GIURISPRUDENZA PENALE

RESPONSABILITÀ DEGLI ENTI: PROBLEMATICHE E PROSPETTIVE DI RIFORMA A VENTI ANNI DAL D. LGS. 231/2001

2021/1-BIS

Reati informatici e tutela dei dati personali: profili di responsabilità degli enti.

di Paolo Balboni e Francesca Tugnoli

16 Reati informatici e tutela dei dati personali: profili di responsabilità degli enti.

di Paolo Balboni e Francesca Tugnoli

Abstract
Gli autori si propongono di analizzare i rapporti tra i reati informatici e il conseguente trattamento illecito di dati personali connesso alla commissione di tali fattispecie. In particolare, verrà approfondito il legame sussistente tra i modelli organizzativi privacy e i modelli di organizzazione e gestione redatti ai sensi del D.lgs. 231/2001, anche in un'ottica di creazione di modelli di gestione integrata dell'ente. Infatti, solo un adeguato presidio privacy che sia efficacemente intersecato con i modelli organizzativi 231 consente all'ente di prevenire adeguatamente la commissione dei reati informatici, ciò anche alla luce delle previsioni di cui all'art. 32 del Regolamento UE 679/16 che impongono alle società di dotarsi di misure tecnico organizzative adeguate alla tutela dei dati personali. Infatti, è solo tramite l'adozione di tali misure di sicurezza che i protocolli allegati alla parte speciale dei modelli potranno definirsi adeguati e idonei a prevenire i rischi di commissione di reati informatici.
Nella seconda parte del contributo, verranno approfondite alcune aree di esposizione a rischio per gli enti, quali la gestione della casella di posta del dipendente da parte del datore di lavoro, nonché le nuove forme di remote working/smart working che si sono rivelate essere foriere di pericoli di esposizione delle società ad attacchi informatici ed infine nuove forme frequenti di attacco, come i ransomware.
In conclusione, verrà analizzata una prospettiva di riforma che possa introdurre tra i reati presupposto quelli di cui agli artt. 167 e ss del Codice Privacy Novellato.

The authors analyze the connection between the cybercrimes and the data protection law. In particular, this article studies the relationship between the Privacy Organizational Model and the Organizational Model pursuant the Italian D.lgs. 231/2001, focusing on the possibility to create an Integrate Organizational Model who is compliant to all the different normative applicable. In fact, only with an adequate data protection linked with Organizational Model pursuant the 231 it is possible for the legal entity to prevent the commission of cybercrimes. This aspect is analyzed also under the provision of the art. 32 of the Regulation EU 2016/679, who imposes to the companies to adopt adequate technical and organizational measure to protect personal data. Only thanks to that measures that the protocols attached to the special part of the Model 231 could be adequate and suitable to prevent the risks of the cybercrimes.
In the second part of this contribution, there is a focus on the new area of risk for the legal entities, as the correct use of the corporate email box of the employers, smart working as a new dangerous space of exposition from cyberattack and the new type of ransomware attack.
In conclusion, a reform perspective will be analysed that could introduce among the predicate offences those referred to in articles 167 et seq. of the Revised Privacy Code.

Sommario

6.4. Profili di diritto definitorio: il concetto di abusività che pervade le norme incriminatrici informatiche - **7.** Prospettive de iure condendo - **8.** Conclusioni.

1. Introduzione

Con l'entrata in vigore del Regolamento Europeo 679/2016 (di seguito "Regolamento"), anche la disciplina ex D.lgs. 231/2001 richiede di essere ripensata alla luce di una nuova idea di compliance integrata.

2. I reati informatici e il trattamento illecito di dati personali: profili di interdisciplinarità

La rubrica dell'art. 24 *bis* del d.lgs. 231/2001, come noto, richiama chiaramente il "*trattamento illecito di dati personali*" ancorché, poi, l'elencazione contenuta nella disposizione non citi nessuna delle fattispecie di cui agli artt. 167 e ss del Codice Privacy novellato. A ben vedere, occorre ricordare come il d.l. n. 93/13 avesse inizialmente disposto l'inserimento delle fattispecie incriminatrici del Codice della privacy (artt. 167,168 e 169) nel novero dei reati presupposto previsti dall'art. 24 *bis* d.lgs. 231/2001 ai fini della responsabilità amministrativa da reato degli enti[1] e, in particolare, proprio tra i 'reati informatici e il trattamento illecito di dati' di cui all'art. 24 *bis* del decreto citato. Tuttavia, in sede di conversione del suddetto decreto-legge, il riferimento esplicito ai delitti privacy è venuto meno, probabilmente per limitare l'impatto che tale nuova impostazione avrebbe comportato sugli enti, anche in considerazione della mole di dati gestiti dagli enti e della quantità di attività di trattamento svolte[2].

Dell'iniziale intento legislativo è rimasta tuttavia la rubrica della norma che mantiene il richiamo al trattamento illecito di dati personali in ragione o di una dimenticanza o, più probabilmente perché – inevitabilmente – in caso di commissione di reati informatici, si intersecano profili di interdisciplinarità con un trattamento illecito di dati personali. Infatti, se si pensa a qualunque delle fattispecie richiamate nel decalogo dei reati indicati all'art. 24 *bis*, si verifica anche un illecito trattamento di dati, tanto che, la società, sia essa titolare o responsabile del trattamento[3], deve avviare le indagini interne al fine di verificare se vi sia stata anche una compromissione dei dati personali trattati ed eventualmente aprire la procedura per la gestione dei casi di violazione dei dati personali ai sensi degli artt. 33 e 34 del Regolamento.

A parere di chi scrive, quindi, l'intento del legislatore, quando ha redatto la rubrica della norma, nonostante l'eliminazione dal decalogo dei reati presupposto dei delitti privacy, è stato quello di sottolineare i profili di interconnessione che sussistono tra l'illecito trattamento di dati personali e i reati informatici.

A ciò si aggiunga che tra le varie tipologie di attacchi informatici ve ne sono diversi che sono spesso caratterizzate da una osservazione – illecita – delle abitudini del soggetto targettizzato volta ad acquisire il maggior numero di informazioni possibili. In altre parole, "*ciò che l'utente medio non attenziona è il valore dell'informazione ed è proprio K.D. Mitnick, un noto informatico e storico hacker statunitense, che parla del "valore nascosto dell'informazione". Qualunque tipo di informazione ha un suo valore economico, che sia poco utile o irrilevante, perché qualsiasi dato che entra in interconnessione con altri dati può consentire di risalire ad infinite informazioni sempre più importanti o significative*"[4]. È evidente, dunque, come quando si affronta il tema dei reati informatici non può non venire in rilievo la tutela e la disciplina in materia di riservatezza e di protezione dei dati personali.

A livello di compliance aziendale, i riferimenti normativi da tenere in considerazione quando si affronta la cybersecurity sono dunque la l. 48/08 che ha introdotto nel novero dei reati presupposto i reati informatici, la Direttiva NIS (2016/1148) attuata in Italia con il D.lgs. 65/2018 e il D.l. 105/2019 in materia di costituzione del Perimetro di Sicurezza Nazionale Cibernetica. Inoltre, si aggiunga la normativa ISO/IEC 27001:2013[5]. Lato privacy ovviamente il Regolamento e il Codice Privacy novellato, oltre ai Provvedimenti del Garante Privacy italiano che seppur fonte di normativa di rango secondario, costituiscono norme vincolanti in materia[6].

3. I reati informatici quale presupposto della responsabilità ex D.lgs. 231/2001

I reati informatici sono disciplinati dall'art. 24-*bis* del D. lgs. 231/2001. Di seguito verranno esaminate le relative fattispecie di reato con esempi di possibili modalità di condotta rilevante per la responsabilità dell'ente.

Accesso abusivo al sistema informatico (615 ter c.p)

Anzitutto, viene punito l'accesso abusivo al sistema informatico ai sensi dell'art. 615 ter c.p. Il delitto viene, come noto, commesso da chi 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 il diritto di escluderlo. Secondo la giurisprudenza ormai consolidata, ne consegue che risponde del delitto in esame anche chi abbia usato il proprio accesso al sistema per il perseguimento di scopi estranei a quelli per i quali era stato autorizzato[7]. Al fine di verificare quando la condotta di accesso sia illecita assume rilievo dunque sia il concetto di abusività che deve appunto caratterizzare l'accesso, sia la presenza di misure di sicurezza[8].
Il reato può essere commesso, ad esempio, nell'ipotesi in cui vengano violati sistemi informatici allo scopo di alterare i dati relativi alla fatturazione dei servizi resi e realizzare un profitto illecito, acquisire informazioni relative alla clientela utili per elaborare strategie di marketing, ovvero allo scopo di acquisire informazioni riservate, ecc.

***Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici* (art. 615-*quater*, c.p.)**
Il delitto è commesso da chiunque, al fine di procurare a sé un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.
Il reato deve ritenersi integrato sia nell'ipotesi in cui il soggetto sia in possesso legittimamente delle credenziali di accesso (è il caso, ad esempio, dell'amministratore di sistema) e le comunichi indebitamente a terzi, oppure nel caso di cui detto soggetto se le procuri indebitamente. La condotta è abusiva quando i codici di accesso siano ottenuti a seguito della violazione di una norma o di una clausola contrattuale che vieti quella condotta. Inoltre, rientra nell'alveo di punibilità della disposizione incriminatrice anche il caso di chi rilascia indicazioni o istruzioni per la ricostruzione del codice di accesso al fine di consentirne un indebito utilizzo.
Ipotesi di commissione del reato si rinvengono nel caso di detenzione ed utilizzo di password per l'accesso alle caselle mail dei dipendenti allo scopo di controllare l'attività, svolta oppure nel caso di un attacco di social engineering[9] al fine di individuare le credenziali di accesso ad un sistema di un concorrente.

Diffusione di apparecchiature, dispositivi, o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)
Il delitto viene commesso da chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.
A titolo di esempio, il reato potrebbe configurarsi qualora il dipendente della Società effettui attacchi di cracking[10], hacking, per alterare i dati relativi ad un concorrente.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater, c.p.)
Il delitto consiste nella fraudolenta intercettazione ovvero nell'impedimento, interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.
Ricorre il reato in esame in caso di intercettazione fraudolenta di enti concorrenti nella partecipazione alle gare di appalto allo scopo di conoscere l'entità dell'offerta dei concorrenti; nell'impedimento o interruzione di una comunicazione per impedire al concorrente di trasmettere i dati/l'offerta per partecipare ad una gara.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
Il delitto può essere commesso da chiunque installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico.
Il delitto viene commesso mediante l'installazione di apparecchiature dirette ad intercettare o impedire comunicazioni informatiche commessi dal personale incaricato della gestione delle infrastrutture di rete aziendale.

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) e danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635 ter c.p.)
Il delitto consiste nella distruzione, deterioramento,

cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui. La giurisprudenza della Suprema Corte è concorde nel ritenere che il delitto in esame sia integrato anche quando «*la manomissione ed alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento recuperatorio postumo comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro. (Fattispecie in cui la Corte ha ritenuto la sussistenza del reato in un caso in cui era stato cancellato, mediante l'apposito comando e dunque senza determinare la definitiva rimozione dei dati, un rilevante numero di file, poi recuperati grazie all'intervento di un tecnico informatico specializzato)*» (cfr. Cass. Pen., Sez. V, n. 8555 del 5 marzo 2012)[11].

Per deterioramento si intende la diminuzione della funzione strumentale, valore o utilizzabilità provocata da un'aggressione fisica su supporto materiale, oppure da un attacco a mezzo di un software che, pur non alterando o manipolando il dato, ne limiti l'accessibilità o la fruibilità. Per alterazione si intende una modifica strutturale del dato, programma o informazione, mediante la manipolazione del suo contenuto, con la conseguente apprezzabile perdita, totale o parziale, della sua funzionalità originaria.

Il reato è commesso nel caso in cui il soggetto proceda alla cancellazione della memoria di un computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Viene integrata l'ipotesi di cui al 635 ter c.p. nel caso in cui il soggetto passivo titolare del programma informatico sia lo Stato o comunque laddove la condotta sia a protezione di programmi di pubblica utilità. A titolo esemplificativo tale ultima ipotesi può essere commessa nel caso in cui il danneggiamento, distruzione o manomissione abbia ad oggetto documenti informatici aventi efficacia probatoria, registrati presso enti pubblici (es. polizia, uffici giudiziari, ecc.), da parte di dipendenti di enti coinvolti a qualunque titolo in procedimenti o indagini giudiziarie.

Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.) e danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)

Il delitto in esame viene commesso, salvo che il fatto costituisca più grave reato, da chiunque mediante le condotte di cui al 635 *bis* c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia o rende inservibili i sistemi informatici altrui o ne ostacola il funzionamento. A differenza, tuttavia, della condotta di cui al 635 *bis*, in questo caso il danneggiamento deve interessare l'intero sistema, ossia l'hardware. Oltre alle condotte di cui al 635 *bis*, il delitto in esame può essere commesso anche mediante l'introduzione o trasmissione di dati, informazioni o programmi. Ciò, ad esempio, riguarda l'ipotesi in cui il reato sia commesso mediante malware atti a cagionare uno degli eventi di distruzione, danneggiamento, procurata inservibilità, o di ostacolo al funzionamento degli stessi. Costituiscono esempio di tali condotte gli attacchi ransoware di cui parleremo più diffusamente nel prosieguo (si veda paragrafo 6.c). Anche in questo caso ove la condotta abbia ad oggetto sistemi pubblici o di pubblica necessità il reato rilevante è l'art. 635 *quinquies* c.p. Esempio di tale ultima ipotesi è il caso di danneggiamento di informazioni, dati o programmi informatici utilizzati da enti pubblici commesso dal personale incaricato della gestione dei sistemi di clienti della Pubblica Amministrazione.

Documenti informatici (art. 491 bis c.p.)

