LABORATORIO 231

LA PREVENZIONE DEI REATI INFORMATICI: IL DOCUMENTO DI APPROFONDIMENTO DI AODV231

Mercoledì 17 gennaio 2024
Ore 15.00 / 18.00
Deloitte Greenhouse
via Tortona, 25 – Milano

L’esperienza del penalista dentro e fuori dall’OdV

Avv. Eleonora Montani
17 gennaio 2024

La **Cybersecurity aziendale** è centrale per le imprese

Transizione digitale nell'economia

Incremento dei rischi informatici

Perimetro di sicurezza nazionale cibernetica

LA LEGGE 231/01 E I REATI INFORMATICI

- Computer Crime _ reati informatici che si concretano nella manomissione dei dati conservati o trasmessi mediante un computer

- Computer Related Crime _crimini comuni realizzati mediante l'utilizzo di strumenti informatici

Assenza di specifica giurisprudenza

LA GESTIONE DELLA CYBERSECURITY

- Prevenzione
  - Regole comportamentali e di sicurezza
  - Definire livelli di accesso
  - ICS policy
- Controllo
  - Amministratore di sistema
  - Audit interni
  - Disaster Recovery
- Formazione
  - Lesson Learned e near miss
  - Responsabilizzazione

IMPATTO SUL MOG

- Lineamento di strategie, controlli e gestione dei rischi (approccio *risk based*);
- Centralità del dialogo con portatori di interesse interni e esterni;
- Implementazione dei flussi informativi verso l'ODV.

Approccio olistico e costruzione di sinergie

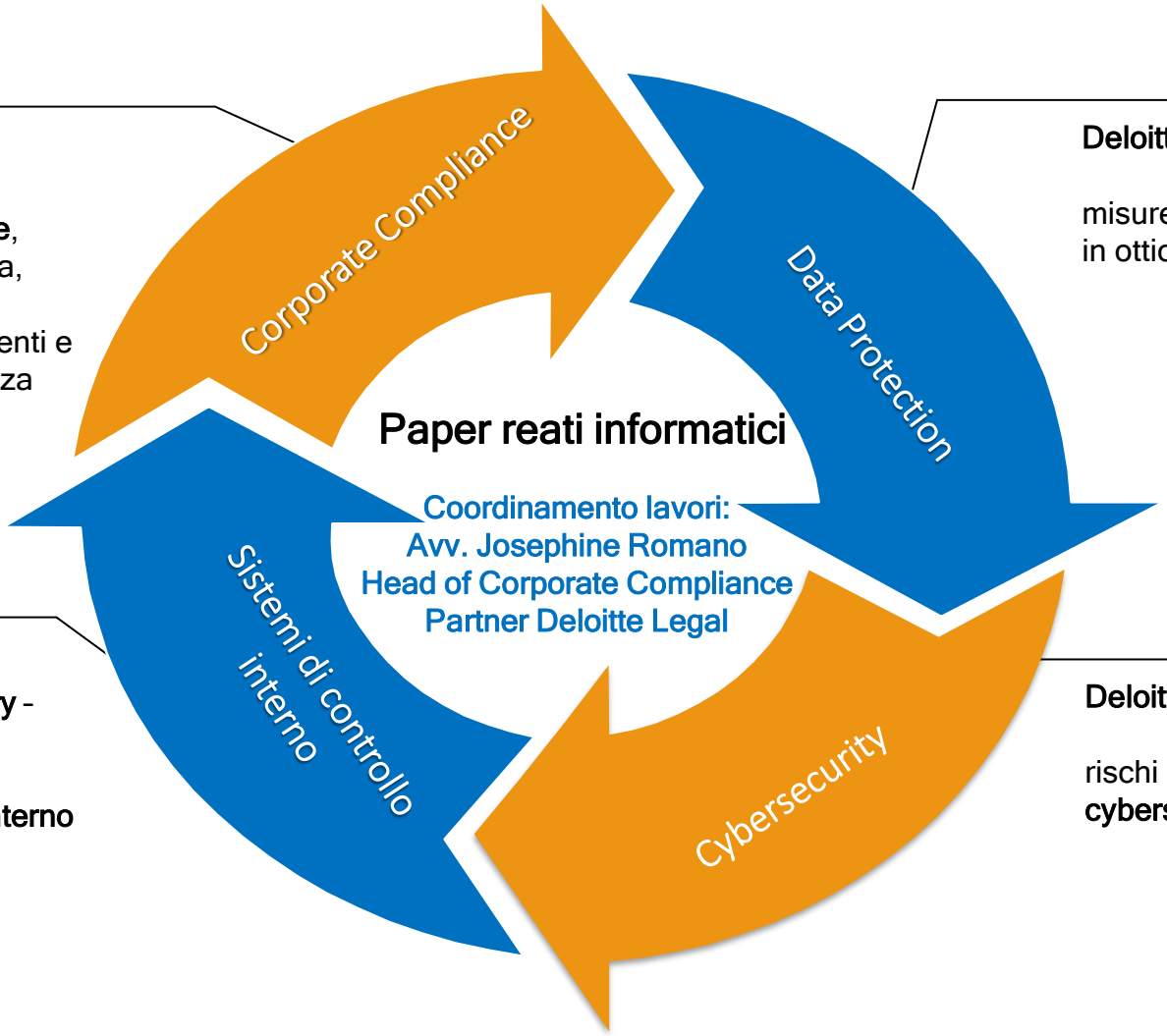
Fare clic per modificare stile

Eleonora Montani

avvocato@eleonoramontani.it

Deloitte Legal –

corporate compliance, criminalità informatica, responsabilità amministrativa degli enti e Organismo di Vigilanza



Deloitte Legal –

misure di sicurezza in ottica **privacy**

Deloitte Risk Advisory –

processi aziendali e sistemi di **controllo interno**

Deloitte Risk Advisory

rischi e minacce in tema **cybersecurity**

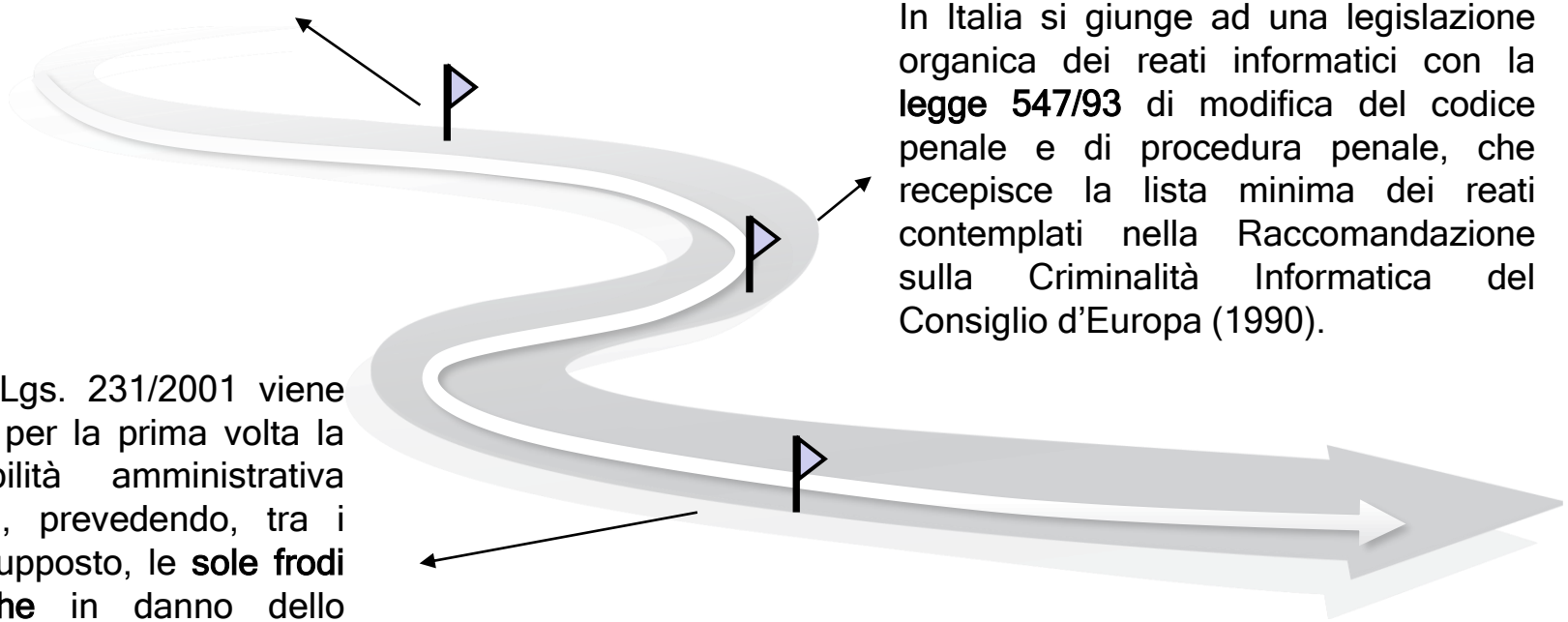
Introduzione normativa sulla criminalità informatica

