OSSERVATORIO
COMPLIANCE 231
di Morri Rossetti

Monthly Roundup

Marzo 2024

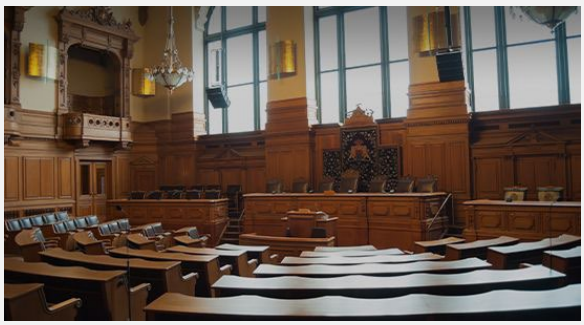
MONTHLY ROUNDUP

Marzo 2024

I principali aggiornamenti in materia di 231 dello scorso mese.

PRINCIPALI AGGIORNAMENTI

Approvato il Decreto correttivo alla Riforma Cartabia: le modifiche nel processo a carico dell'ente



Nella seduta dell'11 marzo scorso il Consiglio dei Ministri ha approvato in via definitiva il c.d. correttivo alla riforma Cartabia relativo al processo penale ("*Disposizioni integrative e correttive del Decreto Legislativo 10 ottobre 2022, n. 150, di attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari*"), ora il Decreto andrà alla firma del Presidente della Repubblica, prima di essere pubblicato in Gazzetta Ufficiale.

Per quanto di interesse in questa sede, il Decreto è intervenuto sul testo del D.lgs. 231/2001 operando due modifiche di natura processuale, volte nella sostanza ad uniformare alcuni aspetti dei procedimenti a carico delle persone giuridiche e delle persone fisiche.

Il correttivo mira, dunque, ad estendere al D.lgs. 231/2001 le modifiche operate dalla Riforma Cartabia sul codice di procedura penale, al fine di evitare contrasti e incongruenze tra le due discipline.

In particolare, l'art. 7 del Decreto "correttivo" interviene sull'art. 59 D.lgs. 231/01 che riguarda la contestazione dell'illecito amministrativo, eliminando il riferimento all'art. 405 co. 1 c.p.p. (che era stato abrogato dalla Riforma Cartabia) e inserendo il riferimento al nuovo art. 407-bis c.p.p.

Operano, dunque, anche nei confronti dell'ente le previsioni relative ai termini concessi al Pubblico Ministero per l'esercizio dell'azione penale o la richiesta di archiviazione, alla scadenza delle indagini.

Sempre l'art. 7 del Decreto prevede altresì la modifica dell'art. 61 D.lgs. 231/01, al fine di garantire che il giudice dell'udienza preliminari utilizzi la medesima regola di giudizio per entrambi gli imputati persona fisica e persona giuridica.

Le parole "*risultano insufficienti, contraddittori o comunque non idonei a sostenere in giudizio la responsabilità dell'ente*" sono, infatti, sostituite con *la nuova regola di giudizio già introdotta dalla Riforma Cartabia per la persona fisica, in base alla quale il G.u.p. pronuncia sentenza di non luogo a*

procedere quando l'illecito non sussiste o gli elementi acquisiti" non consentono di formulare una ragionevole previsione di condanna dell'ente".

* * *

Irregolarità negli appalti: le novità in materia penale contenute nel Decreto PNRR 4

Il D.L. n. 19/2024 (c.d. "Decreto PNRR 4"), pubblicato in Gazzetta Ufficiale lo scorso 2 marzo, è intervenuto, tra le altre, anche in materia di salute e sicurezza dei lavoratori e di regolarità dei rapporti di lavoro. Le disposizioni urgenti contenute negli articoli 29, 30 e 31 del Decreto sono chiaramente il frutto della pressione concentratasi sul Governo affinché intervenisse celermente con misure concrete idonee ad arginare il grave fenomeno degli infortuni sul lavoro, purtroppo sempre più protagonista della cronaca attuale.

Il Decreto PNRR, oltre a prevedere il meccanismo della "patente a punti" nei cantieri in cui si realizzano lavori edili o di ingegneria civile (di cui abbiamo parlato qui), ha altresì riformato le norme in materia di contrasto agli appalti irregolari, reintroducendo fattispecie penali e inasprendo le pene già previste dalla precedente normativa.

Strettamente connessi al tema della sicurezza sul lavoro sono, infatti, i fenomeni di illecita somministrazione di manodopera celati dietro la stipula di fittizi contratti di appalto di servizi. L'intervento repressivo in tale ambito, come spiegato dalla ministra del Lavoro Marina Calderone, è giustificato dal fatto che la somministrazione illecita «è uno dei reati più commessi» nell'ambito degli appalti e, soprattutto in un settore come l'edilizia, dove più alto è il rischio di incidenti, bisogna intervenire ponendolo «sotto la massima attenzione».

È in questo contesto, dunque, che il Decreto PNRR 4 reintroduce i reati di somministrazione irregolare e somministrazione fraudolenta, originariamente introdotti dalla Legge Biagi (D.lgs. 276/2003) e successivamente depenalizzati dal D.lgs. n. 8/2016.

In particolare, l'art. 29 del Decreto PNRR 4 prevede una prima ipotesi criminosa (meno grave) che si concretizza nei casi di appalto e distacco irregolari (in quanto privo dei requisiti previsti dalla legge: art. 1655 c.c. e artt. 29 e 30 D.lgs. 276/2003) e che prevede l'irrogazione in capo a utilizzatore e somministratore della pena dell'arresto fino a un mese o dell'ammenda di Euro 60 per ogni lavoratore occupato e per ogni giornata di occupazione.