L'art. 491 bis c.p. stabilisce che qualora le falsità regolate dal Capo III del Titolo VII del c.p. riguardino un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici. Il d.lgs. 7/2016 ha depenalizzato la corrispondente fattispecie relativa ad atti informatici privati e le disposizioni concernenti le scritture private in ragione della corrispondente abrogazione dell'art. 485 c.p.

Un esempio di commissione del reato in esame riguarda l'ipotesi di falsificazione di documenti informatici contenenti gli importi dovuti dall'ente alla PA nel caso di flussi informatizzati dei pagamenti tra privati e pubblica amministrazione.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)

Commette il reato in esame solo il soggetto che presta servizi di certificazione di firma elettronica il quale al fine di procurare a sé o ad altri ingiusto profitto o di arrecare un danno viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Esempio di commissione del reato in parola concerne l'ipotesi di aggiramento dei vincoli previsti per la verifica dei requisiti necessari al rilascio dei certificati da parte dell'amministratore di sistema allo scopo di concedere un certificato e produrre un guadagno all'ente.

4. I diritto penale della privacy: gli artt. 167 – 171 del Codice Privacy

La prima volta che in Italia è stata introdotta una norma diretta a tutelare la riservatezza dei dati personali è stato con l'art. 38 dello Statuto dei Lavoratori. Il successivo intervento in materia si è avuto con la legge disciplinante la gestione dei dati personali contenuti nelle banche dati in uso alle forze dell'ordine per la prevenzione e la lotta contro la criminalità, volta a prevenire la commissione di abusi commessi dai pubblici ufficiali preposti al loro trattamento e poi con la legge 23 dicembre 1993, n. 547, integrativa delle nuove fattispecie criminose che hanno completato la parte del codice dedicata al diritto penale dell'informatica. Tuttavia, è stato solo con la legge 31 dicembre 1996, n. 675 («Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»), che il legislatore ha introdotto il primo presidio organico in materia a corollario della nuova concezione costituzionale della riservatezza quale espressione della solidarietà sociale di cui all'art. 2 Cost. e al principio di uguaglianza dell'art. 3 Cost.[12].

Detta legge, più in particolare, è stata introdotta sia allo scopo di assolvere alle sollecitazioni di matrice sovranazionale ed europea, sia al fine di introdurre per la prima volta un sistema normativo organico, volto a disciplinare le corrette modalità di trattamento dei dati personali che fosse anche corredato da un ampio catalogo di sanzioni, modulate secondo il criterio del duplice binario amministrativo e penale ed in conformità al principio di *extrema ratio* che deve caratterizzare il precetto penale.

Anche il Codice in materia di protezione dei dati personali emanato con il D.lgs. 30 giugno 2003 n. 196, si è posto sulla stessa direttrice già iniziata con la precedente l. 675/1996, riproponendo le medesime problematiche ermeneutico-applicative.

Su questa cornice normativa si sono recentemente inserite anche le nuove disposizioni sia del Regolamento che del Codice della Privacy novellato con il D.lgs. 101/2018 che hanno in parte emendato, in parte abolito ed in parte mantenuto le precedenti fattispecie incriminatrici già previste dal d.lgs. 196/2003.

Con riferimento alla tutela penale nell'ambito della protezione dei dati personali, il Considerando 149 in combinato con l'art. 84.1 del Regolamento sanciscono che i singoli Stati debbano poter stabilire le disposizioni concernenti le sanzioni penali applicabili per la violazione del Regolamento e delle norme nazionali attuative dello stesso[13].

Detta soluzione operata dal legislatore europeo ha però ha restituito all'interprete un sistema caotico, «*caratterizzato da continui rimandi tra normative eterogenee, con problemi interpretativi complessi discendenti dalla sovrapposizione di fonti, potenzialmente, autosufficienti. Ne è scaturito un corpus iuris connotato da sistemi sanzionatori disomogenei — che talvolta conduce alla repressione della mera inosservanza di regole di condotta e/o trattamento pericolosamente omogenee — destinati ad entrare ben presto in conflitto tra loro, con inevitabile vulnus ai principi di logicità e ragionevolezza, con il canone di proporzione e col principio di ne bis in idem*»[14].

Infatti, la scelta di utilizzare norme penali in bianco per sanzionare comportamenti lesivi della privacy mal si concilia con la tassatività e determinatezza che devono invece caratterizzare i precetti penali[15]. La tecnica del rinvio, infatti, rischia non solo di estendere eccessivamente l'ambito di rilevanza penale a fatti che sarebbero privi di quel disvalore che dovrebbe caratterizzare il sistema penale quale *extrema ratio*, ma soprattutto porta con sé il rischio che il rimando a norme secondarie che possono non essere ancora state emanate o successivamente emendate, renda l'opera di interpretazione della condotta vietata di estrema difficoltà per l'interprete e soprattutto per il cittadino che, come noto, deve invece conoscere il precetto (e la conseguente sanzione) prima della possibile commissione del fatto di reato, con conseguenze in termini di certezza del diritto e della pena[16].

A ciò si aggiunga che l'avvenuta abrogazione di alcune delle precedenti sezioni del codice previgente cui le norme penali facevano rimando, determina notevoli problemi anche sotto il profilo di diritto intertemporale e di successione di leggi penali nel tempo. Infatti, come noto, se la condotta assumeva rilevanza penale solo sulla base della norma precedentemente in vigore, ma non più ai sensi del nuovo codice privacy, deve ovviamente ritenersi sussistente un'ipotesi di *abolitio criminis* con la conseguenza che il fatto non è più previsto dalla legge come reato[17].

4.1. Trattamento illecito di dati personali (art. 167 Codice privacy)

Con riferimento ad alcune delle più importanti norme del diritto penale della privacy, si ricordi che l'art. 167 del Codice, punisce chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno, «*operando in violazione di quanto disposto dagli articoli 123[18], 126[19] e 130[20] o dal provvedimento di cui all'articolo 129[21]*» provoca nocumento all›interessato (comma 1).

Inoltre, ai sensi del secondo comma, è punito chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato,

procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento[22] in violazione delle disposizioni di cui agli articoli 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante) e 2-octies (Principi relativi al trattamento di dati relativi a condanne penali e reati) , o delle misure di garanzia di cui all'articolo 2-septies (Misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute) ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies (Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico) (comma 2) oppure, ai medesimi fini, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento» (comma 3), arreca nocumento all'interessato.

Si tratta, come sopra anticipato, di una norma penale in bianco in quanto non contiene la descrizione esaustiva delle condotte vietate, ma per l'identificazione del precetto vietato fa rinvio ad altre norme del codice privacy che stabiliscono i criteri di liceità di un determinato trattamento di dati personali la cui violazione integra appunto la fattispecie *de quo*. In aggiunta a ciò, talvolta, la condotta a cui la norma fa riferimento è addirittura contenuta in altre disposizioni di rango secondario e di futura emanazione o in provvedimenti generali del Garante, con evidenti conseguenze di cui si è detto in termini di tassatività e determinatezza della fattispecie.

La precedente giurisprudenza che si era formata in materia aveva da sempre interpretato il nocumento in termini di condizione obiettiva di punibilità, ossia quale elemento esterno alla fattispecie che di per sé è già perfetta in termini di rispondenza all'ipotesi prevista in astratto dal legislatore, che tuttavia risultava punibile solo al ricorrere di un danno effettivo per l'interessato[23]. Ciò imponeva di interpretare la condotta in termini di pericolo concreto. Si leggeva: «*il reato di trattamento illecito di dati personali, di cui all'art. 167 d.lg. n. 196/03, è un reato di pericolo effettivo e non meramente presunto; conseguentemente, la illecita utilizzazione dei dati personali è punibile, non già in sé e per sé, ma in quanto suscettibile di produrre nocumento alla persona dell'interessato e/o del suo patrimonio. Il nocumento può essere non solo economico, ma anche più immediatamente personale, come, ad esempio, la perdita di tempo nel vagliare mail indesiderate e nelle procedure da seguire per evitare ulteriori invii*».

Nel revirement operato dalla Suprema Corte appena citato, invece, la Corte della Nomofilachia afferma che «*affinché tale condotta assuma rilievo penale, occorre che si verifichi per ciascun destinatario un effettivo "nocumento", che non può certo esaurirsi nel semplice fastidio di dover cancellare di volta in volta le mail indesiderate, ma deve tradursi in un pregiudizio concreto, anche non patrimoniale, ma comunque suscettibile di essere giuridicamente apprezzato, richiedendosi in tal senso un'adeguata verifica fattuale volta ad accertare, ad esempio, se l'utente abbia segnalato al mittente di non voler ricevere un certo tipo di messaggi e se, nonostante tale iniziativa, l'agente abbia perseverato in maniera non occasionale a inviare messaggi indesiderati, creando così un reale disagio al destinatario. "Nocumento" non può essere il solo disagio di dover cancellare pochi e occasionali messaggi non desiderati, richiedendosi, al fine di attribuire rilevanza penale al fatto, un quid pluris, consistente in un pregiudizio effettivo, che si riveli proporzionato rispetto all'invasività del comportamento di chi invia i contenuti sgraditi, restando magari indifferente a eventuali richieste di porre termine alta spedizione di una determinata tipologia di messaggi*»[24].

È proprio su questo peculiare aspetto da cui si evince il cambiamento nell'impostazione giurisprudenziale che dimostra di aver accolto un'interpretazione del nocumento quale elemento costitutivo della fattispecie tipica[25]. Nella parte motiva della sentenza, infatti, la Corte di Cassazione ha precisato infatti che «*la nozione di nocumento, in definitiva, coerentemente con l'etimologia del termine (derivante dal verbo nuocere, ovvero arrecare un danno anche morale), evoca l'esistenza di una concreta lesione della sfera personale o patrimoniale, che, nell'ottica della fattispecie per cui si procede, deve ritenersi direttamente riconducibile a un'operazione di illecito trattamento dei dati protetti*»[26]. Tale modifica interpretativa ricade sia sulla sussistenza in sé della rilevanza penale della condotta, poiché in difetto del nocumento manca il reato, sia sull'elemento soggettivo in quanto il dolo dovendo investire tutto il fatto tipico, ora deve abbracciare anche il nocumento. In altre parole, oggi, secondo questo nuovo orientamento, per rispondere di trattamento illecito di dati personali, è richiesto al titolare del trattamento di agire nella coscienza e volontà di realizzare un trattamento illecito, non solo al fine di profitto, ma anche nella consapevolezza di determinare un nocumento altrui (o quantomeno prevedendo e accettando che tale nocumento vi sia). E tale nocumento, come visto, non consiste più nel mero fastidio di dover cancellare qualche e-mail indesiderata, ma è necessario un *quid pluris* inteso come vero e proprio pregiudizio consistente nella ricezione di molte e-mail indesiderate, ricevute anche dopo una formale opposizione/revoca del consenso.

Ciò, ad avviso di chi scrive, riduce sensibilmente l'ambito di rilevanza penale della condotta, quantomeno sulla sussistenza del profilo soggettivo.
I commi 4 e 5 della norma in esame si occupano di descrivere le modalità di collaborazione tra il Garante e il Pubblico Ministero nei casi di notizia delle predette ipotesi di reato. È previsto infatti sia che il Pubblico Ministero, quando riceve una notizia di reato di cui all'articolo 167, informi senza ritardo il Garante che viceversa, nell'ipotesi in cui il Garante, nel corso delle proprie attività ispettive, rinvenga gli elementi che facciano ritenere sussistente la sussistenza di un reato. La trasmissione degli atti al Pubblico Ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni del Codice. Ciò in quanto entrambe le Autorità dovrebbero modulare le rispettive sanzioni conformemente a quanto previsto dal Considerando n. 149 del Regolamento e nel rispetto del principio del *ne bis in idem* ed in particolare prevedendosi una riduzione della sanzione penale in caso in cui sia già stata riscossa una sanzione amministrativa[27].

4.2. Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (art. 167-bis)
Si tratta di una fattispecie di nuovo conio volte a punire la comunicazione o la diffusione illecita di un archivio automatizzato o di una parte sostanziale di esso al fine di trarne profitto o di arrecare un danno. Tale fattispecie in realtà costituisce la riproposizione della condotta che era contenuta nel precedente schema di decreto. Il secondo comma punisce la comunicazione di un archivio o di una parte sostanziale di esso di dati personali oggetto di trattamento su larga scala senza consenso quando il consenso è stabilito per l'attività di trattamento.
Tale nuova fattispecie ha lo scopo di reprimere quei comportamenti che per vastità di dimensioni non si esauriscono nella mera violazione delle norme sul trattamento ed è volta a censurare quella prassi di creazione di database privati, anche utilizzati per fini commerciali, in spregio alle norme sulla liceità dei trattamenti.
Anche questa disposizione presenta elementi di difficile compatibilità con il principio di tassatività stante la mancanza di una definizione univoca di "parte sostanziale" dell'archivio[28] sul quale deve ricadere la condotta e sul concetto di larga scala[29]. Il Gruppo di Lavoro dei Garanti Europei WP29, ora EDPB (European Data Protection Board) suggerisce di tenere in considerazione, per la determinazione della larga scala, fattori quali il numero di soggetti interessati dal trattamento, in termini assoluti o espressi in percentuale alla popolazione di riferimento, il volume dei dati o le diverse tipologie di dati oggetto del trattamento, la durata o la persistenza della attività di trattamento e la portata geografica.
A differenza del trattamento illecito di dati personali che può essere commesso solo dal titolare e dal responsabile del trattamento, in questo caso trattasi di reato comune.

