrazione che gran parte delle aziende devono soddisfare, come dati relativi alle dichiarazioni fiscali inviati all'Agenzia delle Entrate, denunce e

[108] Si esprime in questo senso VITALE, *Brevi riflessioni,* cit., 10

[109] Viene valutata come una "svista inconsapevole" il non inserimento della previsione della responsabilità giuridica degli enti in dipendenza della commissione di frode informatica (art. 640-*ter* c.p.) commessa in danno di soggetto diverso dallo Stato o di altro ente pubblico. Così BELTRANI, *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in responsabilità amministrativa degli enti, in *Riv. 231, 2008, 4, 4*. L'autore scrive: «trattasi all'evidenza di sviste inconsapevoli (lo conferma il silenzio tombale sul punto dei lavori preparatori), che provocano una disparità di trattamento assolutamente irragionevole, cui non sarà peraltro possibile ovviare in sede d'interpretazione».

variazioni relative a dati gestiti dalla Camera di Commercio, dati previdenziali inviati all'INPS.

L'area di rischio può poi estendersi nel caso in cui l'azienda attivi strumenti e procedure di finanza agevolata e/o svolga attività di negoziazione/stipulazione e/o esecuzione di contratti/convenzioni di concessioni con soggetti pubblici ai quali si perviene mediante procedure ad evidenza pubblica che prevedono l'iscrizione a registri informatici della Pubblica Amministrazione;

Infine, possiamo trovarci in presenza di aziende che, sulla base di un rapporto di appalto/concessione con un'Amministrazione Pubblica o in qualità di società miste partecipate da un'Amministrazione/Ente locale e da un privato imprenditore - si assumono l'incarico di realizzare, sviluppare e gestire un sistema informativo pubblico o un sistema informativo di interesse pubblico.[110]

8.8 – Art.25-*novies*: delitti in materia di violazione del diritto di autore

Come già riportato in precedenza[111], la dottrina ha messo in evidenza la presenza di reati informatici *in senso stretto*, che hanno come caratteristica di potere essere realizzati solo con l'utilizzo di un mezzo informatico, e di reati che possono anche essere commessi con mezzi informatici, ma non solo: l'utilizzo dello strumento informatico è eventuale, non indispensabile, rappresenta solo uno dei diversi modi in cui si può realizzare la fattispecie criminosa.

Fra questi reati rientrano sicuramente i delitti in materia di violazione dei diritti d'autore, che sono compresi, per quanto attiene la responsabilità dell'ente nel d.lgs. 231/2001, nell'art.25-*novies*[112].

---

[110] Si esprime in questo senso PREVITALI, *Il reato di frode informatica ai sensi del d.lgs.231/2001: standard di controllo e procedure per la compliance del modello organizzativo*, in *Responsabilità amministrativa delle società e degli enti*, in *Rivis. 231, 2007, 1*.

[111] *Supra*, cap. III, par.8

[112] V. art.25-*novies*: delitti in materia di violazione del diritto d'autore: «1.in relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-*bis*), e terzo comma, 171 *bis*, 171-*ter*,171-*septies* e 171-*octies* della legge 22 aprile 1941, n.633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote. 2.Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'art.9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174 *quinquies* della citata legge n.633 del 1941».

L'articolo viene inserito nella normativa 231/2001 con la legge 23 luglio 2009, n.99 recante «disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in tema di energia», e prende in considerazione alcune disposizioni penali sulla violazione del diritto d'autore[113].

L'introduzione dell'articolo avviene in presenza di istanze comunitarie relative all'adozione di misure penali per assicurare il rispetto dei diritti di proprietà intellettuale, tema particolarmente attuale già in quegli anni viste le diffuse condotte di plagio e di piraterie su opere dell'ingegno. In dettaglio, nei confronti delle persone giuridiche, si richiedevano sanzioni particolarmente dissuasive, al fine di arginare il fenomeno con un coordinamento a livello europeo, e prevedendo non solo sanzioni pecuniarie, ma anche interdittive, con la chiusura totale o temporanea dello stabilimento usato per realizzare il prodotto contraffatto, la perdita della licenza commerciale, e la confisca non solo del profitto del reato ma degli stessi strumenti utilizzati per la realizzazione dei beni.

In realtà l'auspicato coordinamento normativo a livello europeo non si è realizzato, pertanto l'art.25-*novies* rappresenta una attività del legislatore nazionale[114].

L'art 25-*novies* richiama solo una serie fra le diverse disposizioni previste della legge 633/1941 sul diritto d'autore[115].

Si tratta innanzitutto dell'art. 171, comma 1, lettera a-*bis*, che prevede l'ipotesi di chi «mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno

[113] Per una breve ricostruzione storica e considerazioni sul reato vedasi D'AGOSTINO, *I reati in materia di violazione del diritto d'autore,* in LATTANZI – SEVERINO (a cura di), *Responsabilità da reato degli enti*, Torino, 2020, 553ss.

[114] In proposito v. D'AGOSTINO, *I reati in materia*, cit., 554: «l'art.25-*novies* […] rappresenta un pregevole tentativo del legislatore nazionale di arginare le diffuse manifestazioni criminose di plagio e pirateria su opere dell'ingegno».

[115] Criticato da alcuni autori il modo in cui il legislatore ha dato corso alla descrizione delle varie figure di reato all'interno della l.633/1941. In questo senso DEZZANI – SANTORIELLO, *Responsabilità delle società e violazioni della normativa sul diritto d'autore in materia di software ed informatica*, in *Responsabilità amministrativa degli enti*, In *Rivis. 231*, 2012, 2, 3, «Assai criticata è stata anche la modalità con cui il legislatore, nel corso dei vari interventi di riforma, ha proceduto alla redazione delle nuove fattispecie incriminatrici. In tali occasioni, infatti, si è presto abbandonato l'obiettivo di dar vita a figure di reato descritte in termini generali ed astratti, per far invece ricorso ad una descrizione dei delitti di tipo casistico con conseguente disordine sistematico, ridondanze definitorie e non infrequenti sovrapposizioni nelle incriminazioni previste»

protetta, o parte di essa»; sempre dall'art. 171, ma al terzo comma, è prevista l'ipotesi in cui i reati «di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione, o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore», stabilendo pene più severe.

Tenendo presente gli inserimenti di altre diverse e successive fattispecie all'interno della l. 633/1941, l'area di incriminazione riconosciuta all'art. 171 risulta ridimensionata, da un lato, «dal sopravanzare del progresso tecnologico che ha consentito l'introduzione di prodotti intellettuali che fanno sembrare decisamente sorpassata l'impostazione della disposizione in commento»[116], e dall'altro proprio dal progressivo inserimento nella legge 633/1941 di ulteriori fattispecie a carattere speciale rispetto a quanto dispone la norma in esame

Il successivo art.171-*bis* è stato introdotto con legge 29 dicembre 1992 n.518, a seguito attuazione Direttiva 91/250/CE, contiene la tutela penale del *software*. L'articolo dispone al primo comma che è soggetto alla pena «chi, abusivamente duplica per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi […]», proseguendo, sempre al primo comma, «se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori». Questa parte dell'art.171-*bis* si riferisce al *software* in generale, e si distingue dal secondo comma, che invece assembla ed evidenzia tutta una serie di comportamenti riferibili alle *banche dati*.[117]

---

[116] In questo senso DEZZANI – SANTORIELLO, *Responsabilità delle società,* che aggiunge: «la previsione di cui all'art. 171 legge 633 è diretta a tutelare i diritti del creatore dell'opera, mentre il più recente orientamento della normativa a protezione del diritto d'autore si preoccupa di garantire gli interessi patrimoniali dei soggetti che provvedono alla distribuzione e commercializzazione dell'opera dell'ingegno, piuttosto che alla sua elaborazione», cit., 37.

[117] Cfr. art.171-*bis co. 2*: « Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una *banca di dati* in violazione delle disposizioni di cui agli articoli 64 *quinquies* e 64 sexies, ovvero esegue l'estrazione o il reimpiego *della banca di dati* in violazione delle disposizioni di cui agli articoli 102-*bis* e 102-*ter*, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro

La finalità messa in evidenza dal dettato legislativo è quella di "*trarne profitto*", espressione che consente una interpretazione estesa delle situazioni di vantaggio realizzabili, ivi comprese quelle relative ad una riduzione di costi. La dicitura è frutto di un intervento legislativo correttivo ad opera della l.18 agosto 2000, n.248 (art.13), che sostituì l'espressione precedente "*a fini di lucro*".

Le ragioni di questa modifica sono legate ad una precedente previsione incriminatrice che andava applicata solo comportamenti guidati dall'esclusivo scopo di conseguire un guadagno di tipo economico. All'espressione "lucro" dottrina e giurisprudenza assegnavano il significato di accrescimento positivo patrimoniale del soggetto agente; venivano pertanto ritenute penalmente non significative le abusive duplicazioni di programmi informatici, realizzate dall'agente al solo scopo di risparmiare la spesa necessaria per il regolare acquisto del *software*. In questa situazione (alquanto comune), gli interessi delle case produttrici dei sistemi informatici non trovavano dunque tutela penale. La nuova formulazione "trarne profitto", assume una valenza più generale, ed estende le situazioni tutelabili anche a quei casi appena riportati, precedentemente esclusi, in quanto la duplicazione effettuata con lo scopo del risparmio di spesa (per sé o per chi riceve la copia privata), determina per il soggetto agente un profitto legato al mancato pagamento dei costi di licenza. [118]

Una delle ipotesi che può essere presa in esame ai nostri fini (responsabilità dell'ente) può essere rappresentata dall'utilizzo di una copia non originale di un programma informatico, inserita da un dipendente all'interno del *software* del sistema aziendale, in grado di avere impatti positivi sulle elaborazioni legate al ciclo di lavoro e allo stesso tempo manlevare l'azienda dai costi di acquisto delle licenze del *software*. Allo stesso modo, il fatto potrebbe essere legato ad una iniziativa solitaria di un dipendente, non ascrivibile all'azienda. Appare evidente come la responsabilità dell'ente in materia desti non poche preoccupazioni, riconducibili anche alle difficoltà che si incontrano in questo settore nella fase

15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità».

[118] Si esprime in questo senso fra altri anche DEZZANI – SANTORIELLO, *Responsabilità delle società*, cit., 14.

dell'individuazione del reo. Vi è il timore che si possa finire con l'attribuire una responsabilità all'ente, solo perché magari è stato utilizzato un suo *computer*, senza che l'autore sia individuato e senza che siano quindi verificate le ragioni del suo agire. Inoltre, un'eventuale responsabilità per omesso controllo o vigilanza potrà favorire decisioni che non tengono conto delle effettive potenzialità dei sistemi e delle reali possibilità di controllo[119].

L'articolo precisa che la condotta deve essere realizzata *"abusivamente"*. Pertanto, non sussiste il reato - perché non può qualificarsi come abusiva la relativa condotta – qualora si vadano a duplicare programmi informatici cosiddetti *freeware*, rispetto alla circolazione ed allo sfruttamento dei quali cioè l'autore o il soggetto titolare del relativo diritto non ha posto alcuna limitazione, oppure quando si vadano a duplicare copie per utilizzare o proteggere al meglio il *software* o la banca dati (ad es. *backup*).

Altro articolo inserito nell'articolo 25-*nonies* è il 171-*ter*, che assembla al suo interno una notevole serie di opere dell'ingegno che vengono poste sotto tutela: «opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali, ma anche opere letterarie, scientifiche o didattiche».[120]

Completano l'articolo 25-*novies* altri due reati: quelli contenuti all'art.171-*septies* e l'art.171-*octies*[121].

---

[119] Sul punto, oltre D'AGOSTINO, *I reati in materia*, cit., 557, v. anche FAGGIOLI– PREVITALI, *Delitti in materia di violazione del diritto d'autore e contromisure organizzative e tecnologiche*, in *responsabilità amministrativa degli enti*, in *Rivis.231, 2010, 1, 3*. Viene messe in evidenza che «In particolare, a nostro avviso la prevenzione del reato in oggetto richiede un'adeguata politica di sicurezza informatica che, nel caso di commissione da parte di un dipendente del reato in esame, evidenzi la presenza di un chiaro comportamento di elusione fraudolenta del Modello Organizzativo al fine della commissione del reato». Gli autori mettono anche in evidenza la necessità di trovare un equilibrio tra l'esigenza di conservare la facilità e la scorrevolezza di utilizzo delle risorse all'interno dell'organizzazione e la necessità di controllare l'accesso a tali risorse.

[120] La sintesi viene descritta da D'AGOSTINO, *I reati in materia*, cit., 558

[121] V. art.171-*septies*: «1. La pena di cui all'articolo 171-*ter*, comma 1, si applica anche: a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-*bis*, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi; b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-*bis*, comma 2, della presente legge».
V. art 171-*otcies*: «Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da lire cinque milioni a lire cinquanta milioni chiunque a fini

Il primo impone degli obblighi preventivi di comunicazione alla SIAE, e la semplice violazione di questo obbligo realizza il reato e la pena prevista è quella dell'art.171-*ter*.

Il secondo tutela i segnali audiovisivi ad accesso condizionato, visibili esclusivamente da un numero definito di soggetti e non aperti ad ogni libero utente, prescindendo dalla presenza o meno di un canone. Vengono pertanto sanzionate le condotte di chi fraudolentemente produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione del segnale.

La valutazione complessiva della normativa di diritto penale a tutela delle opere dell'ingegno fatta dalla dottrina è della necessità di una profonda risistemazione: il continuo intervento del legislatore che ha innestato sulla normativa originaria contenuti sempre nuovi, in modo non sempre organico ha dato luogo ad un prodotto definito caotico.[122]Ai nostri fini, tuttavia, è da ricordare il collegamento realizzato tramite l'art.25-*novies*, che vuole essere oggetto di approfondimento ai fini della 231/2001 e della responsabilità aziendale.

Come noto, presupposto ai fini della responsabilità dell'ente è che la condotta criminosa procuri *interesse o vantaggio* all'ente stesso. Posizionandoci sulle fattispecie collegate all'art.171-*bis*, ed in particolare all'ipotesi classica dell'utilizzo abusivo di programmi informatici, (che rappresenta uno dei casi più frequenti) non sarà individuabile una responsabilità d'impresa nel caso ci sia un agente interno all'azienda che duplichi illecitamente un programma che viene utilizzato sul *pc*

---

fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio».

2. La pena non è inferiore a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

[122] In questo senso nuovamente DEZZANI – SANTORIELLO, *Responsabilità delle società,* cit., 22, che cita fra gli altri per avere condiviso le stesse conclusioni BERSANI, *La tutela penale del software*, in *Impresa*, 2005, 793*;* COLUCCI-FIORE, *La tutela penale del diritto d'autore,* Torino 1996, 10 ss.*;* FORLENZA, *Strumenti di contrasto al passo con la tecnologia*, in *Guida Diritto*, 2000, 34, 57*;* RINALDI, *Le nuove norme sulla tutela del diritto d'autore*, in *Legisl. Pen.*, 2002, 1-2, 87

aziendale, installandolo sul proprio *pc* personale, e facendone un uso altrettanto personale. In situazioni del genere la responsabilità dell'illecito risiede tutta nella persona fisica.

Situazione diversa è quella in cui il *software* viene duplicato per un utilizzo all'interno dell'azienda: in questi casi l'utilizzo per finalità aziendali, sommata al mancato pagamento delle licenze per l'utilizzo del *software*, determinano un risparmio di costi per l'ente che si trasforma in un vantaggio; l'ente, quindi, potrebbe essere chiamato a rispondere dell'illecito.

La chiamata in causa dell'ente in una situazione come quella appena descritta può avvenire anche in presenza di un comportamento illecito che sia frutto dell'iniziativa estemporanea di un dipendente che, rendendosi conto di avere bisogno di un determinato programma informatico per svolgere al meglio un compito lavorativo, si procuri una copia abusiva di quanto gli è necessario.

Anche in tale caso, infatti, sarebbe configurabile il vantaggio dell'ente che, senza essere stato chiamato a sostenere i costi per acquisire la licenza del *software* utilizzato dal proprio dipendente per finalità aziendali, ne ha beneficiato; e, come evidente, la condotta illecita del dipendente sarebbe ascrivibile ad una colpa organizzativa dell'ente, che non aveva predisposto idonei meccanismi volti a prevenire anche la suddetta condotta estemporanea.

Emerge allora inequivoca l'esigenza, per le persone giuridiche, di predisporre quei sistemi e quelle cautele atte non solo ad impedire la formazione di una volontà sistematica di attuare gli illeciti che ci occupano, ma anche a prevenire quelle condotte estemporanee che sarebbero comunque idonee e comportarne la responsabilità amministrativa.

Il collegamento è quindi con la disciplina del Modello di Organizzazione e Gestione previsto nel d.lgs.231/2001: l'unico modo che ha l'ente per sottrarsi a responsabilità derivanti dall'art.25-*novies* è predisporre, ed attuare in modo efficace, prima della

commissione del reato, un Modello organizzativo idoneo alla prevenzione del reato stesso.[123]

Affinchè ciò possa avvenire in modo completo ed organico è necessario che l'ente vada innanzitutto ad individuare l'area di rischio a cui è esposta, vale a dire, nel caso specifico, vada a individuare i rischi di verificazione di reati in materia di violazione di diritto d'autore al proprio interno. Successivamente dovranno essere predisposti protocolli di prevenzione idonei ad affrontare il rischio; infine, è necessaria l'attività dell'Organismo di Vigilanza.

Riprendendo e sviluppando l'esempio proposto in precedenza, l'area di rischio nel caso evidenziato deve essere individuata avendo a riferimento l'art. 171-*bis* legge 633/1941. Tenendo sempre ben presente che il *software* appartiene alla proprietà intellettuale del programmatore che lo ha creato, o della *software house* che lo distribuisce all'utente finale viene concesso un uso attraverso la stipula di un contratto, che funge da licenza. Quindi, nel caso in cui vengano utilizzati all'interno di una società programmi informatici senza l'acquisto della relativa licenza, si commette il reato in esame e l'ente rischia di essere di violare l'art. 25-*novies* citato con possibile applicazione alla società delle sanzioni amministrative di cui al d.lgs. 231/2001.

Ipotizzato che un soggetto interno alla società, operando in modo autonomo (e nonostante l'ente abbia sposato una *policy* diretta al controllo della provenienza di ogni *software* installato sui macchinari) decida di scaricare dal *web* un programma senza che avvenga il previsto acquisto di licenza (il programma può anche essere gratuito, ma con obbligo di licenza), abbiamo una esposizione della società a responsabilità ex d.lgs. 231/2001.

