



SEMINARIO

Dlgs 231 e i reati informatici : normativa e concetti di prevenzione



Ing. Roberto Francini

*Presidente Commissione 231 e modelli organizzativi
Ordine degli Ingegneri della Provincia di Roma*



PERCHE' questa presentazione? : la storia

In un contesto in cui il peggioramento dei dati è una costante da diversi anni, è importante valutare **come si muove l'Italia rispetto agli altri Paesi**.

Nel **Rapporto Clusit 2024**, presentato durante il Security Summit di Milano, il nostro Paese si conferma un bersaglio primario per i cybercriminali, con un **aumento del 65% degli attacchi cyber in Italia** rispetto al 2022:

11% la percentuale di attacchi in Italia sul totale nel resto del mondo

Colpisce la maggior capacità di far male dei criminali: nel 2023 gli attacchi di severità “critica” o “grave” rappresentano l’81% del totale-





I settori più colpiti in Italia da attacchi HACKER 2023

I primi 10 settori per incidenza degli attacchi in Italia sono:

- 1) 19% Il settore **Government / Military / Forze dell'Ordine** sono al primo posto, sul totale degli attacchi;
- 2) 13% il **Manufacturing** si attesta al secondo posto, con il 13%, dato molto al di sopra della media globale (**il 25% degli attacchi mondiali è a imprese manifatturiere italiane!**);
- 3) 12% il settore **Logistica e Trasporti** rappresenta il 12% del totale;
- 4) 11% i **Multiple Targets**, cioè campagne generalizzate senza specificità di settore;
- 5) 9% al quinto posto il settore **Finance / Insurance**, con il 9% di attacchi;
- 6) 9% il **Retail** è in sesta posizione, con il 9%;
- 7) 6% segue l'**ICT**, con il 6%;
- 8) 4% un tritico formato da **Healthcare, Professional / Scientific / Technical e Organizations**.



Obiettivo della presentazione

I reati informatici rappresentano una realtà sempre più diffusa nella società moderna, in cui la tecnologia e l'informatica giocano un ruolo fondamentale. In questo contesto, è importante comprendere la **responsabilità penale che può ricadere sull'ingegnere** in caso di violazione delle norme in materia.

La normativa italiana recentemente aggiornata dalla legge 90/2024 prevede una serie di disposizioni specifiche per contrastare i reati informatici.

Tra queste, il **Codice Penale all'articolo 615-ter** stabilisce che

chiunque, mediante l'utilizzo di strumenti informatici o telematici, commette una serie di reati, come l'accesso abusivo a un sistema informatico o telematico, la distruzione o la modifica di dati informatici, l'intercettazione illecita di comunicazioni telematiche, può essere punito con la reclusione da 2 – 10 anni.

Ing. **Alberto Francini**

Roma 11 Dicembre 2024

Data



Obiettivo della presentazione: L'INGEGNERE

- **L'ingegnere / manager** può essere coinvolto in situazioni che comportano la commissione di reati informatici.
- Utilizzare le proprie competenze per accedere in modo illecito a un sistema informatico altrui al fine di ottenere informazioni riservate, implica la responsabilità penale prevista dalla legge.
- La responsabilità penale **dell'ingegnere/manager** non è automatica, ma dipende dalla dimostrazione della sua volontà di commettere il reato e della sua consapevolezza.
- **L'ingegnere** può essere ritenuto responsabile anche per i reati commessi da terzi attraverso l'utilizzo delle sue competenze o delle sue infrastrutture informatiche.

In conclusione, è importante che l'ingegnere sia consapevole della responsabilità penale che può ricadere su di lui in caso di commissione di reati informatici. È necessario quindi conoscere ed attenersi alle norme in materia e utilizzare le proprie competenze in modo etico e legale, al fine di evitare conseguenze penali e tutelare la propria reputazione professionale.



Uguualmente e in accordo a principi già più volte espresse,
il **DLGS 231** prevede una responsabilità **anche** dell'ENTE in
caso di reati informatici .