4.3. Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167-ter)
Si tratta di una nuova ed ulteriore fattispecie incriminatrice che sanziona l'acquisizione con mezzi fraudolenti di un archivio automatizzato o una parte sostanziale di esso contenente dati personali al fine di trarre profitto per sé o per altri. È una fattispecie di nuovo conio volta a punire l'acquisizione fraudolenta di dati personali.
Gli elementi essenziali di tale reato sono i medesimi di quelli dell'art. 167 bis.
Il reato in parola presenta elementi di comunanza con i reati informatici e soprattutto rispetto all'accesso abusivo al sistema informatico che, come visto sopra, tutela contro le intrusioni non autorizzate volte a ledere la riservatezza di quei dati personali che sono contenuti nei sistemi informatici protetti da password. «*Non v'è dubbio, infatti, che anche il delitto di accesso abusivo a sistema informatico, per quanto non disciplini espressamente sistemi informatici contenenti dati personali, sia posto a presidio della tutela della riservatezza individuale, coerentemente con la propria collocazione nel Codice penale tra i delitti contro la libertà individuale*»[30].
In realtà, poiché l'accesso al sistema informatico non presuppone l'acquisizione dei dati contenuti nel sistema informatico, deve ritenersi che le due fattispecie siano in concorso tra loro in quanto con l'acquisizione illecita viene punita una condotta ulteriore e consequenziale all'accesso abusivo.

4.4. Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (art. 171)
Si tratta della fattispecie penale volta a reprimere le violazioni dell'art. 4 dello Statuto dei lavoratori, ossia di quelle disposizioni che sono funzionali ad evitare le forme anche remote di controllo a distanza dei lavoratori.
Rientrano a titolo esemplificativo nell'alveo di tale fattispecie tutte quelle ipotesi relative alla violazione delle regole sull'installazione degli impianti di videosorveglianza. Sul punto, si ricordi la recente giurisprudenza della Corte di Cassazione a norma della quale «*integra il reato previsto dall'art. 4 st.*

lav. (l. 20 maggio 1970, n. 300) l'installazione di un sistema di videosorveglianza potenzialmente in grado di controllare a distanza l'attività dei lavoratori, anche quando, in mancanza di accordo con le rappresentanze sindacali aziendali e di provvedimento autorizzativo dell'autorità amministrativa, la stessa sia stata preventivamente autorizzata per iscritto da tutti i dipendenti» (cfr. Cass. Pen. Cassazione penale sez. III, 15/07/2019, n.50919). Analogamente, si tratta di tutte quelle ipotesi in cui, nonostante il potenziale controllo del lavoratore, non vengano rispettate le prescrizioni di cui all'art. 4 dello Statuto dei Lavoratori (ossia richiesta di autorizzazione alla ITL o l'accordo con le rappresentanze sindacali aziendali). Si pensi, ad esempio, alle registrazioni delle chiamate di un call center o alle forme introdotte a seguito del proliferare di meccanismi di smart-remote working funzionali a garantire il corretto espletamento dell'attività lavorativa, nonostante l'impossibilità di verificarne l'effettivo svolgimento da parte del datore di lavoro.

5. I modelli di gestione ex D.lgs. 231/2001 e i modelli organizzativi privacy per una compliance integrata: l'art. 32 del Regolamento.

Nella redazione dei modelli di gestione ex d.lgs. 231/2001, come per tutti i reati presupposto, occorre introdurre specifici presidi per la prevenzione dei reati informatici. Tuttavia, nel settore di cui trattasi la redazione dei protocolli dedicati alla prevenzione dei rischi informatici è particolarmente complessa sia in ragione dell'interconnessione con i profili di riservatezza di cui si è cercato di rendere conto, nonché in forza delle necessarie competenze informatiche che posseggono gli autori di tali illeciti e che devono possedere necessariamente anche i soggetti deputati alla prevenzione della commissione degli stessi. Ciò in aggiunta all'evoluzione delle tecnologie e dei dispositivi in uso che aumenta esponenzialmente le possibilità di commissione di tali reati. Peraltro, l'elevatissimo grado di innovazione tecnologica fa sì che tali reati possano essere commessi anche attraverso dispositivi mobili di larghissimo utilizzo se non regolarmente normati e regolamentati attraverso una serie di rigide politiche aziendali redatte sulla base delle best practice enunciate dai principali standard internazionali in materia di sicurezza informatica e delle informazioni, allo scopo di limitarne l'uso non corretto ed il rischio riconducibile a fattispecie di reato. Va considerato, in tale ottica, come la strumentazione aziendale mobile risulti essere quella maggiormente vulnerabile a sottrazione da personale della Società non autorizzato che potrebbe, tramite la stessa, integrare condotte penalmente rilevanti.

Per tale motivo risulta quanto mai essenziale l'adozione di specifici presidi e protocolli di gestione dell'azienda che siano il più possibile integrati ed interconnessi tra le diverse aree di compliance.

Le policy e i protocolli aziendali, infatti, più in generale, assolvono alla necessità di formalizzare e regolamentare un particolare processo aziendale e indirizzare i comportamenti dei soggetti che a vario titolo sono coinvolti in quell'attività. «*La redazione della policy è il momento in cui si comprende la prassi in essere (c.d. "as is"), si valutano eventuali necessità di miglioramento (sia per tematiche di compliance che di efficienza, nonché di mitigazione dei rischi anche operativi) e si formalizzano le fasi dello stesso, in base a criteri di segregazione e delle funzioni*[31]».

La gestione delle compliance aziendale presuppone in tutti settori un approccio basato sulla responsabilizzazione dei soggetti (*accountability*) e, nell'analisi del processo, occorre adottare necessariamente metodo di analisi basato sul rischio (cd. *risk assessment*) coerente con i presidi aziendali predisposti. Tale mappatura dei rischi impone l'attribuzione di uno specifico punteggio a ciascuna attività o processo sensibile (con riferimento a possibili modalità di commissione dei reati presupposto), oltreché di analisi di quali processi effettivamente possono essere oggetto di rischio per la realtà aziendale e verificare se, alla luce dei presidi in essere, vi sia anche un rischio residuo, ossia la possibilità di commissione dei reati alla luce delle misure correttive e dei protocolli in essere[32]. La mappatura si conclude con l'attribuzione di un livello di rischio esistente che dovrà essere mitigato tramite uno specifico presidio di controllo.

Sono considerate aree di rischio di commissione dei reati informatici le seguenti attività quali (i) la gestione degli accessi, (ii) la gestione dei profili autorizzativi, (iii) la gestione delle attività online, (iv) la gestione della sicurezza informatica, (v) la gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT, (vi) la gestione del processo di creazione, trattamento, archiviazione e distruzione delle informazioni sensibili, (vii) la manutenzione degli applicativi, (viii) la gestione e tenuta dell'inventario, dell'infrastruttura informatica e degli strumenti informatici in uso ai dipendenti, (ix) la gestione della progettazione e della installazione dei software applicativi aziendali interni ed esterni. Ognuna di tali aree di rischio, che si riferiscono

principalmente alle aziende tecnologiche e digitali, ma possono estendersi a tutte le realtà di business che prevedano comunque processi IT e servizi online, dovrebbe essere presidiata con specifici protocolli per la mitigazione degli specifici rischi[33].
Tale approccio al rischio è quello anche disegnato dal Regolamento nell'ambito della tutela dei dati personali. Il predetto nuovo approccio presuppone una tutela non più successiva, ma una preventiva, basata sulla responsabilizzazione del titolare e del responsabile del trattamento (cfr. art. 24 del Regolamento) che si sostanzia nello svolgimento della analisi dei rischi su tutti i trattamenti effettuati, con il riscorso – ove necessario – alla valutazione di impatto sulla protezione dei dati personali (cfr. art. 35 del Regolamento) in un'ottica di *privacy by design* e *by default* che presuppone un approccio di analisi del trattamento sin dalla fase della sua progettazione al fine di ridurre al minimo l'impatto sull'interessato (cfr. art. 25 del Regolamento).
Vi sono essenzialmente tre diversi livelli di valutazione: un primo livello, incentrato su una valutazione del rischio generica e non formalizzata che trova fondamento negli artt. 24 e 35 del Regolamento, strettamente connessa con l'esigenza di effettuare trattamenti che siano il minimo lesivi ed impattanti sui soggetti interessati; un secondo livello, al quale si ricorre se il trattamento è suscettibile di provocare un rischio elevato per i diritti e le libertà delle persone fisiche oggetto del trattamento che presuppone il riscorso ad una valutazione d'impatto sulla protezione dei dati ed infine, un terzo livello, a cui si ricorre ove il risultato della valutazione restituisca un rischio elevato che non può essere mitigato dall'adozione di ulteriori misure aggiuntive e che dunque necessita il riscorso ad una valutazione preventiva da parte dell'Autorità di controllo[34].
Con riferimento, più nello specifico ai profili di interdisciplinarietà tra la tutela della riservatezza, la tutela della sicurezza informatica e la responsabilità amministrativa degli enti, si può individuare il trade d'union nell'art. 32 del Regolamento che sancisce, come noto: «*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*». Come anticipato, con l'entrata in vigore del Regolamento, è sensibilmente cambiato il modello di approccio alla verifica sul rispetto delle misure di sicurezza introdotte dalla Società, trasformando da una modalità di tutela di tipo formale, ad un approccio sostanziale, anche esso basato sul rischio[35].
Il diritto alla riservatezza e alla tutela della privacy prende in questo ambito un'accezione di riservatezza informatica, termine con il quale si intendono «*quelle nuove aree virtuali ove i soggetti titolari memorizzano ed elaborano con una certa facilità e velocità un'ampia quantità di informazioni e di dati, con conseguente libera valorizzazione della personalità individuale e svolgimento di qualsiasi attività di natura economica, libero-professionale, sociale, culturale [...] L'ambito di tutela di tale bene giuridico è rappresentato dall'esigenza di salvaguardare il pieno diritto di godimento di tali confini virtuali da parte del legittimo titolare, e ciò si proietta non solo sul contestuale sviluppo della personalità umana, ma prefigura anche la possibilità di escludere soggetti terzi dall'illimitata possibilità di intrusione nel sistema informatico altrui*»[36]. Corollario di tale concetto è la sicurezza informatica che consente tra gli altri di salvaguardare la sicurezza e l'intangibilità di dati informatici.
Le misure di sicurezza possono essere sia di natura tecnica che di natura organizzativa (esempio delle prime sono le tradizionali password o altre credenziali logiche di accesso ad un sistema, mentre le seconde possono consistere in un presidio fisico anche solo del luogo ove l'elaboratore è collocato come, ad esempio, l'accesso regolamentato dal badge di servizio o anche semplicemente da una chiave nella sala server o nella stanza ove è custodito il sistema che si intende proteggere, programmi di formazione periodica del personale, predisposizione di procedure formalizzate)[37].
Il punto di contatto tra le due discipline si rinviene anche nell'ipotesi patologica in cui si abbia un incidente di sicurezza in quanto a seguito dello stesso è possibile il verificarsi anche di una violazione dei dati personali; in altre parole, quando la Società subisce un attacco informatico, deve verificare che non vi sia stata anche una perdita di riservatezza, integrità e disponibilità e attivare tutte le azioni di mitigazione dell'incidente anche lato privacy che consistono, tra gli altri, nella valutazione della necessità di notifica al Garante e comunicazione agli interessati ai sensi degli artt. 33 e 34 del Regolamento.
È per questa ragione che le misure di sicurezza adottate sono elemento essenziale per la prevenzione dei reati informatici. In altre parole, nelle realtà aziendali sempre più digitali e complesse, come quelle attuali, il protocollo dedicato alla prevenzione dei reati informatici è quello che maggiormente richiede di essere implementato

e arricchito da una serie di procedure preventive volte alla mitigazione concreta di esposizione ai rischi informatici. In particolare, non sono più sufficienti semplici prescrizioni, ma è sempre più necessario analizzare i rischi informatici e i rischi privacy e assicurare misure di sicurezza adeguate anche di elevata complessità. Solo in tal modo, la società, da un lato riuscirà ad evitare di incorrere in responsabilità penali ai sensi del D.lgs. 231/2001, e dall'altro lato riuscirà ad essere altresì compliant lato privacy ed evitare di incorrere nelle sanzioni amministrative e penali previste dal Codice e dal Regolamento.

