FORNARI E ASSOCIATI
STUDIO LEGALE

FOCUS

Il trattamento dei dati: rischi penali e compliance dell'impresa

fornarieassociati.com

Milano • Roma

Gennaio 2021

PREMESSA

Uno degli *hot topics* al centro del dibattito politico, sociale e giuridico di questi mesi segnati dalla pandemia è quello della tutela della *privacy*.

In auge dal 2018, quando è entrato in vigore il noto GDPR (Reg. UE n. 679/2016), la protezione dei dati personali ha visto una crescente attenzione da parte dell'opinione pubblica e degli operatori del diritto, questi ultimi letteralmente travolti dalla repentina necessità di confrontarsi con gli effetti collaterali dell'uso della tecnologia.

Sotto il profilo della riservatezza e della protezione dei dati, i rischi connessi all'utilizzo degli strumenti digitali sono infatti molteplici e in continuo aumento: basti pensare alle recenti spinose questioni riguardanti l'informativa sulla *privacy* della piattaforma di messaggistica *Whatsapp*, il "controllo a distanza" dei lavoratori imposto dallo *smart-working*, la falla del sito dell'INPS in uno dei noti *click day* della scorsa primavera e, ancora, l'acceso dibattito sviluppatosi intorno al tracciamento dell'*app* Immuni.

Ben consapevole di tali pericoli, il legislatore nazionale, su impulso di quello comunitario, è intervenuto al fine di approntare una concreta tutela, anche di natura penale.

Sono stati quindi introdotti alcuni obblighi che le imprese – a pena di sanzioni molto salate – sono chiamate a rispettare nell'esercizio delle loro attività, così da garantire il diritto delle persone fisiche alla riservatezza e l'interesse collettivo a un trattamento sicuro dei dati personali.

Già nel 2008, e quindi ben prima del GDPR, il legislatore italiano aveva avviato un processo di responsabilizzazione delle società rispetto ai rischi penali di matrice digitale con l'introduzione dell'art. 24 *bis* nel d.lgs. n. 231/2001, che sancisce la responsabilità amministrativa da reato dell'ente sia per le fattispecie strettamente informatiche, tra cui l'accesso abusivo ad un sistema informatico (art. 615 *ter* c.p.), l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.), il danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.), sia per alcune ipotesi di reato comune realizzate facendo ricorso all'informatica, come la falsità ideologica o materiale commessa su documenti informatici pubblici (art. 491 *bis* c.p.).

Considerata la crescente rilevanza che la protezione penale della riservatezza e dei dati personali ha nel nostro ordinamento, l'obiettivo di questo *focus* è quello di ripercorrere le principali tappe dell'evoluzione normativa in materia e svolgere una disamina dei tratti essenziali della disciplina penale attualmente vigente, per poi soffermarsi sulle modalità con cui il diritto alla *privacy* può trovare tutela nelle realtà societarie.

I. DAL DIRITTO ALLA RISERVATEZZA ALLA PROTEZIONE DEI DATI PERSONALI: L'EVOLUZIONE NORMATIVA

Data la materia altamente dinamica, e il suo progressivo evolversi di pari passo con la tecnologia, abbiamo assistito a un susseguirsi di interventi normativi in tema *privacy*.

In ambito penale, sulla scorta dell'insegnamento europeo, il legislatore ha ampliato il novero delle condotte rilevanti e inasprito il trattamento sanzionatorio, intervenendo altresì sulla individuazione del bene giuridico protetto dalle norme.

In particolare, muovendo dal concetto originario di riservatezza di matrice statunitense, intesa come "*the right to be let alone*" (il "diritto ad essere lasciato da solo"), la tutela penale si è estesa al *dato personale*, ossia a "*qualunque informazione relativa a persona fisica, identificata od identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*" (art 4, n. 1, GDPR).

Come si declina quindi oggi il diritto alla *privacy*?

