PARTE SPECIALE - C -

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI E DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

G. Del Priore srl
Sede Legale: Via Parmenide 260 84131 - SALERNO (SA)
Partita IVA: 02481440655

Sommario

1. LE FATTISPECIE DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI E DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

Con l'approvazione della legge n. 48 del 18 marzo 2008 è stata recepita in Italia la Convenzione di Budapest del 2001 sul cyber crime riguardante, in particolare, i reati commessi avvalendosi in qualsiasi modo di un sistema informatico manipolandolo o arrecando un danno allo stesso.

Tale legge ha inserito nel D. Lgs. n. 231/2001 l'art. 24-*bis* (successivamente modificato dai D.lgs. 7 e 8 del 2016) estendendo quindi il regime della responsabilità amministrativa per l'ente anche per i c.d. reati informatici.

Inoltre, sono state prese in considerazione altre tipologie di reati che trovano come presupposto l'impiego di sistemi e programmi informatici ovvero di opere tutelate dalle norme in materia di diritto d'autore e, dunque, in particolare:

- Delitti in materia di violazione del diritto d'autore (art. 25 novies d.lgs. 231/01);
- Reati commessi nei rapporti con la Pubblica Amministrazione (con riferimento alla frode informatica in danno dello Stato o di altro ente pubblico - art. 640 ter c.p.- art. 24 d.lgs. 231/01);
- Delitti contro la personalità individuale (con riferimento ai delitti di pornografia minorile e detenzione di materiale pornografico (artt. 600-ter e 600-quater c.p.- art. 25 quinquies d.lgs. 231/01).

Per il dettaglio delle fattispecie di reato presupposto del D.Lgs. 231/01 oggetto della presente Parte Speciale si rinvia all'Appendice A.

2. FUNZIONE DELLA PARTE SPECIALE C

Data la peculiarità dei reati e la larga diffusione dell'utilizzo degli strumenti informatici si ritiene che il rischio di commissione dei suddetti reati sia astrattamente verificabile per tutti gli operatori . La presente Parte Speciale si riferisce a comportamenti posti in essere dai destinatari del Modello (Organi Sociali, Dipendenti, Consulenti, Partner, etc.), coinvolti nelle "attività sensibili" (ovvero di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto n. 231/2001).

Verranno quindi indicati:

a) le attività e/o i processi aziendali definiti "sensibili" ovvero a rischio di reato;
b) i principi fondamentali di riferimento in attuazione dei quali dovranno essere adottate le specifiche modalità ai fini della corretta applicazione del Modello (principi di prevenzione generali e protocolli specifici di controllo).

3. IDENTIFICAZIONE DELLE ATTIVITÀ SENSIBILI

I reati sopra considerati trovano come presupposto l'impiego di sistemi e programmi informatici. Al riguardo, è opportuno evidenziare che tutti i dipendenti aziendali che utilizzano ordinariamente sistemi informatici hanno conseguentemente ampia possibilità di accesso a strumenti e dati informatici e telematici nel contesto dell'ordinaria attività lavorativa.

Ai sensi dell'art. 1 della Convenzione sopra citata, rientra nella nozione di "sistema informatico" "qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati". Tra i "dati informatici" rientra, inoltre, "qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione".

Pertanto, non essendo possibile circoscrivere soltanto ad alcune specifiche funzioni o aree operative il rischio di commettere reati sopra menzionati e, quindi, collegare in via generale a singole funzioni / attività aziendali il rischio di commissione degli illeciti considerati dal Decreto, l'analisi dell'operatività aziendale si è focalizzata, nell'ambito di tali attività sensibili sulle seguenti fasi operative:

- Sviluppo e gestione attività ICT:
    - Gestione degli hardware aziendali;
    - Gestione dei software aziendali;
    - Gestione e presidio dei sistemi informativi;
    - Utilizzo di banche dati;
    - Gestione dei server della Società o dei siti internet.
- ICT Security:
    - Protezione degli hardware, software, banche dati, server, siti internet e sistemi informativi;

- Utilizzo della postazione di lavoro;
- Gestione degli aspetti inerenti alla sicurezza fisica;
- Gestione degli output di sistema e dei dispositivi di morizzazione (es. USB, CD);
- Gestione di documentazione con valore probatorio.