L'area di rischio è individuabile nel processo di acquisto dei *software* aziendali (in che modo l'azienda acquista *software*), che dovrà essere caratterizzato dall'ottenimento delle idonee licenze per il loro utilizzo, nonché in quello per

[123] Sul punto vedasi MILANI – BONINSEGNA, *I reati in materia di diritto d'autore e il modello organizzativo 231: configurabilità e prevenzione, in Responsabilità amministrativa delle società e degli enti, in Rivis.231, 2013, 3, 5*, che individua area di rischio, protocolli di prevenzione e Organismo di Vigilanza nell'ipotesi di abuso ex art.171-*bis*. L'esempio riportato nel testo della tesi è tratto da questa elaborazione.

l'implementazione dei programmi da installare sui *personal computers* presenti in azienda (in che modo i programmi sui *pc* sono implementabili). Ulteriore elemento di rischio può essere ravvisato, infine, in tutte le attività che potranno essere attuate da ogni singola risorsa aziendale che avrà accesso al *web*, sussistendo la possibilità del *download*.

Definite le aree di rischio, dovranno essere stabiliti dei protocolli che consentano di prevenire la realizzazione del reato in esame. Nell'ipotesi esaminata sarà dunque necessaria una campionatura accurata dei macchinari e dei *software* installati; quindi occorrerà che l'ente si doti in modo formalizzato di un apposito "registro dei macchinari" sul quale devono essere inventariati i personal computers di proprietà dell'azienda, con indicazione del codice di ogni macchina e con un elenco dei programmi installati su ciascuna di esse; ogni programma, poi, dev'essere qualificato come "a pagamento" o "*freeware*"; se "a pagamento" dev'essere indicato il numero del contratto e/o licenza d'uso con l'espressa indicazione della data di scadenza dell'eventuale licenza; devono essere inoltre individuati tutti gli operatori che utilizzano detti macchinari, che devono essere previamente soggetti a idonea formazione. Per quanto ovvio, il sistema deve essere dotato di *password* di accesso personali, le stesse devono avere una data temporale di scadenza contenuta, onde costringere al rinnovo periodico, per migliorarne la capacità di sicurezza nell'accesso.

Sarà inoltre necessario installare su ogni *personal computer* un *firewall* che impedisca al singolo utente di poter scaricare di propria iniziativa sull'unità lavorativa programmi non campionati.

Questa attività deve essere devoluta ad una risorsa specifica, appartenente alla struttura *IT*, che si occuperà anche dell'aggiornamento e dell'implementazione dei singoli macchinari e dell'eventuale introduzione di nuovi programmi. Ogni singolo soggetto che interagisce con i *personal computers* deve essere adeguatamente formato ed informato, preliminarmente e con momenti di aggiornamento, sui rischi legati ad un improprio utilizzo del sistema informatico e sulle condotte da seguire. Si stabiliranno inoltre a carico di *IT* una serie di controlli periodici sui macchinari e sul *software*.

Definito un percorso virtuoso come quello appena riportato, si aggiungerà l'attività dell'ODV, che dovrà verificare la presenza in azienda del "registro dei macchinari" e del suo aggiornamento; effettuare dei controlli a campione, sempre legati ai programmi presenti sui singoli macchinari e sulla scadenza delle licenze.

Verso l'Organismo di Vigilanza, saranno anche presenti flussi informativi in virtù dei quali ciascun soggetto sarà tenuto a segnalare possibili elementi di anomalia nelle procedure standardizzate appena riferite, al fine di ottimizzare le attività di verifica e garantire il tempestivo intervento dell'Organismo.

In presenza di un percorso organizzativo come quello riportato, si può affermare che le condotte anomale come quelle di un abuso estemporaneo dovrebbero essere prevenute; e che, in caso contrario, dovrebbe valere l'esimente a favore dell'ente ai sensi del d.lgs. 231/2001, laddove, in presenza di quanto previsto dall'art. 5 d.lgs. cit., si può ragionevolmente sostenere l'elusione fraudolenta del Modello Organizzativo.

CAPITOLO IV

OLTRE LA 231/2001: GLI ULTERIORI INTERVENTI NORMATIVI

SOMMARIO: 1. Oltre la 231/2001: gli ulteriori interventi normativi – 2. Il Regolamento Generale sulla Protezione dei Dati (*GDPR*). – 2.1. Il Sistema 231 ed il GDPR. – 3. Direttiva NIS I, NIS II. – 4. *Cybersecurity Act*. – 5. Il Perimetro di Sicurezza Nazionale Cibernetica. – 6. L'Agenzia per la *Cybersecurity* Nazionale.

1 - Oltre la 231/2001: gli ulteriori interventi normativi

Lo schema costruito dalla 231/2001 prevede un intervento che si attiva nel momento in cui viene realizzato un reato-presupposto. La prevista generazione di un modello organizzativo efficace e adeguato, stabilita dalla stessa normativa 231, consente da un lato all'ente di sottrarsi dalla responsabilità prevista, dall'altro di detenere uno strumento in grado di evitare lo stesso sorgere del reato, in chiave preventiva. Tutto questo, come noto, in una situazione in cui l'ente trae interesse o vantaggio dal reato.

La componente preventiva è diventata sempre più centrale in tema di *cybercrime*, ed il modello 231 non sempre viene coinvolto dalle fattispecie che si possono generare, prima fra tutte quelle in cui è l'ente stesso ad essere oggetto di attacco informatico, (ad esempio da parte di un singolo *hacker*), o tutte quelle situazioni in cui ad esempio manca lo stesso interesse o vantaggio a favore dell'ente.

L'attività preventiva assume dunque valenza autonoma, e viene normativizzata con una serie di interventi, dove emergono almeno tre punti di particolare rilievo: la collaborazione fra autorità statuali ed *internet service provider*, l'interazione

"obbligatoria" in capo a determinate figure definite in modo chiaro in caso di incidente informatico con obbligo di comunicazione (sanzionato in caso di omissione), l'obbligo di adozione di misure interne atte a ridurre il rischio informatico.

La logica a cui rispondono questi punti si discosta da quella della 231: "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 od un suo vantaggio. La prospettiva […] è di richiedere, rispettivamente, agli operatori di servizi essenziali in determinati settori (energia, trasporti, bancario, infrastrutture, ecc.) e al titolare e al responsabile del trattamento dei dati, l'adozione di diverse misure tecniche e organizzative adeguate a fronteggiare i rischi esistenti nei diversi ambiti di intervento, nonché di imporre puntuali obblighi di comunicazione alle autorità individuate, a seconda dei casi, degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti e dei *data breach*"[1]

Fra le più importanti normative in materia sono citabili il GDPR e la Direttiva NIS.

2 - Il Regolamento Generale sulla Protezione dei Dati (*GDPR*)

Il GDPR entra nel nostro ordinamento con il Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, direttamente applicabile in tutti gli Stati Membri dell'Unione. Rappresenta una disciplina armonizzata a livello europeo su un tema di fondamentale e delicata importanza.

Le imprese che trattano o intendono trattare dati personali all'interno dell'Unione Europea (anche se esterne all'UE) devono necessariamente adeguarsi al nuovo contesto normativo, che sviluppa: regole più chiare in materia di informativa e consenso, definisce i limiti del trattamento automatizzato dei dati, disciplina il trasferimento transfrontaliero, impone importanti obblighi di notificazione in caso di *data breach*, ed attribuisce grande rilievo alle autodisciplina e *compliance* aziendale: viene valorizzato il principio di *accountability*, in forza del quale i

[1] La considerazione è di GULLO, *I reati informatici*, cit., 389

soggetti gravati dagli obblighi del GDPR dovranno adottare precise strategie per assicurare il rispetto delle previsioni normative.

A differenza delle passate regole, viene rivoluzionato il modo di approcciarsi alla tutela dei dati personali ed alla gestione degli stessi. La precedente disciplina, legata alla Direttiva 95/46/CE del Parlamento Europeo e del Consiglio, del 24 ottobre 1995, poi implementata in Italia con il Decreto Legislativo del 30 giugno 2003 n. 196 (c.d. Codice della *Privacy*), prevedeva che la gestione dei dati personali e le operazioni di trattamento avvenivano in un contesto normativo molto schematico dove il legislatore forniva indicazioni precise su come trattare i dati personali. Con il nuovo Regolamento viene modificata radicalmente la prospettiva di riferimento, e viene rimesso alla discrezione di ciascun titolare del trattamento il compito di operare in maniera adeguata alle tipologie di trattamento condotte.

Venne a suo tempo concesso un periodo di due anni (dal 2016 al 25 maggio 2018) affinché ciascun titolare del trattamento potesse adeguarsi al passaggio da una normativa "prescrittiva" come quella precedente del Codice della *Privacy* ad una normativa di "responsabilizzazione" come quella del Regolamento dove il vero protagonista è proprio il Titolare del trattamento, "unico artefice del proprio destino"[2] scegliendo in che modo bilanciare gli interessi, suoi e dei soggetti interessati, nel trattare dati personali di questi ultimi: l'impostazione del Regolamento risiede nel principio di *accountability*, che, come già detto, rappresenta un cambio di paradigma: piuttosto che indicare *ex-ante* una serie di regole immutabili da rispettare, vengono fissati principi di impostazione alla sicurezza informatica, basati sulla valutazione del rischio, obbligo di organizzazione interna, figure dedicate, rimandando i controlli di conformità dell'autorità competente, che è una autorità specializzata ed aggiornata, in linea con l'evolversi dei processi tecnologici, e che opera con un approccio *ex-post*, in funzione dell'avvenuto incidente di sicurezza , della violazione dei dati, o secondo controlli a campione.[3]

[2] L'espressione è di D'AGOSTINO, *il sistema di gestione della privacy*, in CASSANO – CERRINA - FERONI – BARBAROSSA, (a cura di), *Il processo di adeguamento al GDPR*, Milano, 2022, 35
[3] VALENTINI, *GDPR e cyber security, le regole normative e le misure tecniche*, in *Cybersecur.*, 2021, 06

Questo tipo di sicurezza deve essere prevista fin dalla progettazione del trattamento dei dati (*data protection by design*), e allo stesso tempo gli scopi di sicurezza dei dati e sui dati non possono eccedere i diritti di *privacy* e quindi non possono eccedere la tenuta sotto controllo delle informazioni private altrui (*data protection by default*).

Il dato personale, viene preso in considerazione sotto due punti di vista, "protezione" e "circolazione" e viene definito dal GDPR, come «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» (art.4, 1). Viene quindi adottata una nozione estesa di "dati personali».

Il regolamento si applica al trattamento "interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi", e viene destinato indifferentemente alle aziende, gli enti pubblici, e gli individui che devono accedere, trattare, conservare, gestire, o trasferire dati personali di cittadini UE.

Riguarda, quindi, un amplissimo ventaglio di aziende o enti pubbliche e private – dalle aziende sanitarie[4] alle federazioni sportive, dai social network alle società di *telemarketing* – che trattano dati personali "nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia

[4] Il *Rapporto Clusit 2023* riporta i due recenti esempi, sintetizzati a seguire, di attacchi informatici con prelievo di dati realizzati su strutture sanitarie. Le stime di valore per ogni "cartella clinica" privata trafugata, negoziata sul *dark web*, è intorno ai duemila dollari. Il 15 gennaio 2022vengono pubblicati su un sito internet non autorizzato migliaia di file prelevati illecitamente da una Usl veneta. L'attacco era stato compiuto il 3 dicembre. L'Asl dichiara l'avvenuto ai cittadini, sottolineando che non c'era sicurezza che i criminali si fossero impossessati di questi dati; che era stata avanzata richiesta di estorsione a cui l'Asl non aveva dato corso; che le forze dell'ordine avevano prontamente avuto conoscenza dell'accaduto. *Ex post* si scoprirà che erano stati sottratti circa 9mila file. Pochi mesi dopo un'altra serie di ospedali, stavolta a Milano, vengono sottoposti ad attacco informatico. Vengono di fatto bloccate le infrastrutture informatiche aziendali, si bloccano anche le procedure di accesso ai clienti. L'azienda farà seguire denuncia. In *clusit.it, sito ufficiale.*

effettuato o meno nell'Unione", ma anche a quelle aziende che, pur stabilite fuori dalla Ue offrono beni o servizi in Europa o monitorano il comportamento.

La relazione fra GDPR e *cyber security* risiede nella modalità di tutela della *privacy*, costringendo a realizzare od implementare misure di d*ata protection* e quindi di attuazione di misure preventive che proteggano i dati mettendoli al sicuro da attacchi che possono provenire dall'interno e dall'esterno.

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento[5]: liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato; limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati; minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento; esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento; limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento; integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Il Regolamento (articolo 5, paragrafo 2) richiede al Titolare del trattamento di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" (o *accountability*) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento."[6]

Il Titolare del trattamento deve quindi predisporre delle adeguate strutture organizzative (infrastrutturali ed informatiche), che garantiscano la sicurezza dei dati e consentano di evitare la responsabilità.

[5] Cfr. *Eur-lex.europa.eu*, sito ufficiale UE
[6] *Principi fondamentali del trattamento*, Garante *Privacy, garanteprivacy.it*

Deve assicurare che gli interessati siano sempre in grado di esercitare i propri diritti in tema di dati personali, deve essere in grado di comunicare prontamente in caso di *data breach* con l'Autorità Garante, seguendo precise regole e tempistiche la cui inosservanza espone a sanzioni, ed inoltre deve redigere un documento che valuti l'impatto potenziale sulla protezione dei dati in funzione del rischio legato al trattamento dei dati.

Altra figura chiave è rappresentata dal DPO: Il *Data Protection Officer* è una figura professionale con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi. Il compito principale del DPO è l'osservazione, la valutazione e la gestione del trattamento dei dati personali allo scopo di far rispettare le normative europee e nazionali in materia di *privacy*. La nomina del DPO è obbligatoria quando le attività del titolare del trattamento consistono in operazioni che per la loro natura, ambito di applicazione o finalità richiedono un monitoraggio regolare e sistematico. Il DPO verifica la conformità dei trattamenti, rende attività di informazione, di consulenza e di indirizzo nei confronti del Titolare e del Responsabile. Assiste il Titolare del trattamento nella valutazione di impatto sulla protezione dei dati (DPIA).[7]

In caso di violazioni della normativa, (quindi ad esempio di trattamento non conforme dei dati, o di omessa comunicazione), le sanzioni (amministrative) irrogate dal Garante, sono particolarmente pesanti, e possono arrivare nelle due ipotesi previste all'art. 83, paragrafi 4 e 5, fino rispettivamente al 2% od al 4% del fatturato mondiale dell'azienda.

Per quanto debbano essere erogate con criteri di riconducibilità alla rilevanza del singolo caso (come stabilito nell'art. 83 del GDPR), ed irrogate tenendo conto che debbano essere effettive, proporzionate e dissuasive (come stabilito da Cassazione Civile, Sez. I, n. 27189/2023[8]), si tratta di sanzioni che sono assimilabili, anche per la gravità e l'intensità della pena, ad interventi di tipo penale.

[7] Per ulteriori spunti v. POLIMENI, *DPO, chi è il Data Protection Officer e perché è una figura controversa*, in A*genda Dig*,2022, 6

[8] Cfr. Cass civ, Sez. I, 22 settembre 2023, n.27189 in *Altalex,*, con commento di Viggiani S., *La Cassazione delinea i parametri delle sanzioni GDPR: rilevanza, effettività e proporzionalità* : «la pronuncia risulta particolarmente rilevante poiché la Corte afferma i seguenti principi di diritto: - il

L'attività del Garante della *Privacy* è crescente, in funzione di un utilizzo sempre più intenso e frequente dei dati personali, sia da parte del titolare degli stessi, sia da parte di chi ne dispone (con attività, ad esempio di *telemarketing*). La Relazione alle attività del 2022[9] riporta nelle sintesi fra i vari dati 317 provvedimenti correttivi e sanzionatori, mentre le sanzioni riscosse sono state di circa 9milioni e 500mila euro.

A seguire una breve serie di sintesi statistiche relative all'anno 2021/2022.[10]

Innanzitutto, il numero di segnalazioni e reclami: sono 13 mila nel 2021 (si è riusciti a rispondere solo a 9mila), diventano 31mila nel 2022, con un inevaso importante di quasi 20mila reclami (si risponde nuovamente solo a 9mila segnalazioni).

La maggior parte delle segnalazioni/reclami viene dal mondo delle imprese (realtà economiche e produttive, circa 3mila), delle reti pubbliche (circa 1500), e poi soprattutto dalle reti telematiche e *marketing* (25mila segnalazioni/reclami, per la stragrande maggioranza rimasti inevasi, costituendo quindi un bacino di arretrato che andrà a pesare negli anni successivi).

Le misure correttive passano da 388 del 2021 a 317 del 2022, ma è facilmente immaginabile che una più numerosa evasione delle segnalazioni (quasi i 2/3 sono rimaste sospese), avrebbe generato un forte aumento dei numeri del 2022.

Contenuto il numero di segnalazioni all'autorità giudiziaria (12 nel 2021 vs 5 nel 2022).

I pagamenti dei contravventori, quasi tutti effettuati spontaneamente, ammontano a 13mln di euro per il 2021, scendendo a 9mln nel 2022 (ma nuovamente è da sottolineare che la grande parte delle segnalazioni del 2022 sono rimaste inevase).

GDPR prevede e disciplina le condizioni generali per irrogare sanzioni amministrative pecuniarie in relazione alla specificità, effettività e proporzionalità del singolo caso concreto;
-il totale della sanzione inflitta non può superare l'importo specificato per la violazione più grave, tenuto conto dei due parametri stabiliti ai paragrafi 4 e 5 dell'art.83.
- il giudice, anche nelle controversie in materia di protezione dei dati personali, può annullare in tutto o in parte il provvedimento o modificarlo anche limitatamente all'entità della sanzione dovuta, determinata in misura non inferiore al minimo edittale», in *Altalex., 2023, 10.*

[9] Cfr. Relazione sull'attività del 2022, in sito istituzionale, *garantedellaprivacy.it*

[10] Relazione annuale 2021 e 2022 Garante della *Privacy*, in *garantedellaprivacy.it*, sito istituzionale

2.1 - Il sistema 231 ed il GDPR

La legge 231/2001 non contiene reati-presupposto legati alla normativa *privacy*.

L'art 24 *bis* cita testualmente "delitti informatici e *trattamento illecito dei dati*". In sede di audizione informale alla Camera dei Deputati, era stata avanzata la proposta di modificare il testo della rubrica dell'articolo 24-*bis* eliminando il riferimento all'inciso "trattamento illecito dei dati": un testo di questo tipo parrebbe preludere all'inserimento di reati-presupposto legati alla normativa in tema di *privacy* ed, in particolare, verso l'art. 167 del Codice della *privacy* [11] (d.lgs. 196/2003) che prevede, appunto, la fattispecie penale "dell' illecito trattamento dei dati personali". Il corpo dell'articolo in questione, però, non fa alcun riferimento alla disciplina relativa al trattamento illecito dei dati personali.

Una nuova occasione di inserimento dei "reati *privacy*" all'interno della 231/2001 si ebbe con il decreto-legge 93/2013; qui, all'art. 9 comma 2 era prevista una modifica all'art.24 *bis* del d.lgs. 231/2001, che avrebbe inserito fra i reati previsti la Parte III. Titolo III, Capo II del d. l. 196/300, vale a dire, fra gli altri, l'art.167 (trattamento illecito di dati), art.168 (falsità nelle dichiarazioni al Garante e interruzioni dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), art.170 (inosservanza dei provvedimenti del Garante).

