***NOTA INFORMATIVA N. 26/2021***

# ILLECITI PRIVACY E 231

## 1. Introduzione

Nel corso dell'ultimo ventennio, si è osservato un intenso processo di estensione dell'ambito applicativo del Decreto Legislativo n. 231/2001, diretta conseguenza dell'evoluzione del contesto economico e degli strumenti tramite cui l'attività aziendale si svolge. Il notevole incremento del numero di disposizioni normative, codicistiche e non, rilevanti ai sensi del D. Lgs. 231/2001 ha inevitabilmente determinato un ampliamento anche delle tematiche d'interesse in tale ambito. Si è, dunque, assistito a un cambio di prospettiva: da un'azione preventiva legata a limitate figure di reato si è traghettati verso una generale gestione di tutti i rischi giuridici connessi ai processi e alle attività aziendali.
Tale progressivo e perdurante sviluppo della normativa in materia di responsabilità amministrativa dell'impresa, si è accompagnato a un processo di riforma della normativa in materia di protezione dei dati personali, correlato in parte alla necessità di adeguare la normativa nazionale agli standard definiti a livello europeo dal Regolamento UE/679/2016, e in parte alla necessità di attuare un sistema di tutele effettivo a protezione dei dati personali di ciascun cittadino. Anche con riferimento a tali norme si è, dunque, verificato un progressivo moto da un sistema di adempimenti formali (quasi simbolici) a un sistema di natura sostanziale, in cui la forma perde ogni rilievo a favore dell'effettività degli adempimenti svolti.
Nondimeno, nonostante la sempre crescente attenzione che la società e il legislatore riconoscono al tema, e gli interessi economici a esso correlati, non può non evidenziarsi che la tutela della privacy si colloca ancora oggi in un'aurea quasi meramente simbolica, in quanto il semplice richiamo formale alla normativa sembra ancora per molti ritenersi sufficiente strumento di attuazione degli obblighi normativi vigenti.
La tutela apprestata dall'ordinamento, che trova oggi il proprio perno nella normativa europea in materia di protezione dei dati personali, potrebbe essere facilmente rafforzata tramite l'inclusione degli illeciti privacy tra i reati presupposto della responsabilità amministrativa delle persone giuridiche di cui al D. Lgs. 231/2001. Non si dimentichi, invero, che la responsabilità da reato degli enti consente una risposta sanzionatoria anche nei casi in cui non sia possibile individuare il singolo responsabile – ipotesi particolarmente ricorrente in ambito privacy – nonché che la stessa assicura una maggiore forza in termini di prevenzione alla luce della causa di esonero dalla responsabilità per gli enti che si siano adoperati nella preventiva adozione ed efficace attuazione dei Modelli 231.
Parimenti, non si può poi trascurare che lo stesso legislatore del 2018 nel costruire i reati a tutela della privacy sembra aver individuato nella disciplina della responsabilità amministrativa della persona giuridica la loro naturale collocazione, come desumibile dalle caratteristiche strutturali delle ipotesi di reato oggi previste dal D.Lgs. 231/2001, modellate sull'interesse/vantaggio dell'impresa, nonché dalla previsione di una specifica ipotesi attenuante correlata al pagamento della sanzione da parte di quest'ultima.

## 2. Le finalità dell'impianto normativo

Benché il Decreto Legislativo 231/2001 nasca come strumento di prevenzione dei fenomeni corruttivi, l'ambito di applicazione dello stesso si è nel tempo notevolmente ampliato. Giova, invero, ricordare che – in attuazione della Legge n. 300 del 29 settembre 2000 – il Governo con il D. Lgs. 8 giugno 2001 n. 231 ha, per la prima volta, riconosciuto la capacità dell'impresa di delinquere nonché la sua natura di autonomo centro di interessi e rapporti giuridici, punto di riferimento di precetti di varia natura, e matrice di decisioni e attività di soggetti che operano in nome, per conto o comunque nell'interesse della società. L'adozione della suddetta normativa ha pertanto consentito da una parte di adempiere agli obblighi discendenti dalla Convenzione OCSE a cui l'Italia aveva aderito, dall'altra di colmare la lacuna normativa consistente nella mancata previsione di una responsabilità degli enti e di rispondere alle esigenze di politica criminale correlate alle sempre più frequenti casistiche di crimini d'impresa. Ebbene, in tal