Ciò che distingue l'appalto lecito da quello irregolare è sostanzialmente l'autonomia di organizzazione e gestione di mezzi di lavoro e personale da parte dell'appaltatore, che assume in capo a sé il rischio di impresa. Spesso tale autonomia manca e lo schema dell'appalto viene usato per mascherare una fornitura che più che i servizi ha ad oggetto i lavoratori, la cui attività viene gestita e organizzata dal committente come se si trattasse di propri dipendenti, senza però assumerne le relative responsabilità giuridiche.

Accanto a questa prima ipotesi di reato, il Decreto reintroduce anche la fattispecie di somministrazione fraudolenta, che si distingue dalla prima per il dolo specifico consistente nella "*specifica finalità di eludere norme inderogabili di*

legge o di contratto collettivo applicate al lavoratore" che giustifica la somministrazione stessa.

Al ricorrere di tale più grave fattispecie, il somministratore e l'utilizzatore sono puniti con la pena dell'arresto fino a tre mesi o con l'ammenda di Euro 100 per ciascun lavoratore coinvolto e per ciascun giorno di somministrazione.

Assumono rilevanza penale anche le ipotesi di somministrazione non autorizzata e di utilizzazione illecita di manodopera; esercizio non autorizzato dell'attività di intermediazione, nell'ipotesi attenuata in cui il fatto sia commesso senza scopo di lucro ed esercizio non autorizzato delle attività di ricerca e selezione del personale e supporto alla ricollocazione professionale, anche nell'ipotesi attenuata in cui il fatto sia commesso senza scopo di lucro.

Quanto alla responsabilità amministrativa degli enti nell'interesse o a vantaggio dei quali tali reati si perpetuano il Decreto invece nulla dispone, lasciando al momento scoperta l'area interessata dal D.lgs. 231/2001.

Tale lacuna emerge con ancor più evidenza se si considera che le condotte contravvenzionali introdotte dal Decreto sono tipicamente realizzate nell'interesse e vantaggio di enti che, con tutta probabilità, risultano sprovvisti di un'organizzazione idonea a prevenire la commissione di questi reati.

Merita infine evidenziare che il contrasto all'utilizzo irregolare degli appalti viene realizzato dal Decreto anche sotto il profilo delle condizioni di lavoro, con una previsione finalizzata a scoraggiare il ricorso all'appalto per motivi di semplice riduzione del costo di lavoro. È infatti stabilito, a carico degli appaltatori (e dei subappaltatori), l'obbligo di riconoscere al personale impiegato nell'appalto di opere o servizi «*un trattamento economico complessivo non inferiore a quello previsto dal contratto collettivo nazionale e territoriale maggiormente applicato nel settore e per la zona il cui ambito di applicazione sia strettamente connesso con l'attività oggetto dell'appalto*».

L'Osservatorio 231 ha più volte affrontato il tema della somministrazione illecita e delle irregolarità sugli appalti, concentrandosi sulle conseguenze (anche penali) derivanti da tali meccanismi.

Per maggiori approfondimenti sul tema:

- Ammissibilità delle contestazioni di cui all'art. 2 D.lgs. 74/2000 nell'ambito dei procedimenti relativi ad intermediazione illecita di mano d'opera

- Somministrazione illecita di manodopera e appalti fittizi: aspetti fiscali

- Archiviazione DHL Supply Chain S.p.A.: l'interessante decisione della Procura di Milano

- Appalti di servizio. La giurisprudenza traccia le linee di confine tra liceità e illiceità

- Somministrazione illecita di manodopera e appalti fittizi

* * *

Patente a punti nei cantieri: le nuove norme per i cantieri temporanei o mobili

È stato pubblicato in Gazzetta Ufficiale il Decreto PNRR 4 (DL 19/2024), contenente disposizioni in materia di salute e sicurezza sul lavoro. L'articolo 29 comma 19 del decreto modifica integralmente l'articolo 27 del D.lgs. 81/2008, TU in materia Salute e sicurezza sul lavoro.

A partire dal 1° ottobre 2024 entrerà in vigore il meccanismo della "patente a punti". La stessa verrà rilasciata dalla competente sede territoriale dell'Ispettorato Nazionale del Lavoro **alle imprese e ai lavoratori autonomi che operano nei cantieri temporanei o mobili, previsti dall'articolo 89, comma 1, lettera a) del D.lgs. n. 81 del 2008**.

La disposizione da ultimo citata rinvia ai cantieri in cui si realizzano i **lavori edili** o **di ingegneria civile** di cui all'allegato X del medesimo provvedimento di legge.