Tuttavia, in sede di conversione del decreto le modifiche previste all'art.24 *bis* sono venute meno.

Come evidenziato dalla stessa Corte di Cassazione nella relazione in tema di novità legislative n. III/01/2013 del 22 agosto 2013 [12] "si rileva che il decreto-legge 14 agosto 2013 n. 93 ha anche provveduto ad inserire - all'art. 24 *bis* del d.lgs. n. 231/2001 - il reato di frode informatica aggravato dalla sostituzione dell'identità digitale, il reato di indebito utilizzo, falsificazione, alterazione e ricettazione di carte

[11] Per considerazioni in questo senso v. CUNIBERTI, in *Commento alla legge di ratifica della convenzione di Budapest del 23 novembre 2011*, in *procura.milano.giustizia.it*

[12] V. Corte di Cassazione, 22 agosto 2013 - Relazione n. III/01/2013 del 22 agosto 2013 - Corte Suprema di Cassazione - Ufficio del Massimario (novità legislative: d.l.14 agosto 2013, n. 93 - disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province), in *Rivis. 231*.

di credito o di pagamento di cui all'art. 55 comma 9 del d. lgs. n. 231/2007, nonché i delitti (ma non le contravvenzioni) in materia di violazione della *privacy* previsti dal d. lgs. n. 196/2003 e cioè le fattispecie di trattamento illecito dei dati (art. 167), di falsità nelle dichiarazioni notificazioni al Garante (art. 168) e di inosservanza dei provvedimenti del Garante (art.170)».

Al riguardo la Relazione osserva che se i primi due aggiornamenti dei cataloghi non paiono destinati ad assumere particolare rilevanza in sede applicativa, «il terzo risulta invece di grande impatto, soprattutto per la configurazione della responsabilità da reato degli enti per l'illecito trattamento dei dati, violazione potenzialmente in grado di interessare l'intera platea delle società commerciali e delle associazioni private soggette alle disposizioni del d.lgs. n. 231/2001».

Un ulteriore possibilità di "abbinare" reati *privacy* alla 231/2001 poteva derivare dal d. lgs 101/2018, contenente "disposizioni per l'adeguamento nazionale alle disposizioni del Regolamento UE 679/2016 […], GDPR. Anche in questa occasione il legislatore, pur intervenendo su disposizioni penali, non ha ritenuto di modificare implementando la 231/2001 nel senso raccontato.

A parere di diversi autori, il non inserimento di reati-presupposto legati alla violazione di *privacy* rappresenta "una occasione mancata".[13]

[13] Così GULLO, *I reati informatici*, cit., 385, che cita in proposito SARZANA DI S. IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una gatta legislativa frettolosa*, in *Dir Pen e Proc*, 2008,1572. Gullo cita in particolare il caso *Cambridge Analytica*, che viene qui sinteticamente riportato in stralci con evidenze tratte da *diritto e consenso* /2021/12/21/il-caso-cambridge-analytica: «*Cambridge Analytica* era una filiale della società britannica *SCL Group* (*Group Strategic Communication Laboratories),* fondata nel 2013 con l'obiettivo di occuparsi delle strategie di comunicazione politica per finalità elettorali e per "affrontare il vuoto nel mercato politico repubblicano negli Stati Uniti». La società SCL si occupava prevalentemente di *big data* e di *data mining*.
Attraverso la raccolta di un enorme quantità di dati e informazioni è in grado di creare dei modelli comportamentali e psicologici che rispecchiano le diverse tipologie di utenti che navigano in rete, *Cambridge Analytic*a ha condotto numerose campagne elettorali in vari Paesi in via di sviluppo utilizzando nuove tecnologie e strategie; il suo primo incarico politico di spessore ha riguardato la campagna presidenziale del senatore repubblicano Ted Cruz.
Ma la vera svolta fu nel 2016, anno in cui si è occupata della campagna presidenziale di quello che sarebbe poi diventato il Presidente degli Stati Uniti d'America, Donald Trump. Non solo: ha assunto un ruolo di spicco anche nella campagna della *Brexit*.
Il sistema che è stato utilizzato da *Cambridge Analytica* è il cosiddetto *microtargeting* psicografico. Quest'ultimo consiste nel valutare la personalità degli utenti online attraverso la raccolta delle impronte digitali che vengono lasciate da questi in *Internet* e successivamente di influenzarne le scelte e le opinioni mostrando agli stessi inserzioni pubblicitarie mirate e personalizzate.

Si possono evidenziare sicuri elementi di vicinanza fra il sistema 231 e quello GDPR.

Entrambi i modelli spingono per l'adozione di un accurato sistema di compliance interna, dove la funzione di vigilanza viene assegnata ad un organismo indipendente: Organismo di Vigilanza (OdV) per la 231, il DPO per la *privacy*.

I due modelli prevedono inoltre entrambi la necessità di mappatura, che per la 231 si riferisce ai processi operativi e per la *privacy* al trattamento dei dati; utilizzano entrambi ruoli assegnati normativamente con ben precise responsabilità all'interno del processo; necessitano di modelli che devono andare a valutare i rischi, con l'obiettivo di prevenire infrazioni o mitigare l'insorgenza del rischio ed evitare responsabilità, o mitigare le conseguenze del danno; devono fornire formazione obbligatoria ai dipendenti[14].

Alla base vi è l'utilizzo di un algoritmo, un modello, elaborato dal ricercatore e psicologo Michal Kosinski. Kosinski, infatti, nel 2013 ha pubblicato un suo studio sulla rivista *Pnas* intitolato "*Private traits and attributes are predictable from digital records of human behavior*", in cui ha mostrato la possibilità di predire le caratteristiche emotive e comportamentali di un utente, basandosi unicamente su un certo numero di "*like*" di *Facebook*.
La società, a causa dello scandalo scoppiato nel marzo del 2018, ha poi dichiarato la chiusura il 2 maggio del 2018. Nel 2014, *Aleksandr Kogan*, un ricercatore dell'Università di Cambridge, sviluppò l'applicazione "*this is your digital life*". Quest'*app* permetteva agli utenti di ottenere profili psicologici e previsionali del proprio comportamento sottoponendosi a dei *quiz*. Per poterla utilizzare bisognava solamente registrarsi utilizzando il *Facebook Login*. Una volta effettuato il login tramite *Facebook*, si accettava che il sito ottenesse alcuni dei dati personali tra i quali: nome, cognome, *e-mail*, sesso ed età. Ma non solo, anche i dati riguardanti la rete delle amicizie sulla piattaforma.
Attraverso tale applicazione, la società di *Kogan*, la *Global Science Research* (GSR), nel 2015 ha raccolto oltre 270.000 iscrizioni e dati di più di 50 milioni di utenti del social.
I problemi sono sorti nel momento in cui Kogan condivise i dati degli utenti di *Facebook*, raccolti lecitamente, con *Cambridge Analytica*, violando di conseguenza i termini d'uso di *Facebook*.
L'ex dipendente di *Cambridge Analytica* ha tra l'altro sostenuto che *Facebook* fosse a conoscenza di tale violazione da addirittura due anni, senza intervenire in alcun modo.
In base al nuovo Regolamento europeo in materia di protezione dei dati personali 2016/679/UE, tale omissione avrebbe integrato una grave violazione della normativa in quanto non sarebbe stato rispettato uno degli obblighi previsti a carico del titolare del trattamento. Il passaggio di informazioni dall'applicazione a *Cambridge Analytica* era avvenuto, tra l'altro, senza che gli utenti fossero stati informati circa l'utilizzo che si sarebbe fatto dei loro dati e senza che avessero prestato il proprio consenso.
Il Garante italiano per la protezione dei dati personali ha applicato *a Facebook* una sanzione di un milione di euro per gli illeciti compiuti nell'ambito del caso "*Cambridge Analytica*".
Il *Social Network* ha invece patteggiato con la *Federal Trade Commission* americana: dovrà pagare due sanzioni, rispettivamente di cento milioni e cinque miliardi di dollari agli enti federali e impegnarsi a sottostare a normative molto più rigide riguardanti la protezione della *privacy* degli utenti, che saranno regolate da un comitato indipendente, con un funzionario nominato direttamente dalla FTC».

[14] In questo senso URICCHIO, *Modello privacy e modello organizzativo* in *Altalex*, 2021, aprile

Ancora un elemento di vicinanza è rappresentato dal fatto che alcuni reati-presupposto della 231/2001 riguardano reati informatici connessi a fattispecie di trattamento illecito di dati. Non a caso, proprio per tale ragione, alcuni modelli organizzativi 231, elaborati da associazioni o enti esponenziali di categorie economiche, prevedono tra i soggetti da coinvolgere nella stesura e nell'applicazione dei modelli organizzativi del codice di comportamento proprio il consulente *privacy* o DPO[15].

Sarebbe quindi opportuno un coordinamento fra i modelli *privacy* e i modelli 231, così come si impone una riflessione sulla opportunità di inserire alcuni dei reati *privacy* all'interno del sistema 231: si è messo in evidenza in precedenza la "pesantezza" del sistema sanzionatorio previsto nel GDPR. Assicurare le garanzie del procedimento penale, previsto nella normativa 231, potrebbe rappresentare un punto di arrivo.

[15] Considerazioni di ZANELLATI, *Valutazione e prevenzione del rischio privacy: adempimenti tra GDPR e d.lgs.231*, in C*ybersecur.*, 2020, 2. L'Autore riporta anche una serie di differenze fra 231 e GDPR: «La differenza è rappresentata dall'individuazione netta e precisa, da parte del decreto legislativo 231/2001, di piena non responsabilità in relazione all'esatta costruzione ed esecuzione ed applicazione del modello organizzativo.
Per quanto lo stesso modello organizzativo sia suscettibile di essere valutato dal giudice nella sua congruità e idoneità, è comunque rinvenibile nell'apparato normativo una declaratoria di non responsabilità connessa alla predisposizione di cautele preventive.
Ci riferiamo in particolar modo all'articolo 6 del decreto legislativo 231/2001, che contiene la dichiarazione di non responsabilità per il reato commesso da chi occupa una posizione apicale, così come all'articolo 7, con riferimento ai reati commessi da soggetti in posizione subordinata. Ebbene, una declaratoria di questo tipo, così netta, non è rintracciabile nel regolamento europeo 2016/679, benché i modelli organizzativi e l'apparato documentale, in cui viene incorporata la responsabilizzazione, così come l'adesione a codici di condotta sono tutti elementi che dovranno essere presi in considerazione dalla autorità di controllo nell'ambito della valutazione della responsabilità del titolare del trattamento.
Analizzando le condotte di reato che devono essere intercettate e prevenute dal sistema dei controlli d.lgs. 231/2001 pare che non vi sia una così stretta relazione tra 231 (reati informatici) e GDPR e/o d.lgs. 196/2003: se è vero che il rischio che l'Azienda è chiamata a prevenire ex d.lgs. 231/01 è quello del reato commesso nell'interesse o a vantaggio dell'Azienda stessa, le misure di sicurezza tecniche ed organizzative messe a protezione (ex GDPR) di quei dati personali che l'Azienda, al suo interno, tratta con i sistemi informatici, talvolta potrebbero risultare ininfluenti nell'ottica del d.lgs. 231/01 visto che, per questo, soltanto la proiezione verso l'esterno delle stesse condotte parrebbe compatibile con la necessaria sussistenza dell'interesse o vantaggio dell'azienda ai fini 231.
Si pensi al noto Allegato B del d.lgs. 196/2003: tutte le misure di sicurezza ivi elencate possono ritenersi idonee e adeguate a prevenire il rischio da reato? È chiaro che condotte di reato (informatico) che muovano dall'interno per un vantaggio personale dell'autore del reato e/o per un interesse incompatibile con l'azienda ovvero condotte che muovano dall'esterno, incompatibili con la responsabilità amministrativa 231 perché addirittura arrecanti – potenzialmente – un danno all'azienda, non devono essere intercettate ai fini della prevenzione del rischio da reato, tuttavia denotano la fragilità del sistema di protezione dei dati e rafforzano la necessità di una valutazione del rischio GDPR».

3 – Direttiva NIS I, NIS II

Con il D. Lgs. 18 maggio 2018 n.65 viene recepita nel nostro ordinamento la Direttiva 1146/2016 NIS.

Si tratta di un ulteriore, intervento europeo nel settore della sicurezza informatica, che riguarda tanto gli operatori pubblici che quelli privati, e rappresenta un altro importante passaggio nella armonizzazione delle legislazioni degli Stati membri nel settore.

La Direttiva NIS impone l'obbligo per gli Stati membri di dotarsi di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; di istituire un gruppo di cooperazione strategica; di creare una rete di intervento in caso di incidente (rete CSIRT); di stabilire su una serie di obblighi di sicurezza e di notifica all'interno di servizi essenziali individuati, obblighi che sono a carico degli operatori di questi settori.

La Direttiva inoltre dava possibilità agli Stati di adottare comunque disposizioni che consentissero un livello di sicurezza più elevato di quello stabilito.

La Direttiva NIS supera la distinzione fra pubblico e privato, riferendo le proprie discipline a quelli che sono individuati come "*servizi essenziali*", prescindendo dalla gestione (pubblica o privata) degli stessi.

I criteri di individuazione sono riportati all'art.5, par 2: sono considerati tali quei servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali; in cui la fornitura di tali servizi dipende dalla rete e dai sistemi informativi, e dove un incidente avrebbe effetti negativi rilevanti sulla fornitura.

A parte, in un allegato, vengono riportati i settori di riferimento: energia e fornitura di acqua potabile, trasporti, settore bancario, mercati finanziari, settore sanitario, infrastrutture digitali. La Direttiva prevedeva inoltre che gli Stati membri (entro il 9 novembre 2018), avrebbero definito gli operatori di servizi essenziali.

Seguendo uno schema che ormai ben conosciamo, definiti gli operatori dei servizi essenziali, sugli stessi gravano una serie di obblighi, che sono funzionali al buon

funzionamento o alla minimizzazione del danno del servizio stesso in caso di incidente. Fra gli obblighi, quindi, c'è quello di pronta comunicazione degli incidenti che hanno impatto rilevante, ma soprattutto di adottare misure tecniche ed organizzative adeguate e proporzionate alla gestione dei rischi.

Il D. Lgs. 65/2018, (attuazione della Direttiva NIS), individua gli organi competenti all'attuazione della strategia nazionale di sicurezza cibernetica; designa le Autorità NIS e il punto di contatto unico; inserisce una appendice sanzionatoria destinata alle violazioni degli obblighi imposti dal decreto.

L'architettura operativa individuata dal decreto prevedeva come designate Autorità NIS vari Ministeri, sostanzialmente "specchio" del servizio essenziale interessato e delle competenze del Ministero coinvolto: quindi, il Ministero dello Sviluppo Economici per il settore energia, infrastrutture e servizi digitali, Economia e Finanze per il settore bancario e le infrastrutture dei mercati finanziari, Salute per l'assistenza sanitaria, ed ancora Ministero dell'Ambiente e delle Infrastrutture e Trasporti; quindi il legislatore nazionale aveva adoperato una scelta nel senso della differenziazione della Autorità NIS competente in base al settore di riferimento. Allo stesso modo, nel decreto viene stabilito il "punto di contatto unico" presso il Dipartimento delle Informazioni per la Sicurezza, con il compito, fra gli altri, di cooperare con l'ENISA e con le altre Autorità NIS transfrontaliere.

Lo scorso 17 gennaio 2023, è entrata in vigore la Direttiva NIS 2[16] (Direttiva UE 2555/2022 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni), che segna un altro importante passo verso la piena definizione della strategia per la *cyber* sicurezza dell'Unione Europea.

La Direttiva nasce in seguito ad una revisione della precedente normativa NIS[17]

[16] Il testo della Direttiva 2555/2022 è visionabile nel sito istituzionale dell'Unione Europea, alla pagina: *digital-strategy.ec.europa.eu/it/policies/nis2-directive*

[17] Sul non completo funzionamento della Direttiva NIS v. SPAGNOLI, *Direttiva NIS 2: la sicurezza delle infrastrutture critiche, tra normativa e buone prassi*: «Per fare ciò, la Direttiva NIS aveva imposto degli obblighi di cyber sicurezza ai soggetti che forniscono servizi o svolgono attività economicamente rilevanti. Nella realtà dei fatti, però, si sono evidenziate notevoli divergenze nell'attuazione di questi obblighi da parte degli Stati membri con variazioni rilevanti in termini di tipo di obbligo, livello di dettaglio e metodo di vigilanza. Una serie di disparità che, come è facile immaginare, hanno comportato costi aggiuntivi e difficoltà applicative per le entità che offrono beni e servizi transfrontalieri. Inoltre, il riesame della Direttiva NIS ha evidenziato divergenze anche nelle

La NIS 2 viene estesa a un maggior numero di settori e servizi ritenuti vitali per le principali attività sociali ed economiche del mercato interno, di fatto superando la precedente differenziazione tra operatori di servizi essenziali e fornitori di servizi essenziali.

In particolare, oltre che agli operatori privati dei settori ritenuti "essenziali" dall'Unione europea, ovvero quelli dell'energia, dei trasporti, delle banche, delle infrastrutture dei mercati finanziari, dell'acqua potabile, della sanità e delle infrastrutture digitali (che comunque rimarranno soggetti alla Direttiva NIS fino alla sua abrogazione), la NIS 2 si applicherà anche ai fornitori di servizi digitali che operano nei seguenti settori: *e-commerce*; motori di ricerca; *cloud computing*; gestione dei servizi ICT, della pubblica amministrazione e dello spazio.

Per definire gli operatori a cui è rivolta la Direttiva, il criterio principale (ma non unico) è quello della dimensione del soggetto che può farlo definire essenziale piuttosto che importante.

Il tratto comune che attraversa tutte le diverse normative esaminate, dalla 231/2001 (con gli "innesti" legati ai reati informatici inseriti con la l.48/2008), alla normativa GDPR e NIS è rappresentato dalla sempre più evidente necessità di costruire dei modelli che siano in grado di alzare il livello di prevenzione del *cybercrime* all'interno dell'azienda attraverso uno schema organizzativo che sappia intercettare i rischi informatici derivanti sia dal mondo interno che da quello esterno all'azienda stessa.

Questo modello non viene disciplinato nei contenuti tecnici dal legislatore: c'è la consapevolezza che l'ente ha una capacità tecnica solutiva più avanzata e più rapida nell'aggiornarsi; altro obbligo comune ai vari modelli disposti da queste diverse normative è rappresentato dalla necessità di individuare, a titolo diverso, un interlocutore unico che sia punto di riferimento sia all'interno che all'esterno dell'azienda, e che nel caso della normativa GDPR e NIS sia in grado di interfacciarsi immediatamente con le *Autority* per comunicare l'eventuale incidente

modalità della sua stessa attuazione da parte degli Stati membri, ai quali è stata lasciata discrezionalità sulla delimitazione dell'ambito applicativo, oltre che sull'attuazione degli stessi obblighi in materia di sicurezza e segnalazione degli incidenti», in *Cybersecur.*, 2023, 5.

in corso; allo stesso modo, all'azienda spetta l'attività di formare i propri dipendenti, facendo assumere consapevolezza dei rischi operativi e dei comportamenti corretti da tenere.