È dunque quest'ottica basata sul rischio che abbraccia tutte le aree di compliance aziendali sulla quale lavorare per creare, per quanto possibile, modelli organizzativi e di gestione integrati tra loro e che "si parlino" affinché la gestione del rischio da compliance, nelle realtà aziendali più complesse, venga gestito in modo sostanziale e non solo formale. In altre parole, per andare esenti da responsabilità, secondo l'orientamento costante della giurisprudenza, è essenziale che i presidi e i protocolli siano realmente calati sulla realtà aziendale e non si rivelino un semplice insieme di carteggi privi di un'effettività di utilizzo da parte dell'azienda. Un efficace modello organizzativo ex D.lgs. 231/2001 deve necessariamente tenere in considerazione e richiamare quelle policies e procedure, o linee guida che sono adottate dalla Società in altri settori che sono ormai intrinsecamente interconnessi tra loro. In particolare, si pensi a quelle procedure del modello organizzativo privacy dedicate alla regolamentazione dell'uso degli strumenti IT o volte a regolamentare i rapporti con l'Autorità di controllo. Ciò si rivela ancor più evidente qualora la Società abbia deciso di ottenere delle certificazioni quali la ISO/IEC 27001:2013[38] i cui presidi costituiscono altresì sistemi fondamentali per la prevenzione dei reati informatici. Infatti, in particolare:

- una efficace politica di gestione delle risorse umane (così come previsto al punto A.7 dell'Annex A. della ISO 27001) prevede che l'organizzazione attui delle regole di condotta specifiche in sede di selezione dei candidati e di amministrazione del personale contrattualizzato, nonché di corretta gestione del rapporto di lavoro, nonché di assolvimento di specifici percorsi formativi (anche dal punto di vista etico), fondamentale presidio anche per la prevenzione dai reati di corruzione, così come previsto dallo standard ISO 37001 in materia di sistemi di gestione per la prevenzione della corruzione. Una politica di gestione del personale efficace, consente di svolgere, compatibilmente con le prescrizioni dello Statuto dei lavoratori, monitoraggi sul dipendente, filtrando così comportamenti nocivi che potrebbero comportare vantaggi illeciti al dipendente stesso o ad una funzione aziendale ad esso collegata;
- le politiche e le procedure di gestione degli asset aziendali (così come previsto al punto A.8 dell'Annex A. della ISO 27001) impongono un uso corretto della strumentazione e della documentazione fornita ai dipendenti e conservata in azienda (sia software che hardware);
- le politiche e le procedure di controllo degli accessi logici (così come previsto al punto A.9 dell'Annex A. della ISO 27001) impongono l'adozione di layer di autorizzazione utili al fine della prevenzione da accessi non autorizzati ai sistemi aziendali conformemente ai principi di *least privilege* e *need to know*;
- le politiche di gestione della sicurezza fisica (così come previsto al punto A.11 dell'Annex A. della ISO 27001) consentono l'adozione di misure di sicurezza volte a prevenire accessi fisici non autorizzati ad ambienti ritenuti critici, come ad esempio le sale server;
- le politiche di gestione sicura delle comunicazioni (così come previsto al punto A.13 dell'Annex A. della ISO 27001) impongono l'adozione di misure infrastrutturali idonee a prevenire accessi alla rete aziendale non autorizzati, prevedendo ad esempio, l'implementazione di firewall perimetrali;
- le politiche e le procedure di sviluppo sicuro (così come previsto al punto A.14 dell'Annex A. della ISO 27001) impongono di adottare linee di condotta al fine di sviluppare stringhe di codice in maniera conforme alle best practice riconducibili ai principali standard in materia;
- le politiche e le procedure di gestione delle terze parti (così come previsto al punto A.15 dell'Annex A. della ISO 27001) impongono lo svolgimento di analisi dei rischi e audit di seconda parte sul fornitore in maniera tale da verificare l'assetto tecnico e organizzativo della propria infrastruttura, la quale dovrà presentare misure di sicurezza idonee al fine di impedire ai soggetti coinvolti nella linea di fornitura, sia interni che esterni all'organizzazione, condotte illecite o a scopo fraudolento.

È di tutta evidenza come l'adozione delle procedure funzionali all'attuazione dei controlli e dei principi dello Standard internazionale sopra citato, consentono l'adozione di misure di sicurezza a tutela e protezione dei dati personali e delle

informazioni trattate dall'ente e parallelamente l'introduzione di processi aziendali idonei alla predisposizione di quel sistema di controlli volto alla prevenzione dei reati informatici.

5.1. I presidi IT quale strumento di prevenzione della commissione di reati informatici

Nella redazione dunque di Modelli Organizzativi 231, occorrerà dunque verificare il grado di sviluppo tecnologico dell'ente che, in un'ottica *risk oriented*, consentirà di individuare misure e presidi stringenti e calati sulla struttura della realtà aziendale. Infatti, se è vero come è vero che una piccola impresa edile è sicuramente maggiormente esposta a differenti aree di rischio in quanto, verosimilmente, gli addetti non usano particolari dispositivi tecnologici (e verosimilmente saranno esclusivamente dotati di una casella di posta aziendale o poco altro), per quanto concerne tutte le altre aziende, minimamente strutturate, la verifica puntuale di possibile esposizione al rischio informatico richiede grande attenzione e investimento nell'adozione di presidi adeguati. Lo spettro delle attività sensibili, tra l'altro, è potenzialmente in continua crescita: infatti il Modello Organizzativo 231 e i principi al medesimo sottesi devono ritenersi applicabili a qualunque tecnologia e sistema di trattamento di informazioni e dati di carattere informatico e su qualunque tipo di supporto. Ciò anche in relazione a future tecnologie. L'obiettivo principale per l'ente, quindi, nel perseguimento della finalità di sicurezza informatica è di garantire i seguenti principi:

- la suddivisione dei profili autorizzativi: tale suddivisione preserva il rispetto dei principi di *least privilege*, tracciabilità delle attività di trattamento svolte, preservando dunque il carattere confidenziale e riservato delle informazioni e inibisce la creazione di determinati documenti informatici o di elaborazione di processi autorizzativi di alto livello a chi non ne abbia specifico incarico;
- la riservatezza: tale obiettivo riguarda la garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla nel rispetto di quanto previsto al punto che precede;
- l'integrità: tale aspetto fa sì che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo da chi ne ha autorità;
- la garanzia generale, quindi, riguarda la tracciabilità delle informazioni e la sicurezza che queste vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- la disponibilità: la corretta conservazione fa sì che i dati aziendali siano correttamente disponibili e reperibili in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Gli obiettivi sopra indicati sono perseguiti tramite protocolli comportamentali che prevedono obblighi e/o divieti specifici per ogni tipologia di reato, riprendono, talvolta specificandole o integrandole, le norme contenute nel Codice Etico e nella Parte Generale del Modello e sono volti ad uniformare il comportamento dei soggetti che operano nel contesto delle attività sensibili. L'adozione di elevati standard di sicurezza come quelli previsti dalle certificazioni internazionali quali la ISO/IEC 27001:2013, costituisce un presidio a mitigazione dei reati informatici[39].

«*Va detto che nessun sistema è del tutto sicuro: esiste un livello accettabile di sicurezza che è definito dal bilanciamento di varie componenti, come il valore di quanto si intende difendere, l'investimento economico che si è disposti a sostenere, il livello di rischio che si è disposti a tollerare. È quindi necessario addivenire ad un ragionevole compromesso tra tutte le esigenze in gioco*»[40].

Un ulteriore elemento di mitigazione circa la prevenzione dei reati informatici concerne il rispetto del Provvedimento del Garante Privacy[41] sulla nomina e sui requisiti che devono possedere gli Amministratori di Sistema (di seguito "AdS")[42]. Tale Provvedimento impone la designazione delle figure che rivestono il ruolo di amministratori di sistema, unitamente al rispetto delle seguenti ulteriori prescrizioni: (i) valutazione delle caratteristiche soggettive degli AdS: l'attribuzione delle funzioni deve essere preceduta da una valutazione del futuro AdS per verificare se abbia i requisiti di idoneità alla funzione che andrà a svolgere a cui deve essere fatta sottoscrivere una nomina, ossia una designazione ad AdS che contiene gli ambiti di operatività e consente di istruire l'AdS per i propri ambiti delineati; (ii) redazione dell'Elenco degli AdS: in tale elenco occorre riportare i nominativi degli AdS con l'elenco delle funzioni assegnate e renderlo disponibile a tutte le persone autorizzate che operano nell'ente. Tale documento, poi, dovrà essere aggiornato nel tempo; (iii) verifica

delle attività: l'operato degli AdS deve essere oggetto di verifica almeno annuale; (iv) registrazione degli accessi: le attività di log-in, log-out e i relativi tentativi devono essere registrati e conservati per almeno 6 mesi. Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità.

6. Nuove forme di esposizione a rischio di commissione dei reati informatici per le Società: case studies

Nei paragrafi che seguono verranno esaminate alcune aree di esposizione a rischio ai sensi del D.lgs. 231/2001 per l'ente.

6.1. La casella di posta elettronica del dipendente.

Un aspetto particolarmente delicato concerne l'uso della casella di posta elettronica del dipendente da parte del datore di lavoro. Infatti, se è vero come è vero che la posta aziendale dovrebbe essere uno strumento di lavoro, tuttavia, sia la giurisprudenza che le pronunce dell'Autorità di controllo, assumono in questo ambito un approccio sempre favorevole al lavoratore, ritenendo comunque la casella di posta, seppur con dominio aziendale, appannaggio del domicilio informatico di disponibilità del lavoratore e in quanto tale meritevole di protezione.

Sul punto, la Cassazione ha espresso un orientamento pressoché costante[43] nel ritenere integrato il reato da parte del datore di lavoro nel caso di accesso alla casella aziendale del dipendente. Invero, «*integra il reato di cui all'art. 615-ter c.p. la condotta di colui che accede abusivamente all'altrui casella di posta elettronica trattandosi di uno spazio di memoria, protetto da una password personalizzata, di un sistema informatico destinato alla memorizzazione di messaggi, o di informazioni di altra natura, nell'esclusiva disponibilità del suo titolare, identificato da un account registrato presso il provider del servizio. (In motivazione la Corte di cassazione ha precisato che anche nell'ambito del sistema informatico pubblico, la casella di posta elettronica del dipendente, purché protetta da una password personalizzata, rappresenta il suo domicilio informatico sicché è illecito l'accesso alla stessa da parte di chiunque, ivi compreso il superiore gerarchico)*» (cfr. Cass. pen. Cassazione penale sez. V, 28/10/2015, n.13057)[44].

Secondo la Suprema Corte, in particolare, la «*casella di posta elettronica rappresenta, inequivocabilmente, un "sistema informatico" rilevante ai sensi dell'art. 615/ter cod. pen.. Nell'introdurre tale nozione nell'ordinamento il legislatore ha fatto evidentemente riferimento a concetti già diffusi ed elaborati nel mondo dell'economia, della tecnica e della comunicazione, essendo stato mosso dalla necessità di tutelare nuove forme di aggressione alla sfera personale, rese possibili dallo sviluppo della scienza*» in quanto la «*"casella di posta" non è altro che uno spazio di memoria di un sistema informatico destinato alla memorizzazione di messaggi, o informazioni di altra natura (immagini, video, ecc.), di un soggetto identificato da un account registrato presso un provider del servizio. E l'accesso a questo "spazio di memoria" concreta, chiaramente, un accesso al sistema informatico, giacchè la casella non è altro che una porzione della complessa apparecchiatura - fisica e astratta destinata alla memorizzazione delle informazioni*».

Quanto poi alla qualificazione dello spazio della casella di posta aziendale come afferente al domicilio proprio del dipendente e dunque in quanto tale meritevole di tutela, la Suprema Corte è chiara nell'affermare che laddove al dipendente siano assegnate delle caselle di posta con il proprio nominativo e che siano protette da password, questo è indicativo del fatto che debbano ritenersi espressione del domicilio informatico del dipendente e che dunque questi sia titolare dello *ius escludendi alios*, tanto che, in caso di accesso non autorizzato da parte del superiore gerarchico, questi integra il reato di cui all'art. 615 ter c.p.

È di tutta evidenza che nell'ipotesi di cui si discorre la persona fisica sarà chiamata a rispondere ai sensi dell'art. 615 ter c.p. e l'ente, invece, ai sensi dell'art. 24 bis, comma 1, D.lgs. 231/2001.

A ben vedere, anche il Garante della Privacy, si pone in linea con le pronunce sopra citate in quanto risulta costante il suo orientamento, da ultimo espresso nel dicembre 2019, che conferma come sia illecito mantenere attive le caselle di posta, anche dopo l'uscita di un lavoratore confermando come la casella di posta debba ritenersi espressione del domicilio del dipendente e dunque protetta da riservatezza anche dopo la cessazione del rapporto di lavoro.

Di seguito riportiamo i punti più salienti del provvedimento da ultimo citato[45]: «*il Garante ha ritenuto che "il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati - riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali" (punto 5.2 lett. b) e che ciò, trasposto in ambito lavorativo, comporta la possibilità che il lavoratore o soggetti terzi coinvolti (i*

cui diritti devono essere parimenti tutelati), possano vantare una legittima aspettativa di riservatezza su talune forme di comunicazione; rilevato che tali esigenze di tutela devono essere tenute in considerazione anche nell´ipotesi in cui venga a cessare il rapporto di lavoro tra le parti»; «*RITENUTO, in particolare, che il datore di lavoro, in conformità ai principi in materia di protezione dei dati personali, dopo la cessazione del rapporto di lavoro debba rimuovere gli account di posta elettronica aziendali riconducibili a persone identificate o identificabili (in un tempo ragionevole commisurato ai tempi tecnici di predisposizione delle misure), previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento, provvedendo altresì ad adottare misure idonee ad impedire la visualizzazione dei messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione; l'adozione di tali misure tecnologiche ed organizzative consente di contemperare l'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività e a garantirne la continuità con la legittima aspettativa di riservatezza sulla corrispondenza da parte di dipendenti/collaboratori nonché dei terzi …*» «*… non risulta conforme ai suesposti principi la prassi già adottata dalla società, consistente nel reindirizzare automaticamente - per un periodo di tempo anche assai ampio - i messaggi pervenuti sull'account dell'ex dipendente su un diverso account aziendale …*».

Le pronunce sopra citate, sono volte ancora una volta ad evidenziare quanto sia necessario il ricorso a policy integrate che siano quanto il più possibili multidisciplinari funzionali ad adempiere sia ai precetti lato privacy che a prevenire la commissione dei reati di cui al D.lgs. 231/2001.

6.2. Lo smart working

La recente pandemia mondiale ha accelerato un processo che era in corso da anni, inducendo le aziende a dotarsi di modalità di *smart-remote working*. La situazione di emergenza in corso, tuttavia, ha imposto l'adozione di questi strumenti senza che nel contempo venissero fatte idonee verifiche tecniche al fine di rendere sicure, sotto il profilo della sicurezza informatica, le modalità di lavoro agile. Infatti, l'impiego forzato ed estemporaneo di strumenti e modalità operative prima poco utilizzate ha creato nuove opportunità per i cybercriminali che, grazie alle vulnerabilità insite nei nuovi strumenti, hanno moltiplicato i propri attacchi nel corso dell'ultimo anno. Gli studi effettuati sul tema, invero, hanno dimostrato che sono stati sferrati 119 attacchi gravi, nel periodo febbraio-giugno 2020 in tutto il mondo. Si tratta del 14% dei cyber attacchi noti. In particolare, oltre la metà degli attacchi a tema Covid-19 (61%) sono stati condotti tramite campagne di phishing e di social engineering, anche in associazione a malware (21%): si tratta di attacchi strutturati per danneggiare il maggior numero possibile di persone e organizzazioni. Tra gli altri spiccano alcuni casi gravi di Bec scam (Business email compromise), portati a segno da cybercriminali nelle prime fasi concitate di approvvigionamento dei presidi di sicurezza (per esempio, le mascherine) che hanno generato danni considerevoli per le loro vittime[46]. Inoltre, il medesimo rapporto Clusit ha evidenziato anche un aumento esponenziale degli attacchi DDoS[47].

