FORNARI E ASSOCIATI
STUDIO LEGALE

# FOCUS

## *Cybercrimes e responsabilità da reato degli enti: rischi penali e prevenzione*

fornarieassociati.com

Milano • Roma

Luglio 2020

# *CYBERCRIMES* E RESPONSABILITÀ DA REATO DEGLI ENTI: RISCHI PENALI E PREVENZIONE

La rivoluzione tecnologica che il mondo ha vissuto negli ultimi cinquant'anni ha avuto un impatto dirompente in tutti gli ambiti della società in cui viviamo. I mezzi informatici e cibernetici di cui oggi disponiamo consentono di svolgere qualsiasi attività in modo automatizzato, grazie a un semplice '*click*' su un dispositivo portatile, quasi sempre non più grande della nostra mano.

Come è facile immaginare, non necessariamente l'utilizzo umano delle nuove tecnologie è orientato a scopi leciti; anzi, è un dato accertato che, sempre più frequentemente, i reati vengono commessi mediante strumenti informatici. I dispositivi cibernetici possono con estrema facilità rendere un individuo vittima e autore di un fatto illecito, con tutta una serie di conseguenze in tema di prevenzione, accertamento e repressione dei crimini.

Se si considera che il nostro codice penale è stato pubblicato in Gazzetta Ufficiale nel 1930, è facile comprendere quanto importante sia lo sforzo continuo del legislatore e degli interpreti del diritto nel tenere la materia giuridica al passo con un'evoluzione informatica che procede incessantemente e a velocità sempre più sostenuta. L'avvento del *cyberspazio* quale luogo di interazione immediata tra persone distanti tra loro anche migliaia di chilometri ha, infatti, reso necessario interrogarsi, da un lato, su quali innovative fattispecie di reato possano caratterizzare la materia penalistica e, dall'altro lato, su quali crimini 'classici' possano trovare nuove forme di commissione, mediante l'utilizzo degli espedienti tecnologici di ultima generazione.

Per fare un esempio: è evidente che il legislatore del 1978, nell'introdurre nel codice penale il reato di riciclaggio, mai avrebbe potuto immaginare che, pochi decenni dopo, sarebbero stati predisposti strumenti in grado di trasferire denaro in pochi secondi da un capo all'altro del mondo e che sarebbero state persino introdotte valute digitali basate sulla crittografia (cc.dd. criptovalute).

Nondimeno, il progresso tecnologico procede su un binario sempre più veloce, generando un vortice di innovazione di cui è possibile prendere contezza su base quotidiana. Pertanto, gli autori e i fruitori della legge penale sono costantemente chiamati a confrontarsi con il compito di tenere tale fonte normativa al passo con ogni nuovo orizzonte tecnologico, adattando alla realtà moderna gli schemi criminosi classici ovvero creandone di nuovi: una sfida in cui non è possibile rimanere indietro, pena il rischio di lasciare scoperta una categoria, più o meno ampia, di condotte potenzialmente illecite.

Nel presente lavoro, approfondiremo il binomio diritto-tecnologia dalla prospettiva delle imprese. Oggi più di prima, le aziende si trovano impegnate nel duplice compito di premunirsi dal rischio di *cyber*-attacchi e di prevenire la commissione di illeciti penali resi possibili dall'impiego di tali strumenti. Da un lato, infatti, potrebbero vedere minata la loro sicurezza interna; dall'altro lato, invece, potrebbero vedersi muovere una contestazione di responsabilità amministrativa derivante da reato (*ex* d.lgs. n. 231/2001): in entrambi i casi, con gravosi impatti sul business. Si pensi che nel 2018 il 'costo *cybercrime*' ha inciso per un importo medio di 13 milioni di dollari ad azienda, facendo registrare un aumento del 12% rispetto al 2017 e ben del 72% negli ultimi cinque anni (report annuale sull'incidenza economica del *cybercrime*, a cura di Accenture e *Ponemon Institute* LLC).

## I. I REATI INFORMATICI COME PRESUPPOSTO DELLA RESPONSABILITÀ DA REATO DEGLI ENTI.

Quando si parla di delitti informatici, è bene anzitutto effettuare una distinzione tra **reati informatici in senso stretto** e **reati informatici in senso lato**.

I primi, ossia i reati informatici in senso stretto, si caratterizzano, in punto di tipicità della norma, per la presenza di **elementi di automatizzazione** di dati o informazioni, che costituiscono il nucleo essenziale della fattispecie incriminatrice. I secondi, invece, altro non sono che dei **reati comuni** commessi per il tramite di strumentazione informatica.

Qualora tali reati – inseriti nel catalogo dei delitti presupposto ai sensi degli art. 24 ss., d.lgs. n. 231/2001 – vengano commessi **nell'interesse o a vantaggio** dell'ente, da un soggetto **apicale** o da un **sottoposto**, potrà configurarsi un'ipotesi di responsabilità della persona giuridica.