4 - *Cybersecurity Act*

Successivo all'approvazione della Direttiva *NIS*, viene adottato un nuovo Regolamento volto a creare un quadro europeo per la certificazione della sicurezza informatica di prodotti *ICT* e servizi digitali, e a rafforzare il ruolo dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)[18], denominato *Cybersecurity Act*. Il Regolamento è stato pubblicato in Gazzetta Ufficiale il 7 giungo 2019 ed è entrato in vigore il 27 giugno 2019.[19]

Il *Cybersecurity Act* si inserisce all'interno della strategia dell'UE per la sicurezza cibernetica; l'obiettivo è rafforzare la capacità di resistere agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali. Lo strumento normativo in questione si affianca, ed è in parte complementare, alla prima normativa in materia di sicurezza cibernetica introdotta a livello dell'Unione, ossia la *Direttiva NIS*.

---

[18] Istituita nel 2004 l'ENISA (Agenzia dell'UE per la *Cybersicurezza*) sostituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione — che l'ha preceduta — ma ha un ruolo rafforzato e un mandato permanente. Fra i suoi compiti l'elaborazione di sistemi di certificazione della *cybersicurezza* che consentono maggiore fiducia nell'utilizzo di prodotti, servizi, e processi digitali, e la collaborazione con le organizzazioni e le imprese digitali, promuovendo la resilienza delle infrastrutture dell'UE. Il regolamento dell'UE sulla *cybersicurezza* ha rafforzato il lavoro dell'agenzia, che opera principalmente a beneficio delle organizzazioni pubbliche, supportando le industrie TIC (telecomunicazioni, fornitori di servizi Internet e società informatiche), e sostenendo gli Stati membri, le istituzioni dell'UE e altre parti interessate nella gestione degli attacchi informatici. L'ENISA non applica sanzioni; di fatto si tratta di una istituzione europea di supporto ed interlocuzione agli Stati membri, le istituzioni, gli organismi dell'Unione per il miglioramento della *Cybersicurezza*, oltre ad assumere con il *Cybersecurity Act* un ruolo di primo piano nella gestione del sistema di certificazione.

[19] Le informazioni e le considerazioni sono tratte dal sito istituzionale dell'Agenzia dell'Unione Europea per la *Cybersicurezza* (ENISA), enisa.europa.eu, e da *Agenda Digitale, agendadigitale.eu/sicurezza/cybersecurity-act.*

Il *Cybersecurity Act* si compone di due parti: nella prima vengono specificati il ruolo e il mandato dell'Enisa, mentre nella seconda viene introdotto un sistema europeo per la certificazione della sicurezza informatica dei dispositivi connessi ad Internet e di altri prodotti e servizi digitali.

Un primo punto chiave del *Cybersecurity Act* riguarda il rafforzamento dell'ENISA, che aveva avuto un ruolo principalmente nell'assistenza tecnica degli Stati membri e delle istituzioni europee nell'elaborazione delle politiche in materia di sicurezza delle reti e dei sistemi informativi, oltre rafforzare la capacità di prevenire, rilevare e reagire agli incidenti informatici. La gestione operativa degli incidenti informatici rimane però una competenza esclusiva degli Stati membri.

Con il *Cybersecurity Act*, l'ENISA diventa un organo permanente che mantiene i compiti di consulenza tecnica, ed assume anche attività di supporto alla gestione operativa degli incidenti informatici da parte degli Stati membri. All'ENISA spetta inoltre un ruolo di primo piano nella gestione del sistema di certificazione introdotto dal *Cybersecurity Act*.

Un altro punto chiave del *Cybersecurity Act* riguarda l'introduzione di un sistema europeo di certificazione della sicurezza informatica dei prodotti e dei servizi digitali. Ciò anche al fine di facilitare lo scambio degli stessi all'interno dell'Unione europea e di accrescere la fiducia dei consumatori nei medesimi.

La costituzione di schemi di certificazione specifici per prodotti e sistemi *ICT* non è di per sé una novità. Infatti, numerosi schemi di questo tipo già esistono nella maggior parte degli Stati membri. Ad esempio, in Italia, l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (*Iscom*, operante presso il Ministero dello Sviluppo Economico) già certifica la sicurezza informatica di prodotti e sistemi ICT secondo lo schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione istituito dal DPCM del 30 ottobre 2003. Analoghi schemi di certificazione esistono anche in altri Stati membri. Esempi ne sono la *Certification de Sécurité de Premier Niveau des Produits des Technologies de l'Information* (CSPN), in Francia; il C*ommercial Product Assurance* (CPA), nel Regno Unito; e il *Baseline Security*

Product Assessment (BSPA), in Olanda. Tuttavia, molti degli schemi di certificazione esistenti non vengono riconosciuti all'estero, o almeno non in tutti gli Stati membri. Ciò obbliga le imprese ad espletare vari processi di certificazione per operare a livello transnazionale. Ad esempio, la Commissione europea ha verificato come un fabbricante di contatori intelligenti (i cosiddetti "*smart meter*") che intenda vendere i propri prodotti in Germania, Francia e Regno Unito debba farli certificare secondo tre schemi differenti.

Il *Cybersecurity Act* intende ovviare ai problemi di cui sopra introducendo un quadro complessivo di regole che disciplinano gli schemi europei di certificazione della sicurezza informatica.

Gli schemi di certificazione previsti non sono tuttavia direttamente operativi, identificano invece una modalità operativa per la certificazione dei prodotti e servizi digitali, differenziata per specifiche categorie di prodotti e servizi, che se rispettata comporterà che i certificati rilasciati secondo tali regole saranno validi e riconosciuti in tutti gli Stati membri.

Una volta adottato uno schema europeo di certificazione da parte della Commissione, le aziende interessate potranno presentare domanda di certificazione dei propri prodotti o servizi a specifici organismi accreditati, salvo che lo schema di certificazione in questione non consenta alle aziende di procedere ad una autovalutazione di conformità (solo per prodotti e servizi a basso rischio). L'utilizzo della certificazione resta però volontario, a meno che la certificazione venga espressamente richiesta per determinate categorie di prodotti o servizi da specifiche norme di settore.

Progettualmente, quindi, gli schemi europei di certificazione andranno gradualmente a rimpiazzare gli omologhi schemi di certificazione nazionali.

Nelle intenzioni del legislatore europeo, l'istituzione di un sistema comune di certificazione di questo tipo favorirà 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 cose" o "*IoT*".

5 - Il Perimetro di Sicurezza Nazionale Cibernetica

Con la legge di conversione 18 novembre 2019, n. 133, al titolo "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica", il legislatore ha previsto l'istituzione del c.d. Perimetro di Sicurezza Nazionale Cibernetica (PSNC)[20].

Lo scopo è quello di assicurare un sempre crescente livello di sicurezza delle reti, dei sistemi informativi, e dei servizi informatici di interesse collettivo.

Al comma 1 dell'art. 1, viene affermato che questa normativa intende «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 e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale».

Saranno quindi da definire, fra l'altro, i soggetti, pubblici e privati, coinvolti; i vari obblighi e adempimenti cui questi soggetti sono tenuti, i rischi a cui sono esposti e le misure da adottare per fronteggiarli, ed ancora i poteri di certificazione, controllo, ispezione, prescrizione delle autorità governative, le norme in materia di acquisizione e utilizzazione delle tecnologie rilevanti.

Le nuove norme definiscono le finalità del perimetro e le modalità di individuazione dei soggetti pubblici e privati che ne fanno parte, nonché delle

[20] Per approfondimenti su tema v. fra gli altri PICOTTI – VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in *Sist. Pen.*, 2019, 12; IASELLI, *Sicurezza nazionale cibernetica: pubblicato il decreto legge*, in *Altalex.*, *2019*,09; Mele S., *Perimetro di sicurezza nazionale, come prende forma con il DPCM 131/2020, in Altalex., 2020, 11*; CATTANI – MULAZZANI -VEGNI, *L'importanza del perimetro di sicurezza nazionale cibernetico per la competitività delle aziende italiane*, in *Riskcompliance*, 2021,10.

rispettive reti, sistemi informativi e servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica;

Coinvolgono il Comitato interministeriale per la sicurezza della Repubblica (CISR) nella fase attuativa;

Stabiliscono un meccanismo di maggiore garanzia e sicurezza per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi di *information and communication technology* (*ICT*) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti;

Prevedono che l'esercizio dei poteri speciali in relazione alle reti, ai sistemi informativi e ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G sia effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa.

Sul piano penale il d.l. introduce all'art. 1 comma 11 una nuova articolata fattispecie a struttura "sanzionatoria"[21], che delinea diversi reati propri, a dolo specifico, che si sostanziano in falsità ideologiche "rilevanti" cui è accessoria, ed in un reato di omissione propria, tutti ascrivibili solo ai soggetti – pubblici e privati – aventi sede nel territorio nazionale, che siano inclusi nel "perimetro di sicurezza nazionale cibernetica" quale definito e disciplinato da detta nuova normativa.[22]

Com'è noto, il d.l. seppur istitutivo del Perimetro di Sicurezza Nazionale Cibernetica, rimanda l'attuazione del dettato normativo ad ulteriori provvedimenti. Pertanto, le condotte delittuose non sono compiutamente tipizzate nella fattispecie penale, in quanto gli obblighi giuridici, con relativi termini di adempimento, verranno definiti nel dettaglio da norme secondarie di attuazione.

[21] Cfr. art.1 co. 11: « Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni».

[22] Così PICOTTI – VADALÀ, *Sicurezza cibernetica*, cit., 12.

Viene quindi stabilito [23] che entro quattro mesi, con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) siano definiti i criteri con i quali i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica predisporranno e aggiorneranno con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza.

Entro sei mesi dalla stessa data i soggetti obbligati comunichino tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico che li inoltreranno al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica.

Al comma 6 dello stesso art. 1, alle lett. a) e c), si prevede che con regolamento da adottare entro dieci mesi siano disciplinati le procedure, le modalità e i termini con cui i soggetti obbligati, che intendano procedere all'affidamento a terzi di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, ne daranno preventiva comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, stabilendo poi in quale modo lo stesso possa procedere.[24]

Particolarmente importante ai fini di questa trattazione è il comma 11-*bis* dell'art.1[25]; si tratta di una modifica aggiuntiva effettuata in sede di conversione del

[23] Così art.1, co. 2, lett b)

[24]Viene riportato in chiaro che «entro quarantacinque giorni dalla ricezione della comunicazione, il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di *hardware* e *software* da compiere anche in collaborazione con i soggetti di cui al comma 2, lettera a), secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento».

[25] La formulazione precedente prevista all'art.11 riportava testualmente: «11. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote».

d. l. n. 105/2019, che inserisce le nuove fattispecie delittuose nel catalogo dei reati presupposto, la cui commissione comporta la responsabilità amministrativa da reato dell'Ente, ai sensi del d.lgs. n. 231/2001. Viene quindi modificato il comma 3 del suo art. 24-*bis*, riguardante i "delitti informatici", prevedendo la sanzione pecuniaria fino a quattrocento quote, oltre alle sanzioni interdittive stabilite dalle lett. c), d) ed e) del comma 2 dell'art. 9.

La modifica effettuata dalla legge di conversione è stata particolarmente opportuna ed ha superato l'anomalia che emergeva dal testo del d.l. n. 105/2019, in cui la responsabilità amministrativa degli enti per gli esaminati delitti era autonomamente prevista, ma senza inclusione espressa nel corpo del d.lgs. n. 231/2001.

Il primo di questi provvedimenti "di rimando" è rappresentato dal DPCM 131/2020 e, conformemente a quanto previsto nel d.l. ha come obiettivo, quello di chiarire i criteri e le modalità di scelta che guideranno il governo nell'individuazione dei soggetti pubblici e privati ricompresi al suo interno. Viene inoltre dato corso al primo degli adempimenti richiesti, ovvero quello di predisporre, comunicare e aggiornare periodicamente l'elenco delle reti, dei sistemi informativi e dei servizi informatici rilevanti per la sicurezza nazionale dell'Italia, in quanto indispensabili per l'esercizio di una funzione essenziale dello Stato o per la prestazione di un servizio essenziale per gli interessi dello Stato.

Il DPCM 131/2020 ha circoscritto l'ambito di applicazione del Perimetro, a soggetti che operano nel settore governativo con riferimento alle attività delle amministrazioni CISR nonché a ulteriori soggetti, pubblici e privati, coinvolti nei seguenti settori (ove non ricompresi in quello governativo): interno; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; tecnologie critiche; enti previdenziali/lavoro.

Un ulteriore tassello che va a completare il quadro normativo del Perimetro di sicurezza nazionale cibernetico, è rappresentato dal DPCM n.92 del 18 maggio 2022[26], con cui è stato reso noto il regolamento che definisce procedure, requisiti e

[26] Per un approfondimento in materia v. anche DELL'ARIA – FRANCHINA – ROSSI, l*a Cyber security che verrà: l'evoluzione normativa in Italia e Ue, in Agenda Digit., 2023, 1.*

termini per la convalida dei laboratori accreditati di prova (LAP)[27] a sostegno del Centro di Valutazione e Certificazione Nazionale (CVCN). Il 30 giugno è iniziata l'operatività del CVCN, per la valutazione di beni, sistemi e servizi ICT destinati a essere impiegati presso infrastrutture che supportano la fornitura di servizi o funzioni fondamentali per lo Stato. Il 30 luglio è entrato ufficialmente in vigore il Regolamento, dopo la pubblicazione nella Gazzetta Ufficiale n.164 del 15 luglio, mentre l'11 agosto sono state approvate le determinazioni tecniche previste in materia di accreditamento dei LAP.

6 - L'Agenzia per la *Cybersecurity* Nazionale

Con il D. L. 82/2021, viene istituita l'Agenzia per la Cybersicurezza Nazionale (ACN) che viene designata come Autorità nazionale competente e "punto di contatto unico" in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al d.lgs. NIS.

Con l'ACN si perde l'impostazione settoriale e frammentata impostata nel d.lgs. 65/2018 a vantaggio di una gestione e di un coordinamento unico, accentrato su questa nuova *Autority*, che diventa anche unico interlocutore transfrontaliero con ENISA e responsabile della attuazione del d.lgs.65/2018. I diversi Ministeri continuano ad operare come autorità di settore.

Si riportano alcune informazioni sull'ACN, assunte dal sito istituzionale: si tratta di un ente autonomo, con personalità giuridica di diritto pubblico, dotato di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, a cui sono state assegnate e trasferite le competenze nel settore della *cybersicurezza* prima distribuite su altri attori.

L'importanza della struttura è rimarcata dall'art.5: la nomina e la revoca del Direttore Generale e del Vicedirettore Generale è definita direttamente dal Presidente del Consiglio dei ministri.

[27] Laboratori Accreditati di Prova, per il supporto alle valutazioni e certificazioni del CVC.

Viene definito quindi un unico soggetto, punto di riferimento a livello nazionale, e punto di raccordo con le istituzioni sovranazionali, in particolare quelle europee. Di conseguenza, interagirà con il Centro europeo di competenza per la cybersicurezza, istituito con il Regolamento (UE) 2021/887, con l'obiettivo di rafforzare e garantire la sicurezza delle infrastrutture, delle reti e dei sistemi informativi digitali in settori cruciali.

L'Agenzia diventa unico punto di contatto nazionale per gli enti pubblici e privati sia per quanto riguarda le misure di sicurezza che per le attività di ispezione relative alla sicurezza delle reti, dei sistemi informativi e delle reti di comunicazione elettronica. Inoltre, essa promuove lo sviluppo della capacità nazionale di prevenire, monitorare e mitigare incidenti e attacchi informatici, con l'obiettivo di migliorare la sicurezza dei sistemi ITC dei soggetti inclusi nel perimetro nazionale di sicurezza informatica (intendendosi per soggetti che gestiscono, attraverso reti, sistemi informativi e servizi informatici, funzioni essenziali dello Stato, o servizi essenziali per il mantenimento di attività strategiche civili, sociali o economiche). All'ACN sono state trasferite anche tutta una serie di competenze dell'Agid.

Tra i principali compiti dell'Agenzia c'è l'attuazione della Strategia Nazionale di *Cybersicurezza*, adottata dal Presidente del Consiglio, che contiene gli obiettivi da perseguire entro il 2026.

Le prerogative assegnate sono sinteticamente definibili in:

Prevenzione e mitigazione: supporto ai soggetti pubblici e privati nazionali, che esercitano funzioni ed erogano servizi essenziali, nella prevenzione e mitigazione degli incidenti, nonché ai fini del ripristino dei sistemi.

Autonomia strategica: persegue la Strategia Nazionale di *Cybersicurezza* ed europea nel settore del digitale, in sinergia con il sistema produttivo e con il mondo della ricerca.

Certificazione e vigilanza: certificare e valutare prodotti e servizi informatici, conduce attività ispettive e di verifica per gli adempimenti normativi nel campo della *cybersicurezza.*

Cultura *cyber*: favorisce percorsi formativi per lo sviluppo della forza lavoro di settore e promuove campagne di sensibilizzazione e diffusione della cultura della *cybersicurezza.*

L'Agenzia, tramite il Servizio Autorità e Sanzioni, svolge le attività regolatorie e attuative della vigente disciplina in materia di *cybersicurezza*, sia di derivazione comunitaria che nazionale, garantendone il rispetto anche attraverso l'esercizio dei poteri sanzionatori.

Le attività sanzionatorie previste per l'ACN sono ricavabili dal decreto legislativo 3 agosto 2022, n. 123, che dispone:

Art.1 lettera c) la definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione con sanzioni effettive, proporzionate e dissuasive.

All'art 10 la normativa prevede che: l'Agenzia può comminare ordini o intimare diffide a coloro che operano in contrasto al quadro europeo di certificazione. Ai soggetti che non ottemperano nel termine indicato nell'ordine o nella diffida l'Agenzia commina la sanzione del pagamento di una somma da 200.000 ad 1.000.000 di euro.

Se le violazioni riguardano soggetti con fatturato pari almeno a 200.000.000 di euro, si applica una sanzione amministrativa pecuniaria non inferiore allo 0,3 per cento e non superiore all'1,5 per cento del fatturato, fermo restando il limite massimo di 5.000.000 di euro.

Come è evidente, si tratta di sanzioni di notevole capacità afflittiva.

Avverso le decisioni dell'ACN è inoltre prevista competenza funzionale inderogabile presso il Tar del Lazio.