Tale ultima forma di attacco, a ben vedere, è molto più frequente di quanto non si pensi in quanto vi sono società informatiche che offrono – anche gratuitamente, seppur in forma limitata – tali forme di penetration test e vulnerability assessment in assenza di verifiche adeguate circa il richiedente l'attacco. In altre parole, qualora una società volesse sferrare un attacco di questo tipo ad un concorrente, sarebbe sufficiente acquistare questo servizio per rendere temporaneamente irraggiungibile, magari in orario di punta, l'e-commerce dell'azienda concorrente oggetto di attacco.

Se l'assenza di misure di sicurezza adeguate atte a prevenire questo tipo di attacchi può già costituire ipso iure un rischio privacy, analogamente non può dirsi lato 231, in cui il rischio da prevenire è quello della commissione di illeciti commessi dall'interno a vantaggio dell'ente. Non si potrà evidentemente incorrere in alcuna responsabilità penale, nel caso in cui, invece, tale attacco venga subito dall'esterno.

È evidente che i maggiori rischi per l'ente sono connessi alla commissione dei reati di accesso abusivo ai sistemi informatici e telematici posti in essere al fine di «*acquisire dati utili alla commissione di ulteriori reati quali il furto di identità, il furto di proprietà intellettuale, lo spionaggio industriale e le estorsioni rivolte alle imprese. Tali reati sono facilitati dall'alta concentrazione di personale tecnico operante con "account ad elevati privilegi" e dall'elevata quantità di dati presenti sulle infrastrutture informatiche, dalla loro diversa natura e grado di sensibilità*»[48]. È proprio a tali reati, come abbiamo visto sopra, che i modelli devono individuare adeguati presidi di controllo e tutela affinché non venga effettuato un uso distorto di tali sistemi. Tra i protocolli da adottare, ad esempio, è opportuno individuarne anche uno

teso a disciplinare correttamente lo svolgimento dell'attività lavorativa in *smartworking,* soprattutto se la stessa venga svolta mediante strumenti personali e non aziendali.

6.3. *Ransomware*

I *ransomware* (dall'inglese *ransom-*, riscatto, e *-ware*, sofware) sono un tipo di *malware (malicious software),* che si infiltrano in un singolo computer o in una rete, ma anche in smartphone e persino dispositivi elettronici come Smart TV, per rubare informazioni, aprire le porte a controlli remoti o, tramite efficaci tecniche di cifratura dei file, per rendere inutilizzabili documenti, archivi, immagini e qualunque altro contenuto memorizzato sul disco fisso. In particolare, l'attaccante, dopo aver criptato i file memorizzati sul disco rendendoli irrecuperabili, invia sulla schermata della vittima una richiesta di riscatto che dovrà essere corrisposta in bitcoin per ottenere il recupero dei propri file. L'effetto del malware in esame può essere anche la compromissione del sistema. L'infezione, più nel dettaglio, avviene in due fasi, prima tramite l'esecuzione di un file contenente, in modo diretto o indiretto, il codice virale: attraverso l'apertura di allegati mascherati da finte fatture, note di credito, bollette di operatori telefonici o elettrici, presenti nelle e-mail e addirittura nella PEC, oppure tramite il download automatico o manuale di file dalla rete e l'istallazione di programmi compromessi, poi con la richiesta di riscatto (*ransom*) perché il virus sia rimosso e sia inviata la chiave di cifratura. Questi malware sono in grado di ricercare i collegamenti in rete e dunque di aggredire non solo il sistema attaccato ma anche il server centrale e i sistemi collegati.

Per giurisprudenza consolidata, i ransomware integrano la fattispecie di cui all'art. 635-*bis* c.p. sopra citato. Infatti, secondo tale orientamento (cfr. *ex multis* Cass. Pen. n. 8555/2012) l'azione malevola condotta tramite i ransomware è da ricondurre alla "soppressione" prevista dalla norma che ricomprende sia i fatti che provocano una eliminazione definitiva dei dati che presuppongono un'impossibilità del loro recupero, sia la temporanea impossibilità degli stessi[49].

In presenza di una condotta estorsiva il soggetto passivo si configura quale vittima. Ne deriva che, anche in caso di pagamento del riscatto, l'utente non commette un illecito, né un reato.

Più delicata è, invece, la posizione di un ente pubblico che effettua il pagamento servendosi della sua disponibilità finanziaria: la Corte dei Conti procederà a un controllo amministrativo e contabile, esponendo eventualmente il funzionario a responsabilità personale per danno all'erario (cfr. Corte dei Conti SU n. 4511 del 2006), salvo la prova che la condotta abbia evitato all'Amministrazione danni maggiori.

Particolare è anche il caso del pagamento del riscatto con risorse aziendali: in base al D. Lgs 231/2001 si potrebbe configurare l'imputabilità della società stessa per responsabilità per illecito da reato presupposto, per reati societari (false comunicazioni sociali, impedito controllo, ostacolo all'esercizio delle funzioni delle autorità di vigilanza) nel caso di una costituzione di una provvista per il pagamento, per autoriciclaggio se il pagamento provenisse da un ulteriore illecito (reato di evasione fiscale), ora per reati tributari, oltre che costituire una espressa violazione dei principi contenuti nel Codice etico. Per le Società quotate, poi, si potrebbero configurare le corrispondenti fattispecie penali.

A ciò si aggiunga, poi, che nelle trattative con l'attaccante, in questi casi, spesso si inseriscono anche terze aziende che fungono da mediatori[50] e il pagamento del relativo compenso dovrà anche esso essere giustificato, pena la violazione delle regole di condotta sopra richiamate.

6.4. Profili di diritto definitorio: il concetto di abusività che pervade le norme incriminatrici informatiche

Si è già approfondito in apertura delle fattispecie di cui agli artt. 615 ter e 615-quater c.p. In questa sede si vuole approfondire il concetto di abusività che permea tali fattispecie incriminatrici.

Infatti, il limine tra la liceità ed illiceità della condotta si sostanzia nel concetto di «abusività» che deve permeare la condotta. Invero, secondo una parte della dottrina con tale avverbio il legislatore avrebbe voluto richiamare il giudice al suo dovere di esaminare con particolare attenzione l'assenza di cause di giustificazione. Nell'ambito informatico, come già anticipato sopra, sono frequenti penetration test e vulnerability assessment al fine di verificare la sicurezza e la "tenuta" di un determinato programma o sistema informatico. La legittimità di tali condotte si interseca con il concetto di abusività che dunque abbraccia il dolo piuttosto che l'antigiuridicità. Invero, deve ritenersi che la condotta dell'amministratore di sistema che effettua tali attività con scopo di profitto dovrebbe ritenersi penalmente rilevante in quanto abusiva. Diversamente, dovrà ritenersi legittima la condotta del medesimo che sia funzionale a verificare il livello di sicurezza informatica dei sistemi interni al fine di migliorare le misure di sicurezza adottate[51].

È evidente dunque, come anche in queste ipotesi, debba assumersi estrema cautela nell'impiego di software e tecnologie atte condurre questo tipo di azioni.

7. Prospettive *de iure condendo*

Ad avviso di chi scrive, stante l'essenziale ed inscindibile collegamento che ormai esiste tra i reati informatici e la tutela della riservatezza, in uno con l'impatto che l'entrata in vigore del Regolamento ha avuto su tutte le Società, è maturo anche il tempo per una nuova riflessione in termini di inclusione tra i reati presupposto ex D.lgs. 231/2001 dei reati privacy previsti dal Codice.

Tale novazione normativa, tuttavia, dovrebbe essere effettuata tramite un intervento legislativo mirato e a tutto tondo che sia funzionale ad intervenire correttamente su tutte le disposizioni rilevanti; ciò al fine di evitare la creazione di un doppio binario sanzionatorio (amministrativo e penale) lesivo del principio del cd *ne bis in idem sostanziale*[52]. Invero, tra le maggiori cause di sanzioni amministrative comminate in questi primi due anni da parte delle Autorità garanti europee si rinvengono nel 12% dei casi ipotesi di violazioni di misure di sicurezze (indagini scaturite a partire da una notifica di un data breach all'Autorità); nel 23% dei casi per violazione della base legale. Tali violazioni corrispondono le prime alle fattispecie di cybercrimes previste dal codice penale e le seconde ad ipotesi di trattamento illecito di dati personali.

È evidente dunque, che laddove a seguito di tali violazioni l'Autorità Garante commini una sanzione amministrativa di cui agli artt. 83 e ss. del Regolamento, introdurre anche una sanzione penale per le medesime violazioni ai sensi del D.lgs 231/2001 potrebbe determinare, come detto, problemi circa il rispetto del principio del *ne bis in idem* sostanziale.

Nei sistemi sanzionatori basati sul c.d. "doppio binario", il fenomeno del concorso apparente[53] della norma amministrativa con quella penale è solitamente risolto attraverso l'applicazione del principio di specialità di cui all'art. 15 del codice penale a norma del quale *lex specialis derogat generali*. Analogamente, l'art. 9 della l. 24 novembre 1981, n. 689, di disciplina i rapporti tra la norma penale e quella amministrativa, sancisce che ove vi sia un concorso apparente di norme debba trovare applicazione quella speciale; tale principio è espresso anche in ambito tributario dall'art. 19, d.lgs. 10 marzo 2000 n. 74[54].

Per comprendere quale sia la norma speciale, la giurisprudenza ha individuato alcuni criteri quali, il principale, è quello che fa leva sulla nozione di «medesimo fatto». Sul punto si ricordi anche la pronuncia del 10 febbraio 2015, «Kiiveri c. Finlandia», con la quale la Corte EDU ha approfondito il tema[55]. All'esito di detto giudizio, è stato espresso il principio di diritto secondo cui per accertare se due pronunce abbiano ad oggetto la stessa presunta violazione («medesimo fatto»), è necessario verificare non tanto la condotta così come descritta dalle norme, amministrativa e penale, bensì l'identità materiale e concreta dei fatti[56].

Con riferimento alla responsabilità amministrativa degli enti, tali problemi potrebbero porsi nell'ipotesi in cui le fattispecie privacy diventassero anche reato presupposto ai sensi del D.lgs. 231/2001. Sul punto, per risolvere il conflitto in applicazione dei criteri ermeneutici elaborati a livello europeo, dovrebbe dunque verificarsi se, il fatto oggetto della sanzione amministrativa comminata dal Garante, sia il medesimo che possa dare origine alla sanzione penale.

A ben vedere, ad avviso di chi scrive, ferma la necessità di un intervento legislativo di ampio respiro che non sia unicamente volto a editare l'elenco dei reati presupposto, con la solita tecnica legislativa del "taglia e cuci", ma che sia invece funzionale a introdurre una vera e propria disciplina organica della materia *de quo*, potrebbe effettivamente ammettersi una sanzione penale accanto a quella amministrativa. Infatti, nonostante la possibile duplicazione delle sanzioni, non si addiverrebbe ad una lesione del principio del *ne bis in indem* nella misura in cui il fatto non possa dirsi il medesimo ove le condotte che danno origine alle sanzioni sono in concreto sostanzialmente diverse, poiché, per aversi la responsabilità penale a monte, vi sono trattamenti illeciti che tuttavia possono abbracciare plurime violazioni amministrative che hanno una rilevanza e una valutazione differente sotto il profilo delle prescrizioni del Regolamento. Ciò in quanto la violazione del Regolamento può derivare da una pluralità di violazioni o principi che non necessariamente coincidono con i confini della norma penale, ma possono essere più ampi ed eterogenei. Si pensi, ad esempio, ad una violazione di riservatezza. In queste ipotesi, l'Autorità Garante potrebbe riscontrare sia una violazione delle norme che impongono la corretta trattazione e gestione del data breach (artt. 33 e 34 del Regolamento che disciplinano le ipotesi di notifica del Data Breach all'Autorità e comunicazione agli interessati), così come violazione delle prescrizioni di cui all'art. 32 del Regolamento (in quanto, ad esempio, si verifica che il data breach è stato causato dall'inadeguatezza di misure di sicurezza adottate dalla Società) e per questo comminare una sanzione amministrativa[57].

La corrispondente sanzione ai sensi dell'art. 24 bis del D.lgs. 231/2001 per il crimine informatico o per un eventuale reato privacy potrebbe dirsi appunto violativa del principio del *ne bis in idem* solo

nella misura in cui, secondo i criteri ermeneutici elaborati dalla Corte di giustizia, il fatto che dà origine alle due sanzioni sia il medesimo in concreto, ossia che il fatto materiale per come verificatosi nella realtà fattuale sia lo stesso. Ciò, dunque, ad esempio, non dirsi nel caso in cui un dipendente dell'ente, utilizzando le credenziali a lui in uso nel precedente impiego e per errore non disattivate, acceda e acquisisca indebitamente l'intero database clienti di un sito e-commerce concorrente per fare marketing in assenza di consenso. Nell'esempio citato, lato amministrativo, davanti al Garante sarebbe probabilmente chiamata a rispondere l'azienda parte offesa della condotta di acquisizione illecita di un database e di trattamento illecito di dati personali per violazione delle disposizioni di cui all'art. 32 del Regolamento. Tali ultimi reati sarebbero invece commessi dall'ente ex d.lgs. 231/2001 a favore del quale questi sono stati commessi.