L'ENTE è infatti responsabile di :

Prevenzione

Regole comportamentali e di sicurezza
Definire livelli di accesso

ICS policy - **ICS** è l'acronimo di Industrial Control Systems,
sistemi di controllo industriale.

Controllo

Amministratore di sistema
Audit interni
Disaster Recovery Plan

Formazione

Lesson learned e near miss
Responsabilizzazione



LA LEGGE 231/01 E I REATI INFORMATICI

Per reato informatico si intende ogni condotta prevista e punita dal Codice Penale in cui lo strumento informatico o telematico rappresenta un elemento determinante ai fini della qualificazione del fatto di reato.

Sostanzialmente nei crimini informatici possiamo suddividerli in due categorie :

Computer Related Crime _

crimini comuni realizzati mediante l'utilizzo di strumenti informatici in assenza di specifica giurisprudenza

Computer Crime

reati informatici che si concretano nella manomissione dei dati conservati o trasmessi mediante un computer

SECTION

La storia normativa nel DLGS 231 della
criminalità informatica

01



Breve storia dei reati informatici e la DLGS 231: come sono entrati nel 231 i crimini informatici ?

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

Necessità di introdurre forme di responsabilità penale per le persone giuridiche con riferimento ai reati informatici più gravi, Convenzione del **Consiglio d'Europa sulla criminalità informatica (Budapest il 23 novembre 2008)**, è stato inserito nel D.L.231 l'art. 24-bis «Delitti informatici e trattamento illecito di dati».



Breve storia dei reati informatici e la DLGS 231

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**».

2019

Direttiva NIS, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica **agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD)**. Il perimetro di sicurezza nazionale cibernetica ed è stato introdotto nell'art. 1, comma 11 D.L. 105/2019
(nell'art. 24-bis D.Lgs. 231/2001).

2024

Legge 90/2024 , inasprimento delle pene previste e rafforzamento dell'"Agenzia per la cybersicurezza nazionale" (ACN).



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.	<i>Documenti informatici</i>
	493-ter, 493-quater c.p.	<i>Reati in materia di strumenti di pagamento diversi dai contanti</i>
	615-ter c.p.,	<i>Accesso abusivo ad un sistema informatico o telematico</i>
	615-quater c.p.	<i>Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici</i>
Delitti contro la persona (in particolare contro la libertà individuale mediante violazione del domicilio e dei segreti)	615-quinquies c.p.	<i>Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico</i>
	617-quater c.p.	<i>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche</i>
	617-quinquies c.p.	<i>Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche</i>



....ed inoltre

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"
(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





UNA CONTINUA EVOLUZIONE

Nuova LEGGE 28 giugno 2024 , n. 90 . Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

I testo apporta modifiche sostanziali e processuali sul tema della sicurezza informatica, prevedendo l'aumento delle pene delle fattispecie di reato, nonché il rafforzamento dell'"*Agenzia per la cybersicurezza nazionale*" (ACN).

Sotto il profilo sostanziale vengono dunque modificati gli artt.

615-ter (Accesso abusivo a un sistema informatico o telematico),

615-quater (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici),

617-quater (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),

tutti reati presupposto alla responsabilità degli enti ai sensi dell'art. 24-bis D.Lgs. 231/2001.

UNA CONTINUA EVOLUZIONE

ESEMPI DI AGGRAVIO DELLE PENE



DL 90/2024 al codice penale sono apportate le seguenti modificazioni:
all'articolo 615 -ter :

- 1) al secondo comma: 1.1) all'alinea, le parole: «da uno a cinque anni» sono sostituite dalle seguenti: «da due a dieci anni»;
- 2) al terzo comma, le parole: «da uno a cinque anni e da tre a otto anni» sono sostituite dalle seguenti: «da tre a dieci anni e da quattro a dodici anni»;

all'articolo 615 -quater :

- 1) al primo comma, la parola: «profitto» è sostituita dalla seguente: «vantaggio»;
- 2) 2) il secondo comma è sostituito dal seguente: «La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 -ter , «La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici

SECTION

I reati informatici in
azienda: casi pratici:

02



ESEMPI PRATICI

Qui di seguito si propongono 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.