Nei paragrafi successivi, si procederà, in primo luogo, ad analizzare, senza alcuna pretesa di esaustività, le **ipotesi di reato** presupposto della responsabilità 231 e, in secondo luogo, si analizzeranno i presidi di prevenzione necessari per approntare un'adeguata ***cyber compliance***.

### I.I I REATI INFORMATICI IN SENSO STRETTO.

Il *corpus* della disciplina qui di interesse è previsto dagli artt. 24 e 24-*bis*, d.lgs. n. 231/2001: la prima norma rientra nel novero dei reati presupposto sin dall'entrata in vigore della disciplina sulla responsabilità amministrativa degli enti, la seconda, invece, è stata introdotta con l'art. 7, legge 8 marzo 2008, n. 48, emanata in ratifica ed esecuzione della **Convenzione del Consiglio d'Europa sulla criminalità informatica** (svoltasi a Budapest il 23 novembre 2001).

L'art. 24, d.lgs. n. 231/2001 prevede quale reato presupposto la **frode informatica *ex* art. 640-*ter* c.p.** commessa in danno dello Stato o di altro ente pubblico. La disposizione tipizza **due diverse modalità** di condotta: **l'alterazione** in qualsiasi forma di sistemi informatici o telematici e **l'intervento**, senza diritto, su dati, informazioni o programmi contenuti nei predetti sistemi. 'L'alterazione' si traduce in una **condotta manipolativa** dei sistemi *hardware* o *software*; mentre 'l'intervento' si sostanzia in un **accesso non autorizzato** al sistema. In entrambi i casi, è comunque richiesta la percezione di un ingiusto profitto con l'altrui danno.

Quanto alla definizione di **sistema informatico**, è opinione consolidata che si tratti di un qualsiasi **complesso di apparecchi informatici** che, tramite strumenti di registrazione e memorizzazione, genera, in maniera organizzata, dati e informazioni. Il **sistema telematico** è invece una qualsiasi rete di comunicazione gestita informaticamente.

Con riferimento al trattamento sanzionatorio previsto dall'art. 24, d.lgs. n. 231/2001, è prescritta la **sanzione pecuniaria** sino a cinquecento quote o, qualora dal fatto sia derivato un profitto di rilevante entità o un danno di particolare gravità, da duecento a seicento quote. È altresì prevista, ai sensi del terzo comma, l'applicazione delle **sanzioni interdittive** *ex* art. 9, co. 2, lett. c), d) ed e) (*id est* divieto di contrattare con la pubblica amministrazione, esclusione da agevolazioni, finanziamenti, contributi o sussidi o la revoca di quelli già concessi e divieto di pubblicizzare beni o servizi).

L'art. 24-*bis*, d.lgs. n. 231/2001 riguarda invece la disciplina dei delitti informatici e del trattamento illecito dei dati. In particolare, il primo comma prevede la **sanzione pecuniaria** da 100 a 500 quote e l'applicazione delle **sanzioni interdittive** di cui all'art. 9, lett. a), b) ed e), d.lgs. n. 231/2001 qualora venga commesso uno dei seguenti reati:

- *(i)* accesso abusivo ad un sistema informatico o telematico (**art. 615-*ter* c.p.**);
- *(ii)* intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (**art. 617-*quater* c.p.**);
- *(iii)* installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (**art. 617-*quinquies* c.p.**);
- *(iv)* danneggiamento di informazioni, dati e programmi informatici (**art. 635-*bis* c.p.**);
- *(v)* 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.**);
- *(vi)* danneggiamento di sistemi informatici o telematici (**art. 635-*quater* c.p.**);
- *(vii)* danneggiamento di sistemi informatici o telematici di pubblica utilità (**art. 635-*quinquies* c.p.**).

Si applicano, invece, la **sanzione pecuniaria** sino a trecento quote e le **sanzioni interdittive** di cui all'art. 9, co. 2, lett. b) ed e) nel caso di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (**art. 615-*quater* c.p.**) e diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (**art. 615-*quinquies* c.p.**).

Da ultimo, per i reati di falsità relative a documenti informatici (**art. 491-*bis* c.p.**) e truffa del certificatore di firma digitale (**art. 640-*quinquies* c.p.**), l'art. 24-*bis*, d.lgs. n. 231/2001 prevede la **sanzione pecuniaria** sino a quattrocento quote, nonché le **sanzioni interdittive** di cui all'art. 9, co. 2, lett. c), d) ed e).

Con riferimento ai reati appena elencati, merita una notazione conclusiva la questione del **rapporto** sussistente tra la **frode informatica** e **l'accesso abusivo** a sistema informatico. Ad avviso della Corte di Cassazione, infatti, in ragione della diversità delle condotte descritte dalle fattispecie incriminatrici, potrebbero essere contestati, nell'ambito della medesima vicenda, sia il reato di frode informatica che quello di accesso abusivo (*Cass. Pen., sez. II, 16 marzo 2013, n. 13475*). È il caso, a titolo meramente esemplificativo, di una persona che si intrometta o si mantenga senza diritto all'interno di un sistema informatico, manomettendo o comunque alterando il funzionamento del sistema stesso.