L'ACN è una struttura giovanissima. L' attivazione dell'Organo ispettivo e di vigilanza è avvenuto nel mese di ottobre 2022, ed avrà il compito di svolgere attività di verifica tecnico-documentale e ispezione, concernenti gli adempimenti di *cybersicurezza* attribuiti all'Agenzia dalla normativa vigente, nei confronti dei soggetti pubblici e privati**.**

CAPITOLO V

IL MODELLO ORGANIZZATIVO DELL'ENTE COME STRUMENTO PER LA RESISTENZA AL RISCHIO-REATO INFORMATICO

SOMMARIO: 1. Il ruolo del Modello Organizzativo nei reati informatici. – 2. Il ruolo dell'Organismo di Vigilanza nei reati informatici. Il Codice Disciplinare – 3. La compatibilità dei meccanismi di controllo informatico con il GDPR e con la Legge 20 maggio 1970 n. 300 e successive modifiche (*Jobs Act*). 4. La compatibilità dei meccanismi di intervento sul software con la violazione del diritto d'autore. – 5. Rilievi conclusivi sui modelli di prevenzione del reato informatico

1. Il ruolo del modello organizzativo nei reati informatici

Come messo in evidenza in precedenza[1] il d.lgs. 231/2001, con innesti realizzati a partire dalla legge 48/2008, ha assorbito una serie di reati-presupposto di natura informatica da cui potrebbe scaturire responsabilità dell'ente.

Nella stessa sede si è specificato che detti reati sono sistematizzati in più modi; una prima classificazione li distingue in reati necessariamente informatici, che possono essere realizzati solo ed esclusivamente tramite lo strumento informatico, ed in reati che possono essere commessi *anche* (ma non solo) con lo strumento informatico.

Se viene considerato quanto generalizzato e diffuso sia l'uso di tali strumenti, per l'ente virtuoso che intendesse prevenire e minimizzare il rischio reato il numero di comportamenti da tenere sotto controllo dal punto di vista informatico è pertanto elevatissimo, ed è indispensabile una accurata attività metodologica affinché le maggiori cautele possano essere adottate. Il modo in cui l'ente si predispone per minimizzare il rischio-reato informatico passa ovviamente attraverso il Modello Organizzativo; questo potrà essere già esistente, e dovrà pertanto essere aggiornato

[1] *supra* cap.III

in funzione dei nuovi reati-presupposto, così come potrebbe essere creato *ex novo* in quanto inesistente.[2]

È bene mettere in evidenza da subito che fra le cautele e le attenzioni indispensabili a sviluppare un modello organizzativo che non violi a propria volta disposizioni di legge, ci saranno quelle ad osservare con attenzione il Regolamento UE 2016/679, in materia di trattamento dei dati personali[3] e lo stesso Statuto dei Lavoratori (legge 20 maggio 1970, n.300 e successive modifiche), in quanto le attività di controllo sui flussi informatici, indispensabili nelle prevenzioni dal rischio-reato, potrebbero avere impatti lesivi su queste normative, se non ben calibrate; allo stesso tempo, possono esserci interazioni con la legge 633/1941, relativa alla violazione del diritto d'autore (per inciso, violazione inserita fra i reati presupposto all'art. 25-*novies*),[4]in quanto le attività di controllo informatico sul *software* devono essere svolte in modo conforme alle autorizzazioni ed alle licenze fornite.

Anche per quanto attiene ai reati informatici l'attuazione delle strategie e degli indirizzi del Modello Organizzativo deve essere resa concreta e manifesta, attraverso un efficace processo, che intercetterà tutti i passaggi menzionati in precedenza: analisi del rischio, protocolli, procedure accurate, coinvolgimento dell'OdV, formazione, sanzioni disciplinari.

---

[2]Per approfondimenti si veda anche MONTI - LUPARIA*; Cybercrime e responsabilità da reato degli enti: prevenzione, modello organizzativo e indagini preliminar*i, Milano, 2022, 175. L' autore mette in evidenza come in un sistema aziendale maturo il tema della sicurezza informatica riguarda più modelli e non è funzionale alla sola 231/2001. In società di questa tipologia, a parte il Modello Organizzativo, sarà sicuramente presente la "*Security Policy",* che è un documento che « costituisce il fondamento dell'intera architettura di protezione delle informazioni e che rappresenta, secondo la formula utilizzata nel controllo *A.5.1.1* della norma internazionale di standardizzazione ISO 27001, "un insieme di politiche per la sicurezza delle informazioni [...]definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti"». Anche la *Security Policy* deve raccordarsi al Codice Etico e deve avere contenuto «precettivo, di norma emanato dal soggetto apicale dell'organizzazione, dal cui potere conformativo esso promana. In relazione ai reati informatici presupposti del citato d.lgs. n.231/2001, è lecito attendersi che la *security policy* contenga la formale espressione di inaccettabilità e la connessa dichiarazione di "tolleranza zero", nei riguardi di quelle condotte che oltre a costituire reato, rappresentano piena violazione dei principi fondanti dell'etica dell'organizzazione».

[3] *supra* cap.2, par.6.1

[4] Per approfondimenti sull'argomento, fra gli altri, DEZZANI – DELL'AGNOLA, *l'implementazione del modello organizzativo, gestionale e di controllo negli enti collettivi a seguito dell'inserimento dei reati informatici fra i reati presupposti ex d.lgs. 231/2001 operato dalla legge 48/2008*, in *La responsabilità amministrativa delle società e degli enti, Rivis. 231,* 2012, 02, 65ss.

L'attività non sarà solo basata sulla tecnologia, ma verrà sviluppata in modo organico: sarà quindi fra l'altro indispensabile un forte, adeguato continuo e convinto *commitment* da parte del vertice aziendale, e tanto dovrà essere affidato alle attività di formazione sui dipendenti in modo da migliorare la cultura del rischio aziendale anche su questi reati.

L'ente che voglia implementare il proprio Modello Organizzativo integrando le cautele necessarie a prevenire il rischio reato-presupposto informatico dovrà operare su più livelli. Seguendo la schematizzazione dei contenuti del MOG riportata nel precedente capitolo, innanzitutto sarà indispensabile aggiornare il proprio Codice Etico[5], che abbiamo detto esserne considerato parte integrante; poi, dovranno essere aggiornati tutti i protocolli operativi; allo stesso modo dovrà essere implementato il Codice Disciplinare; lo stesso OdV dovrà vedere estese le proprie attività ai controlli informatici.[6]

Il Codice Etico come noto enuncia principi e valori ai quali l'azienda si ispira e che considera da perseguire diffusamente. Potranno quindi essere inserite dichiarazioni che affermino ed enfatizzino: la necessità di un corretto utilizzo dello strumento informatico; la non accettazione di comportamenti che realizzino o consentano accessi abusivi a sistemi altrui, aggiungendo che l'ente rifugge dal danneggiamento di qualunque sistema informatico; considerata la delicatezza della materia, può essere opportuno inserire anche nel Codice Etico dichiarazioni in sintonia con la disciplina dell'utilizzo dei dati informatici in funzione della normativa *privacy*.

I protocolli, come messo in evidenza nel precedente capitolo, sono ascrivibili alla parte speciale del modello, pertanto entrano nel merito operativo aziendale. La prima valutazione che dovrà essere effettuata è relativa al rischio reato-presupposto informatico, seguendo lo stesso schema già adottato in sede di costituzione, ma implementando ovviamente le attività di analisi ai nuovi reati-presupposto inseriti. Si verificherà quindi la commissibilità di reati informatici in senso stretto, e si

[5] In realtà viene messo in evidenza che il Codice Etico potrebbe già essere aggiornato e contemplare regole e principi relativi ad un corretto utilizzo degli strumenti informatici in quanto l'art. 640-*ter* è presente ab origine all'interno della 231/2001, DEZZANI – DELL'AGNOLA, *L'implementazione del modello, cit., 65.*

osserveranno anche gli altri reati-presupposto realizzabili con strumenti informatici.

L'utilizzo di strumenti informatici si estende ormai in modo così generalizzato che è difficile trovare aree o processi operativi che non ne siano coinvolti; questo anche considerando che per realizzare un reato informatico non è necessario essere inseriti all'interno di un particolare processo, ma è sufficiente utilizzare anche un semplice *device* od un *personal computer*. Ben presente quanto sopra, quindi sarà molto probabile definire aree di rischio estese; ciò non toglie che si potranno comunque anche evidenziare, all'interno delle stesse, delle attività a maggiore rischio.

In presenza di aree di rischio particolarmente estese la soluzione più naturale per ridurre i potenziali pericoli può consiste nell'impedire in modo generalizzato gli utilizzi tramite mezzi tecnici; ad esempio, bloccare l'accesso ad *internet* costringendo gli utenti ad operare all'interno della *intranet* aziendale; più in generale, si deve in qualche operare per ridurre od eliminare la possibilità di installare autonomamente strumenti informatici, o di estrarre dati trasferendoli su *keys* di memoria personali.

Questo è tecnicamente possibile, ed in presenza di un protocollo che stabilisca in questo senso, oltre a stabilire che fra le regole di utilizzo non sono previsti i comportamenti sopra riportati, si potranno inserire dei *firewall* che impediscano accessi di vario tipo. Allo stesso modo dovrà essere regolamentato l'uso delle *e-mail*, la classificazione del materiale allegato e la non esportazione dello stesso, prevedendo anche dei *warning* informatici tutte le volte in cui una *e-mail* venga indirizzata verso l'esterno, a maggior ragione se contiene un allegato.

Tecnicamente è anche possibile bloccare, ad esempio, l'accesso ai *social-network* ed impedire l'acquisto e lo scarico di *software.*

Particolarmente importante è prevedere all'interno del sistema informatico la tracciabilità, innanzitutto degli ingressi, e poi delle attività svolte, attraverso dei *log,* che sono delle *"scatole nere"*[7] che registrano e memorizzano quanto accade

[7] In questo senso DEZZANI – DELL'AGNOLA , *l'implementazione del modello,* cit., 71.L'autore mette inoltre in rilievo che sarà opportuno in questo, come in altre situazioni analoghe di controllo, un preventivo accordo sindacale per evitare violazioni normative; viene anche sottolineato che «per

informaticamente; il protocollo ovviamente sarà molto chiaro nel disporre in modo trasparente, in modo che ogni dipendente abbia piena conoscenza e consapevolezza che le attività svolte sono oggetto di registrazione, precisandone modalità e limiti; questo avrà anche un probabile effetto dissuasivo nei confronti di chi volesse commettere un reato.

Considerata l'enorme possibilità di realizzare reati informatici, la presenza di *log* accurati e ben visionati/valutati dalle strutture preposte al controllo (anche l'OdV viene coinvolto in tal senso), viene considerato uno degli strumenti tecnici più efficace per ridurre il rischio.

Altro contenuto che i protocolli dovranno necessariamente prevedere è relativo al modo in cui la funzione informatica è organizzata, indicando in chiaro i diversi livelli di responsabilità, le deleghe assegnate, le responsabilità ed i poteri dell'amministratore di sistema e la sua stessa possibilità di delegare funzioni.

Verrà sviluppato un protocollo legato alle attività formative, che dovranno essere particolarmente accurate, ed in grado di fornire anche gli accorgimenti necessari per ridurre il rischio di reati-informatici (complessità di *password*, cura riservata delle stesse, *education* su *e-mail* sospette e rischio apertura allegati), e prevedere un protocollo di comunicazione interna che in caso di consapevolezza da parte del dipendente di una avvenuta potenziale violazione (ad esempio apertura di un *file* in una *e-mail* che poi si riveli proveniente da mittente dubbio), consenta una immediata segnalazione di *warning* alle strutture di controllo.

La revisione del protocollo e suoi aggiornamenti in una materia in così rapida evoluzione è ben più di una semplice eventualità; anche in questo caso l'OdV, come vedremo a seguire, ha un compito ben preciso.

---

quanto riguarda la registrazione di *Log* delle attività della rete informatica, è molto importante tener conto del provvedimento del Garante della *Privacy* intitolato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente all'attribuzione delle funzioni di amministratore di sistema" datato 27 Novembre 2008 e pubblicato sulla Gazzetta Ufficiale n. 300 del 24 Dicembre 2008. Con questo provvedimento viene reso obbligatorio il monitoraggio della rete con la registrazione di opportuni *Log* che consentano di prevenire accessi abusivi alla rete informatica eventualmente commessi da amministratori di sistema, di rete, di data base».

2. Il ruolo dell'Organismo di vigilanza nei reati informatici. Il Codice Disciplinare

Fra i compiti che rientrano nelle responsabilità dell'OdV[8], vi è quello di proporre di propria iniziativa agli organi di vertice l'implementazione del Modello Organizzativo; tutte le volte in cui durante le attività di continuo e sistematico monitoraggio dell'azienda e della normativa esterna, si renda necessario un aggiornamento dello stesso, l'Organismo di Vigilanza esprimerà un parere affinchè dal vertice aziendale vengano fornite congrue disposizioni realizzative. Si tratta di una incombenza ben precisa, che nel nostro caso è finalizzata alla novità rappresentata dall'inserimento di nuovi reati-presupposto a cui l'ente deve rispondere in modo organizzato predisponendo le necessarie cautele.

L'aggiornamento che l'OdV andrà a proporre riguarderà ovviamente tutte le parti del Modello, ivi comprese le attribuzioni dell'OdV stesso. In funzione del nuovo inserimento di reati-presupposto informatici, non cambia l'impianto dell'OdV, che resta quindi inalterato; piuttosto vengono estese le funzioni dello stesso, in quanto andranno ad esaminare la congruità, la completezza, la effettività, l'efficacia del Modello di Organizzazione anche sotto l'aspetto della prevenzione e delle cautele del rischio reato-presupposto di natura informatica.

Si pone dunque un problema di acquisizione di competenze informatiche, che dovranno essere tali da consentire all'OdV di potere operare con piena cognizione e capacità, anche considerato che l'inserimento di un esperto non realmente tale inficerebbe la capacità dell'ente di resistere all'attività indagatoria del giudice (il quale, a sua volta, si avverrebbe certamente di esperti nel verificare il MOG presentato dall'ente), in presenza di una attività di indagine legata alla presenza di un reato-presupposto da cui possa scaturire responsabilità.

Si può ragionevolmente supporre che l'OdV non possegga livelli di competenze del genere, che sono assolutamente specifiche e risiedono in funzioni diverse rispetto a quelle che solitamente vanno a comporre l'OdV (provenienza da *internal control* piuttosto che *legal*); si dovrà pertanto acquisire all'interno dell'organismo un membro in grado di risolvere questo *gap*, o, molto più facilmente, si farà ricorso a

[8] *Supra,* cap.II par.3

consulenti esterni a cui affidare l'incarico. In questi casi l'OdV si esprimerà in modo autonomo sulle proprie necessità, ed in modo altrettanto autonomo ed utilizzando il proprio *budget*, andrà a remunerare questa attività esterna. Sempre a tutela della propria autonomia e indipendenza, il *budget*, qualora non sufficiente, dovrà ovviamente essere rivisto e reso adeguato al compito assegnato.

Anche qualora dovessero essere presenti all'interno dell'ente una o più professionalità adeguate, in nessun caso, tuttavia, è immaginabile che questi compiti vengano svolti, ad esempio, dall'amministratore di sistema, che rappresenta, al contrario, una delle funzioni che per l'elevato livello di competenza e l'ampia serie di deleghe a proprie mani, esprime un alto rischio potenziale di commissione di reato informatico; e neanche è quindi immaginabile un inserimento dello stesso nell'OdV.

Per quanto riguarda invece l'implementazione e l'aggiornamento del Codice e del sistema disciplinare legato alla presenza dei reati informatici, si segue lo stesso meccanismo previsto per qualunque altro tipo di implementazione di reati-presupposto: sarà da aggiungere, con la consueta trasparenza, la comunicazione delle sanzioni legate alle nuove ipotesi di violazione.

3. La compatibilità dei meccanismi di controllo informatico con il GDPR e con la legge 20 maggio 1970 n. 300 e successive modifiche (*Jobs Act*)

Il controllo delle attività informatiche sviluppate nell'ambito delle attività lavorative dai dipendenti di un ente impatta sia sulla disciplina prevista nello Statuto dei Lavoratori, che con il GDPR, in quanto la necessaria invasività delle attività svolte rappresenta una interferenza costante con queste normative.

Il tema dei controlli sulle attività informatiche dei lavoratori non nasce certo con l'inserimento dei reati-presupposto informatici all'interno della 231/2001, ma in simile contesto viene amplificato alla massima potenza, perché il modo per prevenire un reato di questo tipo, all'interno di un ente, passa inevitabilmente attraverso il controllo del sistema stesso, e quindi indirettamente vengono coinvolti coloro che il sistema utilizzano.

Il meccanismo difensivo previsto originariamente nello Statuto dei Lavoratori a proposito dei controlli a distanza è stato innovato con il c.d. *jobs act* del 2015; uno dei fini della revisione normativa è stato indubbiamente di bilanciare al meglio le esigenze dei controlli datoriali e la tutela dei lavoratori, alla luce anche delle nuove tecnologie. Abbiamo ben presente come *pc, tablet*, siano allo stesso tempo preziosi strumenti di lavoro, ma potrebbero essere utilizzati come i più accurati sistemi di controllo, in grado di tracciare e registrare tutte le attività realizzate informaticamente dal dipendente nel corso delle giornate lavorative.

L'art.4 prevede che 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 sul lavoro e per la tutela del *patrimonio aziendale*, previo accordo collettivo stipulato con le Associazioni Sindacali, o in mancanza di tale accordo previa autorizzazione dell'Ispettorato Nazionale del Lavoro.

Al comma successivo viene stabilito che la disposizione appena riportata non si applica agli strumenti utilizzati dal lavoratore *per rendere la prestazione lavorativa* e agli strumenti di registrazione degli accessi e delle presenze: in questo caso le cautele previste al precedente comma non sono necessarie.[9]

Non è dubbio che i *personal computer* siano strumenti per rendere la prestazione lavorativa, e che possano essere anche (ma non solo) strumenti dai quali si può verificare l'accesso e la presenza. Ci si può dunque chiedere se l'ente ha la possibilità di disporre in modo autonomo protocolli di sicurezza informatica, senza il preventivo consenso o le autorizzazioni previste.

Senza addentraci in questa materia, è da riportare una sentenza della Corte di Cassazione (Sezione Lavoro, 12 novembre 2021, 34092[10]). La Corte ha precisato

[9] Il terzo comma dell'art.4 riporta poi che 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 previsto dal decreto legislativo 30 giugno 2003 n.196.

[10] Cfr. Cass. Sez. lavoro, 12 novembre 2021, 34092. La Corte, nell'affermare la legittimità dei controlli difensivi, ha tuttavia ribadito che «va riaffermato il principio, già richiamato, espresso dalla giurisprudenza di questa Corte formatasi nel vigore della precedente formulazione dell'art. 4 dello Statuto dei lavoratori, secondo cui in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore » e che occorre « dunque, nel

che, tenuto conto anche della elaborazione giurisprudenziale maturata nel vigore della disciplina precedente al *jobs act*, si deve andare a distinguere fra controlli difensivi in senso lato, che sono quelli 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 con tale patrimonio, e controlli difensivi in senso stretto, volti ad accertare, in presenza di indizi, condotte illecite di singoli dipendenti. Mentre quest' ultimi «anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situino, anche oggi, all'esterno del perimetro applicativo dell'art. 4», i primi dovranno essere invece realizzati nel rispetto delle previsioni dell'art.4.