Si ricorda infatti 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 ESEMPIO

IL SOGGETTO ATTIVO

Dipendente dell'Ispettorato Generale dell'Albo Nazionale dei Costruttori del Ministero dei lavori pubblici e i titolari delle imprese private “beneficiarie” del reato.

LA CONDOTTA ED IL REATO

Immissione 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 VANTAGGIO

Gli esponenti di una società potrebbero avere tutto l'interesse ad ottenere certificazioni e documenti (rilasciati dalla P. A. 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 ESEMPIO

IL SOGGETTO ATTIVO

Dipendenti della società.



LA CONDOTTA ED IL REATO

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

QUALE VANTAGGIO

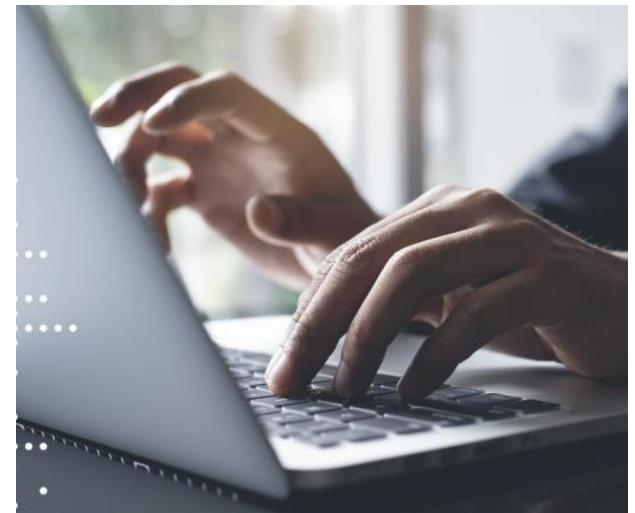
Interesse (e a vantaggio) della società ad acquisire nuova clientela, sviandola dal concorrente. Oppure anticipare l'immissione sul mercato di un nuovo prodotto guadagnando tempo sulla concorrenza .



3 ESEMPIO

IL SOGGETTO ATTIVO

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



LA CONDOTTA ED IL REATO

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 VANTAGGIO

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 ESEMPIO

IL SOGGETTO ATTIVO

Dipendente di una ditta individuale/consulente.

LA CONDOTTA ED IL REATO

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 VANTAGGIO

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.

SECTION

Reati informatici e attività
di vigilanza dell'OdV:

03



Condizione Esimente e i reati informatici

- 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”***.

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



Flussi informatici verso ODV

Ciò posto,

i flussi informatici 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.

L'Ente 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 nella gestione dell'infrastruttura informatica (i.e. la funzione Internal Audit, la funzione IT/ICT o outsourcer incaricato);**
- **eventuali consulenti ad hoc, specializzati nelle investigazioni informatiche**

SECTION

Prevenzione dei rischi per reati
informatici

04

Modello organizzativo per la prevenzione dei rischi - 1

Analizziamo la prevenzione dei rischi informatici non da un punto di vista tecnico,

ma come può difendersi l'Ente in caso di procedimento legale a seguito di un crimine informatico commesso al suo interno.



A fini processuali, a poco valgono ai fini dell'esclusione della responsabilità penale eventuali procedure, misure di sicurezza o sistemi di gestione adottati che non risultino inseriti all'interno del MOG ex D.Lgs. 231/2001.

Al *corpus* generale di modello MOG contenente tutte le prescrizioni di legge (normativa 231/2001), occorrerà prevedere e introdurre dei protocolli specifici per la prevenzione dei reati informatici.