### I.II I REATI INFORMATICI IN SENSO LATO.

I reati informatici in senso lato possono essere ricondotti al paradigma del ***computer facilitated crime***, in quanto, come già detto, rappresentano dei delitti comuni commessi attraverso l'uso delle nuove tecnologie. L'impiego della tecnologia, oltre a incidere sulle modalità di manifestazione delle condotte, rende ancora più complesso l'accertamento da parte degli organi inquirenti, che si trovano infatti a dover

indagare in merito a fenomeni delittuosi di difficile decifrazione.

A tal proposito, meritano di essere menzionate due delle principali ipotesi criminose che, in ragione dell'impiego degli strumenti informatici, stanno assumendo in tempi recenti una manifestazione fenomenica del tutto nuova rispetto all'ordinario atteggiarsi delle condotte tipiche di questi due reati: si tratta della **manipolazione del mercato**, reato presupposto ai sensi dell'art. **25-*sexies*, d.lgs. n. 231/2001** e delle fattispecie di **riciclaggio e autoriciclaggio**, presupposto della responsabilità da reato degli enti a norma dell'art. **25-*octies*** del medesimo decreto.

Con riferimento al reato di cui all'art. 185 T.U.F. (*i.e.* art. 25-*sexies* per la responsabilità 231), l'aspetto qui di interesse riguarda la prassi sempre più diffusa nel mercato di impiegare i cc.dd. ***High-Frequency Trading*** (HFT). Quest'ultimi consistono in sistemi *hardware* e *software* capaci di operare sulle piattaforme di negoziazione ad **alta intensità operativa**. Più precisamente, gli HFT – così come definiti dalla Direttiva (UE) 2014/65 – sono delle **tecniche di negoziazione algoritmica** caratterizzate da:

(i) "*infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere*;
(ii) *una determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine* ***senza intervento umano*** *per il singolo ordine o negoziazione*, e
(iii) *da un elevato traffico infragiornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni*" (**art. 4 Dir. 2014/65/UE, c.d. MIFID II**).

Su questo terreno si annidano potenziali condotte delittuose – idonee a integrare la disciplina del ***market abuse*** – che, se poste in essere in ambito societario, potrebbero giustificare l'applicazione della disciplina di cui al d.lgs. n. 231/2001. Il tema, in verità, è di non semplice risoluzione: con l'intervento degli algoritmi ad alta frequenza, progettati come detto per operare in autonomia, le condotte manipolative non verrebbero infatti commesse direttamente da un essere umano e, pertanto, potrebbero non essere rimproverabili secondo i **canoni tipici del diritto penale**, a meno di non voler ampliare notevolmente il perimetro dei soggetti astrattamente rimproverabili (si pensi, ad esempio, al programmatore o all'utilizzatore iniziale dell'algoritmo di mercato). Conseguentemente, non essendovi una **condotta umana penalmente rilevante**, potrebbe venire altresì meno la responsabilità dell'ente. Tuttavia, non è da escludere che in futuro, per colmare una tale lacuna sanzionatoria, si opti per un'interpretazione dell'art. **8, d.lgs. n. 231/2001** – che sancisce l'autonomia della responsabilità degli enti – affinché quest'ultimi possano essere sanzionati per fatti previsti dalla legge come reato, ma commessi da intelligenze artificiali e, dunque, in difetto dei crismi di colpevolezza.

Quanto ai reati di **riciclaggio e autoriciclaggio** (rispettivamente artt. 648-*bis* e 648-*ter.*1 c.p. e, per la responsabilità 231, art. 25-*octies* d.lgs. n. 231/2001), se commessi nell'ambito del **cyberspazio**, assumono le sembianze del c.d. **cybericiclaggio**. È il caso, ad esempio, del trasferimento di denaro su conti correnti aperti presso istituti di credito aventi sede in Stati *offshore* o dell'impiego delle cc.dd. *smart card*, vale a dire carte che, senza la specifica

apertura di una posizione di conto corrente, possono essere ricaricate e, quindi, utilizzate.

Un altro rilevante fenomeno che oggi più che mai si interseca con le fattispecie di riciclaggio riguarda l'utilizzo delle valute virtuali (o **criptovalute**). Si consideri che, secondo un'indagine di ricerca condotta in tempi recenti in merito all'utilizzo negli Stati Uniti della più nota moneta virtuale (ossia il *BitCoin*), la quasi totalità dei cittadini americani ha contezza di cosa siano le criptovalute e circa il 60% della popolazione più giovane ha affermato di utilizzare il *trading* con moneta virtuale. In Italia, invece, nel 2018 l'ammontare delle persone che possedevano criptovalute era già pari all'8% della popolazione nazionale.