4. PRINCIPI DI PREVENZIONE GENERALI

Con specifico riguardo alle problematiche connesse al rischio informatico, consci dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica; in particolare, tale sicurezza viene perseguita attraverso:

- la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza, e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi);
- la garanzia della massima continuità del servizio.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che sono:

- riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- integrità: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. L'azienda ha previsto la realizzazione di misure volte a garantire che le informazioni vengano trattate in modo tale da impedire la manomissione o la modifica da soggetti non autorizzati;
- disponibilità: garanzia di reperibilità di dati aziendali in funzione delle

esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

È fatto divieto in particolare di:

- alterare documenti informatici (definiti dalla legge come la "rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti"), pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di

pubblica utilità;

- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- visitare siti internet che contengono materiale recante offesa al pudore, alla pubblica decenza o di istigazione alla realizzazione o rappresentazione di condotte criminali in genere;
- trasmettere o scaricare, dalla rete internet, materiale considerato osceno, pornografico, minaccioso o che possa molestare la razza o la sessualità o, comunque tale da arrecare offesa, di qualsiasi natura, alla persona.

Pertanto, i soggetti Destinatari della presente Parte Speciale osservano i seguenti principi:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile (o "Amministratore di Sistema", ai sensi del D. Lgs. n. 196/03 e delle successive delibere emesse dal Garante per la protezione dei dati personali);
- in caso di smarrimento o furto di apparecchiatura informatica aziendale, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
- evitare di introdurre e/o conservare nella Società (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico, di proprietà di terzi, salvo acquisiti con il loro espresso consenso, nonché applicazioni/software che non siano state preventivamente approvate dal Responsabile o la cui provenienza sia dubbia;
- evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della

Società, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;

- evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc…);
- evitare l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile; qualora l'utente venisse a conoscenza della password di altro utente, è tenuto a darne immediata notizia al Responsabile;
- evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare,

  alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

- utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

5. PROTOCOLLI SPECIFICI DI CONTROLLO

Ai fini dell'attuazione delle regole e divieti elencati al precedente par.4, oltre che dei protocolli generali di controllo già contenuti nella Parte Generale del presente Modello al paragrafo 2.6. e nel Codice Etico, con riferimento alle singole Attività Sensibili di seguito descritte, si osservano i seguenti protocolli specifici di controllo.

Politiche di sicurezza: esistenza di una politica in materia di sicurezza del sistema informativo che preveda, fra l'altro:

a) le modalità di comunicazione anche a terzi;
b) le modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi.

Organizzazione della sicurezza per gli utenti interni: esistenza di uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.

Classificazione e controllo dei beni: esistenza di uno strumento normativo che definisca i ruoli e le responsabilità per l'identificazione e la classificazione degli asset aziendali (ivi inclusi dati e informazioni).

Sicurezza fisica e ambientale[1]: esistenza di uno strumento normativo che disponga l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in

[1] Come definito dall'ISO 27002, lo standard in oggetto fa riferimento ad un sistema di controlli volto a impedire l'accesso, il danneggiamento e l'interferenza dei soggetti non autorizzati, all'interno del flusso delle informazioni del business, nonché la manomissione o il furto delle informazioni.

sicurezza delle aree e delle apparecchiature

Gestione delle comunicazioni e dell'operatività: esistenza di uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite policy e procedure. In particolare, tale strumento normativo assicura:

a) il corretto e sicuro funzionamento degli elaboratori di informazioni;
b) la protezione da software pericoloso;
c) il backup di informazioni e software;
d) la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
e) gli strumenti per effettuare la tracciatura delle attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
f) una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
g) il controllo sui cambiamenti agli elaboratori e ai sistemi;
h) la gestione di dispositivi rimovibili.

Controllo degli accessi: esistenza di uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni.

In particolare, tale strumento normativo prevede:

a) l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
b) le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
c) una procedura di registrazione e de-registrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;

d) la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;

e) la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;

f) l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;

g) la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;

h) la chiusura di sessioni inattive dopo un predefinito periodo di tempo;

i) la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk

esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati.

Gestione degli incidenti e dei problemi di sicurezza informatica: esistenza di uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo prevede:

a) appropriati canali gestionali per la comunicazione degli incidenti e problemi;

b) l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;

c) la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;

d) l'analisi di report e trend sugli incidenti e sui problemi e l'individuazione di azioni preventive;

e) appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;

f) l'analisi della documentazione disponibile sulle applicazioni e

l'individuazione di debolezze che potrebbero generare problemi in futuro;

g) l'utilizzo di basi dati informative per supportare la risoluzione degli incidenti;
h) la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;
i) la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.

Audit: esistenza di uno strumento normativo che disciplini i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.

Risorse umane e sicurezza: esistenza di uno strumento normativo che preveda:

a) la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
b) specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
c) l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
d) la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di

cambiamento della mansione svolta.

Crittografia: esistenza di uno strumento normativo che preveda l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche.

Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi: esistenza di uno strumento normativo che definisca:

a) l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
b) la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
c) la confidenzialità, autenticità e integrità delle informazioni;
d) la sicurezza nel processo di sviluppo dei sistemi informativi.