Modello organizzativo per la prevenzione dei rischi-2

Ruoli e responsabilità

È fondamentale che tutte le responsabilità

in materia di sicurezza delle informazioni

siano definite e assegnate in conformità con le politiche e le procedure di sicurezza.

- A. Modello Organizzativo
- B. RACI
- C. Grandi Enti /Impianti: D.P.O.
- D. DPR / Data Breach policy .



Modello organizzativo per la prevenzione dei rischi -3

A questo punto l'ente può integrare le varie procedure, misure di sicurezza o sistemi di gestione implementati.

Un'utile guida da seguire per la creazione dei protocolli di prevenzione è offerta dagli standard ISO , anche certificabili :

ISO 27001 – Tecnologia dell'informazione - Tecniche per la sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti";

ISO 27002 – Linee guida per l'implementazione di sistemi di gestione per la sicurezza delle informazioni.

Modello organizzativo per la prevenzione dei rischi ESEMPIO

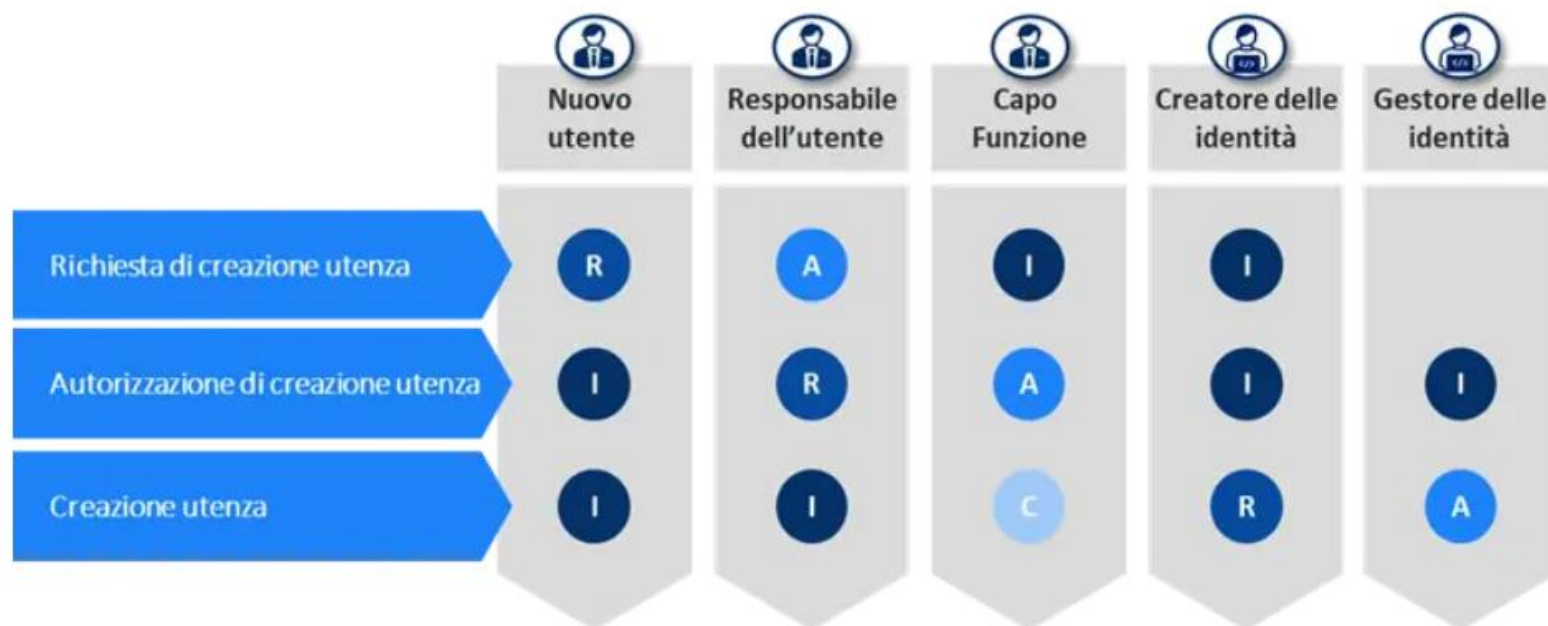


Figura 1 - Esempio di Matrice RACI

- R (Responsible) –esegue operativamente l'attività;
- A (Accountable) –supervisiona l'avanzamento e il completamento;
- C (Consulted) –supporta fornendo input e feedback;
- I (Informed)