contesto, al momento della redazione del Decreto Legislativo, ai fini dell'individuazione dell'ambito oggettivo di operatività della responsabilità da reato delle persone giuridiche, si prospettarono dinanzi al Legislatore due diverse scelte metodologiche: quella c.d. della *Natur der Sache* e quella, opposta, dell'elencazione tassativa dei reati-presupposto. Il Legislatore italiano ha optato per la seconda alternativa metodologica.

Ciò posto, in modo più o meno inconsapevole, lo stesso ha tuttavia intrapreso la via della c.d. formazione progressiva del Catalogo 231, procedendo in principio all'inserimento nella c.d. Parte Speciale del Decreto (i.e. artt. 24 e 25) del ridottissimo numero di reati indicati nelle convenzioni europee e internazionali che il Decreto Legislativo era chiamato a ratificare in attuazione della Legge Delega n.300/2000. Difatti, mentre nella prima bozza il Decreto presentava una struttura complessa in quanto articolata in ben sedici autonome fattispecie (tra cui, oltre ai reati di corruzione, anche i reati in materia di radiazioni ionizzanti, i reati in materia dei pericoli di incidenti rilevanti connessi con determinate sostanze pericolose, etc.), al momento del varo definitivo della norma il Legislatore ha operato un improvviso ridimensionamento della Parte Speciale, sopprimendo molti dei reati ascrivibili alla politica di impresa e alla criminalità economica. Tale impostazione minimalista è però stata ben presto abbandonata.

Il numero eccessivamente ridotto delle fattispecie-presupposto che costituiva la Parte Speciale originaria e che si era rivelato sproporzionato per difetto rispetto agli intenti del Legislatore è stato, infatti, successivamente oggetto di plurime integrazioni, aventi quale unico comune denominatore – alle volte solo in principio, altre anche in concreto – la prevenzione e repressione della cd. politica criminale d'impresa e nelle sue logiche del profitto. Non può tuttavia negarsi che tale meccanismo di formazione progressiva ha determinato un'estensione del Catalogo 231 spesso disorganica, caotica e sorretta da ragioni meramente simboliche, correlate a temi di politica criminale propri del momento storico in cui si colloca il singolo intervento normativo.

Da quanto sopra deriva che, in taluni casi, le modifiche normative operate sono state caratterizzate da un'effettività pressoché nulla. Si fa in particolare riferimento alle riforme della prima metà degli anni duemila che hanno portato all'inserimento nel catalogo dei reati-presupposto dei delitti di falsificazione di monete e in carte di pubblico credito, di terrorismo internazionale o di eversione dell'ordine democratico e di mutilazioni degli organi genitali femminili: reati che non hanno trovato ancora applicazione, né probabilmente mai la troveranno.

Di contro, alcune fattispecie di sicura pregnanza e che trovano frequente applicazione nella realtà, non sono ancora oggi state inserite all'interno del Catalogo 231 e tra esse figurano anche i cd. illeciti privacy, che costituiscono il focus del presente elaborato.

**3. L'incrocio tra illeciti privacy e 231**

L'enorme valore del bene giuridico protetto dalle disposizioni in materia di protezione dei dati personali e la rilevanza da questo assunta nell'ambito delle attività d'impresa sono state oggetto di un primo riconoscimento da parte Legislatore del 2013, il quale – seppur in ritardo e con modalità non pienamente condivisibili dal punto di vista sistematico – aveva inserito i cd. delitti privacy all'epoca vigenti all'interno del catalogo dei reati presupposto del D. Lgs. 231/2001 per il tramite del D. L. 93/2013. Il Decreto Legge in parola nasce in realtà come strumento di rimedio a un errore sistematico commesso precedentemente dal Legislatore. Difatti, già nel 2008, in attuazione della Convenzione Cybercrime di Budapest del 20015, con la L. n. 48/20086, era stato introdotto nel D. Lgs. 231/2001 l'art. 24-bis, che, pur se rubricato Delitti informatici e trattamento illecito di dati, ha inserito nel novero del Catalogo 231 i soli reati di natura informatica. Tale scollamento tra la rubrica e il contenuto della disposizione normativa fu sin da subito oggetto di attenzione. Tanto è vero che, in sede di audizione informale alla Camera dei deputati, era stata avanzata la proposta di modificare il testo della rubrica dell'articolo 24-bis eliminando il riferimento all'inciso trattamento illecito dei dati per una maggiore coerenza sistematica della norma.