Anni '80

Con la nascita di internet e con l'evoluzione informatica è emersa l'esigenza di apprestare un **sistema di prevenzione e tutela dai reati informatici** commessi mediante l'abuso di elementi della tecnologia informatica.

1993

In Italia si giunge ad una legislazione organica dei reati informatici con la **legge 547/93** di modifica del codice penale e di procedura penale, che recepisce la lista minima dei reati contemplati nella Raccomandazione sulla Criminalità Informatica del Consiglio d'Europa (1990).

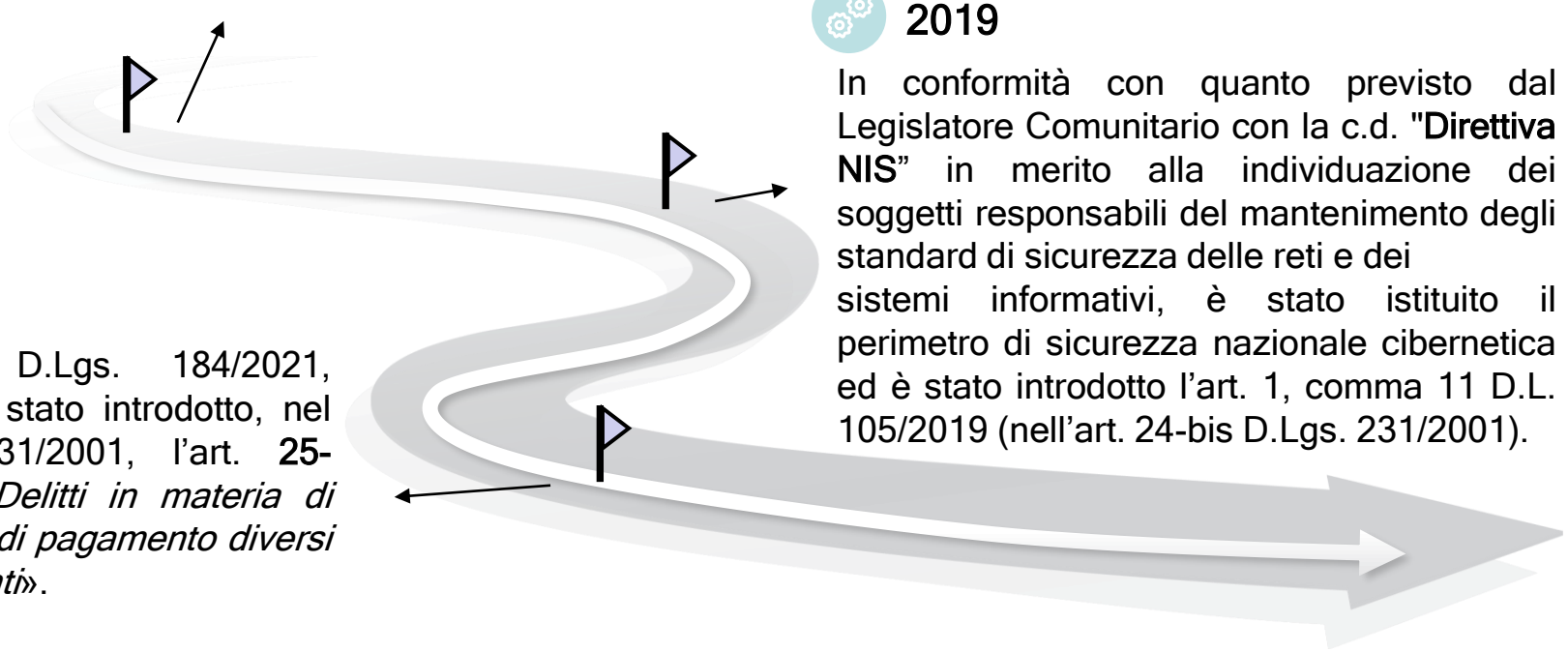


2001

Con il D.Lgs. 231/2001 viene introdotta per la prima volta la responsabilità amministrativa degli enti, prevedendo, tra i reati presupposto, le **sole frodi informatiche** in danno dello Stato o di un Ente pubblico.

2008

Attesa la necessità di introdurre forme di responsabilità penale per le persone giuridiche anche con riferimento ai reati informatici più gravi, con la legge di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest il 23 novembre 2001),è stato inserito nel Decreto 231 l'**art. 24-bis** «*Delitti informatici e trattamento illecito di dati*».



2019

In conformità con quanto previsto dal Legislatore Comunitario con la c.d. "**Direttiva NIS**" in merito alla individuazione dei soggetti responsabili del mantenimento degli standard di sicurezza delle reti e dei sistemi informativi, è stato istituito il perimetro di sicurezza nazionale cibernetica ed è stato introdotto l'art. 1, comma 11 D.L. 105/2019 (nell'art. 24-bis D.Lgs. 231/2001).

2021

Con il D.Lgs. 184/2021, invece, è stato introdotto, nel D.Lgs. 231/2001, l'art. **25-octies1** «*Delitti in materia di strumenti di pagamento diversi dai contanti*».

I reati informatici 231: le fattispecie in vigore

I reati informatici 231 non sono contenuti in un singolo titolo del codice penale, avendo il legislatore privilegiato il criterio del **bene giuridico tutelato**:

- delitti **contro la fede pubblica** (in particolare sulla falsità in atti)

491-bis c.p.	*Documenti informatici*
493-ter, 493-quater c.p.	*Reati in materia di strumenti di pagamento diversi dai contanti*

- delitti **contro la persona** (in particolare contro la libertà individuale mediante violazione del domicilio e dei segreti)

615-ter c.p.,	*Accesso abusivo ad un sistema informatico o telematico*
615-quater c.p.	*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*
615-quinquies c.p.	*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*
617-quater c.p.	*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*
617-quinquies c.p.	*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*

- delitti **contro il patrimonio** (in particolare mediante violenza e truffa)

635-bis c.p.	*Danneggiamento di informazioni, dati e programmi informatici*
635-ter c.p.	*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*
635-quater c.p.	*Danneggiamento di sistemi informatici o telematici*
635-quinquies c.p.	*Danneggiamento di sistemi informatici o telematici di pubblica utilità*
640-ter c.p.	*Frode informatica in danno dello Stato o di altro ente pubblico*
640-quinquies c.p.	*Frode informatica del certificatore di firma elettronica*

- **"Direttiva NIS"** (in merito al mantenimento degli standard di sicurezza informatica)

1, comma 11, D.L. n. 105/2019	*Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica*