Modello organizzativo per la prevenzione dei rischi-4

Le aree per le quali le persone sono responsabili dovrebbero essere indicate. In particolare, **in Aziende o Enti di grandi dimensioni si suggerisce :**

1. dovrebbero essere identificati e definiti gli asset e i processi di sicurezza delle informazioni;
2. dovrebbe essere identificato un responsabile per ciascun asset o processo di sicurezza delle informazioni e dovrebbero essere documentati i dettagli di questa responsabilità;
3. i livelli di autorizzazione agli accessi dovrebbero essere definiti e documentati;

Per essere in grado di adempiere alle responsabilità nell'area assegnata, i soggetti designati devono essere competenti e avere l'opportunità di tenersi aggiornati.

È inoltre opportuno tenere sotto controllo anche i fornitori esterni che possono avere impatti in relazione alla sicurezza delle informazioni.



Modello organizzativo **privacy** per la prevenzione dei rischi

In ogni caso indipendentemente dalle dimensioni dell'Ente si suggeriscono le seguenti misure organizzative, oltre alle già citate individuazione dei ruoli :

Misure organizzative

- formazione e awareness aziendale;
- **nomina di un Data Protection Officer (DPO);**
- registri dei trattamenti;
- linee guida e procedure;

Il Regolamento (UE) 2016/679 del 27 aprile 2016, più noto come GDPR, ha introdotto una nuova figura

il Data protection officer (DPO) o Responsabile della protezione dei dati (RPD).

Il DPO è colui che, forte di competenze specialistiche, si occupa di verificare la normativa e la prassi riguardo alla protezione dei dati personali.

Agli skill sulla legislazione e sulle best practice inerenti alla gestione dei dati personali, il DPO deve abbinare competenze informatiche.



Data Breach policy

Un piano di Disaster Recovery (**DRP**) è un **documento dettagliato che definisce le procedure e le istruzioni necessarie per aiutare un'organizzazione a ripristinare e recuperare le sue operazioni IT in caso di interruzione o disastro**. L'obiettivo principale di un DRP è

minimizzare il tempo di inattività e prevenire la perdita di dati.

I componenti principali di un DRP possono includere piani per il backup e il ripristino dei dati, la sostituzione di hardware e software, e la ripresa delle operazioni IT.

Adozione di una data breach policy, è utile 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 : 72 h max);
- e persone coinvolte (incluso il DPO, ove nominato).

SECTION

Il sistema sanzionatorio per reati
informatici

05



Il sistema sanzionatorio



Il sistema sanzionatorio del D.lgs. 231/01, a livello di importo, è **“contenuto”** in confronto alle sanzioni in caso di violazioni dettate nel **GDPR** (General Data Protection regulation Articolo 83) che in alcuni casi potrebbero raggiungere l'importo di 10 o 20 milioni di euro (secondo il tipo di infrazione) o al 2% o 4% del fatturato mondiale annuo riferito all'esercizio precedente.

Massimo di poco più di 1,5 M euro secondo un sistema basato su quote fissate dal giudice che ne determina il numero (non inferiore a 100 e non superiore a 1000) e, in seconda valutazione, dall'organo giurisdizionale che stabilisce il valore pecuniario della quota il cui ammontare massimo è di 1549 euro, stabilito in considerazione di alcune variabili: gravità del reato, grado di responsabilità dell'ente, volontà e azioni riparatorie e azioni di riorganizzazione aziendale.

Da qui la determinazione del caso di massimo importo citato poc'anzi:
 $1.549 \times 1.000 = 1.549.000$ di euro.