La fase di gestione amministrativa del personale (gestione anagrafica dei dipendenti, rilevazione delle presenze, elaborazione delle paghe/ cedolini e il pagamento delle imposte) è affidata in outsourcing.

La gestione dello sviluppo e manutenzione dei sistemi informativi è affidata in outsourcing.

Per tale attività, nell'ambito del contratto con l'outsourcer si osservano i seguenti principi:

- dettaglio puntuale di tutti i servizi da erogare;
- definizione dei livelli di servizio minimo e le relative penali che il fornitore deve impegnarsi a rispettare. A tal fine è necessario definire le modalità e la reportistica utile ai fini della supervisione da parte di Nucleco dei servizi ricevuti e degli esiti degli stessi;
- definizione degli strumenti e modalità di verifica dei livelli di servizio e per la condivisione dei risultati delle attività/controlli eseguiti dal fornitore;
- definizione dei documenti procedurali di riferimento e le istruzioni

operative da seguire con indicazione dei responsabili;

- per ogni servizio indicato nel contratto, individuazione dei referenti tecnici dell'azienda a seconda della rispettiva area di competenza;
- previsione di specifiche clausole nei contratti con cui i terzi:

- si obbligano a non tenere alcun comportamento, non porre in essere alcun atto od omissione e non dare origine ad alcun fatto da cui possa derivare una responsabilità ai sensi del D.Lgs. n. 231/01;
- dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Codice Etico e nel Modello adottati dalla Incentive nonché clausole risolutive espresse che attribuiscano alla Società la facoltà di risolvere i contratti in questione nel caso di violazione di tale obbligo.

6. AGGIORNAMENTO DEI REATI INFORMATICI ALLA NIS2

L'adeguamento dei Modelli Organizzativi (MOG) previsti dal **D.Lgs. 231/2001** in seguito al recepimento della direttiva **NIS2** (recepita in Italia con il D.Lgs. 138/2024, in vigore da ottobre 2024, con scadenze operative tra il 2025 e il 2026) è diventato cruciale per le aziende, specialmente quelle nei settori "essenziali" e "importanti". La NIS2 impone una governance rigorosa della cybersecurity, trasformando la sicurezza informatica in un obbligo di compliance di alto livello che si integra direttamente nella responsabilità amministrativa degli enti.

Ecco i principali adeguamenti richiesti per la legge 231/01 a seguito della NIS2:

1. **Revisione della Mappatura dei Rischi (Risk Assessment)**
   - **Integrazione dei rischi cyber:** La mappatura dei rischi del Modello 231 deve includere i rischi legati alla sicurezza informatica, alle reti e ai sistemi informativi.
   - **Identificazione degli asset critici:** È necessario aggiornare la valutazione delle vulnerabilità, la probabilità di un incidente e il suo impatto economico e reputazionale.
   - **Supply Chain Security:** Il modello deve prevedere procedure di controllo sui fornitori critici, valutandone il livello di sicurezza.
2. **Aggiornamento dei Protocolli e delle Procedure**
   - **Policy di sicurezza:** Formalizzazione di nuove policy che regolano l'uso delle risorse IT, l'accesso ai dati e la sicurezza delle informazioni.
   - **Procedure di notifica incidenti:** Implementazione di procedure rapide per l'identificazione e la segnalazione degli incidenti significativi, garantendo il flusso informativo verso l'Organismo di Vigilanza (OdV) e, quando necessario, al CSIRT Italia.
   - **Business Continuity:** Aggiornamento delle procedure di ripristino dei sistemi in caso di attacco cyber.

3. **Responsabilità degli Organi Apicali**
   - **Responsabilità diretta del CDA:** La NIS2 impone che i vertici aziendali (CdA, Amministratori) approvino le misure di gestione del rischio cyber e ne controllino l'attuazione.
   - **Formazione obbligatoria:** I membri del consiglio di amministrazione devono ricevere formazione specifica per acquisire competenze in materia di cybersecurity.
   - **Responsabilità 231:** In caso di mancata implementazione delle misure, gli organi apicali possono incorrere in responsabilità dirette, riflessi sulla colpa organizzativa dell'ente.
4. **Ruolo dell'Organismo di Vigilanza (OdV)**
   - **Monitoraggio cybersecurity:** L'OdV dovrà vigilare non solo sul rispetto delle procedure interne, ma anche sull'adeguatezza delle misure tecniche adottate per la NIS2.
   - **Flussi informativi dedicati:** Istituzione di flussi periodici tra il responsabile della sicurezza informatica (CISO) e l'OdV.