Le caratteristiche essenziali del sistema criptovalutario sono le seguenti:

- **decentralizzazione delle negoziazioni**, affidate non a una Banca o altro ente regolatore, bensì ai singoli utenti, il cui operato prende forma nella c.d. *blockchain*;
- **anonimato** degli operatori di mercato. Il sistema della *blockchain*, infatti, consente di tracciare le operazioni compiute in rete, ma non rende nota l'identità dei soggetti coinvolti;
- la **rapida circolazione** nella rete internet.

Tali peculiarità, evidentemente, agevolano la diffusione capillare del fenomeno del **cybericiclaggio**, rendendo ben più arduo il lavoro investigativo dell'autorità giudiziaria, costretta a dover fronteggiare episodi delittuosi che, per via delle tecnologie impiegate, sono di difficile decifrazione.

### I.III PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA E PROFILI DI INTERESSE AI SENSI DEL D.LGS. N. 231/2001.

Di particolare rilievo, per la tematica qui affrontata, è la disciplina dettata dal d.l. 21 settembre 2019, n. 105 (convertito con la legge 18 novembre 2019, n. 133), che istituisce il c.d. **perimetro di sicurezza nazionale cibernetica**, previsto – recita l'art. 1, co. 1, d.l. n. 105/2019 – "*al fine di assicurare un **livello elevato di sicurezza delle reti**, dei **sistemi informativi** e dei **servizi informatici** delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato*".

È stato previsto un articolato sistema di procedure e di controlli cui gli enti inseriti nel perimetro di sicurezza cibernetica dovranno ottemperare. Più nello specifico:

- **ai sensi dell'art. 1, co. 2, lett. b), d.l. n. 105/2019**, gli enti devono predisporre e aggiornare con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici, che sia comprensivo della relativa architettura e componentistica;
- **ai sensi dell'art. 1, co. 6, lett. a), d.l. n. 105/2019**, gli enti devono dare apposita comunicazione al Centro di valutazione e certificazione nazionale (CVCN) qualora siano intenzionati a procedere con l'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti,

sui sistemi informativi e per l'espletamento di servizi informatici;
- **ai sensi dell'art. 1, co. 6, lett. c), d.l. n. 105/2019**, la Presidenza del Consiglio dei Ministri e il Ministero dello sviluppo economico svolgono attività di ispezione e verifica, impartendo, qualora necessario, specifiche prescrizioni.

Nel caso in cui, allo scopo di condizionare o ostacolare l'espletamento delle procedure e delle attività ispettive sopra indicate, vengano fornite informazioni, dati o elementi di fatto **non rispondenti al vero** o ne venga **omessa** la comunicazione, è applicabile la pena della reclusione da uno a tre anni (art. 1, co. 11, d.l. n. 105/2019).

Nei riguardi dell'ente, in ragione dell'inserimento del suddetto reato nell'ambito dei **delitti presupposto** *ex* art. 24-*bis*, d.lgs. n. 231/2001, possono applicarsi la **sanzione pecuniaria** fino a quattrocento quote, nonché le **sanzioni interdittive** del divieto di contrattare con la pubblica amministrazione, dell'esclusione da agevolazioni, finanziamenti, contributi o sussidi o l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni o servizi.

L'apparato normativo appena descritto, tuttavia, è improduttivo di effetti, in quanto non è stato ancora pubblicato il **decreto del Presidente del Consiglio dei Ministri** – atteso entro i quattro mesi successivi dall'entrata in vigore della legge di conversione – relativo all'individuazione dei criteri e delle modalità di individuazione degli enti inclusi nel **perimetro di sicurezza nazionale cibernetica** e, pertanto, soggetti al rispetto delle misure e degli obblighi previsti dalla disciplina. Lo schema di D.P.C.M. *ex* art. 1, co. 2, d.l. n. 105/2019, infatti, dopo il parere reso dal Consiglio di Stato il 21 maggio 2020, è oggi sottoposto al vaglio del Parlamento.

## II. LA *COMPLIANCE* AZIENDALE AL BANCO DI PROVA DELLE NUOVE TECNOLOGIE.

È di palmare evidenza come il processo di crescita legato al progressivo aumento della circolazione di dati digitali e di strumenti informatici necessiti di creare soluzioni in grado di gestire tale fenomeno.

La ***cyber compliance*** costituisce l'occasione per procedere alla valutazione dei **rischi** in seno all'impresa e va a mutare quel rapporto tipico che tradizionalmente guarda all'interno della struttura dell'ente: nel caso della *cyber compliance*, infatti, si configura un rapporto biunivoco tra il rischio esogeno e il rischio endogeno, alla luce del fatto che un modello organizzativo che importa l'adeguata sicurezza dell'impresa mette al riparo quest'ultima non solo da attacchi interni, ma altresì da quelli esterni.

Come evidenziato nei paragrafi precedenti, oramai da tempo il legislatore ha inserito i reati informatici nel catalogo dei reati presupposto della responsabilità 231.