Il sistema sanzionatorio



È però bene precisare che, se detto importo potrebbe sembrare irrisorio ad una grande e solida multinazionale, non sarebbero irrisori altri effetti che un reato delle fattispecie elencate nel decreto potrebbe comportare:

sanzioni interdittive

confisca

pubblicazione della sentenza

- divieto di contrattare con la pubblica amministrazione (con eccezioni di prestazioni per un pubblico servizio);
- l'esclusione da finanziamenti, sussidi, agevolazioni e l'eventuale revoca di quelli già concessi;

Appare chiaro che una sanzione interdittiva blocca quasi totalmente l'attività di un Ente a cui dobbiamo aggiungere una grave conseguenza di reputazione (ancor più grave se il reato viene commesso da una società che produce soluzioni anti-intrusion, antivirus, analisi di vulnerabilità ecc.)



Il sistema sanzionatorio



Se il reato fosse commesso da Amministratori di Sistema, potrebbero inoltre esserci delle aggravanti. L'AdS è infatti un professionista a cui risulterebbe molto facile commettere un illecito e successivamente cancellarne le tracce, ragion per cui, le azioni di questa figura professionale devono poter essere in qualche modo controllate/verificabili secondo le disposizioni di quanto disposto dal Garante della Privacy.

Una violazione del D.lgs. 231 potrebbe quindi mettere in luce altre violazioni di altra natura: nel caso appena preso in esame potrebbero essere evidenziate carenze come, per esempio, una mancanza di access log, che devono essere trattati con particolari criteri per garantirne la completezza

SECTION

RIASSUMENDO

06



Responsabilità dell'Ente

Sorge spontanea la seguente domanda: ma l'azienda è sempre responsabile?

La risposta è: non in tutti i casi. L'ente potrebbe essere esente da responsabilità se prova, ad esempio, di aver adottato un modello di organizzazione, gestione e controllo ("MOGC") adeguato, o se la persona che ha commesso il reato è riuscita a commetterlo eludendo fraudolentemente il modello. Le sanzioni potrebbero essere in taluni casi evitate, in altri, notevolmente ridotte se l'ente si è adoperata per risarcire totalmente il danno e le conseguenze provocate dall'illecito.

Appare evidente che nei reati 231 (come pure nel GDPR del resto) la dimostrazione di aver adottato le misure logiche e organizzative idonee è fondamentale.



Soluzioni per prevenire i reati informatici

Le soluzioni che consentono di evitare tali reati si possono così sinteticamente riassumere:

1. dotarsi di un modello di organizzazione, gestione e controllo (“**MOGC**”) che, ricordo, non ha in nessun caso carattere di obbligatorietà ma esplica un’efficace azione preventiva;
2. implementare controlli e applicare misure tecniche e organizzative adeguate per prevenire tali fattispecie di frodi e che, nella maggior parte dei casi risultano utili anche per la prevenzione di altri illeciti, per esempio di non conformità al GDPR;
3. aderire a standard internazionali, in particolare allo standard ISO 27001 (norma internazionale per i Sistemi di Gestione della Sicurezza delle Informazioni denominata anche SGSI) e ISO27002 o altri standard in relazione a specifiche esigenze di Business



Soluzioni per prevenire i reati

L'adesione a modelli di gestione e norme internazionali **non è obbligatoria**, non rende automaticamente l'ente "**compliant**" anche al GDPR e alla normativa Privacy nazionale (D.lgs. 196/2003 novellato dal D.lgs. 101/2018) e neppure esula l'organizzazione da altri adempimenti, se previsti: tuttavia questi modelli, norme e standard che agiscono in armonia rafforzando ancor di più la tutela dell'Ente sono quindi da considerarsi come efficaci sostegni per la protezione di organizzazioni di qualsivoglia dimensione.