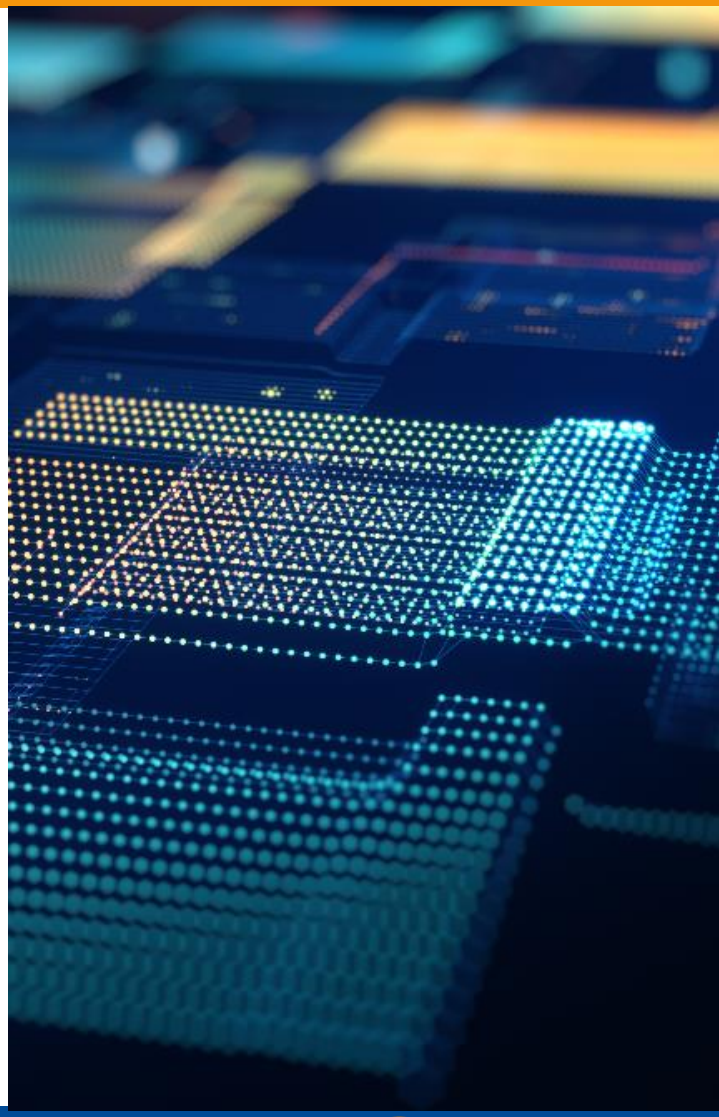
I reati informatici in azienda: casi pratici

Il Paper analizza *casi pratici* affrontati dalla giurisprudenza di legittimità che, pur avendo coinvolto solo persone fisiche, possono fornire una serie di spunti interessanti anche in tema di responsabilità delle persone giuridiche, alla luce:

1. dei soggetti agenti;
2. delle condotte contestate;
3. dell'interesse o vantaggio astrattamente ravvisabile in capo alla società.

Presupposti di responsabilità

Si ricorda che la società risponde *ex* D.Lgs. 231/2001 se i reati sono stati commessi nel proprio **interesse o vantaggio**, da parte di **soggetti apicali e/o** di persone **sottoposte** alla direzione o vigilanza di questi ultimi.



1

Il soggetto agente

Dipendente dell'Ispettorato Generale dell'Albo Nazionale dei Costruttori del Ministero dei lavori pubblici e, in concorso, i **titolari delle imprese private "beneficiarie"** del reato.

La condotta contestata

Imissione **nell'archivio informatico dell'Albo Nazionale dei Costruttori di dati non corrispondenti alle delibere adottate** dai competenti organi deliberativi, in modo da far risultare iscritte determinate imprese per categorie e per importi di lavori non corrispondenti a quelli reali (art. 491-bis c.p. - Documenti informatici).

Quale interesse?

Gli **esponenti** - apicali o sottoposti - di una società potrebbero **avere tutto l'interesse** ad ottenere certificazioni e documenti (rilasciati dalla Pubblica Amministrazione in formato elettronico) necessari alla conduzione del business della società di appartenenza godendo così l'impresa dei **vantaggi conseguenti a indebiti provvedimenti amministrativi**, emanati in assenza dei presupposti di legge.

2

Il soggetto agente

Dipendenti della società.

La condotta contestata

Accesso abusivo al sistema informativo di un'impresa concorrente e raccolta di informazioni utili per acquisirne la clientela (615-ter c.p. – Accesso abusivo)

Quale interesse?

Interesse (e a vantaggio) della società ad acquisire nuova clientela, sviandola dal concorrente.

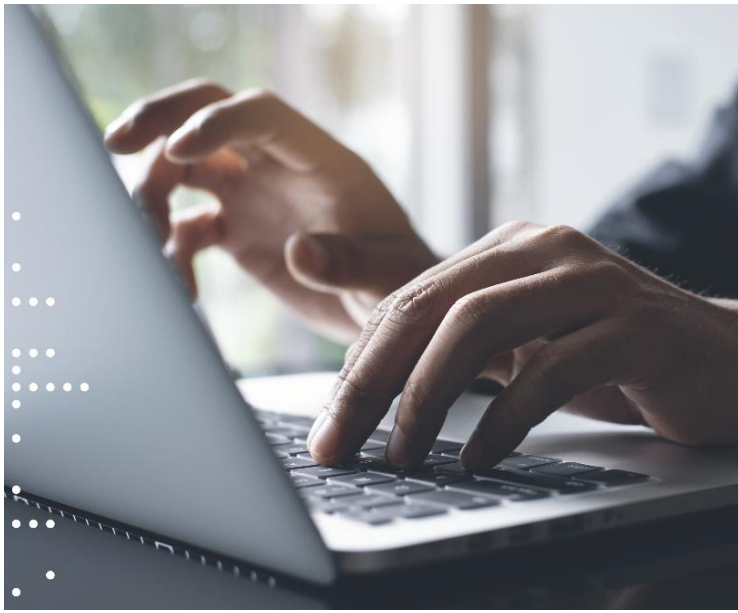
3

Il soggetto agente

Responsabile del **centro elaborazione dati** della società e Amministratore di sistema.

La condotta contestata

Intercettazione delle comunicazioni di posta elettronica indirizzate ad amministratori e dipendenti, mediante apposito programma (art. 617-quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche).



Quale interesse?

Si pensi a tutti quei comportamenti che l'amministratore di sistema potrebbe attuare per accedere a informazioni dei dipendenti su *input* degli apicali della Società, eventualmente interessati ad ottenere **maggiore efficienza produttiva sfruttando informazioni sensibili** acquisite illecitamente.

4

Il soggetto agente

Dipendente di una ditta individuale

La condotta contestata

Cancellazione di una gran quantità di dati dall'*hard disk* del computer aziendale, per poi sottrarre delle copie di *back-up.* La Corte ha delineato la condotta infedele che un dipendente può attuare a vantaggio di un altro datore di lavoro (attuale, nel caso di un impiego parallelo; futuro, nel caso di dimissioni) e ha stabilito che la condotta non presuppone necessariamente la cancellazione definitiva o irreversibile del file, ma sussiste anche qualora il suo recupero comporti oneri di spesa o, comunque, l'impiego di unità di tempo lavorativa (635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici).

Quale interesse?

Della **società** per la quale i dipendenti «infedeli» avrebbero illecitamente agito, danneggiando i sistemi informatici del *competitor*. Questo naturalmente nel periodo in cui i dipendenti (soggetti apicali o sottoposti) lo siano **al contempo** di entrambe le realtà aziendali.

5

Il soggetto agente

Gestore di attività di giochi e scommesse

La condotta contestata

Acquisto e utilizzo di due macchinette slotmachines per le quali, attraverso un telecomando, era possibile modificare il funzionamento in modo da procurarsi un ingiusto profitto derivante dall'incasso totalmente in nero di somme soggette a prelievo erariale unico, che l'imputato ometteva di versare all'Agenzia delle dogane e dei Monopoli (640-ter c.p. – Frode informatica)

Quale interesse?

Nel caso in cui la modifica del funzionamento della macchina fosse effettuata dalla stessa **impresa produttrice**, in capo a tale società potrebbe sorgere una responsabilità amministrativa: la stessa trarrebbe infatti un evidente vantaggio dal reato di frode informatica, consistente nella **maggiore appetibilità sul mercato** dei dispositivi ovvero in una eventuale **partecipazione ai profitti illeciti** del gestore.