Come concordemente ritenuto, i controlli informatici rappresentano dei c.d. controlli anelastici [11], e sono preventivi ed automatici, riguardano inoltre la generalità dei lavoratori; rientrano quindi all'interno delle situazioni disciplinate nel comma 1 dell.art.4, soggetti a limiti operativi e alla necessità di autorizzazioni e accordi sindacali. L'ente che voglia operare nel rispetto delle normative dovrà quindi avere cura di procedere ad un accordo preventivo con le Associazioni

rispetto della normativa Europea, e segnatamente dell'art. 8 della Convenzione Europea dei diritti dell'uomo come interpretato dalla giurisprudenza della Corte europea dei diritti dell'uomo, assicurare un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, con un contemperamento che non può prescindere dalle circostanze del caso concreto»; in *onelegale.wolterskluwer.it*

[11] Per un approfondimento sul tema dei controlli anelastici v. MONTI -LUPARIA*; Cybercrime e responsabilità*, cit., 272 «è pacifico che un *antivirus* controlli senza interruzione l'attività di un *computer*, compresi *file* generati dall'utente o ivi introdotti per i canali più diversi, dall'accesso a una risorsa di rete al *download* di un allegato a un messaggio di posta elettronica, al collegamento di un supporto di memorizzazione esterno al *computer*. È altrettanto fuori discussione che all'atto della rilevazione di un potenziale oggetto maligno, l'*antivirus* segnali l'evento all'utente e/o all'amministratore di sistema. Questo, tuttavia, non trasforma l'attività di monitoraggio del *software* di sicurezza in un controllo (anelastico) perché nemmeno indirettamente esso "entra nel merito" del contenuto, per così dire, "semantico" del file. In altri termini, con una metafora colorita ma efficace, si può dire che "il *computer* non sa leggere". La situazione è sostanzialmente diversa nel caso dei servizi di *IP* e *ID* perché questi si basano, invece, su liste di minacce e/o controlli euristici che associano il singolo *computer* dell'utente a specifici contenuti, come nel caso delle *blacklis*t che impediscono il raggiungimento di determinate risorse perché inopportune o palesemente illecite. Se, dunque, i servizi di *IP* e *ID* sono erogati a "memoria zero" —tenendo cioè traccia solo degli eventi che costituiscono una minaccia e non memorizzando gli altri — potrebbero concettualmente rientrare nella modalità di funzionamento da "analfabeta" che caratterizza il funzionamento base di un *antivirus*. Viceversa, se i servizi in questione sono erogati con un maggiore livello di intrusività nell'operato degli utenti rientrano in gioco tutte le problematiche alle quali si è fatto cenno in termini di condizioni per la lecita erogazione e fruizione del servizio».

Sindacali o ad ottenere le dovute autorizzazioni da parte dell'Ispettorato Nazionale (o Territoriale) del Lavoro.

Ancora, rimanendo in argomento, è possibile citare la sentenza 494/2021 del Tribunale di Venezia, [12] che ha ritenuto legittimo il licenziamento del dipendente che, navigando ripetutamente su siti non sicuri per fini personali, abbia messo a rischio la sicurezza dell'azienda.

Nel caso di specie, il comportamento del lavoratore aveva esposto l'azienda al rischio, che si era poi realmente verificato, di un attacco informatico; l'azienda aveva dovuto pagare un riscatto per poter recuperare i dati catturati e criptati. Il Tribunale ha ribadito, prendendo spunto dalla sentenza di Cassazione n. 4871 del 24 febbraio 2020, che «a fronte di una corretta informativa ai lavoratori, come nel caso di specie – l'articolo 4 dello Statuto dei lavoratori, così come modificato dall'articolo 23 del D.lgs. 151/2015 e integrato successivamente dal D.lgs. 185/2016 consente al datore di lavoro di effettuare controlli su tutti i dispositivi informatici in uso ai dipendenti, a condizione che sussistano i requisiti di cui ai commi 1 e 2 del predetto articolo 4. Condizione essenziale, a tal fine, è che venga fornita idonea notizia ai dipendenti circa le modalità di uso degli strumenti di lavoro e di effettuazione dei controlli c.d. "difensivi", nel rispetto di quanto previsto dal Codice della *Privacy*».

Fermo questo quadro normativo, possiamo citare una proposta mitigativa dell'Associazione Italiana *Internet Provider*[13], con 'obiettivo di attualizzare quanto più possibile la normativa in funzione delle crescenti necessità di un accurato controllo informatico da parte dell'ente. La proposta dell'Associazione era di semplificare «l'adozione delle misure di sicurezza eliminando l'obbligo di

[12] Tribunale di Venezia, sentenza 494/2021, con note di CAPOLUONGO, *Lavoratori: privacy verso controlli alla luce delle ultime pronunce*, in *Cyberlaws., 2021,11.*

[13] Così MONTI -LUPARIA*; Cybercrime e responsabilità da reato,* cit., 236, l'autore ricorda che la proposta effettuata si si tradusse nel chiedere l'aggiunta al Codice dei dati personali di un secondo comma dell'art.171: «Non costituisce violazione degli articoli 4 commi 1 e 2, e 8 della legge 20 maggio 1970 n. 300 l'adozione di misure di sicurezza per finalità di protezione delle reti pubbliche di comunicazioni, di servizi di comunicazione elettronica, di infrastrutture critiche e di sistemi informatici pubblici e privati», proposta che non fu comunque accolta; viene evidenziato inoltre che «una norma analoga è stata proposta il 18 novembre 2021 come emendamento all'Atto Camera 3354 che contiene la legge di conversione del decreto legge sul Piano nazionale di ripresa e resilienza, nella forma di un articolo 7-*bis* intitolato "Potenziamento delle misure di sicurezza di reti e sistemi informatici"».

autorizzazione della direzione territoriale del lavoro o dell'accordo sindacale quando la finalità delle misure di sicurezza è la protezione dei dati personali, prevedendo nel contempo il divieto di utilizzo dei dati eventualmente raccolti per finalità disciplinari, sanzionatorie o dirette all'interruzione del rapporto di lavoro». In questo modo, sarebbe stata resa «più agile la gestione della sicurezza dei dati, tutelando nel contempo il lavoratore in termini diretti (i dati non possono essere utilizzati nei suoi confronti) e indiretti (il Garante per la protezione dei dati personali e le autorità competenti possono sempre rilevare, in sede ispettiva, l'uso eccedente di questi dati e sanzionare di conseguenza il titolare del trattamento che ha abusato delle misure di sicurezza)».

In tema di GDPR, possiamo innanzitutto mettere in evidenza come, pur partendo da una logica comune, che è quella delle prevenzione e gestione del rischio tramite il modello organizzativo, e per quanto accomunate da un fine altrettanto comune, che è il rispetto della legalità, le necessità del GDPR e quelle della 231/2001 siano sostanzialmente opposte: il GDPR limita al massimo, per quanto possibile, le attività e le interferenze sui dati personali, anche in termini di archiviazione minima degli stessi; la 231/2001 al contrario tende a ridurre il rischio reato in presenza di grande invasività e stabile archiviazione e tracciamento di tutte le attività svolte.[14]

Di conseguenza anche qui l'ente potrebbe trovarsi nella situazione di realizzare un illecito sanzionato dal Garante della *privacy* per avere attivato sistemi di controllo non in linea con la normativa di tutela dei dati personali piuttosto che, come visto nell'ipotesi precedente, essere condannato dal giudice del lavoro per violazione della normativa dei controlli a distanza.

Come noto la normativa di riferimento è costituita dal Regolamento europeo in materia di protezione dei dati personali n. 679/2016 ("GDPR") adottato il 25 maggio 2016 e definitivamente applicabile dal 25 maggio 2018; e dal Decreto Legislativo n. 196/2003 ("Codice della *Privacy*") così come novellato dal Decreto Legislativo n. 101/2018; a tale normativa dobbiamo aggiungere una serie di

[14] Per note e riflessioni in argomento v. fra gli altri DI MAIO, *Prevenzione e dissuasione dei reati informatici,* cit., 185

provvedimenti e pareri emessi da autorità competenti, fra questi le Linee guida del Garante per posta elettronica e *internet.*[15]

Nella ben definita presenza di linee di principio salde, quali: il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice); il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), ed i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), osservando il principio di pertinenza e non eccedenza, trattando i dati "nella misura meno invasiva possibile", il Garante per la protezione dei dati personali raccomanda l'adozione da parte dei datori di lavoro pubblici e privati di un regolamento interno**[16]**, invitando anche ad una integrazione con le norme stabilite nello Statuto dei Lavoratori.

Seguendo schemi e contenuti che ormai ci sono familiari, nel regolamento sarà necessario specificare fra l'altro che tutti gli strumenti utilizzati dal lavoratore, quali *PC, notebook, tablet, smartphone, e-mail* ed altri strumenti informatici sono messi a disposizione dall'Ente unicamente per svolgere la propria attività lavorativa**.**

Sarà ricordato che nell'utilizzare gli strumenti informatici messi a disposizione dall'azienda, il dipendente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile, utilizzandoli

---

[15] Linee guida del Garante per posta elettronica e *internet*, in Gazzetta Ufficiale n.58 del 10 marzo 2007. Per approfondimento in materia anche MARTINI - PUDDA, *Controllo a distanza dei dipendenti: gli aspetti giuslavoristici, privacy e cybersecurity*, in *Agenda Dig.*, 2021,12. Fra le ulteriori fonti di riferimento citati dagli autori abbiamo il: «*Vademecum* dell'Autorità Garante del 15 maggio 2015 in materia di *privacy* e lavoro; le Linee-guida del Gruppo Articolo 29 adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 in materia di valutazione di impatto sulla protezione dei dati; il Parere n. 2/2017 del Gruppo Articolo 29 adottato l'8 giugno 2017 sul trattamento dei dati sul posto di lavoro; il Provvedimento dell'Autorità Garante dell'11 ottobre 2018 il cui Allegato 1 reca un elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto». Il Gruppo dell'articolo 29 per la tutela dei dati *(29 Working Party* o *WP29*) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati, oggi sostituito dall'EDPB il 25 maggio 2018 con il GDPR. L'EDPB (Comitato europeo per la protezione dei dati) è un organismo europeo indipendente. È l'organizzazione sotto la cui egida si riuniscono le Autorità nazionali per la protezione dei dati personali (Autorità nazionali di controllo) dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati (EDPS).

[16] Per approfondimento in materia anche BARONI, *Regolamento sull'uso degli strumenti informatici aziendali: ecco come redigerlo a norma GDPR,* in *Cybersec., 2019,11.*

esclusivamente per ragioni di servizio, e che comportamenti difformi possono causare gravi rischi alla sicurezza ed all'integrità dei sistemi aziendali e possono essere oggetto di valutazione da un punto di vista disciplinare oltre che da un punto di vista penale.[17]

Una ampia informazione come quella descritta, consente di ottemperare alla disposizione contenuta all'art.12 del GDPR, che stabilisce che «[…] il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 […] in forma concisa, trasparente, intelligibile e facilmente accessibile […]. Le informazioni sono fornite per iscritto o con altri mezzi, anche se del caso, con mezzi elettronici […]».

A livello tecnico-operativo, i controlli saranno svolti a campione (da parte degli amministratori di sistema su istruzione del titolare del trattamento e secondo le prescrizioni del Provvedimento dell'Autorità Garante del 28 novembre 2008), ed in nessun caso tali controlli verranno utilizzati per un monitoraggio dell'attività lavorativa del dipendente, nel rispetto delle disposizioni dello Statuto dei Lavoratori

[17] Linee guida del Garante per posta elettronica e *internet*, in Gazzetta Ufficiale n.58 del 10 marzo 2007., cit., 3.2: «Quest'ultimo esplicita anche le linee guida di un disciplinare interno, che ricalca attività che abbiamo già messo in evidenza nel corso della trattazione. Afferma il Garante che esso dovrà essere redatto in modo chiaro e senza formule generiche, e sarà da pubblicizzare adeguatamente ed aggiornare con periodicità, In esso verrà specificato se determinati comportamenti non sono tollerati rispetto alla "navigazione" in *Internet* (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di *file* nella rete interna; in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro); quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente; se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di file di *log*); se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime —specifiche e non generiche— per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni); quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete *Internet* sono utilizzate indebitamente; le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti; se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato; quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali; le prescrizioni interne sulla sicurezza dei dati e dei sistemi».

e dei provvedimenti autorizzativi (accordo sindacale o autorizzazione dell'Ispettorato competente).

Come emerge dalla sintesi sopra riportata, c'è piena considerazione sulla necessità del datore di lavoro di esercitare attività di controllo, e sul suo diritto/dovere; quello che si vuole assolutamente evitare è che vengano travalicati determinati limiti, rispetto alla persona fisica esaminata sotto i due punti di vista di lavoratore e di individuo, e che tutto avvenga nella massima trasparenza e consapevolezza del lavoratore stesso, evitando attività occulte. Da questo punto di vista le elaborazioni della legge da un lato (che prevede l'intervento di soggetti "forti" come le Associazioni Sindacali o l'Ispettorato – territoriale o nazionale – del lavoro), e del Garante dall'altro sono meccanismi che devono essere intesi come *di garanzia*: il datore di lavoro prima di implementare strumenti da cui possa derivare un controllo anche solo potenziale o indiretto dell'attività del lavoratore, è tenuto a osservare una serie di prescrizioni preliminari, che, come appena detto, rappresentano procedure di garanzia per il dipendente.

4. La compatibilità dei meccanismi di intervento sul software con la violazione del diritto d'autore.

La complessità tecnologica del mondo informatico ha fatto sì che nel tempo un numero relativamente contenuto di *Big Player* assumessero una posizione dominante in termini di capacità e qualità del servizio reso; gli enti, che hanno sempre più necessità di sistemi informatici attuali, performanti, sicuri, hanno quindi esternalizzato una serie sempre maggiori di servizi informatici (a titolo di esempio, la memorizzazione dei dati, piuttosto che alcune piattaforma applicative per la gestione dei clienti -*Customer Relationship Management* -*CMR* , o si pensi ai servizi di posta elettronica).

In questo modo l'ente ha ottenuto un servizio specializzato di maggiore qualità, risparmio di costi, una riduzione di complessità gestionali, ovviamente non operando più su propri prodotti informatici, ma legandosi contrattualmente ai vari fornitori sulla base di licenze d'uso; quest'ultimi provvedevano anche alle attività

di sicurezza sul sistema installato, attività quindi rivolte al proprio prodotto in modo generale e non personalizzate sull'azienda.

Nel tempo anche la protezione della rete informatica interna è diventata oggetto di parziale ulteriore esternalizzazione, sempre in funzione dei buoni principi aziendali prima espressi: servizio migliore perché svolto in modo specializzato da professionisti del settore, risparmio di costi, semplificazione organizzativa. Ha sicuramente contribuito in questa evoluzione l'aumento di complessità della rete informatica interna, composta spesso non più da un solo fornitore ma da apparati che fanno riferimento a più *player*, per soddisfare esigenze diverse.

All'interno di una rete informatica aziendale possono essere quindi essere presenti uno o più fornitori di *software*, e altri soggetti, sempre esterni all'ente, che hanno il compito di controllare all'interno della rete di quell'ente, il *software*, tramite altro *software* di sicurezza.

Nella evoluzione del sistema commerciale avviene poi che il produttore del *software* di sicurezza (per esempio un *antivirus*), è specializzato solo su questa attività, che viene distribuita tramite una piattaforma *online* a dei rivenditori, che a loro volta, tramite una sala di controllo, hanno accesso ai propri clienti.

Aumentano quindi gli operatori esterni all'ente (il produttore -o i produttori - del *software* e il rivenditore del sistema di protezione) che hanno accesso diretto a tutta la rete informatica ed ai personal computer dell'azienda.[18]

Si è quindi passati da un modello iniziale dove era presente un solo soggetto fornitore di servizi e cautele informatiche, ad un modello attuale molto più sofisticato dove diversi soggetti sono presenti, a diverso titolo, all'interno della rete aziendale, come proprietari di *software* o titolari di licenze d'uso, e l'azienda sarà

[18] Un cospicuo approfondimento in materia proviene da MONTI -LUPARIA*; Cybercrime e responsabilità da reato,* cit., 250ss. L' autore evidenzia come «questa ulteriore evoluzione della modalità di erogazione del servizio (si parla anche in questi casi di *security operation centre*— SOC) allunga ulteriormente la catena degli enti coinvolti nel garantire le obbligazioni contrattuali in materia di sicurezza informatica. Da un modello operativo nel quale produttore del *software* di sicurezza ed erogatore del servizio coincidevano, si passa ad uno schema nel quale il produttore gestisce la piattaforma tecnologica e un intermediario contrattuale interagisce direttamente con i sistemi informatici del cliente finale verificando, da un lato, la funzionalità dei servizi e, dall'altro, eseguendo le attività di aggiornamento e manutenzione» del sistema di sicurezza

legata contrattualmente ad ognuno di essi secondo le modalità stabilite in fase negoziale.

Sarà inoltre presente anche la struttura *IT* interna all'ente, che svolgerà le sue attività di miglioramento e di controllo operando sui *softwar*e esistenti, forniti, come abbiamo scritto, da terzi.

Nella contemporanea presenza di esigenze diverse in alcuni casi si possono avere situazioni dove l'adozione da parte del prestatore di servizi di sicurezza informatica di misure tecnologiche di protezione del proprio *software* genera danni al fruitore. Viene citato il caso dell'impiego di «"*bombe logiche*" — programmi informatici occultati in quello oggetto di utilizzo — che bloccano il funzionamento del *software* installato sul *computer* dell'utente al verificarsi di determinate condizioni che possono andare dall'uso non autorizzato al mancato rispetto delle condizioni contrattuali di licenza d'uso, pur in assenza di un accertamento giudiziale della responsabilità».[19]

Come interagiscono i vari interventi di *IT* piuttosto che di *security* su un *software* di proprietà od in licenza di terzi è materia di tipo contrattuale: in linea generale sia per chi offre servizi di *cybersecurity* sia per chi li utilizza, i termini dell'accordo sono quelli dell'esistenza e dell'efficacia scriminante del consenso dell'avente diritto rispetto a condotte che potrebbero generare diversi reati legati a violazioni di opere intellettuali.

Le complessità sono notevoli: tornando all'esempio dei servizi di verifica della sicurezza di un *software*, si mette in evidenza come «l'analisi del codice sorgente (il "progetto" dettagliato di come è fatto un programma per elaboratore) presuppone innanzi tutto la verifica delle condizioni giuridiche per l'esecuzione dell'attività. È infatti necessario assicurarsi che il committente abbia titolo per conferire ad un soggetto terzo l'esecuzione di analisi di sicurezza (non solo sul programma) e a quali condizioni. Astrattamente, un'azienda potrebbe avere la legittima disponibilità di codici sorgenti e documentazione tecnica, ma solo per uso interno e per attività di assistenza e manutenzione, ma non per altre finalità. Inoltre, il

[19] Così ancora MONTI -LUPARIA*; Cybercrime e responsabilità da reato,* cit., 250ss

software potrebbe essere composto da (o utilizzare esternamente) porzioni di codice informatico regolate da differenti regimi di proprietà intellettuale che, di conseguenza, dovranno essere valutate individualmente. Infine, pur essendo autorizzate anche le verifiche di sicurezza, potrebbero sussistere dei vincoli di riservatezza o degli obblighi di comunicazione al detentore dei diritti di proprietà intellettuale dei risultati ottenuti». [20]

Così anche potrebbe presentarsi il caso di un *software* legittimamente acquistato, tutelato da diritto d'autore, dotato di misure di protezione tecnologiche e che non preveda la possibilità di eseguire una "copia di riserva", che invece è indispensabile all'ente che utilizza tale *software* e che il titolare non consegna.