La *privacy* è il **diritto alla riservatezza** delle informazioni personali e della propria vita privata, ma anche il diritto a non vedere trattati i propri dati senza **consenso**, nonché ad esigere l'adozione di tutte quelle cautele tecniche e organizzative che garantiscano il **trattamento corretto e sicuro dei dati.**

Il diritto alla riservatezza fa il suo esordio nel Bel Paese grazie all'importante pronuncia della Corte di Cassazione n. 2129/1975 (**caso Soraya**), che ne ha delineato i connotati essenziali.

In particolare, la Suprema Corte ha affermato che tale diritto protegge "***tutte quelle vicende […] il cui carattere intimo è dato dal fatto che si svolgono in un domicilio ideale****, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza)*".

Il merito di questa pronuncia si individua proprio nell'aver accordato **protezione autonoma al rispetto della vita privata di per sé considerato**, ossia anche nel caso in cui le vicende – personali e familiari – bisognose di tutela si collocassero al di fuori delle ipotesi allora espressamente previste dalla legge ordinaria (*e.g.*, la violazione di domicilio punita dall'art. 614 c.p., a tutela dell'intimità domestica).

La giurisprudenza sia di merito che di legittimità, che nel tempo ha elaborato e affinato il concetto di riservatezza, ha sin da principio riconosciuto il suo fondamento normativo nell'**art. 2 della Costituzione**, elevandolo a **diritto inviolabile** della persona e della personalità.

Come già accennato, l'evoluzione culturale ha poi comportato la necessità di focalizzare la tutela anche su un piano diverso.

Non era più sufficiente tutelare il solo diritto a non vedere diffuse le proprie informazioni personali senza prima aver espresso uno specifico consenso, ma era divenuto necessario prevedere un **"*sistema*" di integrità e trattamento** dei dati che identificano la persona.

Si era dunque avvertita l'esigenza di passare da una struttura "escludente", ossia tale da allontanare l'altrui sguardo indesiderato, a una struttura che ponesse ancor di più la persona e la sua identità – digitale – al centro della tutela; in altri termini, l'esigenza di introdurre un sistema di protezione che andasse oltre la sfera meramente personale, garantendo **il controllo sulla circolazione dei propri dati.**

Con l'entrata in vigore del GDPR, e la consequenziale modifica al Codice della *Privacy* intervenuta con il **d.lgs. 10 agosto 2018, n. 101**, trova finalmente realizzazione nell'ordinamento italiano quel microsistema autonomo, basato sul nuovo bene giuridico di settore: il trattamento dei dati personali.

Si consideri che anche la giurisprudenza – principalmente europea – condivideva il bisogno di mutare l'approccio consolidatosi negli anni precedenti, basato sulla mera tutela della riservatezza.

La Corte di Lussemburgo, infatti, aveva più volte evocato il concetto di "*sovranità digitale*", allo scopo di indurre i legislatori nazionali a prendere in debita considerazione l'esistenza di un nuovo ordinamento giuridico, ***l'ordinamento digitale,*** inteso come spazio immateriale in cui confluiscono e vengono trattati i dati personali digitali.

Sul versante penale, la nascita di questo microcosmo ha oltremodo migliorato l'efficienza e l'effettività della tutela; si può pacificamente ritenere che sia nato un vero e proprio ***statuto penale della riservatezza digitale***, seppur suscettibile di miglioramenti.

In definitiva, con il GDPR viene coronato il mutamento nell'approccio alla tutela della *privacy*, concetto di natura poliedrica e dalla valenza polisemantica.

Architravi della nuova disciplina sono i fondamentali principi del consenso e di *accountability*, quest'ultimo inteso come la responsabilizzazione di chi è titolato a trattare i dati, cui viene imposta, tramite l'onere di rendicontazione, una gestione idonea a garantire la piena conformità del trattamento ai principi sanciti dal Regolamento e dalla legislazione interna.

L'individuazione del diritto alla *privacy* con il diritto alla protezione dei dati personali è dunque il punto di arrivo di una lunga evoluzione concettuale, resasi necessaria in virtù dello sviluppo delle nuove tecnologie, nell'ottica di

garantire al singolo un'ampia visuale sull'effettivo uso che viene fatto dei propri dati, per consentirgli di autodeterminarsi in merito.