Riprendendo pertanto la classificazione delle fattispecie incriminatrici più sopra evidenziata, di seguito si andranno ad analizzare alcune delle tipiche aree di attività dove possono annidarsi condotte delittuose sussumibili sotto i reati presupposto 231 e i relativi **presidi *compliance*** che potranno essere adottati dalle imprese per mitigare il **rischio-reato**, oltre che per tutelarsi da attacchi esterni.

### II.I REATI INFORMATICI IN SENSO STRETTO. QUALI PRESIDI APPRONTARE?

Al fine di elaborare un modello organizzativo adeguato ed efficace, occorre che esso venga predisposto ricalcando le specificità del singolo ente. Nella costruzione del modello, pertanto, il ***risk assessment*** diviene un passaggio obbligato per individuare le aree di attività maggiormente esposte al rischio criminogeno.

In particolare, volgendo lo sguardo alla ***cyber compliance***, quelle che tipicamente prestano il fianco alla penetrazione delittuosa sono le seguenti funzioni:

1. amministrazione;
2. finanza e controllo;
3. *marketing;*
4. ICT (*Information and Communications Technology*);
5. R&D (*Research and Development*);
6. acquisti e appalti.

Con riferimento a ciascuna delle attività sopra evidenziate, è opportuno che il modello organizzativo preveda, in termini generali: ***policy*** specifiche per i dispositivi prescelti, **reti *cloud*** per la selezione di programmi e *software*, un efficiente **sistema di controlli**, la costituzione di un **ufficio *IT*** al quale attribuire poteri di controllo specifici e, infine, un processo di segnalazione delle **anomalie**.

Senza alcuna pretesa di esaustività, nel prosieguo si passeranno in rassegna alcuni esempi delle aree di maggiore esposizione al rischio-reato comuni alle realtà imprenditoriali, con il proposito di fornire alcuni moniti utili alle imprese per prevenire la commissione degli illeciti informatici inseriti nel catalogo 231.

**1. Gestione degli accessi e dei profili di autorizzazione ai sistemi informatici/telematici e alle applicazioni.**

Allo scopo di sventare il rischio di accessi anomali mirati a sottrarre o danneggiare i dati in possesso dei dipendenti, può rivelarsi adeguato: (*i*) adottare un **regolamento** relativo all'utilizzo delle risorse informatiche aziendali e le ulteriori procedure in materia di sicurezza; (*ii*) definire formali requisiti di **autenticazione**; (*iii*) procedere ad una verifica periodica dei sistemi di accesso; (*iv*) definire criteri e modalità di definizione delle ***password***, ovvero definire procedure di registrazione per accordare o revocare l'accesso ai sistemi informativi.

**2. Gestione delle attività *on-line* svolte dai dipendenti.**

Con l'obiettivo di approntare specifici presidi atti a monitorare e neutralizzare la potenziale pericolosità delle attività del personale, è raccomandabile: (*i*) adottare meccanismi di garanzia a protezione da *software* pericolosi; (*ii*) predisporre strumenti di protezione volti a garantire la sicurezza nello scambio di informazioni sensibili in relazione al *business* di impresa; (*iii*) rendere obbligatoria la registrazione di attività eseguite su sistemi, applicazioni e reti, potenzialmente lesive per la sicurezza.

**3. Gestione della sicurezza informatica.**

In tale frangente, è consigliabile: (*i*) identificare i ruoli e le responsabilità del trattamento dei dati, nonché delle informazioni e i relativi principi di classificazione dei soggetti coinvolti con particolare attenzione ai rapporti con informatici ***outsourcer***, con i quali sarà altresì opportuno definire clausole contrattuali relative alla gestione delle misure di sicurezza;

inoltre, è necessario garantire: (*i*) il corretto e sicuro funzionamento degli **elaboratori di informazioni**; (*ii*) la protezione da *software* pericolosi; (*iii*) il ***backup*** di informazioni e *software*; (*iv*) la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione, anche con terzi; (*v*) gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti; (*vi*) una verifica dei ***log*** che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza.

## 4. Gestione delle informazioni sensibili.

Al fine di neutralizzare i rischi connessi alla trattazione di informazioni e dati è possibile adottare un regolamento avente ad oggetto il corretto utilizzo delle risorse informatiche aziendali, oltre che ulteriori procedure in materia di sicurezza informatica/telematica da rispettare, che dovrà essere debitamente divulgato tra i dipendenti. Sarà inoltre opportuno che l'ente ricorra: (*i*) all'utilizzo di **sistemi crittografici** in relazione alla trasmissione in rete di documenti informatici; (*ii*) a controlli tesi a rintracciare eventuali falle o debolezze dei sistemi, c.d. ***vulnerability assessment***, a cui far seguire eventuali c.d. ***penetration test***, finalizzati a valutare la tenuta del sistema dinnanzi a eventuali attacchi esterni.