Nondimeno, il Legislatore – pur intervenendo sulla rubrica della norma eliminando il riferimento all'attentato a impianti di pubblica utilità – ha mantenuto inalterato il riferimento al trattamento dei dati. L'intervento legislativo del 2013 ebbe dunque il fine – tra gli altri – di coordinare la rubrica della norma introdotta cinque anni prima con il testo della disposizione, integrando il comma I dell'art. 24- bis D. Lgs.

231/2001 come segue: in relazione alla commissione dei delitti di cui agli articoli 615- ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quarter, 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. 23139, 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.

L'inclusione dei reati privacy tra i reati presupposto del D. Lgs. 231/2001 fu però molto breve: solo due mesi più tardi, nell'ottobre 2013, la Legge di conversione n. 113 ha disposto l'eliminazione di ogni riferimento alle fattispecie delittuose contenute nel D. Lgs. 196/2003 (cd. Codice Privacy).

Le motivazioni poste a fondamento di tale mancata finalizzazione sono probabilmente riconducibili alle critiche provenienti da due fronti.

La dottrina fu, infatti, critica soprattutto con riferimento alla collocazione sistematica delle disposizioni normative in parola. Contrari furono anche gli stessi soggetti destinatari della norma, ossia i rappresentanti delle categorie imprenditoriali che, con molta probabilità preoccupati dell'ingente esborso economico correlato alla necessaria revisione dei Modelli 231 adottati ex art. 6 D. Lgs. 231/2001, chiesero l'abrogazione dell'art. 24-bis D. Lgs. 231/2001 o almeno l'esclusione dal testo del richiamo ai reati privacy.

Unica voce di senso opposto fu quella della Suprema Corte: gli Ermellini ebbero invero modo di apprezzare l'opportunità e adeguatezza dell'intervento normativo nella Relazione n. III/01/2013 del 22 agosto 2013, in cui definirono l'introduzione dei reati privacy nel D. Lgs. 231/2001 un evento 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 231/2001. Come spesso accade a fronte dell'inerzia del Legislatore, è proprio la giurisprudenza a tentare di colmare il divario determinato dalla mancata estensione del Catalogo 231 agli illeciti privacy, ricorrendo alle categorie degli illeciti amministrativi dei reati informatici, dell'associazione per delinquere e del riciclaggio e autoriciclaggio.

A conferma di quanto sopra, giova richiamare una recente sentenza pronunciata dal T.A.R. Lazio nell'ambito di un procedimento istruttorio avviato nei confronti di *Facebook Inc. e Facebook Ireland Limited*, su input dall'Autorità Garante per la Concorrenza e il Mercato nel dicembre 2018. Con la sentenza n. 261 del 10 gennaio 2020 (TAR Lazio, sez. I, 18 dicembre 2019, dep. 10 gennaio 2020, n. 261), il T.A.R. Lazio ha invero espressamente riconosciuto il valore economico dei dati personali. Difatti, la società ricorrente aveva sollevato un'eccezione di incompetenza affermando che la stessa spettasse all'Autorità Garante per la privacy, non ritenendo sussistente nel caso de quo alcun corrispettivo patrimoniale e, quindi, un interesse economico dei consumatori da tutelare.