Reati informatici e attività di vigilanza dell'OdV

Condizione esimente

Uno dei requisiti per poter beneficiare della **condizione esimente** prevista dall'art. 6 D.Lgs. 231/2001 è rappresentato dall'efficace attuazione del Modello e dalla nomina di un **Organismo di vigilanza** dotato "*di autonomi poteri di iniziativa e di controllo*".

Attività dell'OdV

L'**attività di monitoraggio** dell'OdV in relazione ai reati informatici deve tuttavia tener conto delle peculiarità dei mezzi tecnologici con cui le condotte dagli stessi criminalizzate vengono realizzate. Se infatti, per alcune fattispecie di reato presupposto, le verifiche dell'OdV possono essere di tipo prettamente documentale e prescindere dalla cooperazione dell'ente sottoposto a vigilanza, per i reati informatici, al contrario, va sottolineata l'assoluta rilevanza della collaborazione dell'ente nelle attività dell'Organismo attraverso:

1. *la predisposizione e il tempestivo invio all'OdV di **flussi informativi specifici**;*
2. *l'**interlocuzione con le funzioni interne preposte** alla gestione dell'infrastruttura tecnologica aziendale ovvero con consulenti/fornitori esterni.*

1. *La predisposizione e il tempestivo invio all'OdV di flussi informativi specifici*

L'attività di definizione o di integrazione del report dei flussi all'OdV, sulla gestione dell'infrastruttura informatica, va senz'altro parametrata sulla scorta delle **specificità** della singola organizzazione aziendale.

Ciò posto, i flussi che si riscontrano nella maggioranza delle realtà aziendali sono rappresentati dall'invio all'OdV di:

- **regolamenti e policy IT**;
- **report su violazioni** da cui si evincono **accessi non autorizzati ai sistemi interni o di terzi**;
- **Anomalie, criticità riscontrate**, etc.

2. *L'interlocuzione con le funzioni interne preposte alla gestione dell'infrastruttura tecnologica aziendale ovvero con consulenti/fornitori esterni*

Dall'analisi del processo di gestione dei sistemi informativi dell'ente si evince chiaramente quanto possa risultare **articolato e complesso** un controllo sul medesimo da parte di un organismo che potrebbe non annoverare al proprio interno uno o più componenti muniti di *expertise* specifica in materia IT.

Alla luce della complessità dell'esecuzione di tali controlli, è dunque opportuno che l'**OdV sia coadiuvato da:**

- **le funzioni aziendali coinvolte** nelle verifiche sulle attività sensibili e/o nella gestione dell'infrastruttura informatica (*i.e.* la funzione Internal Audit, la funzione IT/ICT ovvero l'eventuale *outsourcer* incaricato);
- eventuali **consulenti *ad hoc***, specializzati nelle investigazioni informatiche e nell'analisi forense informatica.

Illeciti penali privacy e reati informatici
La compliance privacy

1. Principi cardine della compliance privacy

- **Fonti legislative**
  - Regolamento (UE) n. 679/2016, cd. GDPR;
  - D.Lgs. 196/2003, cd. Codice Privacy;
  - Carta dei diritti fondamentali dell'UE;
  - Linee guida delle Autorità europee garanti per la protezione dei dati personali.

- **Risk based approach** → modello privacy tagliato sulla struttura dell'ente, valutando a monte i rischi connessi ai trattamenti di dati personali che contraddistinguono il business.

- **Principio di accountability** → flessibilità nella strutturazione del modello privacy accompagnata all'onere di dimostrare l'adeguatezza dei presidi.

- Principi di **privacy by design** e **privacy by default** → adeguate misure di sicurezza, minimizzazione, pseudonimizzazione, trasparenza, limitare l'accesso ai dati, consentirne l'accesso all'interessato, ecc. Protezione dei dati fin dalle prime fasi dello sviluppo di prodotti, servizi e applicazioni.

2. Illeciti penali privacy e reati informatici

- **Illeciti penali privacy**

  La normativa vigente sulla protezione dei dati personali non solo fornisce principi fondamentali, ma include anche disposizioni di dettaglio. Il Codice Privacy, riformato nel 2018, prevede specifiche fattispecie di illeciti penali:

  - **trattamento illecito di dati** (art. 167);
  - **comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala** (art. 167-bis);
  - **acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala** (art. 167-ter);
  - **falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante** (art. 168);
  - **inosservanza di provvedimenti del Garante** (art. 170).

  Il **D. Lgs. 231/01 non opera alcun rinvio a tali reati** (l'originario art. 9 c. 2 D. L. 93/2013 includeva nel "Catalogo 231" anche i delitti in materia di privacy, tuttavia questa previsione è stata soppressa in sede di conversione ad opera della L. 119/2013).

2. Illeciti penali privacy e reati informatici

- **Reati informatici**

  Il D. Lgs. 231/01 richiama una serie di articoli del Codice Penale, che includono anche, tra altri:

  - l'**accesso abusivo ad un sistema informatico o telematico** (art. 615-ter);
  - l'**installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche** (art. 617-quinquies);
  - il **danneggiamento di informazioni, dati e programmi informatici** (art. 635-bis) **o di sistemi informatici o telematici** (art. 635-quater).

  Le fattispecie dei **reati informatici possono coinvolgere dati personali**, con **potenziali conseguenze negative sui diritti e le libertà degli interessati**.

  Es. accesso abusivo ad un sistema informatico: benché questo sia protetto da misure di sicurezza, nell'ambito della condotta quasi certamente verranno sottratti o distrutti dati.

  Le suddette **norme tutelano in via indiretta anche la riservatezza, integrità e disponibilità dei dati personali**, che sono sottoposti ad elevato rischio al concretizzarsi di tali fattispecie.

3. Modello organizzativo privacy per la prevenzione dei rischi

- Rispetto dei **principi in materia di protezione dei dati personali** (i.e. liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, accountability, privacy by design e by default).
- **Risk based approach** e **mappatura dei rischi** (elementi comuni alla disciplina 231).
- La probabilità e la gravità dei **rischi privacy** (e.g. data breach, furti di identità, pregiudizi alla reputazione dell'azienda o dell'ente pubblico, perdite finanziarie, richieste di risarcimento da parte di interessati, sanzioni da parte dell'Autorità di controllo) devono essere valutate considerando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento.

  Queste valutazioni devono essere svolte **prima e durante il trattamento**.

3. Modello organizzativo privacy per la prevenzione dei rischi

- È fondamentale costruire modelli privacy che siano correttamente **implementati**, attentamente **presidiati** e **integrati con altri modelli organizzativi** (tra cui il MOG 231).
- **Misure organizzative**, tra cui anche:
  - individuazione di specifici ruoli e funzioni in ambito privacy;
  - formazione e awareness aziendale;
  - nomina di un Data Protection Officer (DPO);
  - registri dei trattamenti;
  - linee guida e procedure;
  - valutazioni di impatto sulla protezione dei dati o altri assessment.
- **Misure tecniche**, tra cui anche:
  - pseudonimizzazione;
  - cifratura;
  - procedure volte a ripristinare tempestivamente l'accesso ai dati in caso di incidenti o a testare l'efficacia delle misure e la resilienza dei sistemi.

4. Data breach policy

- **Art. 4 GDPR**: «*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*».

- **Adozione di una data breach policy**, corredata da altri **strumenti operativi** (es. registro dei data breach) per identificare:
  - gli step da seguire nella gestione dell'incidente;
  - le tempistiche da rispettare (anche per una eventuale notifica all'Autorità privacy e/o comunicazione agli interessati);
  - le persone coinvolte (incluso il DPO, ove nominato).