Oltre a ciò – e più in generale – un significativo investimento mirato alla **formazione** del personale è sempre da ritenersi meritevole: invero, riuscire a diffondere una cultura aziendale virtuosa contraddistinta da elevati *standard* di sicurezza potrà costituire indubbiamente un *surplus* per ciascuna impresa.

### II.I.I. *COMPLIANCE* E *PRIVACY*: DUE LATI DELLA STESSA MEDAGLIA.

Come noto, la ***privacy*** costituisce un bene giuridico che trova piena tutela, *in primis*, nell'ordinamento europeo con il Regolamento (UE) 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e, secondariamente, nel panorama nazionale, con il d.lgs. 10 agosto 2018, n. 101, adottato dal legislatore a recepimento della normativa europea. Punto focale della disciplina GDPR risiede proprio nella valorizzazione del momento della **prevenzione**, per mezzo dell'incentivazione all'adozione di efficaci misure di protezione dei dati personali, soprattutto nelle reti e nei sistemi informatici.

Ebbene, stante il gran numero di dati – comuni e sensibili, di dipendenti, agenti, fornitori, clienti e professionisti – che le imprese si trovano a dover trattare, anche per tali soggetti diverrà necessario attuare specifiche misure **preventive** di ***compliance***, idonee a garantire la sicurezza dei dati, in conformità alla normativa **GDPR**.

Sebbene nell'elenco di cui all'art. 24-*bis*, d.lgs. n. 231/2001 non rientrino i reati in materia di *privacy*, non può trascurarsi, tuttavia, come i reati informatici contemplati dalla normativa 231 siano strettamente connessi alla tutela di tale bene giuridico, atteso che il mondo virtuale rappresenta una delle principali fonti di rischio per il trattamento illecito dei dati personali. I reati informatici inseriti nel codice penale tutelano indirettamente la riservatezza, in quanto nel proteggere **l'integrità** di un sistema informatico e dei dati ivi contenuti, ne assicurano imprescindibilmente l'elemento privato. A tal riguardo, si pensi ai casi di ***data breach*** dove i

fenomeni di illecita diffusione, distruzione o di accesso non autorizzato ai dati personali richiamano le condotte oggetto di alcuni delitti informatici quali, ad esempio: il danneggiamento di informazioni o dati o anche la distruzione di un sistema informatico che contiene dati personali (art. 615-q*uinquies* c.p.), la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti di cui all'art. 615-*bis*, co. 3, c.p.

In questi termini, tra i reati in materia di trattamento dei dati personali e quelli informatici vi sono dei punti di naturale connessione. Alla luce di tale circostanza, sarà pertanto opportuno per le imprese valutare di integrare reciprocamente i presidi posti a tutela di ciascun ambito (reati informatici e *privacy*), allo scopo di costruire un modello organizzativo adeguato a rispondere alle esigenze di prevenzione derivanti dalle normative 231 e GDPR.

A tal fine, la metodologia ancora una volta sarà quella del ***risk based approach***, che si sostanzia nella **mappatura dei rischi** legati al trattamento dei dati personali al fine di ottenere la piena consapevolezza dei rischi cui l'impresa è esposta, così da agevolare il processo di protezione.

A titolo esemplificativo, il modello organizzativo dovrà:

1. **regolare l'uso del sistema informatico** all'interno dell'azienda, per garantire la trasparenza delle decisioni aziendali e dei flussi informatici di dati, tramite un criterio di tracciabilità delle decisioni e delle operazioni, per impedire o almeno facilmente rintracciare l'individuazione delle condotte di illecito utilizzo delle strutture informatiche aziendali;
2. **nominare un amministratore di sistema e un responsabile delle credenziali di accesso**, deputato a occuparsi delle attività di gestione, controllo e monitoraggio delle procedure informatiche, come il controllo degli accessi e della sicurezza;
3. imporre, conformemente al ***Data Protection Impact Assessment*** (DPIA), al titolare e al responsabile del trattamento di effettuare uno ***screening*** **aziendale**, per comprendere che tipo di dati personali vengono trattati e quali infrastrutture tecnologiche vengono utilizzate, in modo da identificare eventuali vulnerabilità e fragilità dei sistemi;
4. **diversificare i processi** e le funzioni inerenti alla *privacy* e formare adeguatamente tutti i propri dipendenti.

Inoltre, al fine di dotarsi di un sistema efficiente, idoneo a garantire un certo grado di affidabilità, nonché elevati parametri di riservatezza e integrità delle informazioni, l'impresa potrà conformarsi a *standard* certificati e internazionalmente riconosciuti, come ad esempio l'**ISO-27001**. Quest'ultima è una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, *i.e. Information Security Management System*) e include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

### II.II REATI COMUNI COMMESSI MEDIANTE L'USO DELLA TECNOLOGIA: CYBERICICLAGGIO.

Terminata la breve panoramica sopra esposta in merito ai presidi *compliance* contro la perpetrazione di reati informatici in senso

stretto, riprendendo la distinzione cui si è fatto cenno nei paragrafi che precedono, non ci si può esimere dallo svolgere alcune considerazioni in punto di prevenzione dai cc.dd. reati comuni ICT.