Nel rigettare tale eccezione, il Giudice amministrativo ha chiarito che tale approccio, basato esclusivamente sulla concezione della tutela del dato personale nella sua accezione di diritto fondamentale dell'individuo, sconta una visione parziale della potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un asset disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di controprestazione in senso tecnico di un contratto. Il T.A.R., dunque, ha evidenziato la sussistenza di un campo di protezione per il dato personale, ulteriore a quelli già riconosciuti e disciplinati dal Regolamento UE 2016/679, che vede il dato stesso quale possibile oggetto di una compravendita tra gli operatori del mercato o tra questi e i soggetti interessati.

Pertanto, la patrimonializzazione del dato personale impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione a un contratto per la fruizione di un servizio, quale è quello di utilizzo di un social network.

**4. GDPR e codice privacy**

A conferma della sempre crescente rilevanza dei dati personali e dell'aumentare del valore economico agli stessi riconosciuto all'interno del sistema odierno, nel corso del 2018 si è assistito a un'importante attività di riforma che si è concretizzata nelle profonde innovazioni operate dapprima dal Regolamento

UE/679/2016 (cd. GDPR) e successivamente dal D. Lgs. 101/2018. I due provvedimenti normativi in parola hanno determinato una netta inversione di marcia, determinando un traghettamento delle aziende italiane da un approccio formale a un approccio sostanziale fondato sul principio di accountability.
Con il Decreto Legislativo n. 101 del 10 agosto 2018, il Legislatore è quindi intervenuto riformando anche gli aspetti penalistici della materia, depenalizzando alcune fattispecie incriminatrici, al fine di scongiurare possibili violazioni del principio del ne bis in idem, e introducendo nuove condotte delittuose.
La prima ipotesi di reato oggi prevista dal Codice Privacy è normata dall'art. 167, rubricato Trattamento illecito di dati. Tale fattispecie, come novellata nel 2018, punisce diverse condotte consistenti nell'arrecare nocumento all'interessato in violazione di specifiche disposizioni normative, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato medesimo.
Con riferimento a tale fattispecie, giova poi evidenziare che il Legislatore ha previsto un'ipotesi di riduzione della sanzione penale applicata nei casi in cui per il medesimo fatto sia già stata applicata e riscossa a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria del Garante per la protezione dei dati personali. Il Legislatore del 2018 ha poi introdotto due ulteriori fattispecie incriminatrici agli artt. 167-bis e 167- ter del Codice Privacy, rubricati, rispettivamente, Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala e Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala. In particolare, l'art. 167-bis punisce la comunicazione e la diffusione, al fine di trarre profitto per sé o per altri o al fine di arrecare danno, di un archivio automatizzato o di una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, anche, ai sensi del comma II, quando la condotta sia attuata senza consenso e questo sia richiesto per le operazioni di comunicazione e diffusione.
Il reato di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala di cui all'art. 167-ter si configura, al contrario, con l'acquisto, al fine di trarre profitto per sé o per altri o al fine di arrecare danno, di un archivio automatizzato o di una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala. A differenza di quanto previsto dall'art. 167-bis, pertanto, l'art. 167-ter punisce esclusivamente il soggetto attivo che, con artifizi o raggiri, acquisisca l'archivio elettronico di dati personali o una sua parte sostanziale. Con riferimento a tali ultime fattispecie, appare opportuno osservare che a dispetto dell'utilizzo del termine chiunque, la relazione illustrativa al D. Lgs. 101/2018 chiarisce che si tratta di reati propri del soggetto tenuto al trattamento professionale dei dati per obbligo di legge.
Un'ulteriore peculiarità di tali disposizioni è poi rinvenibile anche nell'assenza di tassatività là dove rinviano al generico concetto di larga scala, che non trova definizione né nel Regolamento UE n. 679/2016 né nel Codice Privacy. La novella del 2018 è intervenuta con riferimento all'art. 168 del Codice Privacy che oggi punisce – oltre alla già prevista condotta di Falsità nelle dichiarazioni al Garante – anche la condotta di Interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante. Trattasi di un reato particolarmente insidioso in quanto astrattamente realizzabile anche nel caso in cui i fatti o le informazioni non corrispondenti alla realtà non siano direttamente comunicati al Garante ma a soggetti delegati da quest'ultimo (es. il corpo della Guardia di Finanza a cui è delegata l'attività ispettiva).
Appare opportuno precisare che in ogni caso la sopradescritta condotta deve essere necessariamente connotata, sotto il profilo dell'elemento soggettivo, dalla consapevolezza della falsità delle informazioni o delle documentazioni trasmesse e, pertanto, non sarà sufficiente a integrare il reato la semplice trasmissione di dati forniti da terzi.
Da ultimo, il D. Lgs. 101/2018 ha posto nuovamente in vigore il reato di Inosservanza dei provvedimenti del Garante di cui all'art. 170 del Codice Privacy, il quale punisce chiunque, essendovi tenuto, non osservi un provvedimento adottato dal Garante. Ci si riferisce in particolare ai provvedimenti in cui il Garante esercita il proprio potere di imporre una limitazione provvisoria o definitiva al trattamento, ai provvedimenti in materia di misure di garanzia per i trattamenti di dati genetici, biometrici o relativi alla salute, nonché ai provvedimenti generali con cui il Garante conferma le prescrizioni contenute nelle vecchie Autorizzazioni Generali, fatta salva la compatibilità con il GDPR.