- **Esempio di data breach**: attacco ransomware che provoca la cifratura dei dati. Questa ipotesi potrebbe integrare gli estremi del reato ex art. 615-ter c.p (accesso abusivo ad un sistema informatico o telematico).
  → una **corretta impostazione nella gestione del rischio in un'ottica privacy e di cybersecurity è complementare** rispetto ai processi da implementare **per la prevenzione dei reati informatici presupposti** dal D. Lgs. 231/2001

5. DPO a confronto con l'OdV 231

- **Compiti del DPO:**
  - sorvegliare l'osservanza della normativa applicabile e delle politiche aziendali in materia di protezione dei dati personali;
  - fornire consulenza in merito agli obblighi di legge;
  - fungere da punto di contatto con l'Autorità di controllo e cooperare con la stessa, in caso di necessità.

  In altri termini, svolge **funzioni consultive e di controllo** ma anche **formative** e **informative** in tema di protezione dei dati, affiancando il titolare del trattamento.

- **Designazione obbligatoria** del DPO se il trattamento è effettuato da:
  - un'**autorità pubblica o da un organismo pubblico** (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali);
  - aziende del settore privato nei casi in cui il titolare effettui trattamenti che comportino il **monitoraggio regolare e sistematico degli interessati su larga scala** ovvero **trattamenti su larga scala di categorie particolari di dati**.

5. DPO a confronto con l'OdV 231

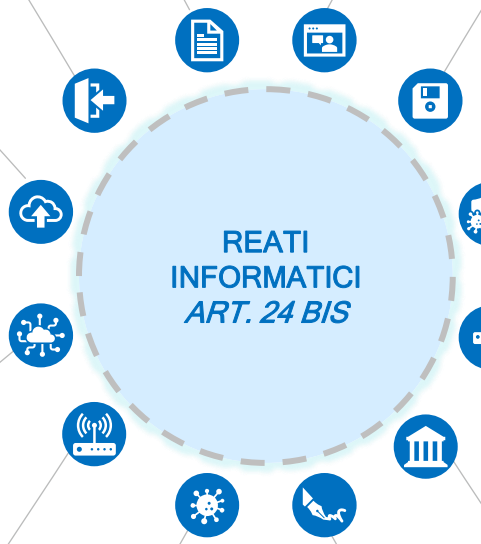
- Il DPO può essere individuato all'**interno dell'organizzazione** o può trattarsi di un **consulente esterno**, nominato con apposito contratto di servizi.

- **Analogie con l'OdV**
  - **poteri di iniziativa e controllo**, in posizione di **indipendenza**;
  - **rapporto di collaborazione con l'ente** che li ha nominati;
  - potere di **vigilanza**;
  - **flussi informativi**;
  - dovere di **riservatezza**.

- **Qualificazione soggettiva ai fini privacy dell'OdV:** i singoli membri devono essere considerati soggetti **autorizzati al trattamento dei dati personali.**

- Resta raccomandabile una **cooperazione effettiva tra DPO e OdV** per garantire una compliance integrata.

I reati informatici ex art. 24-bis del D.Lgs. 231/2001 …



FALSIFICAZIONE DI DOCUMENTI INFORMATICI
Art. 491 bis c.p.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO TELEMATICO
Art. 615 ter c.p.

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI TELEMATICI
Art. 615 quater c.p.

DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO
Art. 615 quinquies c.p.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE
Art. 617 quater c.p.

VIOLAZIONE DELLE NORME IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA
Art . 1 ,comma 11, D.L. 21.09.2019, n. 105 c.p.

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATCHE
Art. 617 quinquies c.p.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI
Art. 635 bis c.p.

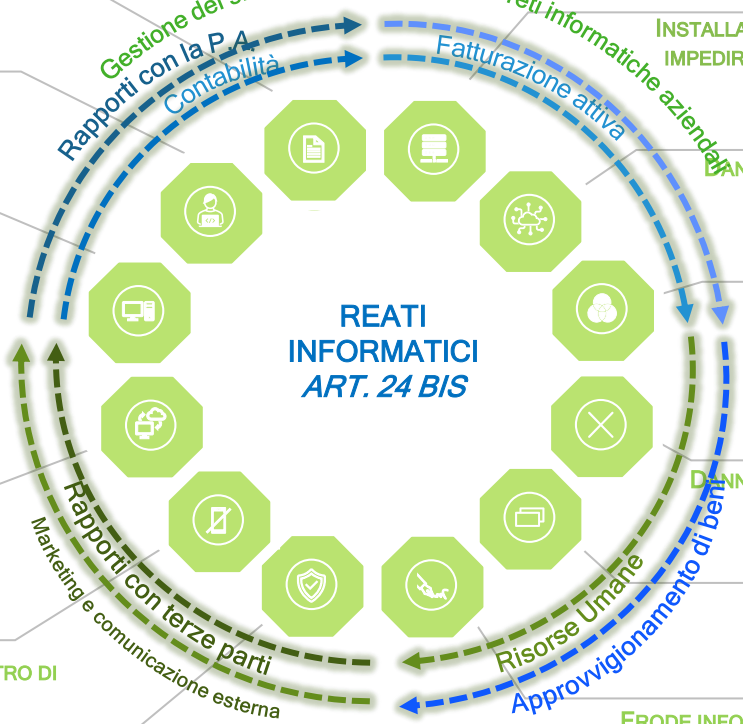
DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITÀ
Art. 635 ter c.p.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI
Art. 635 quater c.p.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ
Art. 635 quinquies c.p.

FRODE INFORMATICA DEL CERTIFICATORE DI FIRMA ELETTRONICA
Art . 640 quinquies c.p.

… in stretta connessione con i processi aziendali



FALSIFICAZIONE DI DOCUMENTI INFORMATICI
(Art. 491 bis c.p.)

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO
(Art. 615-ter c.p.)

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI
(Art. 615-quater c.p.)

DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO
(Art. 615-quinquies c.p.)

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE
(Art. 617-quater c.p.)

VIOLAZIONE DELLE NORME IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA
(Art. 1,comma 11, D.L. 21.09.2019, n. 105 c.p.)

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE
(Art. 617 quinquies c.p.)

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI
(Art. 635-bis c.p.)

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.)

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI
(Art. 635-quater c.p.)

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ
(Art. 635-quinquies c.p.)

FRODE INFORMATICA DEL CERTIFICATORE DI FIRMA ELETTRONICA
(Art. 640-quinquies c.p.)