In altri termini, la vigente normativa in materia di dati personali è volta ad assicurare a ciascuno il diritto ad esercitare un controllo su quei dati personali – prodotti più o meno consapevolmente – che diventano oggetto di trattamento da parte di apparati informatici che li elaborano.

Le violazioni di tale diritto sono duramente sanzionate, su entrambi i piani, amministrativo e penale; ed è proprio di quest'ultimo che ci occuperemo nel prosieguo.

II. I REATI PREVISTI DAL NUOVO CODICE *PRIVACY*

Al fine di poter raggiungere una maggiore efficienza nella tutela dei dati personali come stabilito dal GDPR, sul fronte penale il legislatore ha previsto nuove fattispecie di reato (artt. 167 *bis, Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala* e 167 *ter, Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*), ha apportato profonde modifiche a quelle già esistenti (art. 167, *Trattamento illecito di dati*) e, infine, ne ha abrogate alcune (art. 169, *Misure di di sicurezza*).

Ci si trova difronte, così, a una **nuova trilogia punitiva.**

Come sopra accennato, la riforma ha comportato anche l'abrogazione di alcune fattispecie preesistenti. Nello specifico, l'art. 27, comma 1, lett. c), numero 2), del d.lgs. n. 101/2018 ha abrogato l'art. 169, che disciplinava le misure di sicurezza da applicarsi nei casi in cui il soggetto che aveva l'obbligo di adottare le misure minime previste dall'art. 33 del Codice *Privacy* (ora anch'esso abrogato) non avesse adempiuto al suo dovere.

Esaminiamo ora le singole fattispecie.

Per quanto riguarda il reato di **trattamento illecito di cui all'art. 167**, il legislatore è intervenuto non solo mediante la previsione di nuovi commi recanti ipotesi aggravate, ma anche andando a mutare radicalmente la struttura del reato.

Più in dettaglio:

- si passa da un reato di pericolo concreto a un **reato con evento materiale di danno**;
- il ***nocumento*** non è più una condizione obiettiva di punibilità, ma diventa l'**evento del reato**;
- si richiede il **dolo specifico**, alternativamente di profitto o di danno;
- il reato resta formalmente comune, anche se, a ben vedere, *chiunque* è un soggetto attivo "condizionato" alla

qualifica di responsabile ovvero titolare del trattamento.

Per quanto è dato conoscere a poco più di due anni dall'entrata in vigore della nuova fattispecie, il risultato di tali incisive modifiche è stato quello di rendere più difficoltoso l'accertamento giudiziale e, per l'effetto, la effettiva punibilità del reato, in controtendenza quindi con le finalità dichiarate e perseguite dal legislatore europeo.

Gli articoli 167 *bis* e 167 *ter*, che disciplinano rispettivamente la **comunicazione e diffusione illecita** e **l'acquisizione fraudolenta di dati personali**, configurano invece due ipotesi di reato del tutto nuove.

Va specificato che, anche per queste fattispecie criminose, il legislatore individua "*chiunque*" quale soggetto agente, anche se è di tutta evidenza che rivestire il ruolo di gestore di un archivio automatizzato o parte di esso sia presupposto necessario per un eventuale addebito penale.

I comuni tratti caratterizzanti di queste nuove ipotesi criminose sono **due concetti** anch'essi **assolutamente nuovi** nel panorama normativo italiano: l'"*archivio automatizzato*" e il "*trattamento su larga scala*".

Archivio automatizzato

Ambedue le condotte descritte negli artt. 167-*bis* e 167-*ter* assumono rilevanza penale solo se la comunicazione, la diffusione o l'acquisizione fraudolenta riguardi un archivio automatizzato o una parte sostanziale di esso, ossia, *ex* art. 4, n. 6 GDPR, "*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*".

Si deduce, pertanto, che l'archivio non è un'indeterminata quantità di dati personali, ma una struttura ben organizzata che li raccoglie, secondo precisi criteri di classificazione e di indicizzazione che rispondono anche al carattere tecnologico del tipo di informazione.

Trattamento su larga scala

Del secondo elemento costitutivo delle nuove fattispecie, ossia "*il trattamento su larga scala*", il GDPR non dà alcuna definizione.