**5. Riforma necessaria?**

Dato il contesto appena delineato ed entrando in *medias res* nel tema oggetto di analisi, la trattazione si deve soffermare sulle ragioni per cui l'inserimento dei reati privacy nel Catalogo dei Reati 231 si configura oggi come un appuntamento non solo opportuno ma anche necessario. In primo luogo, l'inclusione degli illeciti privacy nel Decreto consentirebbe al Legislatore di dotare l'Italia di un ulteriore e più pregnante strumento di contrasto dei cybercrimes, in accordo alle previsioni della citata Convenzione di Budapest del 2001. Difatti, le disposizioni in parola furono adottate prima in sede europea e, successivamente, nazionale al fine di contrastare e prevenire in modo efficace la criminalità in rete.

Non si può però non evidenziare che il cybercrime si è nel tempo evoluto, al pari della società e dell'economia: nel 2008 le condotte oggetto di attenzione si identificavano per lo più in accessi illeciti ai sistemi informatici o in attività finalizzate a comprometterne il corretto funzionamento.

Lo stato evolutivo dei dispositivi e delle applicazioni dell'epoca esauriva invero in tali ambiti le attività concretamente eseguibili. È però innegabile che nell'ultimo decennio si è assistito a un'evoluzione straordinaria delle funzionalità dei sistemi informativi e, di conseguenza, delle condotte tramite questi esplicabili.

In tal scenario, l'attore principale è dunque divenuta l'identità digitale, ovvero l'insieme di informazioni – comuni e particolari – che il singolo sistema o un insieme di sistemi informatici può porre in correlazione con riferimento a una persona fisica. Informazioni che così strutturate costituiscono una sorta di alter ego digitale di ciascun cittadino. Pertanto, muovendo dal presupposto che nella mente del Legislatore del 2008 il bene giuridico di rilievo per le previsioni normative in commento era la sicurezza dei sistemi informatici, le fattispecie introdotte all'art. 24-bis D. Lgs. 231/2001 si configuravano come più che sufficienti a soddisfare le esigenze correlate alla Convenzione di cui erano attuazione. Nondimeno, nel contesto socioeconomico odierno in cui il vero valore è rappresentato non dal sistema informatico strettamente inteso bensì dalle informazioni in esso contenute, è necessario compiere un'opera di attualizzazione.

Le finalità di tutela proprie della Convenzione del 2001 e della L. 48/2008 potranno quindi essere effettivamente soddisfatte solo quando l'ordinamento vigente sarà implementato con strumenti in grado di perseguire non solo l'integrità dei sistemi ma anche la legittimità dei trattamenti e delle operazioni effettuati per il loro tramite. Un ulteriore elemento da cui discende l'opportunità di integrazione del Catalogo 231 in ambito privacy è poi ravvisabile nelle caratteristiche strutturali delle fattispecie incriminatrici previste nel Codice Privacy.