Dal diritto all'impresa: dai rischi-reato ai processi ed ai presidi

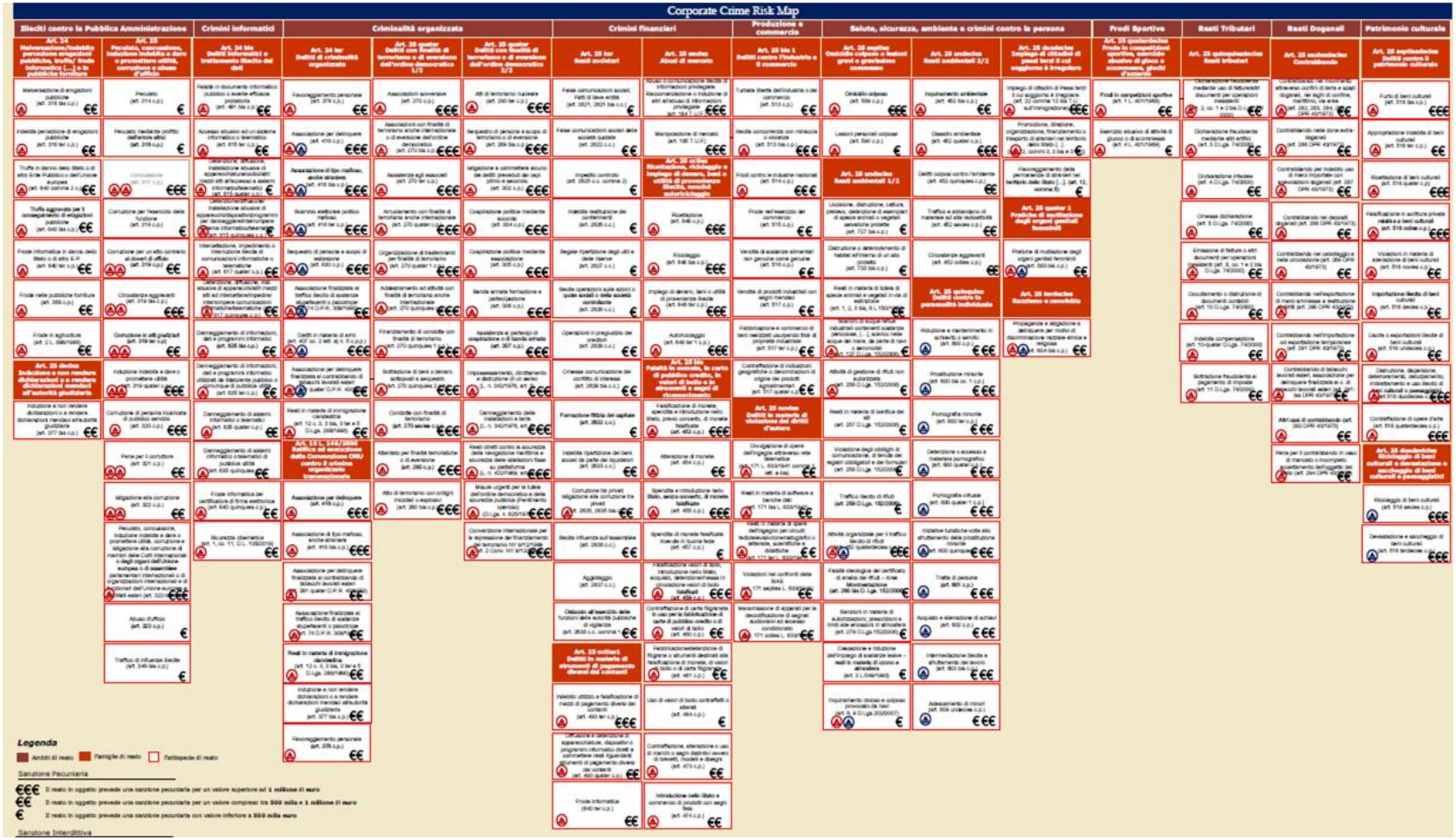
Mappatura dei rischi-reato specifici dell'organizzazione e (con particolare riferimento alle fattispecie di cui all'art. 24 bis del D.Lgs. 231/01) in coerenza con:

- business
- dimensioni
- articolazione organizzativa
- storia dell'ente

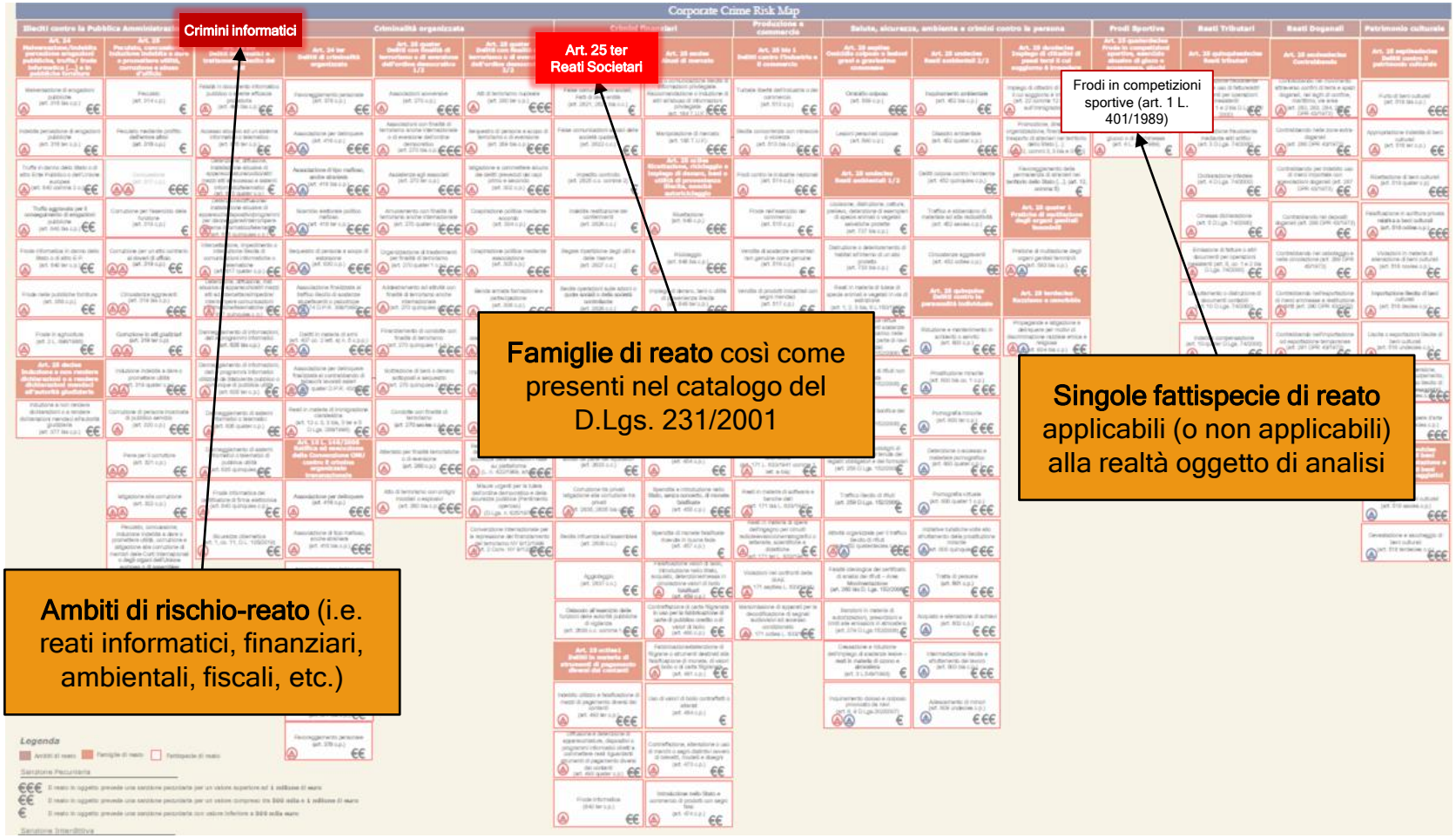
Identificazione dei **processi/attività sensibili** ai rischi-reato individuati nella fase precedente e dei **principi/presidi di controllo** atti a **prevenire** e **mitigare** i **rischi-reato** identificati

Redazione / Aggiornamento della Parte Speciale del **Modello 231** in coerenza con quanto emerso nella **mappatura dei rischi e dei presidi**