Saranno dunque tenute a richiedere e potranno ottenere la patente a punti le imprese e i lavoratori autonomi che svolgano nei cantieri temporanei o mobili:

1. *I lavori di costruzione, manutenzione, riparazione, demolizione, conservazione, risanamento, ristrutturazione o equipaggiamento, la trasformazione, il rinnovamento o lo smantellamento di opere fisse, permanenti o temporanee, in muratura, in cemento armato, in metallo, in legno o in altri materiali, comprese le parti strutturali delle linee elettriche e le parti strutturali degli impianti elettrici, le opere stradali, ferroviarie, idrauliche, marittime, idroelettriche e, solo per la parte che comporta lavori edili o di ingegneria civile, le opere di bonifica, di sistemazione forestale e di sterro.*

2. *Sono, inoltre, lavori di costruzione edile o di ingegneria civile gli scavi, ed il montaggio e lo smontaggio di elementi prefabbricati utilizzati per la realizzazione di lavori edili o di ingegneria civile.*

La normativa individua i criteri e i requisiti in base ai quali verrà rilasciata la patente a punti in formato digitale:

"*la patente è rilasciata, in formato digitale, dalla competente sede territoriale dell'Ispettorato nazionale del lavoro subordinatamente al possesso dei seguenti requisiti da parte del responsabile legale dell'impresa o del lavoratore autonomo richiedente*:

a*) iscrizione alla camera di commercio industria e artigianato;*

b) adempimento, da parte del datore di lavoro, dei dirigenti, dei preposti e dei lavoratori dell'impresa, degli obblighi formativi di cui all'articolo 37;

c) adempimento, da parte dei lavoratori autonomi, degli obblighi formativi previsti dal presente decreto;

d) possesso del documento unico di regolarità contributiva in corso di validità (DURC);

e) possesso del Documento di Valutazione dei Rischi (DVR);

f) possesso del Documento Unico di Regolarità Fiscale (DURF)".

Stando alle nuove disposizioni, ciascuna impresa o lavoratore autonomo sarà dotato di un punteggio iniziale di trenta crediti ed è consentito

ai soggetti di operare nei cantieri temporanei o mobili con una dotazione pari o superiore a quindici crediti.

La patente subisce inoltre decurtazioni che sono correlate alle risultanze degli accertamenti e dei conseguenti provvedimenti definitivi emanati nei confronti dei datori di lavoro, dirigenti e preposti dell'impresa o del lavoratore autonomo.

Tra le diverse ipotesi disciplinate di decurtazioni vi è quella *di "riconoscimento della responsabilità datoriale di un infortunio sul luogo di lavoro da cui sia derivata*:

1) la morte: venti crediti;

2) un'inabilità permanente al lavoro, assoluta o parziale: quindici crediti;

3) un'inabilità temporanea assoluta che importi l'astensione dal lavoro per più di quaranta giorni: dieci crediti".

A ciò si aggiunga che "*Nei casi di infortuni da cui sia derivata la morte o un'inabilità permanente al lavoro, assoluta o parziale, la competente sede territoriale dell'Ispettorato nazionale del lavoro può sospendere, in via cautelativa, la patente fino a un massimo di dodici mesi. L'ispettorato nazionale del lavoro definisce i criteri, le procedure e i termini del provvedimento di sospensione. Ciascun provvedimento [...] riporta i crediti decurtati. Gli atti ed i provvedimenti emanati in relazione al medesimo accertamento ispettivo non possono nel complesso comportare una decurtazione superiore a venti crediti*".

Sotto un profilo più strettamente procedurale si evidenzia che l'amministrazione che ha formato gli atti e i provvedimenti definitivi ne dà notizia, entro trenta giorni dalla notifica ai destinatari, anche alla competente sede territoriale dell'Ispettorato nazionale del lavoro, la quale procede entro trenta giorni dalla comunicazione alla decurtazione dei crediti.

Si precisa inoltre che I crediti decurtati possono essere reintegrati a seguito della frequenza, da parte del soggetto nei confronti del quale è stato emanato uno dei provvedimenti, a specifici corsi formativi.

Con una dotazione inferiore a quindici crediti della patente le imprese e i lavoratori autonomi non sono nelle condizioni di operare nei cantieri temporanei o mobili, fatto salvo il completamento delle attività oggetto di appalto o subappalto in corso al momento dell'ultima decurtazione dei crediti nonché gli effetti degli eventuali provvedimenti di sospensione.

Chi svolga comunque l'attività in violazione delle disposizioni in materia di patente a punti può essere chiamato al pagamento di una sanzione amministrativa da euro 6.000 ad euro 12.000 e all'esclusione dalla partecipazione ai lavori pubblici di cui al codice dei contratti pubblici, per un periodo di sei mesi.

Le informazioni relative alla patente confluiranno all'interno di un apposito portale.

Da ultimo il nuovo testo di legge chiarisce che le **imprese in possesso dell'attestato di qualificazione SOA, non sono tenute al possesso della patente a punti per la sicurezza sul lavoro**.

La Certificazione SOA è un attestato obbligatorio, rilasciato da Organismi di Attestazione autorizzati, comprovante la capacità economica e tecnica di un'impresa di qualificarsi per l'esecuzione di appalti pubblici di lavori di importo maggiore a € 150.000,00.

Tale iniziativa legislativa denota una sempre crescente attenzione alle tematiche Salute e

sicurezza sul lavoro nell'ottica di prevenire i troppi infortuni sul lavoro attraverso un sistema che rafforza l'obbligo di rispetto della normativa di settore esistente.

* * *

Rivelazione di segreto industriale e illecito utilizzo del "reverse engineering"

Nella sentenza n. 3211/2024, la Corte di cassazione ha affrontato il tema della tutela penale del know-how aziendale, giudicando un caso in materia di accesso abusivo a sistema informatico (art. 615-ter c.p.) e rivelazione di segreti industriali e commerciali (art. 623 c.p.).