Infine, occorre altresì rilevare che in una eventuale riforma della responsabilità amministrativa degli enti, i soggetti chiamati a rispondere delle violazioni penali privacy ai sensi degli artt. 167 e ss. del Codice Privacy, sono i titolari o i responsabili che, in caso di organizzazioni (*rectius* enti), sarebbero i medesimi soggetti chiamati a rispondere della violazione ai sensi del D.lgs. 231/2001, rischiando sì, in questo caso di incorrere in una violazione del principio del *ne bis in idem* sostanziale. Per superare *l'empasse* dovrebbe ritenersi dunque che – in ipotesi di riforma – la responsabilità penale da Codice Privacy sarebbe limitata ai titolari persone fisiche o a quelle società cui non si applichi la responsabilità ex D.lgs. 231/2001, mentre per gli altri prevedersi esclusivamente la responsabilità ai sensi del D.lgs. 231/2001.

8. Conclusioni

In queste brevi note, emerge un quadro variegato dal quale si desume come comune denominatore l'esigenza sempre più stringente, anche in un'ottica di riforma, di unificare le discipline privacy e 231 al fine di raggiungere livelli di compliance sempre più elevati e coordinati tra loro e ridurre così i cd rischi di compliance.

A ben vedere, infatti, ad esempio, dagli studi condotti dagli analisti economici e finanziari per comprendere le cause della crisi del 2008, è emerso che una delle concause sia certamente da individuare nella mancanza di una adeguata cultura di gestione del rischio. «*Molto spesso, le dinamiche aziendali, che si sono stratificate nel corso dei decenni (dettate da tradizionali sistemi di incentivazione, controllo e valutazione), spingono gli attori organizzativi verso comportamenti non corretti che, a loro volta, portano a scelte errate e potenzialmente dannose. Tali comportamenti possono rappresentare una vera propria minaccia quando rappresentano la prassi e la norma in azienda. Ecco perché è necessario impostare una cultura del rischio che spinga le persone a comportamenti corretti*»[58]. La cultura del rischio è l'insieme delle norme e comportamenti che gli individui e i gruppi dell'organizzazione seguono al fine di accettare i livelli di rischio, dopo adeguate valutazioni volte ad indentificarli, comprenderli e adottare le opportune misure di mitigazione. Per raggiungere questo obiettivo si possono sviluppare diverse direttrici ed in particolare sviluppare piani di formazione, creare modelli di esempio, sensibilizzare le diverse competenze, creare meccanismi di rinforzo, ossia meccanismi premiali nella valutazione delle performance dei singoli dipendenti.

Le linee guida di Confidustria[59] identificano i processi operativi per la gestione dei rischi 231. In particolare, occorre procedere secondo una triplice direzione ossia mediante (i) l'inventariazione degli ambiti aziendali di attività il cui output finale del processo sarà la mappa delle aree aziendali a rischio e dei reati rilevanti, (ii) l'analisi dei rischi potenziali che restituirà la mappa documentata delle potenziali modalità attuative degli illeciti nelle diverse aree a rischio, (iii) la creazione di meccanismo di adeguamento del sistema dei controlli preventivi attraverso la descrizione documentata del sistema dei controlli preventivi attivato e degli adeguamenti si rendano necessari. In particolare, rispetto a quest'ultimo profilo, questo dovrà essere progettato in modo da far sì che i rischi individuati siano ridotti ad un livello accettabile e ciò dovrà avvenire mediante specifici protocolli diretti a programmare la formazione e l'attuazione dell'ente in relazione ai reati da prevenire. Sotto il profilo dei controlli Confindustria chiarisce che dovrebbero essere previsti questi controlli a carattere generale:

- previsione nel codice etico di specifiche indicazioni volte a impedire la commissione dei reati informatici;
- previsione di un idoneo sistema di sanzioni disciplinari;
- predisposizione di strumenti tecnologici funzionali a impedire la commissione di reati informatici da parte dei dipendenti;
- pianificazione di programmi di formazione;
- previsione di idonee clausole contrattuali con i provider dei servizi legati all'information technology;
- adozione di procedure volte a disciplinare l'uso de cd BYOD (ossia l'uso di strumenti personali

sul luogo di lavoro);
- utilizzo di sistemi *cloud* che prevedano una selezione dei fornitori ammessi, restrizione nell'uso dei servizi *clouding* per la trasmissione dei documenti aziendali, diffusione di linee guida.

Anche le Linee guida di Confindustria, poi, chiariscono che il rispetto di framework e standard internazionalmente riconosciuti in tema di ICT Security Governance, Management & Compliance rappresenta un elemento qualificante ai fini della predisposizione di possibili presidi e ai fini dell'implementazione di un adeguato sistema di controllo. Tra gli altri possono essere utili i COBIT (Control for information and related technology) e la ISO/IEC 27001:2013 di cui si è detto.

Anche nelle citate Linee guida, poi, viene evidenziato come sia essenziale il richiamo al rispetto delle norme in materia di protezione dei dati personali, nonché ai provvedimenti del Garante.

A ciò si aggiunga che il proliferare di norme e standard certificabili e il richiamo da parte degli stakeholder ad un approccio sistemico alle discipline inerenti alla qualità ha favorito lo sviluppo di plurimi sistemi di gestione. Tuttavia, non è sempre facile integrare i diversi sistemi di gestione, anche al fine di razionalizzare i relativi costi senza incidere sull'efficacia ed efficienza dei modelli e dei sistemi di controllo. L'ISO ha recepito tale necessità e ha revisionato gli standard dei sistemi gestionali prevendendo la creazione di una struttura base comune che ne rappresenta il framework e che è stata denominata *High Level Structure*.

In particolare, al fine di garantire, come detto, livelli di compliance sempre più elevati, soprattutto in quei settori interconnessi come la tutela della riservatezza, la sicurezza informatica e la responsabilità ex D.lgs. 231, sarebbe opportuno predisporre questo framework unico che potrebbe essere comune anche alla parte generale del Modello Organizzativo 231, a partire dal quale sviluppare i diversi modelli di gestione integrati tra loro per consentire in questo modo all'ente di ammortizzare i diversi rischi di compliance a seconda dell'area di riferimento a cui conformarsi.

Solo in questo modo, ossia mediante un approccio comune, multilivello e multidisciplinare integrato, gli enti potranno definitivamente interiorizzare politiche e procedure attuate, applicarle efficacemente al loro interno e realizzare quella cultura del rischio di cui si è detto.

---

1 L'art. 9 del d.l. n. 93/2013 recante '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', qualora convertito (dalla l. n. 119/2013) senza modifiche, avrebbe previsto che «*In relazione alla commissione dei delitti di cui agli articoli 615ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies e 640-ter, terzo comma, del codice penale nonché dei delitti di cui agli articoli 55, comma 9, del decreto legislativo 21 novembre 2007, n. 231, e di cui alla parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote. (...) 4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel co. 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)*».

2 Sul punto, si veda la relazione della Corte di Cassazione n. III/01/2013 del 22 agosto 2013, che commenta affermando come il richiamo ai delitti previsti dal Codice della privacy sia «*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*» (disponibile online su: www.cortedicassazione.it). Si pensi non solo ad aziende di grandi dimensioni con migliaia di dipendenti e clienti, ma anche le piccole medie imprese, a seconda del settore di riferimento in cui operano, effettuano molteplici attività di trattamento e trattano un elevato quantitativo di dati personali.

3 Per un approfondimento sui ruoli di titolare e responsabile del trattamento si vedano le recenti Linee Guida emanate dall'EDPB 7/2020 (*Guidelines07/2020 on the concepts of controller and processor in the GDPR*, in https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf). Inoltre, cfr. art. 4 del Regolamento:

«*7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinate dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*

n. 8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica o il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

4 Cfr. Peluso F. (a cura di), *La responsabilità nei nuovi reati informatici. Mezzi di ricerca e acquisizione della prova*, MAGGIOLI EDITORE; 2020, cit. p. 180.

5 Lo standard ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) è uno standard di sicurezza informatica che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

6 Ai sensi dell'art. 21 del D.lgs. 101/2018, *"Autorizzazioni generali del Garante per la protezione dei dati personali"* «*1. Il Garante per la protezione dei dati personali, con provvedimento di carattere generale da porre in consultazione pubblica entro novanta giorni dalla data di entrata in vigore del presente decreto, individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9,paragrafo 2, lettera b) e 4, nonché' al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento di cui al presente comma è adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica. 2. Le autorizzazioni generali sottoposte a verifica a norma del comma 1 che sono state ritenute incompatibili con le disposizioni del Regolamento (UE) 2016/679 cessano di produrre effetti dal momento della pubblicazione nella Gazzetta Ufficiale della Repubblica italiana del provvedimento di cui al comma 1. 3. Le autorizzazioni generali del Garante per la protezione dei dati personali adottate prima della data di entrata in vigore del presente decreto e relative a trattamenti diversi da quelli indicati al comma 1 cessano di produrre effetti alla predetta data. 4. Sino all'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-quater e 2-septies del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 producono effetti, per la corrispondente categoria di dati e di trattamenti, le autorizzazioni generali di cui al comma 2 e le pertinenti prescrizioni individuate con il provvedimento di cui al comma 1. 5. Salvo che il fatto costituisca reato, le violazioni delle prescrizioni contenute nelle autorizzazioni generali di cui al presente articolo e nel provvedimento generale di cui al comma 1 sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento (UE) 2016/679*». Il Garante ha poi emesso un provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018 [9068972] disponibile online al seguente link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972.

7 Cfr. Cass. Pen., sez. V, 27 febbraio 2019, n. 8541. Occorre domandarsi cosa si intende per accesso abusivo. Per abusivo, in particolare, analogamente a quanto accade rispetto alla protezione del domicilio personale, si intende un'introduzione non autorizzata, ovvero una permanenza contro la volontà del titolare dello *ius escludendi alios*. L'introduzione abusiva consiste pertanto in un «*accesso alla conoscenza del contenuto del sistema informatico o telematico concretamente considerato: l'immissione nello stesso, infatti, è propedeutico alla cognizione di dati ed informazioni rinvenibili nella memoria di un elaboratore o trasmissibili da una apparecchiatura telematica*» (cfr. Cfr. Cuomo I., Izzi B., *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in "Cass. pen.", fasc.3, 2002, pag. 1018).

8 Quanto alle misure di sicurezza poste a protezione del sistema informatico, queste possono essere costituite dai meccanismi logici, tecnologici ed organizzativi che tendono ad impedire la commissione di reati (ciò unitamente alle misure poste a protezione del luogo ove è collocato il server). Pertanto, tali presidi costituiscono al contempo una condizione per la verifica dell'abusività dell'accesso e per semplificare l'accertamento dell'aspetto soggettivo del reato, avvertendo l'attaccante dell'abusività del suo accesso (cfr. Cfr. Cuomo I., Izzi B., Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico, in "Cass. pen.", fasc.3, 2002, pag. 1018). Sul punto, deve rilevarsi che la Suprema Corte ha ribadito un importante principio, in base al quale per comprendere quando l'accesso debba ritenersi abusivo occorre valutare come detto la presenza delle misure di sicurezza poste a protezione dello stesso che identificano evidentemente la volontà dello ius escludendi alios. A tal fine «*assume rilevanza qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso al sistema informatico, anche quando si tratti di strumenti esterni al sistema e meramente organizzativi*» (cfr. Cass. Pen., 07 novembre 2000, n.12732, sez. V), il che equivale a dire che la complessità e l›efficacia dei meccanismi di protezione prescindono dall›integrazione della fattispecie incriminatrice.

9 Per «*social engineering*» si intende l'analisi dei comportamenti di una persona al fine di sottrarre informazioni utili. Il social engineer è quella forma di attacco tramite la quale l'attaccante si finge una persona vicina alla sua vittima per ottenere, ad esempio tramite email (phishing), all'interno di un sistema per cogliere le informazioni utili per l'attacco informatico che verrà sferrato solo una volta individuata la vulnerabilità del sistema. Per un approfondimento cfr. PELUSO F. u. cit.

10 Con l'espressione *hacking* si è soliti indicare quelle tecniche volte a conoscere, accedere o modificare un sistema informatico. *L'hacker* infatti agisce per prendere possesso di un sistema informatico e di adattarlo alle sue esigenze. Con il termine craking si intendono le attività del craker che consistono, tramite il cd *reverse engineering*, ovvero una tecnica che consente di comprendere il funzionamento del software e studiarne i meccanismi di funzionamento per ricostruirlo in spregio del copywright.

11 «*Il lemma cancella che figura nel dettato normativo non può essere inteso nel suo precipuo significato semantico,*

rappresentativo di irrecuperabile elisione, ma nella specifica accezione tecnica recepita dal dettato normativo, notoriamente introdotto in sede di ratifica di convenzione europea in tema di criminalità informatica (con legge 23 dicembre 1993, n. 547). Ebbene, nel gergo informatico l'operazione della cancellazione consiste nella 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. L'uso dell'inciso per evidenziare il termine "definitiva" è dovuto al fatto che neppure tale operazione può definirsi davvero tale, in quanto anche dopo lo svuotamento del cestino i files cancellati possono essere recuperati, ma solo attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze nel campo dell'informatica. Di talché, sembra corretto ritenere conforme allo spirito della disposizione normativa che anche la cancellazione, che non escluda la possibilità di recupero se non con l'uso — anche dispendioso — di particolari procedure, integri gli estremi oggettivi della fattispecie delittuosa. Il danneggiamento che è presupposto della previsione sostanziale, sottospecie del genus rappresentato dal reato di danneggiamento di cui all'art. 635 c.p., deve intendersi integrato dalla manomissione ed alterazione dello stato del computer, rimediabili solo con postumo intervento recuperatorio, e comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro. Si tratta, dunque, di attività produttiva di danno, in quanto il recupero, ove possibile, comporta oneri di spesa o, comunque, l'impiego di unità di tempo lavorativo» (cfr. Cass. Pen. Sez. V, 18 novembre 2011 n. 2728). Inoltre, l'oggetto materiale del reato può anche ricadere non necessariamente su un sistema ma anche su un supporto esterno (es. dvd, chiavette usb, hard disk rimovibili).