Tuttavia, il Considerando n. 91 del Regolamento ne delinea i contorni, definendoli come operazioni "*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*** *che potenzialmente presentano un* ***rischio elevato***".

Dinanzi a questo concetto, abbastanza fumoso, il 13 dicembre 2016 il Gruppo di lavoro al GDPR, (Articolo 29 WP), ne ha individuato alcuni standard, come:

- il **numero** di soggetti interessati dal trattamento in termini assoluti ovvero

espressi in percentuale della popolazione;

- il **volume** di dati e le **tipologie** di dati oggetto di trattamento;
- la **durata** del periodo di trattamento;
- la **portata geografica** dell'attività di trattamento.

Sulla base di questi standard, sono state individuate alcune ipotesi di "trattamenti su larga scala":

- trattamento dei dati relativi alla clientela da parte di una **compagnia assicurativa** o di una **banca** nell'ambito delle ordinarie attività;
- trattamento dei dati di **geolocalizzazione** raccolti in tempo reale per finalità statistiche da un responsabile specializzato, rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento dei dati personali da parte di un **motore di ricerca** per finalità di pubblicità comportamentale, o trattamento di dati (metadati, contenuti, ubicazione) da parte di **fornitori di servizi telefonici o telematici.**

Nonostante la casistica, in assenza di una specificazione del concetto da parte del legislatore interno, sarà pura discrezione del giudice valutare la sussistenza o meno di tale elemento costitutivo del reato, con evidenti ricadute in termini di tassatività (e quindi effettiva punibilità) della fattispecie e, prima ancora, di prevedibilità delle conseguenze della propria condotta in capo ai soggetti agenti.

In ogni caso, deve precisarsi che la "larga scala" deve essere **rapportata alle modalità di trattamento** dei dati contenuti nell'archivio da parte del gestore, e non invece al numero di dati personali acquisiti fraudolentemente né al numero di destinatari cui gli stessi sono stati diffusi o comunicati illecitamente.

Conclusa questa breve disamina delle fattispecie di trattamento illecito, appaiono opportune alcune considerazioni di carattere generale.

La prima riguarda l'architrave dell'assetto normativo *privacy*, ossia il **consenso** espresso dell'interessato ai fini del trattamento dei dati personali, e della sua valenza a fini penali.

Tale fondamentale principio è stato rafforzato dalla recente riforma.

Ma cosa si intende esattamente per consenso?

Il consenso è un atto giuridico non negoziabile, che deve essere libero e rilasciato *ab origine*; pertanto, non può definirsi tale un atto condizionato o sopravvenuto rispetto al trattamento.

Il soggetto che rilascia il suo consenso deve poter aver pieno controllo dei dati che lo riguardano e, al contempo, permetterne l'uso nella piena consapevolezza delle finalità: è per tale ragione che si parla di *consenso abilitante*, piuttosto che autorizzativo.

Considerate tali caratteristiche, dal punto di vista della struttura del reato può affermarsi che il rilascio del consenso costituisce **un elemento negativo del fatto tipico**, e non invece una scriminante ai sensi dell'art. 50 c.p.

La seconda è una precisazione sull'**oggetto della tutela penale**: la protezione normativa si rivolge ai soli *dati personali*, intesi alla luce dell'art. 1 GDPR (*Oggetto e finalità*) come **dati riferiti esclusivamente alle persone fisiche**, così escludendo le persone giuridiche dal novero degli interessati.

Sul punto, occorre però puntualizzare che se l'impresa è identificabile attraverso una persona fisica (ad es., l'esponente della proprietà o l'amministratore delegato), le previsioni normative di cui sopra troveranno comunque applicazione, poiché ad assumere rilievo saranno i dati della persona fisica legata alla persona giuridica.

II. I PROFILI PROCEDURALI

In aggiunta alle modifiche di diritto sostanziale, il legislatore del 2018 ha anche definito alcune regole procedurali per l'accertamento dei reati in materia di trattamento dei dati personali, rispetto alle quali appare doveroso svolgere alcune considerazioni critiche.