Nel confermare la condanna degli imputati, la Corte ha dato una lettura attuale dell'art. 623 c.p. rilevando che, alla luce dei rilevanti e crescenti costi che oggi caratterizzano la ricerca scientifica orientata allo sviluppo di tecnologie competitive su mercati ormai globali, il reato deve ritenersi configurabile anche quando il segreto indebitamente rivelato riguarda una sola parte del processo produttivo, senza che sia necessario che detta rivelazione attenga a tutte le componenti del prodotto medesimo. La Corte ha preso poi posizione sul "reverse engineering" - processo che mediante l'esame di un macchinario o di un prototipo di esso lo ricostituisce, così trasformando oggetti reali in modelli informatici - stabilendo che, lungi dal rappresentare una legittima modalità di copia di un prodotto, rappresenta invece un'attività rientrante nel novero dell'impiego di segreti industriali penalmente sanzionato dall'art. 623 c.p.

Il contributo è stato realizzato per la Newsletter Norme & Tributi del mese di febbraio 2024 di AHK Italien.

La Newsletter Norme & Tributi di AHK Italien relativa al mese di febbraio 2024 è disponibile qui.

* * *

Cybersicurezza: novità normative e responsabilità amministrativa degli enti

1. Premessa

Il cybercrime è oggi un fenomeno in crescita, di cui stupiscono la preoccupante precisione e la capacità invasiva, nonché le tecniche sempre più sofisticate e automatizzate, potenzialmente molto dannose per privati, società, enti governativi o multinazionali e per l'intera collettività. La digitalizzazione avanzata, il lavoro a distanza e l'evoluzione tecnologica rendono tali soggetti più esposti a minacce e incidenti informatici, mettendo in pericolo la continuità operativa e la protezione dei dati.

La continua evoluzione delle tecnologie informatiche ha condotto all'incremento di attività criminose, favorite dall'abuso di software (ransomware, cryptolocker, virus, worm e trojan),

e dal numero dei dispositivi connessi a Internet: smartphone, notebook, laptop, etc.

La gamma dei possibili attacchi informatici è molto ampia e varia in base alle tecniche utilizzate per portarli a termine: tra le più comuni, quella di Phishing, finalizzata ad estorcere dati attraverso una richiesta esplicita al legittimo possessore[1] e di **Malware**, ovvero applicativi creati appositamente per penetrare le difese informatiche e danneggiare i device[2].

I rischi informatici, per loro stessa natura, non sono prevedibili né programmabili, in quanto l'evoluzione tecnologica, costante e continua, spesso rende assai complesso individuare tutte le possibili categorie di azioni da prevenire e, di conseguenza, le relative misure di protezione da implementare.

Le problematiche sulla sicurezza informatica emerse a seguito dei numerosi e gravi attacchi subiti di recente da enti pubblici e privati hanno reso sempre più urgente e necessario un intervento da parte delle Istituzioni al fine di favorire il coordinamento della legislazione vigente in materia, di colmare le lacune normative e di garantire una maggiore tutela a fronte dei rischi informatici cui gli enti sono quotidianamente esposti.

Ai singoli e alle società è richiesta particolare attenzione nell'utilizzo dei supporti informatici, e si rende sempre più indispensabile la capacità di riconoscere le relative condotte delittuose, di sviluppare le necessarie competenze e di svolgere una specifica formazione in materia.

È fondamentale, inoltre, l'ausilio di consulenti esperti con specifiche competenze nel settore sia per l'attività di prevenzione sia per gli interventi successivi in caso di attacchi informatici andati a buon fine.

2. Attacchi informatici: un fenomeno in crescita

Secondo il **Rapporto CLUSIT (Associazione italiana per la sicurezza informatica) aggiornato all'ottobre 2023,** confrontando il numero di attacchi informatici alla sicurezza delle informazioni di un'organizzazione rilevati nel primo semestre 2018 in Italia con quelli del primo semestre 2023 la crescita è stata dell'86% (da 745 a 1.382). Nello stesso periodo la media mensile di attacchi gravi è passata da 124 a 230 (quasi 8 al giorno).

Nel complesso, inoltre, si è registrato un significativo incremento (+40%) di attacchi andati a buon fine nel primo semestre 2023 rispetto al 2022.

Quanto al confronto con gli altri Paesi, l'aumento di attacchi rilevati verso enti italiani è percentualmente maggiore rispetto alla crescita osservata a livello globale, che nel primo semestre 2023 è stata pari all'11%.

Il **Global Data Protection Index** realizzato da Dell Technologies in collaborazione con Vanson Bourne, ha evidenziato che **in Italia il 76% delle aziende ha sperimentato nel 2023 almeno un'interruzione dei propri sistemi informatici a seguito di cyberattacchi**, **incidenti che hanno ostacolato l'accesso ai dati o causato perdite di dati.**

Oltre a essere aumentata la frequenza, sono aumentati anche gli impatti: la stima della loro

[1] Il principale metodo per porre in essere il phishing è quello di inviare false email apparentemente provenienti da un istituto bancario o da un ente qualificato, che motivano l'utente a cliccare sul link riportato nella mail e inserire i propri dati

[2] Una delle tipologie di malware più diffuse di recente è il **ransomware**, ossia "software per il riscatto", un particolare tipo di software che, una volta penetrato in una rete, cripta le informazioni contenute al suo interno richiedendo alla vittima di pagare un riscatto per avere nuovamente accesso ai propri dati

"Severity" (indice di gravità) è cresciuta costantemente.

L'indagine evidenzia anche le rilevanti ripercussioni economiche che tali eventi possono avere sulle imprese. In Italia, circa il **60% delle aziende ha dovuto sostenere costi significativi, compresi tra 500.000 e 1 milione di dollari, a causa degli attacchi informatici e degli incidenti correlati subiti**.