12 Circa la costituzionalizzazione del diritto alla riservatezza si è avuto un dibattito che è corso in parallelo con la ritenuta natura di clausola aperta dell'art. 2 della Costituzione. Analogamente, per altra parte della dottrina la tutela della riservatezza trova fondamento nell'art. 3 ed in particolare nella parte in cui si riconosce il diritto al pieno sviluppo della persona umana. Per altra parte della dottrina tale tutela si rinviene negli artt. 13 che tutela la libertà individuale, nell'art. 14 posto a protezione dell'inviolabilità del domicilio, nell'art. 15 volto a garantire l'inviolabilità della corrispondenza e art. nell'art. 21 che sancisce e consacra l'espressione della libertà di manifestazione del pensiero. Per un approfondimento cfr. Bellocci M., Magnanesi S., Passaglia P., Rispoli E. (a cura di), *Tutela della vita privata: realtà e prospettive costituzionali, Quaderno predisposto in occasione dell'incontro trilaterale delle Corti costituzioni spagnola, portoghese e italiana*, Lisbona,1° –4 ottobre 2006 disponibile online https://www.cortecostituzionale.it/documenti/convegni_seminari/STU_190_Vita_privata.pdf

13 Per un approfondimento cfr. Pelino E., Bolognini L., Bistolfi C., Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016.

14 Solinas M., Tutela penale della privacy dopo il gdpr: la Frettolosa giustapposizione delle fonti è scaturigine di un sistema farraginoso, che crea Confusione, in "Responsabilità Civile e Previdenza", fasc.1, 1° gennaio 2020, cit. pag. 342.

15 I principi di tassatività e di determinatezza della fattispecie penale costituiscono corollario del principio di legalità secondo il quale *nullun crimen nulla poena sine legit.* Il primo di questi principi implica il divieto di analogia *in malam partem* che consiste nel divieto di applicare il caso previsto e disciplinato dalla norma penale ad altre ipotesi non previste, ma simili o analoghe. Tale principio deve differenziarsi dalla cosiddetta interpretazione estensiva che invece è ammessa in quanto il precetto penale contiene già in sé le esemplificazioni o le ipotesi di applicazione del precetto che vengono semplicemente estensi nella loro portata applicativa. Quanto alla determinatezza, questo principio richiede che la fattispecie tipica sia chiusa ossia chiaramente delimitata nella descrizione della condotta tipizzata e avente rilevanza penale. Come anche di recente ha ribadito la Corte Costituzionale tali principi «*per un verso,* - sono volti - *nell'evitare che, in contrasto con il principio della divisione dei poteri e con la riserva assoluta di legge in materia penale, il giudice assuma un ruolo creativo, individuando, in luogo del legislatore, i confini tra il lecito e l'illecito; e, per un altro verso, nel garantire la libera autodeterminazione individuale, permettendo al destinatario della norma penale di apprezzare a priori le conseguenze giuridico-penali della propria condotta*» (sentenza n. 327 del 2008). In altre parole, ciò che discende dall'art. 25 Cost. è che le disposizioni penali devono essere "*chiaramente formulate*", e devono essere rese altresì *conoscibili dai destinatari grazie ad una pubblicità adeguata* (art. 73, comma 3, Cost.): i principi in esame comportano dunque -secondo la Corte -l'adempimento da parte dello Stato di precipui doveri costituzionali, attinenti, anzitutto, alla formulazione del divieto, che deve essere tale da consentire di distinguere tra la sfera del lecito e quella dell'illecito (si vedano, sul punto, i rilievi puntualizzati nella sentenza n. 364 del 1988). Per un approfondimento cfr. Pavarini M., *Corso di Istituzioni di diritto penale,* Bologna: Bononia University Press, 2013, pp. 244; Insolera G., Mazzacuva N., Pavarini M., Zanotti M. (a cura di) *Introduzione al sistema penale,* VOL. 1, Terza edizione, Giappichelli, Torino, 2000.

16 Per un approfondimento cfr. Pavarini op. ult. cit. Sul punto inoltre si vedano anche la Sentenza della Corte Costituzionale n. 364/88 in ordine alla rilevanza della scusabilità dell'ignoranza legit e gli approfondimenti circa il divieto di irretroattività della legge penale, anch'esso espressione dell'art. 25 della Costituzionale e disciplinato a livello di norma di rango primario dall'art. 2 c.p.

17 Cfr. Cass. pen., Sez. fer., 13 agosto-1° ottobre 2019, n. 40140, con riferimento alla fattispecie di trattamento illecito di dati personali ha chiarito che il «nuovo» testo dell'art. 167 — «*che nei due commi della previgente formulazione sanzionava anche la violazione delle disposizioni, oggi abrogate, di cui agli artt. 18, 19, 23 (comma 1), 17, 20, 21, 22, 26, 27, 45 (comma 2) — ha tenuto ferma la rilevanza penale solo di alcuni specifici comportamenti*», seppur differenti da quelli rilevanti nel regime

previgente, connotati «*dal dolo specifico di trarre per sé o per altri profitto, o di recare all'interessato un danno, e purché produttive di "nocumento" a quest'ultimo*». Per un approfondimento cfr. Pavarini op. ult. cit.

18 L'art. 123 disciplina le modalità con le quali risulta ora lecito, secondo il nostro codice, il trattamento dei dati di traffico. La norma, in particolare, stabilisce che «*1. I dati relativi al traffico riguardanti contraenti ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.*

2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per il contraente, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se il contraente o l'utente cui i dati si riferiscono hanno manifestato preliminarmente il proprio consenso, che è revocabile in ogni momento.

4. Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento il fornitore del servizio informa il contraente o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico è consentito unicamente a persone che, ai sensi dell'articolo 2-quaterdecies, risultano autorizzate al trattamento e che operano sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione della persona autorizzata che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione».

19 L'art. 126 si occupa di disciplinare il trattamento dei dati di ubicazione. «*1. I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o ai contraenti di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o il contraente ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto. 2. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e i contraenti sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. 3. L'utente e il contraente che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni. 4. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente a persone autorizzate al trattamento, ai sensi dell'articolo 2-quaterdecies, che operano sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione della persona autorizzata che accede ai dati anche mediante un'operazione di interrogazione automatizzata*».

20 L'art. 130 del Codice privacy disciplina le cd comunicazioni indesiderate. In particolare, la norma stabilisce che le comunicazioni di marketing possono essere inviate solo previo consenso dell'interessato, salva l'eccezione di cui al comma 4 (cd. soft spam) a norma del quale, se la finalità del trattamento è adeguatamente descritta nell'informativa, è possibile inviare comunicazioni all'interessato a mezzo email relative a prodotti analoghi a quelli acquistati, salvo che l'interessato non si sia opposto al trattamento e purché l'email dell'interessato sia stata fornita nel contesto delle attività di vendita di un prodotto o di un servizio.

21 «*1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 4, e in conformità alla normativa dell'Unione europea, le modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico.*

2. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale nonché per le finalità di cui all'articolo 21, paragrafo 2, del Regolamento, in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca del contraente

per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri».

22 Si tratta del trattamento delle particolari categorie di dati personali ossia i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati biometrici o genetici e di dati relativi a condanne penali o reati.

23 Cfr. Cass. Pen. Sez. 3, n. 7504 del 16/07/2013, dep. 2014, Rv. 259261 e Sez. 5, n. 44940 del 28/09/2011, Rv. 251448.

24 Cfr. nota precedente.

25 La Corte di Cassazione, nei passaggi della sentenza, dimostra di accogliere un opposto indirizzo che si era formato sul punto e che richiedeva che **"***il nocumento per la persona alla quale i dati illecitamente trattati si riferiscono costituisce, per la sua omogeneità rispetto all'interesse leso, e la sua diretta derivazione causale dalla condotta tipica, un elemento costitutivo del reato, e non una condizione oggettiva di punibilità, con la conseguenza che esso deve essere previsto e voluto o comunque accettato dall'agente come effetto della propria azione, indipendentemente dal fatto che costituisca o si identifichi con il fine dell'azione (Sez. 3, n. 40103 del 05/02/2015, Rv. 264798)".*

26 Cfr. sentenza qui in commento

27 Cfr. Bolognini L., Pelino E., Codice privacy: tutte le novità del d.lgs. 101/2018, Milano, 2019

28 Ai sensi dell'art. 4.6 del Regolamento: «*archivio*»: *qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*».

29 Sul concetto di larga scala il Considerando 91 del Regolamento stabilisce: «*Ciò dovrebbe applicarsi in particolare ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito ad una valutazione sistematica e globale di aspetti personali relative alle persone fisiche, basata sulla profilazione di dati dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione de dati è altresì richiesta per la la sorveglianza di zone accessibili al pubblico mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un contratto, oppure perchp sono effettuati sistematicamente su larga scala. Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati*».

30 Cfr. Gasparini I., *La tutela penale della 'privacy sanitaria' nell'era del GDPR. the criminal law protection of 'health privacy' in the GDPR era*, in "Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)", fasc.3, 1 GIUGNO 2019, pag. 863

31 Cfr. Adotti A., Bozzolan S (a cura di), *La gestione della compliance. Sistemi normativi e controllo dei rischi*, LUISS University Press, 2020, cit. p. 67.

32 Cfr. Linee guida di Confindustria disponibili qui https://www.confindustria.it/.

33 Per un approfondimento cfr. Vaciago G., *Il settore delle Nuove Tecnologie*, in Luparia donati L., Vaciago G. (a cura di), *Compliance 231. Modelli organizzativi e OdV tra prassi applicative ed esperienze di settore*, Gruppo Sole 24 Ore, Milano, 2020, pp. 187 e ss.

34 Cfr. Iuliani A., *Note minime in tema di trattamento dei dati personali*, in Europa e Diritto Privato, fasc.1, 1 MARZO 2018, pag. 293 e ss.

35 Tale nuova impostazione è di portata rivoluzionaria in quanto rispetto alla precedente impostazione che prevedeva, per garantire la compliance aziendale, il rispetto delle misure elencate nell'Allegato B del Codice Privacy; ora tale elencazione non esiste più e il titolare deve verificare i rischi connessi ai trattamenti svolti e stabilire quali siano i presidi più idonei a scongiurare i relativi rischi.

36 Cfr. Casellato M., Di maio A., La muscatella D., *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali. The Gordian knot of the "misuse of power" in the abusive access to an information system, between dogmatic suggestions and jurisprudential reflections*, in Cassazione Penale, fasc.7, 1 LUGLIO 2019, pag. 2771 e ss.

37 Il legislatore nel Regolamento tipizza solo due misure di sicurezza la psuedonimizzazione e la crittografia. Al fine di individuare le ulteriori misure di mitigazione adeguate per la prevenzione dei rischi individuati, è necessario, pertanto, ricorrere a linee guida e standard internazionali. «*Alla luce del contenuto letterale dell'art. 32 GDPR, risulta come le misure di sicurezza che ne derivano e ne contemplano la ratio, siano dettagliate all'interno del documento "Technical Guidelines for*

the implementation of minimum security measures for Digital Service Providers" dell'European Union Agency for Network and Information Security", redatto da ENISA. Tali linee guida, a loro volta, incorporano vari standard, quali ad esempio ISO/IEC 27001:2013 "Information technology - Security techniques - Information security management systems - Requirements" (ISO27001), che, trattandosi di uno standard internazionale, viene spesso usato come parametro per quanto riguarda la gestione dei sistemi di informazioni. Il 7 giugno 2019, è stato pubblicato nella Gazzetta ufficiale dell'Unione europea il nuovo regolamento sulla sicurezza informatica, Regolamento 2019/881, noto come "Cybersecurity Act" . ENISA, ossia l'agenzia europea per la sicurezza informatica, dal 2004, ha svolto un ruolo centrale per quanto riguarda la sicurezza informatica in Europa, emanando linee guida e fornendo pareri agli Stati membri, al fine di rafforzare il perimetro di sicurezza dell'Unione.
Il mandato dell'ENISA, con l'introduzione del Cybersecurity Act, diventa permanente. Il Regolamento 2019/881, infatti, istituisce un quadro comunitario di certificazione della sicurezza informatica, elaborato dalla stessa ENISA. Il Cybersecurity Act crea, pertanto, un framework di garanzie dell'applicazione delle misure di sicurezza tecniche in prodotti, servizi e processi, aiutando gli utenti finali a compiere scelte informate. ENISA, pertanto, avrà anche il compito di diffondere informazioni sul livello di sicurezza informatica di prodotti, servizi e processi, nonché di effettuare segnalazioni ai produttori o ai fornitori di servizi e processi, e avrà il potere di richiedere loro di migliorare il loro livello di sicurezza informatica.
Il Cybersecurity Act, rafforzando il ruolo di ENISA, fornisce indirettamente indicazioni relativamente al valore delle linee guida sinora emanate dall'agenzia.
Le succitate linee guida rappresentano, pertanto, il fondamentale punto di partenza per definire quali siano le misure di sicurezza nell'ottica del Regolamento 2016/679, poiché provenienti da una fonte autoritativa dal riconosciuto valore e dotate di un buon livello di completezza.
Si ritiene, inoltre, che, sia per il valore intrinseco delle fonti e per la loro autorevolezza internazionalmente riconosciuta, sia per il carattere di operatività che i documenti stessi possiedono, tali misure di sicurezza possano qualificarsi come quanto più prossimo allo stato dell'arte della sicurezza informatica, anche non esclusivamente relativa al trattamento dei dati richiesto dall'art. 32 GDPR.
Tali linee guida contengono un totale di 27 controlli, definiti da ENISA come "Security Objective", la cui implementazione risulta rilevante al fine di evitare e mitigare i rischi sottesi al trattamento dei dati personali». Per un approfondimento cfr. Capparelli F., commento all'Art.32 in Alagna i.m., Bolognini l., Capparelli F., Carpenelli M. E., Cristofari G., d'Ottavio A., Fiaschi A., Grieco L., Macinati A., Marchese M., Pelino E., Policella E., RossiChauvenet C., Sartore F., Toma A., Zipponi S., *Codice della disciplina della privacy*, Giuffrè, 2019

38 Per la definizione si veda nota n. 5.

39 Si veda ut supra quanto specificato al paragrafo 5.

40 Luparia donati L., Vaciago G. (a cura di), *Compliance 231. Modelli organizzativi e OdV tra prassi applicative ed esperienze di settore*, Gruppo Sole 24 Ore, Milano, 2020, cit. p. 196.