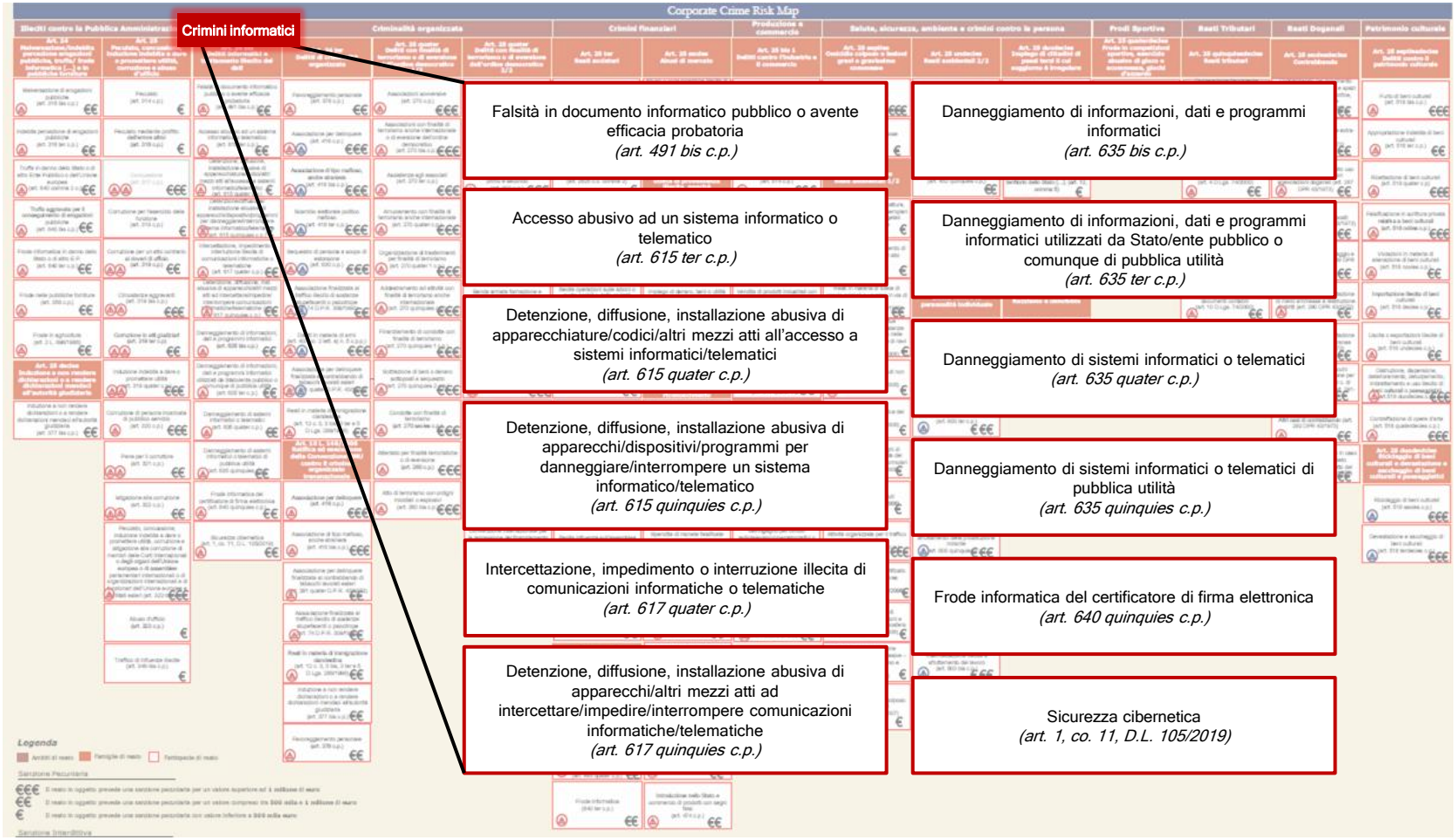
Mappatura dei rischi-reato | Corporate Crime Risk Map



Mappatura dei rischi-reato | Corporate Crime Risk Map



Mappatura dei rischi-reato | focus reati informatici



Risk Assessment di dettaglio

Step successivo all'**identificazione e mappatura** strutturata dei **reati applicabili** è lo svolgimento di un Risk Assessment di dettaglio che **analizzi** puntualmente **i rischi-reato 231**, in coerenza con i requirement del *comma 2, lett. a), dell'art. 6 del Decreto*

OBIETTIVO

Comprendere se, in quali circostanze e con quali modalità, un determinato **illecito possa essere commesso nell'interesse o a vantaggio dell'ente**, nell'ambito dell'organizzazione oggetto di analisi

MODALITÀ

Coinvolgimento dei soggetti responsabili delle **aree operative**, attraverso un **approfondito assessment dei rischi-reato specifici** delle rispettive aree di competenza (eventualmente supportati da risorse interne e/o esterne esperte in materia legale, di risk management, internal auditing e sistemi di controllo interno)

OUTPUT

Matrice rischio-reato

Art. 25 quinquies D.lgs. 231/2001		ESEMPI DI ATTIVITA' "SENSIBILI"	DIREZIONI COINVOLTE	POSSIBILI FINALITA' DI REALIZZAZIONE DEL REATO	ESEMPI DI POSSIBILI MODALITA' DI REALIZZAZIONE (a titolo esemplificativo e non esaustivo)	PROCESSI SENSIBILI
Riduzione o mantenimento in schiavitù o in servitù *(art. 600 c.p.)*	59	**Gestione degli acquisti**, con particolare riferimento ad affidamento di attività che prevedono l'utilizzo di manodopera di terze parti.	✓ Service erogato da Iren S.p.A.	Approfittando di una situazione di inferiorità ovvero di una situazione di necessità, si costringe una persona al proprio esclusivo servizio promettendo denaro o altra utilità.	Utilizzo o impiego di manodopera di soggetti terzi (e.g., prestatori d'opera nell'ambito di attività di appalto), nei casi in cui questi ultimi sottopongano i propri lavoratori a condizioni di sfruttamento approfittando del loro stato di bisogno.	1. Gestione degli acquisti di beni, servizi/consulenze e lavori
Intermediazione illecita e sfruttamento del lavoro *(art. 603 bis c.p.)*	60	**Gestione del personale**, con particolare riferimento alla definizione: - dell'orario lavorativo; - delle condizioni retributive; - degli impatti in ambito salute e sicurezza e delle condizioni lavorative in senso lato.	✓ Service erogato da Iren S.p.A.	Ottenere un risparmio di costi derivante dall'affidamento delle attività in appalto a terze parti che non rispettano pienamente, nei rapporti con i propri dipendenti, le condizioni fissate dai contratti collettivi nazionali ed ulteriori regolamentazione di riferimento.		3. Selezione, assunzione e gestione del personale e del sistema premiante

Reato

...fattispecie presupposto applicabili alla determinata attività sensibile

Attività sensibili

... potenzialmente esposte alla commissione del reato

Direzioni coinvolte

...che per procura o delega o responsabilità gestorie potrebbero commettere il reato

Finalità

...esemplificative di realizzazione del reato

Modalità

... esemplificative di realizzazione del reato

Processi sensibili

... in cui può verificarsi l'illecito

Dai rischi-reato ai presidi: percorso logico di analisi

PROCESSI
Identificazione dei PROCESSI SENSIBILI ai reati informatici

ATTIVITÀ SENSIBILI
Per ogni processo identificato, mappatura delle ATTIVITÀ sottostanti, SENSIBILI AL RISCHIO-REATO

PRESIDI DI CONTROLLO
Identificazione dei PRESIDI DI CONTROLLO da porre in essere al fine di MITIGARE / CONTRASTARE I RISCHI-REATO a cui è potenzialmente soggetta la società

Reati informatici: processi e attività sensibili

RILEVANZA DIRETTA

Gestione dei sistemi informativi e delle reti informatiche aziendali che sottende:

- Gestione degli accessi e dei profili di autorizzazione ed autenticazione ai sistemi informatici/telematici e alle applicazioni informative aziendali

Predisposizione e aggiornamento, con cadenza almeno annuale, di un elenco delle reti, dei sistemi informativi e dei servizi informatici (che comprenda la relativa architettura e componentistica interna)

Artt. 1, comma 11-bis L. 133/2019

Gestione della sicurezza informatica

Artt. 1, comma 11-bis L. 133/2019

Gestione delle attività on-line svolte dai dipendenti

Artt. 615 quater, 615 quinquies

Gestione delle informazioni sensibili

Artt. 491 bis, 615 ter, 635 bis, 635 quater

«STRUMENTALI»

Processi di natura operativa non direttamente rientranti nel processo di gestione delle infrastrutture tecnologiche, ma con riflessi ipotetici sullo stesso e potenzialmente rilevanti per la commissione dei reati informatici. Es.:

- Gestione acquisti di beni e servizi
- Gestione attività di ricerca e sviluppo
- Gestione attività di marketing e comunicazione esterna