Un caso giudiziario concreto può fornire un esempio di quanto complessa è la tematica:[68] a fronte della necessità di una serie di verifiche di sicurezza informatica, un primario istituto bancario italiano, contatta la filiale italiana di una multinazionale statunitense operante nel settore *IT*. Il servizio che viene immaginato durante la fase di consulenza è un *penetration test*[21].

Sulla base di informazioni non corrette provenienti dai reparti commerciali, due tecnici della società informatica, ritenendo che l'accordo fosse già stato formalizzato, attaccano i sistemi della banca. Il contratto sarà in effetti formalizzato, ma questo avverrà successivamente all'attacco, che ha esito positivo in quanto il sistema viene violato: i tecnici installano nei sistemi informativi un *software* che avrebbe consentito nuovi accessi abusivi senza difficoltà. Un consulente informatico della banca si accorge dell'accesso (a tutti gli effetti) abusivo e sporge querela, da cui consegue il processo. Premesso che gli imputati sono stati assolti, quello che si intende mettere in evidenza è che la condotta dei tecnici, sulla base di

[20] Così ancora MONTI -LUPARIA*; Cybercrime e responsabilità da reato,* cit. L'autore riporta inoltre nella sua trattazione un caso concreto, ripreso e riportato in questa tesi (*un caso di studio*, 274); viene specificato che il caso non ha « riguardato l'imputazione 231 di un ente (impossibile, essendo i fatti stati commessi nel febbraio 2001 e dunque antecedenti seppur di poco alla pubblicazione in Gazzetta Ufficiale del decreto legislativo avvenuta il 19 giugno dello stesso anno)» ed è stato «deciso parzialmente dalla I sezione penale del Tribunale di Milano con sentenza n. 716 del 7 giugno 2006, poi integralmente riformata dalla Corte d'appello con sentenza n. 158 del 1 aprile 2008, (ed) è paradigmatico di ciò che può accadere a chi offre servizi di *cybersecurity* senza un adeguato governo dei processi di prevenzione dei reati-presupposto».

[21] Il *penetration test* è un test di sicurezza che consiste nel lancio di un falso attacco informatico per identificare eventuali vulnerabilità di un sistema.

non corrette informazioni, era certamente abusiva; non solo, nelle modalità di attacco (che come detto supponevano essere già contrattualizzate), hanno inoltre coinvolto altri soggetti, utilizzando prima il *router* di un operatore di telecomunicazioni e poi un *server* di *test* di un'istituzione pubblica come "sponde" per poi arrivare sulla rete della banca. Ed anche ammesso che ci fosse stata contrattualizzazione con relative manleve ad operare con la banca, queste avrebbero avuto validità nei confronti degli altri soggetti che sono stati coinvolti ed avrebbe retto alla valutazione giudiziale?[22]

Viene anche messo in evidenza che una situazione assimilabile a quella descritta, che sembrerebbe essere non rara, in cui si inizia ad operare sulla base di una successiva ratifica, in assenza di contrattualizzazione, certamente non reggerebbe una valutazione giudiziale positiva in ottica modello di servizio 231 nel dimostrare da parte dell'ente il controllo delle procedure di *cybersecurity*.

A conclusione, un ulteriore ambito del quale si dovrebbero occupare i protocolli relativi alle attività di controllo informatico è quindi rappresentato dalla verifica del *software* utilizzato, non solo nella logica del legittimo acquisto/utilizzo, e non solo per verificare la presenza di *software* non noto all'ente, ma anche per stabilire il riutilizzo legittimo di programmi, di dati ed informazioni, mappando analiticamente tutto quanto viene prodotto, utilizzato, licenziato, sub-licenziato da terzi, per evitare, che proprietà intellettuale sviluppata su commissione e di

[22] MONTI -LUPARIA*; Cybercrime e responsabilità da reato,* cit., 277 l'autore mette in evidenza che nel caso riportato l'assenza di querela non ha fatto esaminare questo aspetto, dando luogo ad una declaratoria di non procedibilità, ma che sarebbe stato di sicuro interesse verificare giudizialmente il limite dell'autorizzazione del committente e, inoltre, le pattuizioni sui metodi da utilizzare nell'esecuzione degli attacchi. Viene inoltre evidenziata l'importanza della chiara definizione del *dies a quo* «per l'avvio dei servizi e dunque per l'efficacia scriminante della manleva rispetto alle singole condotte poste in essere dal fornitore di servizi di *cybersecurity.* Capita di frequente, nella prassi, quello che è stato il *leit-motif* del processo milanese: il committente versa nella contradditoria condizione di avere necessità urgente di determinate prestazioni, la cui attivazione è frenata dalle procedure interne di autorizzazione all'acquisto dei servizi. È vero che, astrattamente, nulla vieta la ratifica, che *medio tempore* ci si può basare sugli elementi della trattativa per i quali c'è già un accordo e che le azioni compiute sulla base di un legittimo affidamento possono essere considerate non penalmente rilevanti. Tuttavia, dal punto di vista del modello organizzativo 231 questa condizione di incertezza costituisce chiaramente prova, a carico di chi eroga servizi del genere, dell'assenza di controllo sulle singole attività di *cybersecurity*».

esclusiva titolarità del committente venga riutilizzata in altri contesti senza le dovute autorizzazioni.

5. Rilievi conclusivi sui modelli di prevenzione del reato informatico

Riassumendo quanto esposto nelle pagine precedenti, nel ribadire le dichiarazioni di principio e valoriali presenti nel Codice Etico, l'ente deve avere come primo elemento di cautela di tipo organizzativo quello di realizzare una effettiva e reale separazione dei compiti all'interno delle strutture *IT*; questo vale in particolare per ruoli od aree che presentano un alto fattore di rischio, quali ad esempio quello di amministrazione di sistema e di gestione delle reti di amministrazione dei *data base* e *data entry*; l' area dei servizi di manutenzione tecnologica dei sistemi e delle reti; la gestione dei processi di *security*.

Altro elemento base è la perfetta conoscenza del proprio patrimonio tecnologico, della propria infrastruttura di rete, e di dove sono custoditi i dati. Ciò è di importanza fondamentale non solo in ottica di gestione della sicurezza delle informazioni, ma anche nel processo di efficace deterrenza ed esercizio dei controlli (*asset inventary*).

Ulteriore passaggio fondamentale è l'adozione del *least privilege:* rappresenta un preliminare obbligatorio che "il sistema" sia in grado di fornire o revocare diritti di accesso e di utilizzo di sistemi ed informazioni in funzione della corretta legittimazione formale, assegnando solo le abilitazioni legate ai compiti strettamente necessari per l'esecuzione delle proprie mansioni; questo principio presuppone, a sua volta, l'esistenza di un efficace sistema di controllo degli accessi, costantemente aggiornato ai profili utente (dinamica abilitazione e disabilitazione di credenziali).

L'ente dovrà essere sempre in grado di associare un evento al terminale dal quale è iniziato (*asset*), e a un'utenza (*identity*) e, quindi alla persona che quell'utenza stava utilizzando. Allo stesso modo l'ente avrà cura di limitare al massimo credenziali di accesso collettive (credenziali non individuali), o di accesso privilegiato. Ogni computer all'interno di una rete deve avere un metodo univoco di identificazione.

Il MOG inoltre conterrà informazioni aggiornate sulla possibilità che, nei casi di assenza del lavoratore (programmata o non) oltre un determinato periodo di tempo, l'Azienda possa adottare una procedura d'emergenza per l'accesso alla postazione di lavoro o sua casella di posta elettronica, affinché sia garantita la continuità lavorativa.

Asset e identity management sono indispensabili a realizzare un sistema di gestione degli incidenti e di tracciamento degli stessi; da non sottovalutare che questo consentirà per un verso un notevole effetto deterrente nei confronti dei dipendenti, e per altro, ai fini dell'idoneità e dell'efficienza del Modello, fornirà testimonianza ad un eventuale valutatore (il giudice) che l'ente si è ben organizzato.

A queste attività l'ente dovrà fare seguire comunicazioni, contenute nei protocolli, molto chiare, in grado di essere ben conosciute da tutti i dipendenti (e da coloro che dovessero interagire contrattualmente con l'ente).

Fra queste, innanzitutto, la dichiarazione relativa all'uso dell'*hardware* e del *software*, esplicitando la piena ed esclusiva proprietà dell'azienda, e con uso finalizzato esclusivamente alle esigenze e necessità aziendali, con divieto categorico di utilizzo per scopi personali.

Verrà specificato che il *software* utilizzato deve essere solo quello autorizzato dall'ente, con divieto di installazione di qualunque altro tipo di *software*, con esplicito riferimento anche a quelli in grado di violare le credenziali di accesso su altri sistemi o di elusione dei presidi di controllo, o che comunque risultino pericolosi per la sicurezza dei dati, dei sistemi e delle reti, dell'organizzazione e di terzi.

Il protocollo indicherà le condotte in contrasto con la legge e con il Codice Etico, con enumerazione meramente semplificativa e non esaustiva, indicando fra queste, anche nella specifica della prevenzione dei reati-presupposto, l'accesso abusivo a sistemi informatici o telematici; la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; la diffusione di programmi o parti di essi diretti a danneggiare o a interrompere sistemi informatici o telematici; l'intercettazione, l'impedimento o l'interruzione illecita di flussi di comunicazione

informatici o telematici; il danneggiamento di informazioni, dati o programmi informatici in qualunque forma e verso qualunque destinatario; la compromissione o danneggiamento di servizi di pubblica utilità; l'alterazione di contenuti di documenti informatici.

Verrà esplicitato il divieto di utilizzo della posta elettronica aziendale, per fini personali, e verrà reso edotto il lavoratore delle ipotesi e delle modalità con cui l'Azienda potrà legittimamente accedere alle comunicazioni aziendali e, eventualmente, salvarle sui propri sistemi.

Verranno previste nel protocollo, attività formative, che saranno volte a fare assumere consapevolezza al lavoratore su come utilizzare gli strumenti aziendali, quali comportamenti sono obbligatori (ad esempio, l'obbligo di proteggere i dispositivi con *password*, le modalità di archiviazione dei documenti ecc..), quali comportamenti sono vietati od a rischio (la manomissione dei dispositivi, la navigazione su siti *internet* non sicuri, l'utilizzo di supporti removibili).

Il lavoratore dovrà essere informato sulle modalità con le quali il datore di lavoro si riserva di effettuare controlli sull' utilizzo degli strumenti aziendali, anche saltuari o occasionali, indicando le specifiche ragioni che legittimano tali controlli (che possono essere legati anche a verifiche sulla funzionalità e sicurezza del sistema).

I controlli dovranno seguire il principio di gradualità: ad un preventivo controllo generale, basato su dati aggregati o anonimi – che potrà concludersi con avvisi generalizzati diretti agli incaricati dell'area o del settore in cui è stata rilevata l'anomalia – potrà seguire un controllo più specifico, anche su base individuale, giustificato da ulteriori anomalie. In questo caso il datore dovrà comunicare al lavoratore l'intenzione di procedere a controlli individuali, specificando l'oggetto, i motivi e le modalità del controllo. Va da sé, inoltre, che gli stessi saranno considerati leciti se rispettosi del principio di pertinenza e non eccedenza, quindi dovranno essere limitati nel tempo e strettamente connessi alla finalità perseguita.

Il lavoratore deve infine essere informato in modo preciso sulle conseguenze, anche di tipo disciplinare, che il datore di lavoro si riserva di trarre qualora constati che

gli strumenti elettronici e la posta elettronica siano utilizzati in modo indebito o scorretto e sulle misure delle sanzioni previste.

Sul sistema dei controlli e su quello disciplinare sarà indispensabile un accordo con le Associazioni Sindacali o con l'Ispettorato del Lavoro.

Una ultima considerazione rileva la gestione delle terze parti, che abbiano un rapporto con l'ente. Valgono le regole dell'analisi del rischio che vengono sviluppate nel MOG, e che sono legate anche alla natura del rapporto, alla nazionalità dell'azienda (restando nel tema della *cybersecurity* certo non si appalterebbero sistemi di controllo informatico ad una società che fa riferimento a paesi stranieri non graditi; restando nei nostri confini, un rapporto lavorativo con la Pubblica Amministrazione porterà a selezionare in modo molto attento i corrispondenti, seguendo regole ben stabilite nei protocolli). Sarà indispensabile la definizione di chiare clausole contrattuali, che ribadiscano i principi definiti nel codice etico e consentano in caso di violazione lo scioglimento del vincolo contrattuale, oltre ed eventuali penali.

CONCLUSIONI

L'analisi sin qui compiuta sulla responsabilità degli enti da reato informatico ha messo in luce l'importanza di prevenire reati di questa specie all'interno dell'impresa, alla luce della forte preoccupazione per la relativa invasività, pericolosità nonché per il loro aumento specie all'interno degli enti, che diventano contemporaneamente soggetti attivi e passivi dell'illecito.

Riprendendo alcuni dati del già citato *Rapporto Clusit* del 2023, relativo al 2022, oltre a mettere in evidenza il forte e continuo incremento del numero di illeciti informatici di cui si abbia notizia ufficiale, viene rilevato come gli enti siano fortemente coinvolti: il 67% delle grandi imprese ha dichiarato di avere subito un aumento dei tentativi di attacco rispetto all'anno precedente, il 14% dichiara di avere subito attacchi con conseguenze concrete; il 20% degli attacchi complessivi è stato rivolto verso strutture "gov" (pubblica amministrazione in senso generale).

In questo senso, dunque, l'innesto nel sistema 231 delle più importanti fattispecie informatiche deve essere salutato con favore. Il decreto prevede, infatti, l'istituzione di una struttura preventiva (che si incarna principalmente nel modello organizzativo), in grado non solo di minimizzare il rischio-reato, ma anche di diffondere la cultura della legalità e la formazione valoriale all'interno dell'ente, attraverso l'imposizione di comportamenti e controlli in linea non solo con il rispetto della normativa, ma con temi etici di cui l'ente diventa portatore sano ed integrato. L'intero sistema dei modelli organizzativi, insomma, è funzionale alla "tutela anticipata": l'ente è sempre più coinvolto nel prevenire il reato, piuttosto che ad essere manlevato da responsabilità nel momento in cui lo stesso viene realizzato.

Deve tuttavia rilevarsi, in questo scenario, un elemento di difficoltà, rappresentato dai costi di queste attività di *compliance*, che di fatto rendono più complessa la loro implementazione da parte delle imprese di dimensioni piccole, che, come abbiamo messo in evidenza, hanno difficoltà a seguire gli schemi previsti anche nella 231/2001.

Abbiamo però al contempo sottolineato come le aziende di dimensioni più grandi abbiano ormai assunto confidenza con questi meccanismi di controllo: si pensi non soltanto all'adozione dei modelli organizzativi previsti dalla 231/2001, ma anche all'ottemperanza alla normativa GDPR.

Se le società di dimensioni medio-grandi, e in particolare le società quotate in borsa, si sono dotate di strumenti, strutture organizzative, norme, regole interne atte a perseguire la legalità all'interno dell'azienda, creando e rafforzando tramite il modello organizzativo la cultura aziendale, la componente reputazionale, le esigenze di sostenibilità, nelle piccole imprese il tema dei costi di applicazione di un efficace modello organizzativo, la sovrapposizione fra titolare dell'impresa e gestore della stessa crea non poche difficoltà in ottica 231/2001 e quindi anche sul rischio reato informatico, il quale, come abbiamo visto, impone di inserire nel modello organizzativo anche presidi di tipo tecnologico.

In questo contesto, allora, sarebbe auspicabile la individuazione di metodologie meno onerose per assicurare anche alle imprese più piccole di raggiungere *standard* preventivi analoghi a quelli di aziende di dimensioni maggiori.

In definitiva, tuttavia, pur presenti tutte le difficoltà legate alla complessità ed alla dinamicità della complessa materia oggetto della nostra analisi, non possiamo che sottolineare e valorizzare l'importante evoluzione registratasi sia in termini di disciplina della responsabilità penale degli enti anche sul fronte dei reati informatici, sia sul piano dello sviluppo di innovativi meccanismi di coordinamento anche sovranazionale che impattano sugli enti nel settore strategico dell'informatica.