3. Quadro normativo europeo

Uno dei primi contributi normativi in materia a livello europeo è costituito dalla **direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. Direttiva NIS – Network and Information Security)** avente la finalità di assicurare un "*livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea*". La direttiva NIS è stata recepita nel nostro ordinamento con il D.lgs. n. 65/2018, cui è seguito il decreto-legge n. 105 del 2019 (convertito e modificato poi in parte dalla Legge 18 novembre 2019, n. 133) che ha formalmente istituito, tra le altre cose, il Perimetro di **Sicurezza Nazionale Cibernetica.**[3]

Nel corso degli anni le istituzioni dell'UE hanno rafforzato ulteriormente la loro cooperazione per contrastare gli attacchi informatici, approvando il 9 aprile 2019 il **Regolamento sulla cybersicurezza, che ha introdotto un insieme di sistemi di certificazione a livello di UE ed ha istituito un'agenzia permanente dell'UE per la cybersicurezza**.

Il Consiglio ha inoltre istituito un quadro che consente all'UE e ai suoi Stati membri di utilizzare tutte le misure PESC, comprese, se necessario, misure restrittive, a fini di prevenzione, dissuasione, deterrenza e risposta nei confronti delle attività informatiche dolose a danno dell'integrità e della sicurezza dell'UE e dei suoi Stati membri.

Per la prima volta nel luglio **2020 l'UE ha imposto misure restrittive nei confronti di sei persone fisiche e tre enti responsabili di aver compiuto attacchi informatici** o di avervi preso parte. Fra questi, il tentato attacco informatico ai danni dell'OPCW (Organizzazione per la proibizione delle armi chimiche) e gli attacchi pubblicamente noti come "WannaCry", "NotPetya" e "Operation Cloud Hopper".

Con la **Direttiva n. 2022/2555 (c.d. Direttiva NIS2)**, il Consiglio ha adottato una nuova normativa per garantire un livello comune elevato di cybersicurezza nell'Unione e migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti del settore pubblico e privato e dell'UE nel suo complesso. La Direttiva NIS2 ha sostituito la precedente direttiva sulla sicurezza delle reti e dei sistemi informativi (Direttiva NIS), ampliando l'ambito di applicazione per le principali attività economiche e sociali del mercato interno. La Direttiva NIS2, infatti, considera come **soggetti meritevoli di attenzione anche gli enti pubblici minori e le piccole e medie imprese** e opera una distinzione ulteriore tra servizi essenziali e servizi importanti. La Direttiva, se da un lato prescrive lo sviluppo di piani di sicurezza informatica individuali, fondati sulle esigenze della specifica organizzazione, dall'altro dispone una valutazione comune, con criteri condivisi e standardizzati, dell'efficacia delle piattaforme adottate, nonché una revisione periodica e l'aggiornamento delle misure di protezione.

[3] I soggetti rientranti nel Perimetro Nazionale sono operatori individuati nei settori dello spazio e aerospazio, energia, telecomunicazioni, trasporti, interno, difesa, economia e finanza, servizi digitali, tecnologie critiche, enti sanitari e previdenziali. Gli stessi, entro sei mesi dalla ricezione della comunicazione che li inserisce nel perimetro devono comunicare le reti, i sistemi informativi ed i servizi informatici (beni ICT) che sono impiegati rispettivamente per l'erogazione delle funzioni e dei servizi essenziali dello Stato inclusi nel perimetro.

L'impatto della Direttiva NIS2 sulle aziende è alquanto significativo, poiché queste sono obbligate non solo ad adottare misure di sicurezza cibernetica più rigorose ma anche a verificare la sicurezza delle supply chain, controllando che i propri fornitori dispongano di adeguati requisiti in materia di protezione dei dati e delle informazioni. Sono particolarmente coinvolti in tal senso i fornitori di servizi digitali nei settori dell'e-commerce, motori di ricerca, cloud computing, e gestione dei servizi ICT.

Lo scorso 7 gennaio è poi entrato in vigore il **Regolamento 2023/2841 del Parlamento europeo e del Consiglio**, che stabilisce nuove misure volte alla definizione da parte di ciascun soggetto dell'Unione di un sistema interno di gestione, di governance e di controllo dei rischi per la cybersicurezza, nonché alla gestione e alla segnalazione dei rischi per la cybersicurezza e alla condivisione delle informazioni.

In particolare, il Regolamento suggerisce **l'adozione di misure tecniche, operative e organizzative proporzionate ai rischi identificati**, nonché l'importanza della **condivisione di informazioni sugli incidenti per facilitare il rilevamento delle minacce**.

Il Regolamento prevede inoltre norme sull'organizzazione, funzionamento e operatività del **CERT-UE (Computer Emergency Response Team dell'UE)**, che si occupa di migliorare la protezione dei sistemi informatici, offrendo supporto nella prevenzione e nella gestione degli incidenti e favorendo la condivisione di informazioni rilevanti sulle minacce informatiche e il coordinamento delle risposte a eventuali emergenze di cybersecurity.

Il Regolamento ha istituito altresì **l'IICB (Interinstitutional Cybersecurity Board)**, composto da rappresentanti di varie istituzioni dell'Unione Europea, allo scopo di promuovere un elevato livello di cybersicurezza comune tra i soggetti dell'Unione, adottando strategie pluriennali e supervisionando l'attuazione del regolamento.