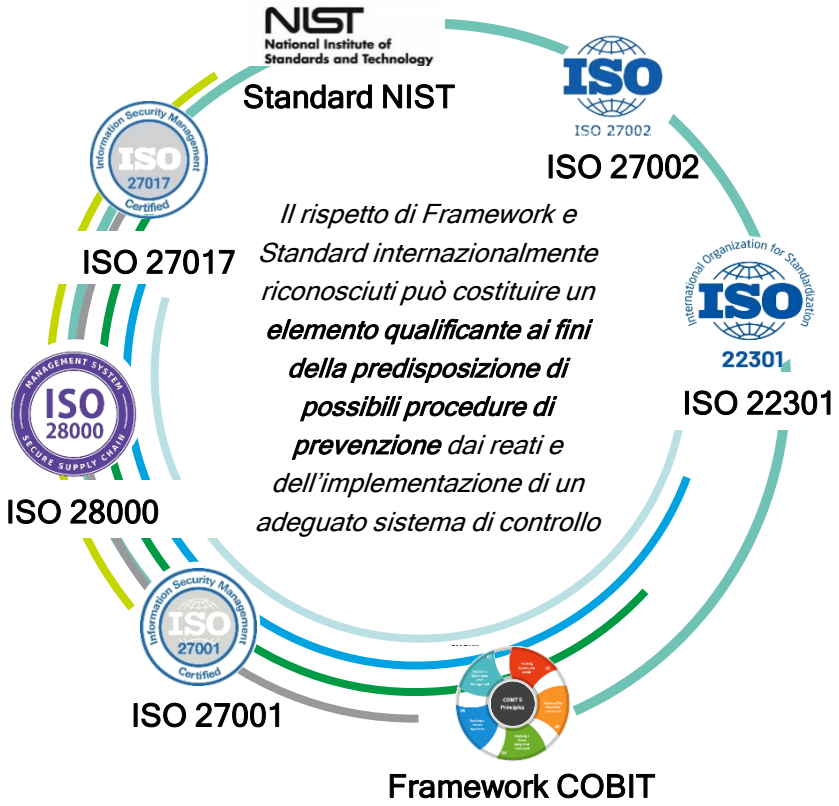
Reati informatici: presidi di controllo - introduzione

Per quanto il rischio, in astratto, non possa essere mai eliminato integralmente, l'**obiettivo prevenzionistico dell'ente** ai sensi del Decreto deve essere finalizzato a **contenerlo nel proprio risvolto di responsabilità penale** attraverso un **efficace ed efficiente** SISTEMA DI CONTROLLO INTERNO e l'adozione di specifici PRESIDI DI CONTROLLO

Il **Modello 231 deve arginare il rischio-reato** in una misura per cui l'agente non solo dovrà volere la commissione del reato, ma potrà attuare il proprio proposito criminoso soltanto AGGIRANDO FRAUDOLENTEMENTE le **prescrizioni dell'ente** e il relativo **sistema normativo interno**

Reati informatici: presidi di controllo - riferimenti

STANDARD E FRAMEWORK



LINEE GUIDA CONFINDUSTRIA

Nuove Linee Guida di Confindustria
per la costruzione dei Modelli di Organizzazione Gestione e Controllo
ai sensi del D.Lgs. 231/01

Le Linee Guida Confindustria forniscono alle imprese **indicazioni metodologiche** utili per l'elaborazione dei modelli, fornendo esempi dei principali processi/attività sensibili, dei relativi rischi-reato e dei presidi di controllo a mitigazione dei rischi

Reati informatici: presidi di controllo – esemplificazioni

ESEMPLIFICATIVO

PRINCIPALI PRESIDI DI CONTROLLO

GESTIONE DEI SISTEMI INFORMATIVI E DELLE RETI INFORMATICHE AZIENDALI

- Gestione delle informazioni sensibili (di business e/o personali)
- Gestione e protezione delle reti
- Gestione degli accessi da e verso l'esterno
- Gestione dei profili utente e del processo di autenticazione
- Gestione delle attività on-line svolte dagli utenti

- **Adozione di regolamenti e procedure** aventi ad oggetto il corretto utilizzo delle risorse informatiche aziendali, la sicurezza informatica/telematica, la protezione dei dati sensibili
- **Predisposizione di strumenti di protezione** volti a garantire la **sicurezza** nello **scambio di informazioni sensibili**, per l'azienda e per gli individui
- Adozione e implementazione di **procedure per la classificazione ed il trattamento delle informazioni**, per l'**utilizzo di sistemi crittografici** in relazione alla trasmissione in rete di documenti informatici, per i controlli tesi a **rintracciare eventuali falle o debolezze dei sistemi** (es. *vulnerability assessment* e *penetration test,* finalizzati a valutare la tenuta del sistema a fronte di eventuali attacchi esterni)
- Definizione di formali **requisiti di accesso e autenticazione al sistema**, dei criteri e delle modalità di **creazione ed utilizzo delle password**, di procedure per la **concessione** o la **revoca** degli **accessi** ai sistemi informativi;
- **Tracciatura e registrazione delle attività eseguite su sistemi, applicazioni e reti**, potenzialmente lesive per la sicurezza;
- **Verifica periodica delle modalità di accesso ai sistemi**, dei **log di registrazione** delle attività sui sistemi, delle **eccezioni e degli eventi** concernenti la **sicurezza**
- **Definizione** e **regolamentazione** delle **attività di gestione e manutenzione dei sistemi**
- **Adozione di meccanismi di protezione da software pericolosi** e procedure di controllo della installazione di software sui sistemi operativi
- Etc.

Reati informatici: presidi di controllo – esemplificazioni

PRINCIPALI PRESIDI DI CONTROLLO

ESEMPLIFICATIVO

RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Gestione del processo di creazione, trattamento e archiviazione di documenti elettronici con valore probatorio

Gestione dei pagamenti elettronici da e verso l'esterno (ivi inclusi quelli dovuti alla P.A.)

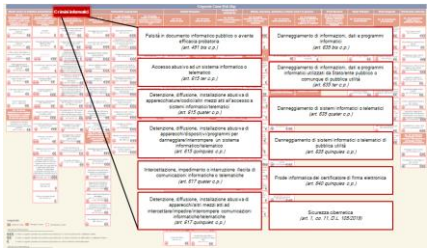
Gestione dei certificati digitali rilasciati da parte di un ente certificatore

Gestione sicurezza fisica e logica dei dati

- **Adozione e implementazione di specifiche misure** che prevedano:
  - individuazione di **ruoli e responsabilità** di documenti, dati ed elenchi
  - definizione delle **modalità** di **raccolta e approvazione della documentazione** da trasmettere alle autorità pubbliche
  - definizione di **attività di monitoraggio** per la **completezza delle informazioni** da comunicare
  - definizione e adozione di **misure tecniche per garantire adeguati livelli di sicurezza/ riservatezza** nel trattamento delle informazioni
  - individuazione delle **modalità comportamentali operative in caso di effettuazione di attività ispettive/vigilanza** da parte delle autorità preposte, etc.
- Definizione di **modalità di accesso ai sistemi informatici aziendali** mediante procedure di autorizzazione (es. concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze)
- Adozione di **procedure di validazione delle credenziali** complesse e previsione di **modifiche periodiche**
- Adozione di **misure di protezione dell'integrità delle informazioni** messe **a disposizione** su un **sistema pubblico** per prevenire modifiche non autorizzate
- Implementazione di **misure di protezione dei documenti elettronici** (es. firma digitale)
- Etc.

Redazione / aggiornamento Parte Speciale MOG231

…. in coerenza con quanto emerso dalla mappatura di rischi e presidi



Crime Risk Map
reati applicabili

Attività sensibili e processi
Risk Assessment di dettaglio

PO-029-02	CONTROLLI SU FORNITURE UTENZE
PO-123-00	GESTIONE DELLE OPERAZIONI ATTIVE E PASSIVE CON SOGGETTI NON RESIDENTI IN ITALIA
PO-124-00	TASSAZIONE DEI REDDITI C.D. "PASSIVE INCOME" (DIVIDENDI, INTERESSI E ROYALTIES) CORRISPOSTI A SOGGETTI NON RESIDENTI
PO-097-02	GESTIONE DELL A CASELLA DI POSTA ELETTRONICA CERTIFICATA AZIENDALE (PEC)

Presidi di controllo
Elenco SOP / istruzioni operative aziendali