Più in dettaglio, si è previsto (art. 167, commi nn. 4, 5 e 6, richiamati dagli artt. 167 *bis* e 167 *ter*, ultimo comma), un rapporto di collaborazione tra il Pubblico Ministero e l'Autorità Garante delle *Privacy*, tale per cui la Pubblica Accusa, non appena riceve una notizia di reato *ex* artt. 167, 167 *bis* e 167 *ter*, ha l'obbligo di **informare *senza ritardo* l'Autorità Garante.**

Quest'ultima, in virtù di poteri autorizzativi e di accertamento riconosciuti *ex lege*, potrà partecipare alle indagini della Pubblica Accusa e svolgerne delle proprie, al fine di raccogliere elementi di prova. Al termine della sua attività istruttoria, l'Autorità Garante dovrà redigere un **parere motivato indirizzato al Pubblico Ministero**, la cui decisione in merito all'esercizio dell'azione penale sarà quindi inevitabilmente influenzata.

L'Autorità Garante assume quindi il ruolo atipico di **"*coordinatore tecnico*" delle indagini preliminari**, con conseguente (almeno potenziale) lesione dell'indipendenza, imparzialità e terzietà costituzionalmente riconosciuti alle Autorità indipendenti.

Ad oggi, ancora non si è formata casistica tale da aiutarci a comprendere esattamente come si articoli il rapporto tra i due organi.

Per il momento, possono senz'altro essere evidenziare i profili di possibile criticità della nuova disciplina, sia rispetto a tale coordinamento (pur previsto all'encomiabile scopo di evitare una sovrapposizione tra il procedimento amministrativo e quello penale), sia per l'aver riconosciuto al Garante poteri e

facoltà che esulano dalla sfera amministrativa, sconfinando in quella penale.

III. COMPLIANCE *PRIVACY* E SISTEMA 231

Come detto in apertura, **stare al passo dell'innovazione tecnologica** e della connessa e rapida evoluzione normativa si è rivelata **un'ardua sfida, specialmente per il mondo imprenditoriale.**

Le aziende hanno, infatti, incontrato notevoli difficoltà nell'adeguarsi prontamente alle disposizioni di legge e ai numerosissimi codici/regolamenti del Garante, che disciplinano la protezione dei dati personali in specifici settori.

Tali difficoltà sono state acuite anche dal fatto che, per lungo tempo, la *privacy* non è stata una priorità fondamentale nella programmazione delle aziende del nostro Paese.

Un'attenzione crescente al tema è stata imposta, invece, solo negli ultimi anni con il GDPR che, dietro la comminatoria di dure sanzioni, ha incentivato le aziende a **investire nella sicurezza dei dati personali** ai fini di una più efficiente ed efficace gestione del rischio.

Eppure, le scelte legislative rispetto al rischio penale nelle imprese non sempre sono risultate soddisfacenti.

È il caso del **mancato aggiornamento della normativa sulla responsabilità da reato degli enti** alle fattispecie previste dagli artt. 167 ss. del Nuovo Codice *Privacy*, che ha destato non poche perplessità.

Sebbene il d.lgs. n. 231/2000 contempli dal 2008 una norma, l'art. 24 *bis,* la cui rubrica fa espresso riferimento anche al "*trattamento illecito di dati*", questa non prevede l'inserimento tra i cd. reati-presupposto delle nuove fattispecie di trattamento illecito (così come, del resto, non era stato inserito il vecchio art. 167).

La scelta è apparentemente inspiegabile, in controtendenza rispetto all'ampliamento dell'area di rilevanza penale voluto dalla recente riforma.

La spiegazione va forse ricercata nella sfida, prima accennata, di stare al passo con i tempi, cui forse non eravamo sufficientemente pronti.

E infatti, prevedere la responsabilità degli enti per i delitti in materia di *privacy* avrebbe imposto alle aziende **un significativo impegno, sia in termini organizzativi che economici.**

Nel timore di imbrigliare le imprese con ulteriori stringenti lacci e lacciuoli e imporre loro significativi esborsi finanziari, si è preferito rinunciare ad una più rigorosa protezione del dato personale, con buona pace della prevenzione di tutte quelle ipotesi di trattamento illecito che la *compliance* 231 avrebbe forse potuto contribuire a scongiurare.