BIBLIOGRAFIA

Abriani, N.- Giunta, F., *L'organismo di Vigilanza previsto dal d.lgs. 231/2001. Compiti e funzioni*. *Rivista 231, in rivista 231.it*., 2012,03, 192ss

Amato, G., *Autore ignoto e responsabilità dell'ente, in "La responsabilità amministrativa delle società e degli enti", Rivista 231, rivista231.it,* 2015,4, 1

Amodio, E., *Prevenzione del rischio penale d'impresa e modelli integrati di responsabilità degli enti,* in *Cassazione Penale*, 2005

Antolisei, F., *Manuale di diritto penale , parte VI, Responsabilità degli enti*. Milano, 2014

AODV, *La modifica dell'art.6 del D.lgs.231/2001: critica ragionata all'attribuzione al collegio sindacale della funzione di organismo di vigilanza*. *aodv231.it*., 2012, 3

Arel, *Schema di disegno di legge di modifica del d.lgs. 231/2001*. *diritto penale contemporaneo, archiviodpc.it.*, 2010

Armone, G., *La Convenzione di Palermo sul crimine organizzato transnazionale e la responsabilità degli enti: spunti di riflessione*. *Rivista 231, in rivista231.it*., 2006, 03

Associazione italiana per la sicurezza informatica, *Rapporto Clusit 2022. Sito istituzionale Clusit.it*

Assonime, *Indagine sull'attuazione del decreto legislativo 231/2001*, *assonime.it*., 2008

Assonime, *L'organismo di Vigilanza nella prassi delle imprese a vent'anni dal d.lgs. 231/2001*, *sito istituzionale, assonime.it*.2021,10

Aterno, S., *Le fattispecie di danneggiamento informatico*, in Luparia (a cura di)*, Sistema penale e criminalità informatica,* Milano, 2009

Baroni, C., *Regolamento sull'uso degli strumenti informatici aziendali: ecco come redigerlo a norma GDPR*, *Cybersecurity 360, in cybersecurity360.it*., 2019, 11

Bartoli, R., *Il criterio di imputazione oggettiva* in Lattanzi-Severino (a cura di)*, Responsabilità da reato degli enti,* Torino 2022

Bartolomucci, S., *Sulla configurabilità del (fantomatico) modello organizzativo ex d.lgs 231/2001 dedicato alla PMI, Rivista 231, rivista231.it*, 2010,2, 100ss

Bellomi D. - Gentile F., *La Cassazione rileva la diversa natura del Piano Operativo per la Sicurezza e del Modello di Organizzazione, Gestione e Controllo, e*

statuisce che la violazione della normativa sulla sicurezza nei luoghi di lavoro non comporta in automatico la sanzione, *Giurisprudenza Penale Web*2020, 2

Beltrani, F., *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest, in Rivista231, rivista231.it,* 2008,4,4

Bernasconi, A.- Presutti, A., *Manuale della responsabilità amministrativa,* Milano, 2013

Borgobello, M., *La Cassazione sul rapporto tra accesso abusivo a sistema informatico, frode informatica e detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*, *Giurisprudenza Penale Web, giurisprudenzapenale.com*, 2020, 1

Borgobello, M, *Il reato di accesso abusivo a sistema informatico di cui all'art.615-ter c.p. alla luce della giurisprudenza più recente*, *Giurisprudenza Penale, giurisprudenzapenale.com*.2021, 02

Borsari, R. - Falavigna, F. *Whistleblowing, obbligo di segreto e "giusta causa" di rivelazione, Rivista 231, rivista231.it,* 2018, 02,41ss

Cadoppi, A., Canestrari, S, Manna, A., Papa, M., *Il diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme, in* Cybercrime. Torino, 2023

Capoluongo, A., *Lavoratori:* privacy *verso controlli alla luce delle ultime pronuncie (riferito a sentenza Tribunale di Venezia 494/2021)*. *Cyberlaws, in cyberlaws.it*, 2021, 11

Cardani, G., *Spunti di riflessione applicativi alla ordinanza del Tribunale di Milano del 20 dicembre 2004, Rivista 231, in rivista231.it*, 2004

Cartisano, M., *Reati informatici, più facile cooperare e condividere le prove: le novità dopo la firma del protocollo della Convenzione di Budapest*, *Agenda Digitale, in agendadigitale.eu*, 2022, 5

Cassazione. *Relazione n.III/01/2013.* Ufficio del Massimario 2013, 8

Cattani, G., Mulazzani, F., Vegni, M., *L'importanza del Perimetro di Sicurezza Nazionale Cibernetico per la competitività delle aziende italiane*, *Riskcompliance, in riskcompliance.it*, 2021, 10

Centonze, F., *La normalità dei disastri tecnologici - il problema del congedo dal diritto penale,* Milano, 2004

Centonze, F., *La responsabilità degli enti e la piccola e media impresa,* in AaVv *la responsabilità degli enti: dieci proposte di riforma*, Bologna 2016

Civello, S., *Una prima lettura della direttiva 2013/40/UE del Parlamento Europeo e del Consiglio, Diritto Penale Contemporaneo, archiviodpc.it*, 2013, 10

Commissione Grosso. *Relazione preliminare al Progetto di riforma del Codice Penale.* in sito *ministerogiustizia.it*, 2000

Commissione delle Comunità Europee. *Libro Verde: promuovere un quadro europeo per la responsabilità sociale delle imprese*, 2001,7

Concas, A., *Il crimine informatico*, *Diritto.it in diritto.it*, 2021,8

Consiglio d'Europa. Convenzione sulla criminalità informatica di Bucarest. *sito istituzionale coe.it*.

Cordero, F., *Procedura penale, processo penale amministrativo,* Milano, 2012

Cuniberti, M., Battista G., Micozzi, F., Aterno, S., *La legge di ratifica della Convenzione di Budapest del 23 novembre 2001*, *Altalex, altalex.it, 2014,3*

D'Agostino, A., *Il sistema di gestione della* privacy*, in il processo di adeguamento al GDPR, a cura di Cassano, Cerrina, Barbarossa,* Milano, 2022

D'Agostino, L., *I reati in materia di violazione del diritto d'autore, in Responsabilità da reato degli enti*, Milano, 2022

De Falco, G., *Interesse e vantaggio dell'ente in tema di salute e sicurezza del lavoro: dal risparmio di costi alle scelte globali di non sicurezza*, *Rivista 231, in rivista231.it*.

De Simone, G., *Profili di diritto comparato,* in Lattanzi - Severino (a cura di*) Responsabilità da reato degli enti,* Torino, 2022

De Simone G., *La responsabilità da reato degli enti, natura giuridica e criteri di imputazione*, *Diritto Penale Contemporaneo*, *dpc.it,2012,10,*19

De Simone G., *la colpevolezza dei soggetti metaindividuali: una questione tuttora aperta,* Milano, 2017

De Simone, F., *La rilevanza dei delitti contro l'intergrità dei dati dei programmi e dei sistemi informatici al tempo della guerra russo-ucraina*, *Giurisprudenza Penale, in giurisprudenzapenale.com*, 2022, 7

De Vero G., *La responsabilità delle persone giuridiche,* Milano, 2008

De Vero, G., *Il progetto di modifica della responsabilità degli enti tra originarie e nuove aporie, Rivista di diritto penale e process*o, 2010

Dell'Aria, D., Franchina, L., Rossi, M., *La* Cybersecurity *che verrà: l'evoluzione normativa in Italia e Ue*, *Agenda Digitale, in agendadigitale.it* 2023,1

Dezzani, G., Dell'Agnola, L., *L'implementazione del modello organizzativo, gestionale e di controllo negli enti collettivi a seguito dell'inserimento dei reati informatici fra i reati presupposti ex d.lgs. 231/2001 operato dalla legge 48/2008*, *Rivista 231, rivista231.it*., 2012, 02, 65ss

Dezzani G., Santoriello C., *Responsabilità delle società e violazioni della normativa sul diritto d'autore in materia di* software *ed informatica, Rivista 231, in rivista231.it*., 2012, 02, 3ss

Dezzani, G., *La criminalità informatica, Diritto.it, in diritto.it*, 2017,2

Dezzani, G., *Reati informatici*, *Diritto.it, in diritto.it*, 2017,2

Di Giovine, O., *Lineamenti sostanziali del nuovo illecito punitivo in Reati e responsabilità degli enti,* Milano, 2022

Di Giovine, O., *Il criterio di imputazione soggettiva*, in Lattanzi - Severino (a cura di), Responsabilità da reato degli enti, *Torino*, 2022

Faggioli, P., *Previtali, G., Delitti in materia di violazione del diritto d'autore e contromisure organizzative e tecnologiche, in responsabilità amministrativa degli enti*, *Rivista231, rivista231.it*, 2010,1

Fiorio, C., *Presunzione di non colpevolezza ed onere della prova*, *Rivista aodv231.it,1785, 8, 1*

Flor R., Papa, M., Cadoppi, A., Canestrari S., Manna, A., *Cyber Criminality*: *le fonti internazionali ed europee, in Cybercrime,* Torino, 2023

Garante per la protezione dei dati personali. (2022). *Relazione alla Camera.*

Garante della *Privacy*. (2021). *Relazione annuale 2021*. *garantedellaprivacy.it, sito istituzionale*.

Garante della *Privacy*. (2022). *Relazione annuale 2022*. *garantedellaprivacy.it, sito istituzionale*.

Giandomenico, S., *Brevi cenni sull'imputazione soggettiva del reato commesso dagli apicali e ruolo del giudice*. *La gestione del rischio come opportunità di crescita aziendale*, Foggia, *giurisprudenza penale web* 2017,12, 1

Grosso, C., *Progetto preliminare di riforma del codice penale. Ministero di Giustizia.it,* 2000

Gullo, A., *I modelli organizzativi,* in Lattanzi - Severino (a cura di)*, Responsabilità da reato degli enti,* Torino 2022

Gullo, A., *Reati informatici*, in Lattanzi - Severino (a cura di)*, Responsabilità da reato degli enti,* Torino 2022

Iaselli, M., *Sicurezza Nazionale Cibernetica: pubblicato il decreto legge*, *Altalex, in altalex.com*, 2019,9

Ielo, P., *Compliance Programs: natura e funzione nel sistema della responsabilità degli enti, modelli organizzativi e d.lgs. 231/2001*, *Rivista 231, in rivista231.it*., 2005, 99

Manna, A., *Rivista trimestrale di diritto penale dell'economia*, 2018, 4, 3ss

Marinucci, G., *Manuale di diritto penale,* Milano, 2020

Martini N., Pudda I., *Controllo a distanza dei dipendenti:gli aspetti giuslavoristici, privacy e cybersecurity*, *Agenda Digitale, in agendadigitale.eu*, 2021, 12

Mattarella, A., *La futura convenzione Onu sul cybercrime e il contrasto alle nuove forme di criminalità informatica, Sistema Penale, in sistemapenale.it*, 2022, 3

Mattarella, A., *Il cybercrime nell'ordinamento italiano e nuove prospettive dell'Unione Europea e delle Nazioni Unite, Rivista Penale, Diritto Penale e Processo*, 2022, 6, 809 ss.

Mattarella, A., *La futura convenzione Onu sul Cybercrime ed il contrasto alle nuove forme di criminalità informatica, Rivista sistema penale, in sistemapenale.it*., 2022, 3, 53s

Mele, S., *Perimetro di sicurezza nazionale, come prende forma con il DPCM 131/2020*, *Altalex, in altalex.com*, 2020, 11

Milani, A., *Boninsegna, M., I reati in materia di diritto d'autore e il modello organizzativo 231: configurabilità e prevenzione, in Responsabilità amministrativa delle società e degli enti. Rivista231, rivista231.it*., 2013, 3, 5ss

Monti, A.; Luparia, L., Cybercrime *e responsabilità da reato degli enti: prevenzione, modello organizzativo ed indagini preliminari*, Milano, 2022

Padovani, T., *Manuale di diritto penale*, *la responsabilità delle persone giuridiche,* Milano, 2023

Paliero, C., *La sanzione amministrativa come moderno strumento di lotta alla criminalità economica*, *Rivista trimestrale Penale Diritto Penale dell'Economia, 1993,* 1043ss

Paliero, C., Piergallini, C., *La colpa di organizzazione*, *Rivista 231, in rivista231.it*.,172

Piccinni, M., *Il reato di danneggiamento di sistemi informatici e telematici disciplinato quale presupposto dell'art.24 bis, d.lgs. 231/2001 per l'applicazione delle sanzioni in materia di responsabilità amministrativa delle società e degli enti*. *in Responsabilità amministrativa delle società e degli enti, Rivista 231, in rivista231.it*, 2017, 4, 2ss.

Picotti, L.,Vadalà, M., *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti, Sistema Penale, in sistemapenale.it*, 2019, 12

Picotti, L., *Il diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione di insieme. in Cadoppi A.,Canestrari S., Manna A., Papa M., Cybercrime , Torino, 2023,5*

Piergallini, C., *Paradigmatica dell'autocontrollo penale*. *Studi in onore di Mario Romano, AAVV.* , Napoli, 2013, 382ss

Pietropaoli, S., *Informatica criminale: diritto e sicurezza nell'era digitale,* Torino, 2022

Pistorelli, L., *Responsabilità da reato nella giurisprudenza di legittimità*, in "*la responsabilità amministrativa delle società e degli enti", Rivista 231, rivista231.it*, 2011,2

Polimeni, A., *Dpo, chi è il data Protection Officer e perchè è una figura controversa*", *Agenda Digitale, agendadigitale.eu*, 2022, 6

Presidenza del Consiglio dei Ministri. *Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico*. *in sito istituzionale Agid, Agid.gov.it*, 2023

Presutti, A., *Manuale della responsabilità degli enti*, Milano, 2018

Previtali, P., *Il reato di frode informatica ai sensi del d.lgs 231/2001: standard di controllo e procedure per la compliane del modello organizzativo, in Responsabilità amministrativa delle società e degli enti*, *Rivista 231, in rivista231.it*, 2017,1

Pusateri, V., *Sussiste il reato di danneggiamento informatico anche quando i file cancellati possono essere recuperati, Diritto Penale Contemporaneo, in archiviodpc.org*, 2012,4

Relazione di Ratifica - Convenzione di Budapest, 23/11/2001*, Ministero della Giustizia.*, *ministerogiustizia.it*

Relazione Ministeriale. *Relazione Ministeriale d.lgs 231/2001.* AODV231.it, 2001

Romolotti, T., *Modello organizzativo e corporate social responsability: la via etica alla 231*, *Rivista 231, in rivista 231.it*, 2009, 2

Rordof, R., *Criteri di attribuzione della responsabilità.I modelli organizzativi e gestionali idonei a prevenire i reati*, *Società e modello 231,* 2001

Rossi, A., *Responsabilità degli enti: i soggetti responsabili*, *Rivista 231, in rivista231.it*.,1

Salcuni, G., *Brevi cenni sull'imputazione soggettiva del reato commesso dagli apicali e ruolo del giudice*, *Giurisprudenza penale web*, 2017, 12, 1s, 3s

Salvatore, A., *Il Codice Etico : rapporti con il Modello Organizzativo nell'ottica della responsabilità sociale dell'impresa*, *Rivista 231, in rivista231.it*, 2008, 4, 71s

Salvatore, A., *La validazione giudiziaria del modello organizzativo*, *Rivista 231, rivista231.it*., 2023, 3, 234

Santi, F., *Responsabilità da reato degli enti e modello di esonero,* Milano, 2016

Santoriello, C., *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti*, *Rivista "31, in rivista231.it*, 2011, 1

Santoriello, C.; Dezzani, G., *Il reato di accesso e trattenimento "abusivi" nel sistema informatico e la responsabilità amministrativa delle persone giuridiche*, *Rivista 231, in rivista231.it*., 2012, 1 57ss

Sarzana di S. Ippolito, *La legge di ratifica della Convenzione di Budapest: una gatta legislativa frettolosa*, in Diritto Penale e Processo, 2008, 12

Scaroina, E., *Principi generali,* in Lattanzi - Severino *(a cura di), Responsabilità da reato degli enti,* Torino 2022

Schettino, F.; Lupariello, M., *La difesa degli enti e dagli enti nel d.lgs. 231/2001,* Milano, 2019

Segretario Generale Consiglio d'Europa. *Discorso del Segretario Generale alla Conferenza di apertura alla firma del secondo protocollo aggiuntivo alla Convenzione sulla Criminalità Informatica*, *sito istituzionale, coe.int*.

Singh, D., *Whistleblowing e riservatezza nel D.Lgs. n. 24/2023*, *Altalex, altalex.com*., 2023, 7

Spagnoli, C., *Direttiva Nis 2: la sicurezza delle infrastrutture critiche, tra normative e buona prassi, Cybersecurity 360, in cybersecurity360.it*, 2023, 5

Trinchera, T., *Diritto penale contemporaneo, Dpc.it, 2021*

Uricchio, G, *Modello di privacy e modello organizzativo*, *Altalex, in altalex.com*, 2021, 4

Valentini, A., *GDPR cyber security, le regole normative e le misure tecniche, Cybersecurity360, in cybersecurity360.com*, 2021, 6

Vitale, F., *Brevi riflessioni sul reato di frode informatica: i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo del cybercrime*, *Archivio Penale, in archiviopenale.it*, 2015, 1, 9ss.

Zanellati, P., *Valutazione e prevenzione del rischio privacy*: *adempimenti tra GDPR e d.lgs.231*, *Cybersicurity360, in cybersicurity360.com*, 2020, 2

GIURISPRUDENZA

Corte di Cassazione Penale; Sezione VI, 3067 (dicembre 14, 1999), in *Massimario - 24356, avvocato.it*

Corte di Cassazione Penale, Sezione V, 12732 (dicembre 6, 2000), in *Diritto Penale Contemporaneo, archiviodpc.it*

Corte di Cassazione Penale, Sezione V, 4576 (novembre 24, 2003), in *onelegale.wolterskluwer.it*

Tribunale di Milano, Ordinanza (novembre 11, 2004), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione II, 3615 (gennaio 30, 2006), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione V, 11689 (febbraio 6, 2007), *Mass. Uff. 236221, avvocato.it*

Corte di Cassazione Penale, Sezione V, 2534 (dicembre 20, 2007), in *Altalex, altalex.com*

Corte di Cassazione Penale, Sezione VI, 39290, (ottobre 8, 2008), in *Altalex, altalex.com*

Corte di Cassazione Penale, Sezione V, 2987 (dicembre 10, 2009), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione VI, 27735 (febbraio 18, 2010), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione V, 39620 (settembre 22, 2010), *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione VI, 2251 (ottobre 5, 2010), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione II, 9891 (febbraio 24, 2011), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione I, 17748 (aprile 15, 2011), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione III, 15657 (aprile 20, 2011), in *onelegale.wolterskluwer.it*

Corte di Cassazione, Sezioni Unite, 4694 (ottobre 27, 2011), in *Archivio Penale, archiviopenale.it*

Corte di Cassazione Penale, Sezione V, 8555 (novembre 18, 2011), in *Diritto Penale Contemporaneo, archiviodpc.it*

Corte di Cassazione Penale, Sezione V, 20060 (aprile 9, 2013), in *Rivista Giurisprudenza Penale, giurisprudenzapenale.com*

Corte di Cassazione Penale, Sezione V, 22024 (aprile 24, 2013), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione V, 4677 (dicembre 18, 2013), in *Diritto Penale Contemporaneo, archiviodpc.it*

Corte Europea Diritti dell'Uomo, 18640/10 (marzo 4, 2014), in *onelegale.wolterskluwer.it*

Corte di Cassazione, Sezioni Unite, 10561 (gennaio 30, 2014), in *Diritto Penale Contemporaneo, archiviodpc.it*

Corte di Cassazione, Sezioni Unite, 38343 (settembre 18, 2014), in *Giurisprudenza Penale, giurisprudenzapenale.com; onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione IV, 18073 (aprile 29, 2015), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione IV, 31003 (luglio 16, 2015), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione I, 35818 (settembre 2, 2015), in *Rivista231, rivista231.it*

Corte di Cassazione, Sezioni Unite, 41210 (settembre 8, 2017), *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione VI, 9047 (gennaio 31, 2018), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione II, 21987 (maggio 20, 2019), in *Giurisprudenza Penale, giurisprudenzapenale.com*

Corte di Cassazione Penale, Sezione VI, 43656 (settembre 24, 2019), in *onelegale.wolterskluwer.it*

Corte di Cassazione Civile, Sezione Lavoro, 4871 (febbraio 24,2020), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione V, 34296 (dicembre 2, 2020), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione VI, 15543 (gennaio 19, 2021), in *Osservatorio 231, osservatorio-231.it*

Corte di Cassazione Penale. Sezione IV, 32889 (gennaio 8, 2021). In *dejure.it*

Tribunale di Venezia, sentenza 494 del 2021, in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione IV, 22256 (giugno 8, 2021), in *Giurisprudenza Penale, giurisprudenzapenale.com*

Corte di Cassazione Sezione Lavoro, 34092 (novembre 12, 2021), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione IV, 18143 (febbraio 15, 2022), in *onelegale.wolterskluwer.it*

Corte di Cassazione Penale, Sezione IV, 570 (gennaio 11, 2023), in *Giurisprudenza Penale, giurisprudenzapenale.com*

Corte di Cassazione Civile; Sezione I, 27189 (settembre 22, 2023), in *Altalex, altelex.com*

.