Scadenze Chiave

- **31 Maggio 2025/Gennaio 2026:** Obblighi di registrazione e notifica degli incidenti significativi al CSIRT Italia.
- **In generale:** È opportuno integrare i sistemi entro il 2025, in linea con l'entrata in vigore delle norme tecniche.

Un Modello 231 non aggiornato alla NIS2 comporta non solo il rischio di sanzioni per violazione della 231 (in caso di reati informatici), ma anche le pesanti sanzioni amministrative previste dalla stessa normativa NIS2, che possono arrivare fino a **10 milioni di Euro o al 2% del fatturato mondiale annuo** per i soggetti essenziali.

7. NIS 2 E SISTEMI 231: NUOVA LINEA DI RESPONSABILITÀ DEGLI ODV NEI SOGGETTI ESSENZIALI E IMPORTANTI

Con l'attuazione della Direttiva NIS 2 nell'ordinamento italiano, molte misure di cyber sicurezza sono ormai obblighi di legge per le imprese classificate

come soggetti essenziali o importanti.

La lettura: il ruolo dell'OdV

Secondo questa interpretazione, la loro inosservanza può tradursi in una vera e propria "colpa di organizzazione" ai sensi del D.lgs. 231/2001.

L'OdV non può più limitarsi a vigilare le tradizionali aree di rischio come sicurezza sul lavoro o reati societari.

Deve spingersi a presidiare anche la cyber sicurezza, perché trascurarla significherebbe, a mio giudizio, non solo rendere inefficace la sua funzione, ma persino esporsi al rischio di essere chiamato a rispondere per omissione di controllo.

Cyber sicurezza e vigilanza 231: il nuovo perimetro dell'OdV

Per anni, l'Organismo di Vigilanza ha svolto un ruolo fondamentale, ma, spesso, nella pratica, confinato alle aree tradizionali del rischio penale d'impresa: la sicurezza sul lavoro o i reati societari.

L'OdV è stato visto – e in molti casi trattato – come un attore tecnico, incaricato di sorvegliare settori ben delimitati, con strumenti collaudati e confini noti.

Ma oggi, qualcosa si è trasformato. L'equilibrio su cui si è retto il sistema della vigilanza negli ultimi vent'anni non sembra più sufficiente.

Il panorama dei rischi si è ampliato. Le vulnerabilità aziendali si sono spostate, spesso silenziosamente, verso territori nuovi e insidiosi e il cuore di questa trasformazione è la cyber sicurezza.

Questa esalogia, con l'entrata in vigore del D.Lgs. 138/2024, che attua la Direttiva NIS 2, molte delle misure tecniche e organizzative in ambito cyber un tempo considerate "best practice" – sono diventate oggi per le imprese riconosciute come soggetti NIS, veri e propri obblighi legali.

Parliamo di gestione del rischio, business continuity, protezione degli accessi, segmentazione delle reti, formazione del personale, risposta agli incidenti e procedure di notifica degli stessi.

Non sono più facoltative. Sono obblighi giuridici e, come tutti gli obblighi, se disattesi, generano responsabilità.

Quando un reato informatico previsto dall'art. 24-bis del D.lgs. 231/2001 – come l'accesso abusivo a sistemi informatici, il danneggiamento di dati o le frodi digitali – si verifica in un contesto dove l'ente aveva l'obbligo giuridico di implementare specifiche misure di sicurezza secondo la NIS 2, la mancata adozione di tali misure non può più essere considerata una semplice carenza organizzativa.

Sembra evidente come invece diventi violazione di un preciso obbligo legale che, evidenziato nei precedenti contributi, trasforma automaticamente l'omissione in colpa di organizzazione ai sensi del D.lgs. 231/2001.

Il perimetro della vigilanza

In tale quadro, risulta coerente ritenere che, in questi particolari contesti, l'OdV venga chiamato in causa in modo diretto e inevitabile. Perché se la cyber security è ormai parte integrante del perimetro giuridico di prevenzione, allora rientra a pieno titolo anche nel perimetro di vigilanza.

Non si tratta più di "tecnologia" ma di diritto, di obblighi, di prevenzione di reati.

Logicamente ne consegue che un OdV che non si attrezza, che non aggiorna il proprio piano di vigilanza, che non acquisisce le competenze minime per comprendere gli assetti cyber dell'organizzazione che ha il ruolo di soggetto NIS, forse non sta adempiendo pienamente al proprio mandato e forse rischia, a sua volta, di diventare parte di un sistema disfunzionale.

l'era in cui bastava presidiare le aree classiche è finita. Appare chiaro che la cyber security è diventata materia 231 e che chi esercita funzioni di vigilanza dovrebbe assumerla come nuova frontiera della responsabilità.