Una valutazione critica di questa (opinabile) scelta legislativa non può però prescindere da un'analisi del contesto entro cui essa si colloca.

Il già richiamato art. 24 *bis*, infatti, contempla una serie di delitti informatici previsti dal codice penale che, in alcuni casi, configurano delle vere e proprie ipotesi di trattamento illecito.

Seppur non accordata in via diretta, **la tutela dei dati personali all'interno dell'ente viene quindi recuperata per il tramite di altre fattispecie.**

A ciò si aggiunga che il GDPR ha imposto l'adozione di politiche e l'attuazione di misure adeguate a garantire che il trattamento dei dati personali sia conforme al Regolamento, così vincolando le imprese a prendere in seria considerazione il problema della **sicurezza delle loro infrastrutture informatiche ai fini della protezione dei dati.**

Un approccio di *cybersecurity by law*, nel segno dell'efficacia e dell'effettività della tutela perseguite dal legislatore europeo.

Volendo fare una panoramica di queste **misure**, possono citarsi le disposizioni in tema di:

- ***accountability***, ossia obbligo di "*rendicontazione*" in capo al titolare del trattamento, che si risolve nella sua responsabilizzazione mediante la predisposizione e attuazione di misure organizzative e tecniche per la protezione dei dati (anche mediante l'adozione di *privacy compliance programs*, codici di condotta e sistemi di certificazione), tali da **assicurare e comprovare la conformità** del trattamento alle disposizioni del Regolamento (art. 24 GDPR);
- obbligo di **notifica dei *data breaches*** all'Autorità di controllo e agli interessati (art. 33 GDPR);
- designazione del ***Data Protection Officer*** (DPO), figura con specifiche competenze sia giuridiche sia informatiche, per le Pubbliche Amministrazioni e le imprese di grandi dimensioni, ovvero per le imprese le cui attività "*richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*" o, ancora, quelle che trattano categorie particolari di dati personali (art. 37 GDPR);
- obbligo di effettuare un ***Data Protection Impact Assessment*** (DPIA) prima di effettuare il trattamento, qualora questo comporti rischi elevati per i diritti e le libertà degli interessati (es., *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi) (art. 35 GDPR);

In considerazione di tali stringenti obblighi imposti alle imprese, può fondatamente ritenersi che le misure adottate – pur a fini diversi – possano **valere a realizzare una efficace prevenzione del rischio-reato nell'ambito della protezione dei dati**.

In questo senso, la prevenzione appare favorita dalle spinte sinergiche che possono derivare dai diversi sistemi di gestione e valutazione dei rischi adottati dall'azienda.

I punti di contatto tra la gestione aziendale del rischio *privacy* e la *compliance* 231, a ben vedere, sono molteplici.

A titolo esemplificativo, i *privacy compliance programs*, ferma restando la diversità di scopo, configurano modelli organizzativi di *compliance* analoghi a quelli utilizzati a fini 231.

Allo stesso modo, anche la DPIA realizza un modello di prevenzione simile a quello richiesto dal decreto 231. Con la DPIA, l'impresa ha infatti l'onere di valutare l'impatto delle proprie specifiche attività sulla *privacy,* ai fini dell'adozione delle misure idonee ad evitare di incorrere in *data breaches*; valutazione, questa, del tutto speculare a quella di *risk assessment* prevista ai fini dell'adozione del Modello Organizzativo e di Gestione.

A ciò si aggiunga che il decreto 231, come detto, contempla delle ipotesi di trattamento illecito "*sotto mentite spoglie*", rispetto alle quali è ragionevole ritenere che l'ente si doti di idonei presidi.

In conclusione, può senz'altro ritenersi che le misure di *compliance* sopra indicate rappresentino un apprezzabile punto di partenza per la realizzazione di un più strutturato meccanismo di controllo e gestione dei rischi connessi alla raccolta e al trattamento dei dati personali che, nell'ottica della realizzazione di una ***compliance* quanto più possibile integrata**, possa spiegare i suoi effetti anche sul versante delle responsabilità penale e amministrativa da reato.