Nell'*iter* comunitario descritto si inserisce anche il piano d'azione dell'UE (noto come "**bussola strategica**") per rafforzare la politica in materia di sicurezza e di difesa – anche digitale – entro il 2030, nell'ambito del quale è possibile ipotizzare che nei prossimi anni saranno adottati ulteriori provvedimenti in materia.

Un ulteriore provvedimento di fondamentale importanza potrebbe essere rappresentato infine dal **Cyber Resilience Act (CRA)**, di cui la Commissione ha presentato una prima proposta il 15 settembre 2022, modificata successivamente lo scorso 20 dicembre 2023.

Il CRA è finalizzato a garantire:

- norme armonizzate per l'immissione sul mercato di prodotti o software dotati di una componente digitale;
- un quadro di requisiti di cybersicurezza che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti;
- l'obbligo di fornire il dovere di diligenza per l'intero ciclo di vita di tali prodotti, tutelando così i consumatori e le imprese che li acquistano o li utilizzano.

4. Il DDL Cybersicurezza e le principali novità

A fronte dell'evoluzione normativa avviata in ambito europeo, il Consiglio dei Ministri, in data 25 gennaio 2024, ha approvato **uno schema di disegno di legge che introduce disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale** (di seguito anche "DDL Cybersicurezza").

Il testo interviene con **significative modifiche sostanziali e processuali della disciplina in materia di reati informatici**, prevedendo l'innalzamento delle pene, l'ampliamento dei confini del dolo specifico, l'inserimento di aggravanti e/o il divieto di attenuanti per diversi reati commessi mediante l'utilizzo di apparecchiature informatiche e finalizzati a produrre indebiti vantaggi a danno altrui per chi li commette o ad accedere abusivamente a sistemi informatici e/o a intercettare/interrompere comunicazioni informatiche e telematiche.

4.1. Reati informatici

Il DDL prevede che la **pena per l'accesso abusivo ai sistemi informatici di cui all'art. 615 ter c.p. venga raddoppiata passando da 1-5 a 2-10 anni di reclusione.**

La stessa cornice edittale è applicata anche a coloro i quali integrino con le proprie condotte la fattispecie prevista dall'art. 615 ter c.p. non solo attraverso l'uso di violenza sulle cose ma anche attraverso la minaccia di uso della stessa.

La medesima pena è prevista anche per coloro i quali, attraverso l'accesso abusivo a sistema informatico o telematico, non solo causino la distruzione o il danneggiamento del sistema ma anche per chi, effettuando l'accesso abusivo, provochi "**la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare**" del sistema informatico o telematico.

Le pene per le condotte punite dal terzo comma dell'art. 615 ter c.p. sono innalzate rispetto all'attuale previsione "da uno a cinque anni e da tre a otto anni" a "da tre a dieci anni e da quattro a dodici anni".

Inoltre, è prevista l'aggiunta di un secondo periodo al terzo comma dell'art. 615 ter c.p. con il quale si stabilisce che per le condotte punite dal summenzionato comma, laddove sussistano anche le circostanze previste dal numero 3 del secondo comma del medesimo articolo, non possono essere riconosciute la quasi totalità delle circostanze attenuanti in misura prevalente o equivalente alle summenzionate aggravanti, salvo che per le circostanze attenuanti previste dagli artt. 89, 98 e 623 quater c.p. (quest'ultimo di nuova introduzione).

Ai fini dell'integrazione del reato di cui **all'art. 615 quater c.p. (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)**, si tiene conto del "vantaggio" e non più del "profitto" ottenuto mediante la commissione del reato: la valutazione dell'antigiuridicità prescinde dunque dal concetto "economico" del profitto e si lega alla categoria più generica del vantaggio.

Viene, inoltre interamente sostituito il secondo comma dell'articolo citato, prevedendo la pena della reclusione da due a sei anni per pubblici ufficiali, incaricati di pubblico servizio, esercenti abusivi della professione di investigatore privato e per coloro i quali abusino della propria qualità di operatore del sistema che, con le proprie condotte, integrino la fattispecie delittuosa prevista dall'art. 615 quater c.p.

Si prevede **l'introduzione di un terzo comma** a tale articolo del codice penale con il quale si specifica che è punito con la pena della reclusione da tre a otto anni chi detiene, diffonde o installa abusivamente apparecchiature, codici e altri mezzi per accedere a sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico (circostanza di cui all'art. 615 ter, comma 3, primo periodo, c.p.).

Il DDL **abroga l'art. 615-*quinquies* c.p**. e prevede l'aggiunta di un nuovo comma all'art. 617-bis c.p. (con il quale si stabilisce la pena della reclusione da due a sei anni per chi viola l'art. 617 bis c.p. e ricopre la posizione di pubblico ufficiale, incaricato di pubblico servizio, esercente abusivo della professione di investigatore privato o operatore del sistema che abusi della propria qualità, circostanza di cui all'art. 615 ter, comma 2, numero 1, c.p.).

Quanto alla fattispecie di cui **all'art. 617 quater c.p., (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)**, il DDL prevede la modifica della cornice edittale prevista dal quarto comma (dalla pena della reclusione da tre a otto anni attuale alla pena della reclusione da quattro a dieci anni) quando il reato è commesso in danno di soggetti specifici indicati dalla normativa. Così come previsto con la modifica dell'art. 615 ter c.p., anche per l'art. 617 quater c.p. è prevista l'introduzione di un ulteriore comma con il quale viene introdotto il divieto di concessione di circostanze attenuanti in misura prevalente o equivalente rispetto alle circostanze aggravanti previste dal quarto comma dell'art. 617 quater.