A tal proposito, stanti le recenti novità legislative in tema di regolamentazione di criptovalute introdotte con il d.lgs. 4 ottobre 2019, n. 125, adottato a recepimento della Direttiva (UE) 2018/843, c.d. Quinta Direttiva, merita senz'altro un cenno il reato di **cybericiclaggio** commesso mediante l'utilizzo di moneta virtuale.

La questione è di interesse poiché la novella ha adottato una definizione piuttosto ampia di ***service provider*** (gli operatori che prestano servizi di gestione di portafogli digitali), ampliando il novero dei soggetti destinatari di obblighi finalizzati alla verifica della clientela nella prospettiva del contrasto al rischio riciclaggio.

Secondo la normativa domestica, è prestatore di servizi relativi alla moneta virtuale "*ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale*". In siffatta definizione, rientrano dunque gli ***exchanger***, ovverosia coloro che conservano e convertono valute virtuali in valute aventi corso legale.

Con il d.lgs. n. 125/2019, l'Italia ha ampliato la definizione di *service provider*, estendendo tale qualifica ai prestatori di servizi di portafogli digitali, c.d. ***wallet provider***, ossia "*ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*".

La definizione accolta tende, in definitiva, a sottoporre alla normativa antiriciclaggio tutti i possibili operatori attraverso i quali i privati possono accedere al **mercato criptovalutario**: pertanto, con l'entrata in vigore del decreto, l'obbligo di adeguata verifica non è limitato alle sole piattaforme di investimento (***exchangers***), bensì anche ai soggetti che, gestendo portafogli virtuali per conto di terzi, svolgono il ruolo di ***broker*** sulle piattaforme stesse.

Tali soggetti, innanzitutto, devono **iscriversi in una sezione speciale** del registro tenuto dall'Organismo degli Agenti e dei Mediatori (ai sensi dell'art. 128-*undecies* del Testo Unico Bancario), risultando così parificati ai tradizionali cambiavalute e parimenti soggetti alle disposizioni antiriciclaggio.

Inoltre, secondo quanto stabilito dagli artt. 17 e ss. del d.lgs. n. 231/2007, come modificato dai d.lgs. nn. 90/2017 e 125/2019, i *service provider* sono obbligati a:

1. provvedere alla **registrazione e alla verifica della clientela**;
2. **acquisire dati identificativi del cliente**, sia esso una persona fisica o giuridica, nel caso di operazione occasionale di importo pari (o superiore) a 15.000 euro, anche se effettuata con più disposizioni collegate;
3. nel caso di instaurazione di un rapporto continuativo, **acquisire dati anagrafici** e richiedere informazioni sullo scopo e la natura degli affari;
4. **comparare i dati raccolti** con quelli di cui l'*exchanger* eventualmente già

disponga, al fine di verificarne la verosimiglianza;

5. **approfondire la verifica** qualora vi sia il fondato sospetto di riciclaggio di denaro o di finanziamento del terrorismo;
6. non limitare il controllo alla fase genetica del rapporto, bensì prolungarlo in modo continuativo per tutta la permanenza del cliente nella sfera operativa del cambiavalute;
7. provvedere ad un **periodico aggiornamento** delle informazioni raccolte presso la clientela e predisporre un adeguato sistema di conservazione dei documenti acquisiti.

Da ultimo, l'art. 35 prevede l'obbligo di segnalare **all'U.I.F.** ogni operazione sospetta, così come tutti i casi in cui si abbia fondato motivo di ritenere che la provenienza dei fondi possa essere illecita.

Al fine di scongiurare il rischio di condotte di cybericiclaggio, i *service provider* dovranno pertanto attenersi pedissequamente al complesso di disposizioni più sopra enucleate e, allo scopo di andare esenti da contestazioni di natura para-penale, dovranno porre in essere tutti quegli accorgimenti necessari a rendere effettivo il rispetto di tali doveri.

In questi termini, ancora una volta, il ***risk based approach*** diviene la strategia da adottare per la costruzione di un modello organizzativo ***tailor made,*** adeguato alle specificità del singolo contesto. A titolo esemplificativo, il livello di attenzione serbato dal *service provider* sarà tanto più elevato quanto maggiore risulti il livello di anonimato garantito dalla valuta virtuale utilizzata (in base ai principi del *risk based approach*); gli strumenti più diffusi come il ***BitCoin*** o l'***Ethereum***, inevitabilmente necessitano di un monitoraggio meno pervasivo di quanto invece sarà richiesto per valute a diffusione locale, reperibili unicamente su alcune piattaforme e nella disponibilità di pochi investitori dall'identità sospetta.