Ciò che però è imprescindibile affinché tali misure siano effettive è un **profondo cambio di mentalità** delle imprese, che devono cogliere l'importanza della prevenzione in ambito *privacy*, nell'ottica – prima ancora che di evitare la fase patologica della commissione del reato – di promuovere una virtuosa cultura aziendale.

Questo in applicazione del principio, caposaldo del GDPR, della ***privacy by design***, ossia quell'approccio che impone alle aziende di prevedere gli strumenti a tutela dei dati personali sin dalla fase di progettazione dei processi aziendali, e non invece a valle, una volta constatate le violazioni.

In assenza di tale consapevolezza, il rischio è che gli enti releghino la protezione dei dati a mero adempimento burocratico e formale, finalizzato a soddisfare gli standard minimi di tutela.

Con la conseguenza che, una volta adempiuti "sulla carta" gli obblighi di *compliance*, si diffonde nella struttura aziendale l'erronea convinzione di aver "risolto" il problema della sicurezza dei dati, senza aver tuttavia implementato alcun reale meccanismo preventivo rispetto ad incidenti informatici ovvero eventi di perdita,

danneggiamento o furto di dati e informazioni aziendali.

IV. CONSIDERAZIONI CONCLUSIVE

Nonostante l'adeguamento interno alle importanti novità introdotte dal Regolamento Europeo, che mirano a rendere più efficiente ed efficace la tutela dei dati personali anche mediante il ricorso al diritto penale, persistono ancora importanti nodi problematici.

È il caso dei dubbi – sotto il profilo della tassatività – sulla concreta applicazione delle nuove fattispecie incriminatrici, legati principalmente all'assenza di una definizione normativa di *trattamento su larga scala*, che inevitabilmente rende più difficoltoso l'accertamento giudiziale.

E ancora, delle perplessità per l'aver riconosciuto ad un'Autorità indipendente (il Garante *Privacy*) poteri di ingerenza nel procedimento penale che esulano dal dettato normativo dell'art. 97 Cost., e che potrebbero invadere la sfera privata del cittadino senza che a questi siano riconosciute le opportune garanzie difensive.

Ulteriori critiche, come si è visto, riguardano la scelta legislativa di escludere dal novero dei reati presupposto per la responsabilità amministrativa da reato degli enti le fattispecie di trattamento illecito previste dagli artt. 167, 167 *bis* e 167 *ter* del nuovo Codice *Privacy*, sebbene le società trattino quotidianamente grandi quantità di dati personali e lo stesso Codice abbia introdotto delle nuove figure professionali responsabili del trattamento dati all'interno dell'organigramma aziendale.

Infine, l'assenza di un *corpus* normativo unitario non agevola di certo le imprese nella comprensione dei rischi, anche penali, cui sono esposte e, di conseguenza, nella individuazione degli obblighi da rispettare; per un imprenditore potrebbe essere senz'altro utile avere accesso a un'unica fonte normativa che raccolga le varie disposizioni, di rango sia primario sia secondario, che regolano la materia.

Quel che si auspica è, da un lato, la presa di coscienza da parte delle imprese che il metodo per gestire al meglio la sicurezza dei dati è quello di realizzare una *compliance* integrata, in sinergia con gli altri sistemi di gestione e controllo; dall'altro lato, un ulteriore intervento del legislatore, teso a una sistematizzazione della disciplina che possa chiarire ai destinatari delle norme quali siano gli obblighi loro spettanti.

CONTATTI

Giuseppe Fornari
Founding Partner

g.fornari@fornarieassociati.com

Lorena Morrone
Partner

l.morrone@fornarieassociati.com

Francesca Procopio
Associate

f.procopio@fornarieassociati.com

Alessandra Tramontelli
Trainee

a.tramontelli@fornarieassociati.com

Milano
Via Chiossetto 18
T: +39 0254122206
E: milano@fornarieassociati.com

Roma
Piazza di San Lorenzo in Lucina 26
T: +39 0622201000
E: roma@fornarieassociati.com