Anche per i reati di cui all'art. 617 quinquies e 617 sexies è previsto un inasprimento delle pene laddove ricorrano determinate circostanze individuate dalla normativa e, anche in questo caso, viene introdotto il divieto di concessione di circostanze attenuanti prevalenti o equivalenti.

Una delle novità più significative introdotte dal DDL è costituita dall'introduzione dell'art. 623 quater c.p., circostanza attenuante prevista per l'autore dei reati informatici (di cui agli artt. 615 ter, 615 quater, 617 quater, 617 quinquies e 617 sexies) che decida di collaborare con la giustizia, evitando che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando la polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi reati. In tali casi, la norma prevede uno sconto di pena dalla metà a due terzi.

Altra importante novità rappresenta l'introduzione della fattispecie di estorsione mediante reato informatico all'art. 629 co. 3 c.p.: colui il quale commette estorsione mediante la commissione o minaccia di commissione dei reati puniti dagli artt. 615 ter, 617 quater, 617 sexies, 635 bis, 635 quater e 635 quinquies c.p. è punito con la reclusione da sei a dodici anni e, qualora sussistano alcune delle circostanze indicate nell'ultimo capoverso dell'art. 628 c.p., la pena prevista è quella della reclusione da otto a ventidue anni.

Il disegno di legge, infine, prevede **un aumento delle pene anche per tutte le varie fattispecie di danneggiamento informatico o telematico** previste dagli artt. 635 bis c.p. e seguenti. Inoltre, anche in questo caso, prevede l'introduzione di un nuovo articolo (l'art. 635 sexies c.p.) con il quale viene inserita la circostanza attenuante, applicabile all'estorsione mediante commissione o minaccia di crimine informatico e alle varie ipotesi di danneggiamento informatico o telematico, che prevede una riduzione di pena dalla metà a due terzi per chi decida di collaborare con le Autorità.

4.2. Agenzia per la cybersicurezza nazionale e obblighi per i soggetti pubblici

Il testo prevede il **rafforzamento delle funzioni dell'Agenzia per la cybersicurezza nazionale (ACN)** e il suo coordinamento con l'Autorità giudiziaria in caso di attacchi informatici, mediante specifiche procedure volte a rendere più immediato l'intervento e il ripristino delle funzionalità dei sistemi informatici.

Il DDL Cybersicurezza stabilisce inoltre, a carico dei soggetti pubblici (incluse le rispettive società in house) individuati dalla normativa, **l'obbligo di dotarsi di sistemi di cybersicurezza, anche individuando un Referente interno per la cybersecurity**, **nonché un obbligo di segnalazione e notifica degli incidenti indicati in apposito provvedimento ACN**, aventi un impatto su reti, sistemi informativi e servizi informatici, disciplinando la relativa procedura. L'inosservanza dell'obbligo di notifica può comportare possibili ispezioni da parte dell'Agenzia, nei 12 mesi successivi all'accertamento del ritardo o dell'omissione, anche al fine di verificare l'attuazione di interventi di rafforzamento della resilienza. Nei casi di reiterata inosservanza dell'obbligo di notifica, si prevede l'applicazione all'ente, da parte dell'Agenzia, di una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000. Inoltre, per i dipendenti delle pubbliche amministrazioni, la violazione delle disposizioni può costituire causa di responsabilità disciplinare e amministrativo-contabile.

Per gli stessi soggetti, in presenza di segnalazioni dell'Agenzia circa specifiche vulnerabilità cui risultano potenzialmente esposti, è previsto l'obbligo di provvedere senza ritardo, e comunque non oltre quindici giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia e, per la mancata o ritardata adozione di tali interventi risolutivi, l'applicazione delle medesime sanzioni.

Il DDL prevede inoltre che, in relazione a specifiche questioni, potrà essere convocato il Nucleo per la cybersicurezza, in composizione di volta in volta estesa alla partecipazione di un rappresentante della Procura nazionale antimafia e antiterrorismo, della Banca d'Italia o di altri soggetti interessati alle medesime questioni.

4.3. Disciplina dei contratti pubblici di beni e servizi informatici

Infine, il disegno di legge modifica le disposizioni relative ai contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, prevedendo che, nell'ambito della fornitura/approvvigionamento di tali infrastrutture informatiche, debbano essere individuati «gli elementi essenziali di cybersicurezza», in assenza dei quali l'ente potrà liberamente revocare l'affidamento.

Tale previsione assume particolare rilevanza in quanto estende di fatto l'ambito di applicazione della normativa anche a tutti i soggetti privati, che siano fornitori di beni e servizi informatici della Pubblica Amministrazione e che, dunque, devono impegnarsi a soddisfare i requisiti di cybersicurezza menzionati.

4.4. Lacune normative

Il DDL Cybersicurezza rappresenta senza dubbio un contributo significativo nella lotta contro il cybercrime in Italia.

Tuttavia, il testo approvato dal Consiglio dei Ministri nulla prevede in merito alla prevenzione degli attacchi informatici, ossia a tutte le possibili misure da porre in essere al fine di evitare il verificarsi di eventi così dannosi, concentrandosi invece principalmente sulle sanzioni e su un intervento successivo dell'ordinamento.