41 Cfr. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499

42 Genericamente, possono essere considerati AdS coloro che nell'ambito della Società svolgono le seguenti attività:
realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati);
- gestione e custodia di credenziali;
- gestione di sistemi di autenticazione e di autorizzazione;
- possibilità di modificare i privilegi di accesso ai dati;
- possibilità di modificare i livelli di accesso del sistema;
- possibilità di modificare la configurazione del sistema, ad esempio modificando gli accessi da reti esterne o annullando un sistema di autenticazione;
- gestione delle policy di backup e i supporti di backup (trasporto/scambio/custodia);
- gestione dei flussi di rete;
- amministrazione di basi di dati;
- amministrazione di reti e di apparati di sicurezza;
- amministrazione di sistemi *software* complessi.

43 A ben vedere, il precedente indirizzo giurisprudenziale che era stato espresso sul punto da parte della Suprema Corte era in senso inverso e volto a ritenere non vi fosse responsabilità del datore di lavoro in caso di accesso alla casella di posta del dipendente (si vedano in particolare le sentenze G.I.P. presso il Tribunale di Milano, 10 maggio 2002, Tribunale di Torino — Sezione distaccata di Chivasso, 20 giugno 2006-15 settembre 2006, n. 143, in Dir. Internet, 2007, 275 ss. con nota di M. Violante, E-mail aziendale? Solo per lavoro. Inoltre, per maggiori approfondimenti sul tema si veda Grotto M., *La rilevanza penale del controllo datoriale attraverso gli strumenti informatici*, in "Diritto dell'Informazione e dell'Informatica (Il)", fasc.1, 2014, pag. 57

44 In senso conforme si veda Cass. pen., sez. V, 6 giugno 2017 (dep. 17 novembre 2017), n. 52572

45 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9215890.

46 Per un approfondimento cfr. Rapporto Clusit 2020 sulla sicurezza ICT in Italia, emesso dall'Associazione italiana per la

sicurezza informatica, aggiornato a ottobre 2020 e disponibile al seguente link https://clusit.it/rapporto-clusit/.

47 Un attacco DoS (denial of service) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio. Alcuni attacchi hanno come target una particolare applicazione o servizio, ad esempio Web, SMTP, FTP, etc., altri invece mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete. Gli attacchi DDoS (distributed denial of service) amplificano la portata degli attacchi DoS. Un attacco DDoS viene infatti realizzato utilizzando delle botnet, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile. Per un approfondimento cfr. Rapporto Clusit 2020 da ultimo citato.

48 Cfr. *Responsabilità degli enti per i delitti informatici e trattamento illecito di dati in contesto Cloud Services*, Cloud Security Alliance, in https://cloudsecurityalliance.it/wp-content/uploads/2012/12/Studio-231-IT-2014.pdf, settembre 2014, Document Sponsor, cit. p. 38.

49 Cfr. in senso conforme Cass. Pen. Sez. V, 18 novembre 2011, nn. 2728, in www.penale.it.

50 Sul punto cfr. Tribunale di Cagliari 19/02/2019, n.548: «*Nel caso in cui il ladro o il ricettatore chieda al derubato il pagamento di una somma di denaro come corrispettivo della restituzione della refurtiva, si configura il delitto di estorsione, anche quando l'iniziativa provenga dalla vittima. Nel caso in cui, invece, non vi sia un concorso nel delitto presupposto, si ravvisano due ipotesi se l'intermediario chiede e ottiene dal derubato una somma di denaro come corrispettivo dell'attività di intermediazione vi è comunque estorsione, in quanto la vittima subisce gli effetti della minaccia implicita della mancata restituzione del bene. Se, invece, l'intervento dell'agente abbia avuto la sola finalità di perseguire l'interesse della vittima, per solidarietà umana, e senza conseguire una parte del prezzo, non è configurabile il reato ex articolo 629 del Cp. (Nella fattispecie, il Tribunale ha assolto l'imputato per non aver commesso il fatto, in quanto costui, dopo essere stato interpellato dalla vittima del furto di un autoradio al fine di ottenere la restituzione della refurtiva, era riuscito a far riavere una parte della stessa, senza ottenere alcun compenso per sé)*».

51 Cfr. Salvatori I., *Criminalità informatica e tecniche di anticipazione della tutela penale l'incriminazione dei "dual-use software"*, in Rivista Italiana di Diritto e Procedura Penale, fasc.2, 1 GIUGNO 2017, pag. 747 e ss

52 Tale principio, come noto, è stato per la prima volta enucleato a livello europeo dalla Corte EDU, sent. 4 marzo 2014, Grande Stevens c. Italia, che ha ritenuto sussistente la violazione dell'art. 4, Protocollo n. 7, CEDU, in relazione alla constatata duplicazione tra il procedimento per l'illecito amministrativo di manipolazione di mercato ex art. 187 D.lgs. n. 58 del 1998 (T.U.F.) ed il procedimento per l'illecito penale per il reato di cui all'art. 185 D.lgs. n. 58 del 1998 (T.U.F.). In termini analoghi, seppur con riferimento alla materia tributaria, ove la violazione del criterio ne bis in idem è stata ritenuta nel duplice giudizio che ha condotto all'applicazione di una sanzione amministrativa pecuniaria e di una pena per frode fiscale, v. Corte EDU, sent. 20 maggio 2014, Nykänen c. Finlandia. Va detto che la Corte EDU era pervenuta a conclusioni analoghe nel caso Jussila (Corte EDU, Grande Camera, 23 novembre 2006, Jussila c. Finlandia) e che si è pronunciata, in termini corrispondenti, nei casi Glantz (Id., sent. 20 maggio 2014, Glantz c. Finlandia) e Lucky Dev (Corte EDU, sent. 27 novembre 2014, Lucky Dev c. Svezia). Detto principio si sostanzia nel divieto che il medesimo fatto possa essere addebitato più volte allo stesso soggetto, qualora l'applicazione di una sola delle norme in cui il fatto è sussumibile ne esaurisca, per intero, il contenuto di disvalore sia da un punto di vista oggettivo, che soggettivo. Il principio in parola trova il suo fondamento negli artt. 15, 84, 61, 62, prima parte, 68, 581, co.2, c.p. che esprimono, all'evidenza, il criterio ermeneutico per cui è inammissibile, a fronte della medesimezza del fatto, la doppia sanzione, ogniqualvolta la natura del reato (ritenuto e sanzionato), il bene giuridico da esso tutelato e l'evento in senso giuridico che esso contempla, esauriscano integralmente il disvalore della condotta, tanto rispetto alla tipicità del fatto che sotto il profilo soggettivo. Tale concetto si distingue dal divieto di *ne bis in idem processuale* di cui all'art. 649 c.p. che si sostanzia nel divieto di un secondo giudizio per il medesimo fatto. Per un approfondimento cfr. Ranaldi G., Gaito F, *Introduzione allo studio dei rapporti tra ne bis in idem sostanziale e processuale*, in Archivio Penale, 2017, n. 1, disponibile online in http://www.archiviopenale.it/File/DownloadArticolo?codice=48dd6ab5-e271-4730-9b52-12ca7eee974d&idarticolo=15119.

53 Il concorso apparente di norme si verifca quando una medesima condotta pare riconducibile a più precetti penali ciascuno dei quali esaurisce il disvalore del fatto. Al fine di comprendere quale delle due norme trovi applicazione la giurisprudenza e la dottrina hanno elaborato diversi criteri che tuttavia sono stati ricondotti esclusivamente al principio di specialità da parte delle Sezioni Unite (cfr. Cass., SSUU, sent. 22 giugno 2017 (dep. 12 settembre 2017), n. 41588). Per un approfondimento cfr. SERRA G., *Le Sezioni Unite e il concorso apparente di norme, tra considerazioni tradizionali e nuovi spunti interpretativi*, in "Diritto Penale Contemporaneo", fasc. 11/2017.

54 L'art. 19 d.lgs. 10 marzo 2000 n. 74 -rubricato «Principio di specialità»-prevede, alco.1, che «*Quando uno stesso fatto è punito da una delle disposizioni del titolo II e da una disposizione che prevede una sanzione amministrativa, si applica la disposizione speciale*» ed, al comma 2, che «*Permane, in ogni caso, la responsabilità per la sanzione amministrativa dei soggetti indicati nell'articolo 11, co.1, del de-creto legislativo 18 dicembre 1997, n. 472, che non siano persone fisiche concorrenti nel reato*». A ben vedere, seppure in ambito tributario viga tale principio, deve rilevarsi come di sovente, nella prassi applicativa, per un identico fatto vengano instaurati entrambi i procedimenti (amministrativo e penale) nonostante la norma appena

citata consacri la specialità (che dovrebbe comportarne l'esclusiva applicazione) di quello penale.

55 In particolare, l'interessato era stato condannato, in sede tributaria, al pagamento di sanzioni amministrative per aver dichiarato falsamente il proprio reddito ed in parallelo era stato instaurato nei suoi confronti un procedimento penale per frode fiscale e per una «accounting offence» (irregolare tenuta delle scritture contabili). Anche tale secondo procedimento, si era concluso con una condanna dell'imputato, cui aveva fatto seguito al ricorso ai giudici di Strasburgo.

56 Nel caso di specie, i giudici, da un lato, hanno accertato che a seguito dell'esame delle due norme – amministrativa e penale – sotto il profilo meramente descrittivo, queste non sembravano regolare una medesima situazione e, dunque, apparentemente non fosse configurabile il «medesimo fatto»; tuttavia, dall'altro lato, la Corte, analizzando i fatti materiali, ha verificato l'identità concreta delle condotte e dunque ha ritenuto che almeno per una parte degli esercizi contabili l'interessato fosse stato perseguito e punito due volte per il medesimo fatto e, in conseguenza, ha riconosciuto la violazione del principio *del ne bis in idem*. Per un approfondimento cfr. Lissi M., Parolini L., *Limiti alla legittimità del doppio binario sanzionatorio amministrativo e penale in ambito 231,* in Rivista 231.it, Luglio-settembre 2015.

57 Recentemente il Garante ha sanzionato Unicredit per 600 mila euro per un data breach causato da accessi abusivi ai dati personali di oltre 700 mila clienti. Gli accessi abusivi sono stati effettuati utilizzando le utenze dei dipendenti di un partner commerciale esterno e riguardavano una molteplicità di informazioni, inclusi dati anagrafici e di contatto, professione, titolo di studio, estremi identificativi di documenti di riconoscimento e informazioni relative a datore di lavoro, salario, importo del prestito, stato del pagamento, «*approssimazione della classificazione creditizia del cliente*» e codice Iban. Il Garante ha ricordato che la sanzione, legata alla mancanza di adeguate misure tecniche ed organizzative, è stata determinata «*applicando la disciplina precedente l'entrata in vigore del Gdpr*», e che essa «*segue la contestazione di violazioni amministrative notificata alla banca nel maggio 2019, originata a sua volta da un provvedimento adottato dall'Autorità nel marzo 2019 con il quale il Garante aveva accertato la violazione, da parte dell'istituto bancario, delle misure minime di sicurezza previste dal Codice privacy e il mancato rispetto delle regole fissate dalla stessa Autorità nel provvedimento n. 192 del 12 maggio 2011 in materia di tracciamento delle operazioni bancarie*». Analogamente ha sanzionato per 50.000 euro la piattaforma Rousseau per la mancanza di misure di sicurezza adeguate. A livello europeo, ICO ha stabilito che British Airways dovrà pagare una multa di 22 milioni di euro (originariamente fissata in 200 milioni di Sterline, poi ridotta per il Covid a 22 milioni) perché per due anni non si è accorta che alcuni criminali informatici avevano sfruttato per 15 giorni la loro app per cellulari e la versione mobile del sito web per raccogliere i dati dei pagamenti effettuati, consistenti in nomi, cognomi, numeri di carte di credito e codici di sicurezza CVV di ogni cliente, nonché anche dettagli sulle destinazioni dei viaggi, dettagli privati e informazioni di log in, dirottando tutte le informazioni verso un server esterno sotto il loro controllo degli hacker con evidente violazione dell'art. 32 del Regolamento. Ancora ICO vuole multare l'hotel Marriott per 99 milioni di sterline in quanto, a causa di un incidente informatico sono stati esposti dati personali contenuti in circa 339 milioni di registri degli ospiti (circa 30 milioni di residenti nel SEE). In particolare, «*Si ritiene che la vulnerabilità sia iniziata quando i sistemi del gruppo Starwood hotels sono stati compromessi nel 2014. Marriott ha successivamente acquisito Starwood nel 2016, ma l'esposizione all'esterno delle informazioni sui clienti è stata scoperta solo nel 2018. L'indagine di ICO ha rilevato che Marriott non è riuscita a intraprendere un'adeguata due diligence quando ha acquistato Starwood e avrebbe dovuto fare di più per proteggere i suoi sistemi*» con conseguente violazione dell'art. 32 del Regolamento.

58 Capparelli O – Lanzino L., *Modelli di Gestione del rischio e compliance ex D.lgs. 231/2001,* Wolters Kluwer, 2016, cit. p. 67

59 Cfr. https://www.confindustria.it/wcm/connect/03561fa6-5ea6-485f-b464-541b1ee7cebb/Linee%2BGuida%2B231%2BConfindustria%2B-%2BP.%2Bgenerale%281%29.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-03561fa6-5ea6-485f-b464-541b1ee7cebb-mu2X6ON

GIURISPRUDENZA PENALE