Ricordo, infine, che i reati informatici non possono essere prevenuti esclusivamente attraverso misure tecniche, ma con un approccio olistico di criteri di sicurezza fisica, logica e organizzativa.



GRAZIE PER L'ATTENZIONE

Relatore

Ing ROBERTO FRANCINI 3332214541





REATI INFORMATICI art. 24 bis E PROCESSI AZIENDALI

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

DETEZIONE 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.

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

Rapporti con la PA;

Fatturazione;

Marketing e
comunicazioni
esterne;

Risorse Umane ;

Gestione dei sistemi e
reti aziendali;

Approvvigionamento

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 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 INFORMAZIONI, DATI E
PROGRAMMI INFORMATICI
Art. 635 bis 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.

RISK ASSESSEMENT IN 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	ESEMPLI DI ATTIVITÀ "SENSIBILI"		DIREZIONI COINVOLTE	POSSIBILI FINALITÀ DI REALIZZAZIONE DEL REATO	ESEMPLI DI POSSIBILI MODALITÀ DI REALIZZAZIONE (a titolo esemplificativo e non esaustivo)	PROCESSI SENSIBILI
Falsificazione o mantenimento in attività o in servizio (art. 231 n. 1 p. 1)	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.	Apprendimento di una situazione di inferiorità su base di una situazione di necessità, al fine di ottenere una persona di propria esclusiva e senza promettere denaro o altra utilità.	Utilizzo o impiego di manodopera di soggetti terzi (p.g., prestatori d'opera nell'ambito di attività di appalto), nei casi in cui questi ultimi sottopongono i propri lavoratori a condizioni di sfruttamento approfittando del loro stato di bisogno.	1. Selezione degli acquisti di beni, servizi o consulenze e lavori
	60	Gestione del personale, con particolare riferimento alla definizione: - dell'orario lavorativo; - delle condizioni lavorative; - 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 terzi partecipe che non rispetti pienamente, nei rapporti con i propri dipendenti, le condizioni fissate dal contratto collettivo nazionale di lavoro (o) regolamentazione di riferimento.		2. 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



NIS II

Nell'ambito di un costante rafforzamento delle misure di sicurezza informatica a livello comunitario, reso necessario dalla crescente digitalizzazione della società, "Direttiva NIS 2". La Direttiva, pubblicata in Gazzetta Ufficiale il 14 dicembre 2022, abroga la precedente Direttiva NIS del 2016 (Direttiva 2016/1148).

Il Legislatore interviene e modifica una normativa che, nel giro di pochi anni, si è dimostrata incapace di gestire i rischi connessi alla repentina digitalizzazione dei vari processi produttivi –

Con l'adozione della Direttiva NIS 2 si è dunque proceduto ad aggiornare il quadro normativo europeo sulla sicurezza informatica, dotando gli enti pubblici e privati di nuovi e rinforzati strumenti per far fronte alle crescenti minacce in questo settore.

Anche il campo di applicazione è stato ampliato



NIS II

In Italia, il recepimento della Direttiva NIS 2 è avvenuto con il D. Lgs. n. 138/2024 del 4 settembre 2024, in vigore dal 16 ottobre 2024. Il Decreto riforma il quadro normativo precedente e introduce nuovi criteri di applicazione basati su tre requisiti principali: dimensionale, territoriale e settoriale.

Ulteriore cambiamento rispetto alla disciplina precedente è rappresentato dal fatto che le imprese vengono classificate in due macrocategorie: soggetti “essenziali” e “soggetti importanti”. I primi includono tutte le attività considerate strategiche per l’economia o per la sicurezza nazionale, mentre i soggetti “importanti”, pur non esercitando direttamente attività indispensabili, forniscono servizi che potrebbero comportare gravi problemi sociali in caso di malfunzionamento.



Riassumendo : Processo logico di identificazione dei rischi ai presidi da attivare



Mappatura rischi-reato e risk-crime assessment

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 processi/attività sensibili e presidi di controllo

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 / agglornamento Parte Speciale MOG 231

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