Nonostante le lacune normative, risulta essenziale dotarsi dei necessari meccanismi di prevenzione del cybercrime, non solo mediante l'adozione di tecnologie di sicurezza informatica avanzate, ma anche tramite sistemi di governance efficaci, l'adozione di policy e procedure interne specificamente volte a minimizzare i rischi informatici, nonché l'attività di formazione e

l'aggiornamento costante delle competenze del personale.

Inoltre, nessun accenno nel DDL in materia di Intelligenza Artificiale. Invero, il rapido sviluppo delle applicazioni di IA negli ultimi anni, il cui impiego si sta diffondendo in numerosi settori d'attività, comporta rilevanti implicazioni giuridiche legate al funzionamento e all'utilizzo di tali strumenti.

Il verificarsi di fatti criminosi riferibili all'utilizzo o al funzionamento di sistemi di IA potrebbe interessare diversi settori del diritto penale (sia in relazione a nuove modalità di realizzazione di reati già tipizzati, sia in relazione alla necessità di incriminare nuovi fatti).

Ad esempio, l'utilizzo delle tecnologie di IA per lo sviluppo di nuovi malware o strumenti di social engineering potrebbe condurre a sempre più pericolosi attacchi o frodi informatiche; potrebbero inoltre essere configurati nuovi reati in relazione alla programmazione di sistemi di IA utilizzati per la realizzazione di attacchi informatici o aventi carattere illecito (ad es. utilizzati a fini estorsivi).

Europol ha pubblicato, in data 27 marzo 2023, un primo rapporto dedicato al potenziale uso di ChatGPT e modelli analoghi per finalità criminali. In tale rapporto si rileva proprio come simili applicativi possano sensibilmente agevolare la commissione di reati, essenzialmente incrementando le potenzialità e le competenze dei singoli (cyber)criminali.

Ad esempio, la particolare abilità imitativa e la capacità di elaborare il linguaggio naturale rendono tali strumenti un ausilio essenziale per la perpetrazione di "frodi" e social engineering, potendo elaborare testi «altamente realistici» capaci di riprodurre lo stile comunicativo di determinati individui o organizzazioni, e perciò dotate di una potenzialità decettiva sicuramente superiore, utilizzabili ad esempio per campagne di phishing estremamente accurate. La medesima capacità generativo-elaborativa, può agevolare i cybercriminali anche nella perpetrazione di crimini informatici in senso stretto, potendo l'IA – su richiesta degli utenti – elaborare stringhe di codice in diversi linguaggi di programmazione e, dunque, fornire a utilizzatori dotati di scarse conoscenze e competenze tecniche mezzi e istruzioni per realizzare cyber-attacchi.

5. Nuovi profili di responsabilità degli enti e prevenzione dei reati informatici

Con la L. 48/2008, che ha ratificato la Convenzione di Budapest del Consiglio d'Europa sul cyber crime, i reati informatici sono stati inseriti nel novero dei reati presupposto del D.Lgs. 231/01, per cui anche l'Ente, oltre che la persona fisica, può esser ritenuto responsabile.

Il DDL Cybersicurezza introduce modifiche rilevanti anche nell'ambito della responsabilità amministrativa dipendente da reato, in particolare all'art. 24 bis del D.lgs. 231/2001, rubricato "Delitti informatici e trattamento illecito di dati", in quanto amplia il novero dei reati-presupposto, includendo anche il nuovo art. 629 co. 3 del codice penale, e ne inasprisce le sanzioni ripartite per quote.

Al fine di prevenire al meglio la commissione dei reati informatici, è opportuno che le Società adottino un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/01 o, qualora lo abbiano già adottato, che lo implementino e lo aggiornino valutando i possibili rischi e i relativi presidi di controllo con riguardo alle novità normative esaminate.

Infatti, la mera adozione di eventuali procedure, misure di sicurezza o sistemi di gestione che non

siano inseriti all'interno di un Modello di Organizzazione, Gestione e Controllo, non vale ad escludere la responsabilità da reato dell'ente.

Occorre dunque effettuare un'analisi dei rischi di reato astrattamente configurabili nell'ambito della realtà aziendale di riferimento, individuare quali sono le attività sensibili, ossia le attività nel cui svolgimento può essere commesso uno dei reati presupposto identificati come astrattamente realizzabili, e integrare, di conseguenza, efficaci presidi di controllo e protocolli di prevenzione.

Un ulteriore strumento di prevenzione è fornito dagli **standard ISO 27001 – Sistemi di gestione per la sicurezza delle informazioni e ISO 27002** – Linee guida per l'implementazione di sistemi di gestione per la sicurezza delle informazioni.

Possibili ambiti di implementazione possono riguardare:

- la definizione di ruoli e responsabilità in materia di sicurezza delle informazioni;
- la definizione di processi interni di sicurezza delle informazioni e di protocolli specifici per la prevenzione dei reati (ad es. per la gestione degli asset, il controllo degli accessi, la sicurezza fisica e ambientale, i controlli operativi, etc.);
- il controllo dei fornitori esterni che possono avere impatti in relazione alla sicurezza delle informazioni;
- la formazione e sensibilizzazione del personale in materia di sicurezza delle informazioni;
- la previsione di misure di protezione delle informazioni anche al termine del rapporto di lavoro o alla scadenza del contratto di fornitura.

* * *

Per maggiori informazioni e approfondimenti, potete contattare

Avv. Francesco Rubino

Partner e Responsabile Osservatorio Compliance 231
(Francesco.Rubino@MorriRossetti.it)

LinkedIn

Morri Rossetti **Osservatorio 231**

OSSERVATORIO
COMPLIANCE 231
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-231.it