## III. NUOVE TECNOLOGIE: OPPORTUNITÀ DI *COMPLIANCE* AZIENDALE.

Per l'attività di impresa il **progresso tecnologico** costituisce senza dubbio un banco di prova colmo di sfide: se, da un lato, le nuove tecnologie hanno visto gli enti costantemente impegnati sul fronte della prevenzione di nuove tipologie di reati venute alla luce con il progressivo sviluppo del cyberspazio, parimenti l'evoluzione tecnologica ha costituito un significativo traguardo per l'armamentario di strumenti innovativi suscettibili di essere adoperati nell'attività di *compliance*.

La **digitalizzazione** sembra avere investito anche questo settore, ove è già possibile scorgere l'impiego di nuove tecnologie da parte di alcuni dei maggiori operatori di mercato che hanno colto i **vantaggi**, nella duplice ottica di **celerità** e **risparmio dei costi**, derivanti dalla digitalizzazione del comparto *compliance.*

Nel prosieguo, alcuni esempi di come le nuove tecnologie siano state applicate dai principali *player* del mercato per **l'efficientamento** della prevenzione del rischio-reato:

1. *Automatic strategic learning*: si tratta di **strumenti per l'identificazione delle novità normative e dei relativi impatti**. Tali strumenti consentono di analizzare e identificare in anticipo i normali *trend* regolamentari a livello globale, europeo e

nazionale, nonché di analizzare l'impatto che la novità legislativa può produrre sull'attività della singola impresa. Si tratta, all'evidenza, di un aspetto cruciale per alcuni *player*, in particolare banche e assicurazioni, che al fine di poter operare nel mercato devono prevedere con anticipo le evoluzioni normative e i relativi impatti sul proprio business;

2. *Data analytics*: consiste in un **processo di raccolta e analisi di grandi volumi di dati per estrarre informazioni nascoste**. La raccolta di ***big data*** – *i.e.* raccolta di dati informatici così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza – si rivela strategica per le imprese poiché consente di formulare previsioni in ordine alle condizioni di mercato, mettendo a disposizione della *governance* un supporto informativo efficace e competitivo. Si tratta di un processo sempre più utilizzato da parte dei grandi *player* del mercato nella lotta ai fenomeni corruttivi e del *market abuse*, ciò perchè, per mezzo dell'analisi comparativa dei dati, diviene possibile individuare con maggiore facilità le operazioni sospette;
3. *Robotic Process Automation*: afferisce a tutte le tecnologie, prodotti e processi coinvolti nell'automazione dei processi lavorativi e utilizza ***software*** '**intelligenti**' (i cc.dd. "*software robot*") che possono eseguire in modo automatico le attività ripetitive degli operatori, ai fini dell'esecuzione dei processi ripetitivi, *ruled-based*, imitandone il comportamento e interagendo con gli applicativi informatici nello stesso modo dell'operatore stesso. Ad esempio, tale *software* può essere impiegato per aumentare il controllo sulle attività tipicamente esposte a errore e per questo foriere di rischio di danno non solo finanziario, ma altresì reputazionale;
4. ***Artificial intelligence and machine learning***: si riferisce all'abilità di apprendimento dei dispositivi, in grado di apprendere e modificare i propri programmi in forza delle nuove informazioni che vengono somministrate. **L'intelligenza artificiale** può essere impiegata in alcuni programmi di analisi, ad esempio, di testi, immagini, audio e video. Alcuni operatori del mercato, quali banche e società finanziarie, impiegano altresì l'intelligenza artificiale nel contrasto a condotte di autoriciclaggio, attraverso la c.d. *transaction monitoring* fondata sulla generazione di *alert.*

## IV. CONCLUSIONI.

È di fondamentale importanza che gli enti colgano appieno la portata determinante che la **sicurezza** e la ***compliance*** rivestono nell'attività di impresa. La tendenza a considerare tali temi alla stregua di meri ostacoli burocratici idonei unicamente a rallentare e rendere più costoso il *business* aziendale, dovrebbe cedere il passo a una prospettiva più lungimirante, in grado di cogliere quali **vantaggi**, in termini di affidabilità e sicurezza, verrebbero a determinarsi in favore dell'ente.

Sicché, *pro futuro*, è auspicabile che le imprese non si limitino a recepire la *compliance* unicamente come un passaggio necessario per evitare le aspre sanzioni pecuniarie e interdittive comminabili ai sensi del d.lgs. n. 231/2001. È opportuno che tali soggetti giungano a concepire la **sicurezza** come un

valore aggiunto, idoneo in alcuni casi a garantire la sopravvivenza dello stesso ente che, in assenza di adeguati meccanismi di prevenzione, dinnanzi a *cyber* aggressioni provenienti dal mondo esterno potrebbe uscirne irrimediabilmente danneggiato.

# CONTATTI

**Giuseppe Fornari**
Founding Partner
g.fornari@fornarieassociati.com

**Emanuele Angiuli**
Partner
e.angiuli@fornarieassociati.com

**Martina Cupella**
Associate
m.cupella@fornarieassociati.com

**Davide Attanasio**
Trainee
d.attanasio@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