Invero, come noto, uno dei nodi fondamentali della normativa sulla responsabilità amministrativa delle persone giuridiche risiede nell'individuazione nel caso concreto dei criteri d'imputazione anche oggettivi, tra i quali figurano l'interesse o vantaggio dell'ente. Le due condizioni applicative in parola sono state nel tempo oggetto di molteplici analisi e commenti, soprattutto con riferimento a quelle fattispecie di reato che, ferma la facile individuazione della persona fisica che con la sua condotta positiva o omissiva ha materialmente integrato la fattispecie di reato, non consentono un'identificazione immediata dell'interesse o vantaggio dell'ente (i.e. reati colposi di cui all'art. 25-septies D. Lgs. 231/2001).

Con riferimento ai reati privacy di cui agli artt. 167 e s. Codice Privacy si ravvisa la circostanza opposta: il fatto di reato è difficilmente imputabile a una persona fisica, in quanto strutturalmente cucito sull'organizzazione societaria: di contro, lo stesso è facilmente riconducibile nell'orbita dell'interesse o vantaggio di un ente. A conferma di tale asserzione, è sufficiente pensare agli ingenti profitti discendenti dall'utilizzo illecito di dati personali da parte di compagnie telefoniche e agenzie di marketing e ai benefici derivanti dalle medesime attività per la singola persona fisica. Dalle riflessioni sopra brevemente condotte con riferimento alla struttura dei reati privacy oggi vigenti discendono ulteriori elementi a sostegno del necessario inserimento dei reati in parola nel Catalogo 231, attinenti alla ratio dell'intero corpus normativo privacy nonché alla disciplina del D. Lgs. 231/2001.

Si badi invero che gli obblighi e i divieti di cui agli artt. 2-sexies e s. Codice Privacy, il cui mancato adempimento integra la fattispecie di reato di cui all'art. 167 del medesimo Codice, sono vincolanti esclusivamente per le persone giuridiche o per le persone fisiche che operano nell'ambito di un'attività economica-commerciale. La normativa privacy oggi vigente trova invero applicazione esclusivamente nel

caso in cui il Titolare esegue un trattamento dei dati personali per l'esercizio di attività a carattere non personale o domestico. Alla luce di ciò, può un privato cittadino commettere un reato di cui non può essere soggetto attivo, non figurando, se non in casi eccezionali, tra i destinatari della normativa la cui violazione è presupposto necessario del reato? La risposta non può che essere negativa.
La mancata menzione degli illeciti privacy tra i reati presupposto appare, dunque, palesemente in contrasto con la logica che anima la normativa europea in materia di dati personali, nonché con lo stesso intervento riformatore del Legislatore italiano del 2018 che sembra aver definito e posto in vigore delle norme atte a punire le condotte illecite eseguite da una persona fisica solo quando opera in nome e per conto di un ente.
La natura *duetreunistica* dei reati in parola emerge poi ancora più chiaramente dal dettato del comma V dell'art. 167 là dove prevede una riduzione della sanzione applicabile al reo quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita. Lo stesso Legislatore sembra dunque porre la persona giuridica tra i soggetti attivi della fattispecie. Ulteriori elementi corroboranti la tesi che si sostiene derivano poi dai profili di connessione e sovrapposizione tra le due normative in commento, il D. Lgs. 231/2001 e il Codice Privacy.
Le due norme si configurano come norme di compliance, che rinvengono la propria funzione teleologica nel prevenire e ridurre il verificarsi dei rischi aziendali e, di conseguenza, si muovono secondo logiche perfettamente coincidenti. Entrambe presuppongono, pertanto, quale primo adempimento un'attenta analisi del rischio specifico dell'impresa. Infatti, al fine di predisporre un Modello di Organizzazione ex art. 6 D.Lgs. 231/01, occorre procedere con un risk assessment e una gap analysis volti a mappare i rischi di verificabilità dei Reati 231 nell'ambito delle attività aziendali e individuare eventuali azioni correttive finalizzate alla loro mitigazione. Parimenti, in materia di protezione dei dati personali, l'art. 35 del Regolamento (UE) 2016/679 prevede l'obbligo di esecuzione del Data Protection Impact Assessment (DPIA), ossia di una valutazione del livello di rischio che una violazione dei dati possa tradursi in una lesione dei diritti e delle libertà degli interessati. Anche nella fase successiva, ovvero quella di adozione di misure idonee a prevenire o ridurre i rischi identificati, le due norme si muovono in modo sincrono.
Invero, così come l'art. 6 D. Lgs. 231/2001 prevede espressamente che l'ente debba dotarsi di Modelli idonei a prevenire i rischi e controllare le aree rilevanti in ottica 231, la normativa privacy richiede l'adozione di sistemi e misure tecnico-organizzative necessarie per il perseguimento del pieno rispetto della disciplina.
A limine di quanto sopra, ci si vuole soffermare su uno dei temi più dibattuti all'indomani dell'entrata in vigore dei nuovi illeciti privacy nel settembre 2018, ovvero la possibile violazione del principio del ne bis in idem di cui agli artt. 4, prot. 7, CEDU e 50 CDFUE nelle ipotesi in cui per gli stessi fatti oggetto di una sanzione amministrativa comminata dal Garante privacy sia avviato un procedimento penale.
Come noto, il principio in parola (come interpretato dall'ormai consolidata giurisprudenza della Corte europea dei diritti dell'uomo, della Corte di giustizia dell'Unione europea e della Corte di Cassazione) vieta di punire due volte un soggetto per un medesimo fatto storico. Il tema del rapporto tra disposizioni penali e amministrative è già stato affrontato dal Legislatore del 2018.
Difatti, nella Relazione al D.Lgs. 101/2018, si è evidenziata la necessità di depenalizzare alcune delle fattispecie incriminatrici vigenti in quanto la loro sovrapposizione alle sanzioni amministrative definite in sede europea avrebbe potuto integrare una violazione del principio del ne bis in idem. Lo stesso Legislatore ha poi provveduto all'istituzione di un flusso immediato di coordinamento tra il Pubblico Ministero e il Garante Privacy, nonché alla previsione di una circostanza attenuante Meccanismi che, a parere di chi scrive, consentono di soddisfare il criterio della *sufficiently close connection* in *substance and time* elaborato dalla giurisprudenza comunitaria.

**6. Conclusioni**

I tempi appaiono oltre modo maturi per una riforma attesa da tempo.
In primo luogo, appare evidente che le fattispecie di reato introdotte dal D. Lgs. 101/2018 ben si coordinano con le caratteristiche normative e i principi ispiratori della responsabilità amministrativa degli

enti. La previsione degli illeciti privacy nel D. Lgs. 231/2001 consentirebbe di dare piena attuazione a un principio cardine del nostro ordinamento penale, ossia il principio di tassatività, riducendo i casi di interpretazioni estensive da parte della giurisprudenza finalizzate a colmare tale anacronistico vulnus, determinato dalla previsione di una tutela normativa a esclusiva protezione del mezzo (i.e. sistema/strumento informatico) e non del suo contenuto e, consequenzialmente, di un bene giuridico particolarmente rilevante quale la dignità umana.

Non può tacersi che, nel contesto odierno, le società e gli enti associativi in genere (soprattutto in ambito medico-farmaceutico) si stanno impegnando in una sempre maggiore digitalizzazione delle attività e delle informazioni e che in tal contesto la compliance privacy ha assunto un'importanza sempre crescente. Di conseguenza, perdono ogni attualità anche gli indugi correlati all'eccessiva onerosità delle attività di aggiornamento dei Modelli organizzativi manifestati dagli imprenditori nel 2013. È, nondimeno, indubbio che solo un intervento strutturato del Legislatore potrà perseguire un diffuso cambio di approccio che consenta di sfruttare al meglio le spinte sinergiche che provengono dalle due normative, nonché di ridurre costi ed energie, evitando sovrapposizioni e duplicazioni, e di rendere l'intero sistema di compliance maggiormente effettivo ed efficace.

17 maggio 2021

A cura di Avv. Bruna Capparelli