Reati informatici e rafforzamento della cybersecurity: gli impatti sul DPO ed ODV

di Tiziana Bastianelli e Silvia Giampaolo, Cugia Cuomo & Associati

Il Ddl recentemente varato dal Consiglio dei Ministri in materia di **reati informatici** e rafforzamento della **cybersicurezza** nazionale interviene su un tema di grande attualità, e lo fa sia attraverso un inasprimento delle pene sia attraverso un rafforzamento delle azioni di contrasto con l'obiettivo di adeguare la posizione italiana all'attuale contesto geo-politico, che vede come noto un crescendo di attacchi informatici nonostante le misure introdotte a livello europeo con la Direttiva (UE) 2016/1148 del 6 luglio 2016, c.d. **Direttiva NIS** – "Network and Information Security", (ora abrogata dagli articoli 44, par. 1, e 45, par.1 dalla Direttiva 14 dicembre 2022, n. 2022/2555/UE, c.d. **Direttiva NIS 2**, con effetto a decorrere dal 18 ottobre 2024).

Il Ddl intende innanzitutto preparare il tessuto normativo propedeutico al recepimento della Direttiva NIS2, finalizzata a rafforzare a livello collettivo la cybersecurity degli Stati membri UE tenuto conto che nell'ambito di applicazione della NI2 rientrano altresì gli **enti della pubblica amministrazione** (ex art. 2).

La Direttiva Nis 2 stabilisce *inter alia* misure volte a garantire un livello comune elevato di cybersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno, definendo gli: a)obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cybersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT); b)misure in materia di gestione dei rischi di cybersicurezza e obblighi di segnalazione per i soggetti di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557; c)norme e obblighi in materia di condivisione delle informazioni sulla cybersicurezza; d)obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

Sul piano sanzionatorio il Ddl cyber security prevede *in primis* pene raddoppiate, che passano da 1-5 a 2-10 anni di reclusione per l'accesso abusivo ai sistemi informatici (articolo 615-*ter* del codice penale), e fino ad un massimo di 2 anni di reclusione e sanzioni pecuniarie da 10.329 euro per chi detiene o fornisce programmi per il danneggiamento di sistemi informatici.

Il provvedimento è diretto ad innalzare il complessivo livello di sicurezza del Paese da eventuali cyber attacchi salvaguardando in particolare **sia le piccole medie imprese, sia il settore finanziario**, **la Pubblica Amministrazione e il sistema sanitario,** target quest'ultimo di diversi incidenti di data breach che hanno reso non più procrastinabile un intervento a tutto tondo. Ad es. solo pochi mesi fa (il 23.10.2023, per l'esattezza) il Garante Privacy è intervenuto per sanzionare la "Asl Napoli 3 Sud" per non aver protetto adeguatamente da attacchi hacker i dati personali e i dati sanitari di 842.000 tra assistiti e dipendenti.

Nel merito, il Ddl prevede un nuovo coordinamento operativo in caso di attacchi informatici da un lato tra ACN (Agenzia per la Cybersicurezza nazionale) e Magistratura, nonché tra l'ACN e i servizi di informazione per la sicurezza (DIS).

Inoltre il Ddl amplia la sfera di soggetti pubblici/erogatori di servizi di pubblica utilità tenuti a dotarsi obbligatoriamente di sistemi di cybersicurezza (**tra i quali i comuni sopra i 100.000 abitanti, le Asl, i capoluoghi di Regione e le società di trasporto con utenza non inferiore a 100.000 abitanti).**

L'art. 8 comma 1 del Ddl in esame dispone anche che tra i soggetti aventi obblighi di notifica di incidenti sono incluse le **società in house** degli enti sopra indicati, per ciò intendendosi le società "*sulle quali un'amministrazione esercita il controllo analogo o più amministrazioni esercitano il controllo analogo congiunto, nelle quali la partecipazione di capitali privati avviene nelle forme di cui all'articolo 16, comma 1, e che soddisfano il requisito dell'attività prevalente di cui all'articolo 16, comma 3*" (art. 2, comma 1, lett. "o" del TUSP). Secondo la giurisprudenza nazionale , in presenza di specifici requisiti, la società in house providing agisce come un vero e proprio organo dell'amministrazione in ragione del controllo analogo a quello esercitato sui propri servizi dall'amministrazione aggiudicatrice e della destinazione prevalente dell'attività dell'ente in house in favore dell'amministrazione stessa (C.d.S. n. 4603 del 23 settembre 2008, Corte d'Appello Lecce, Sez. Unica, Sent., 11/08/2023, n. 1185).

Il provvedimento introduce altresi' l'obbligo di notifica entro 24 ore all'ACN, per i soggetti sopra individuati, in caso di attacco cyber subìto ed avente impatto su reti, sistemi informativi e servizi informatici , in modo da garantire un sistema adeguato di reazione. Nel caso in cui l'obbligo della notifica non venga rispettato la procedura prevede inizialmente un richiamo seguito da un'eventuale sanzione comminata dalla stessa ACN che può variare da venticinquemila a centoventicinquemila euro. Per i dipendenti delle PA in caso di sanzione può anche individuarsi una causa di responsabilità disciplinare o amministrativo-contabile;

Il Ddl introduce anche la figura del **Referente per la cybersicurezza** per le PA interessate. La figura deve essere individuata in ragione delle qualità professionali possedute e deve svolgere anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalle disposizioni di legge e regolamentari applicabili in materia di cybersicurezza cui è soggetta la medesima amministrazione. A tal fine, il nominativo del Referente per la cybersicurezza deve essere poi comunicato all'Agenzia per la cybersicurezza nazionale.

Detto Referente Cybersecurity e' chiamato a curare le attività di coordinamento tra l'Autorita' preposta ed i soggetti pubblici sopra indicati che devono (laddove non sia già presente) dotarsi di una struttura, anche tra quelle esistenti, che provvede: a) allo sviluppo delle politiche e procedure di sicurezza delle informazioni; b) alla produzione e all'aggiornamento di un piano per la gestione del rischio informatico; c) alla produzione e all'aggiornamento di un documento che definisca ruoli e organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione; e) alla pianificazione e all'implementazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d); f) alla pianificazione e all'implementazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

E' senz'altro ipotizzabile che il Referente cybersecurity rappresenti la figura incaricata di operare la notifica degli incidenti di sicurezza informatica aventi un impatto rilevante "*sulla continuità dei servizi essenziali prestati*" (art. 14) gia' previsti per gli operatori, pubblici o privati, di servizi essenziali (OSE) operanti (ad esempio) nel settore sanitario, del trasporto, dell'energia, delle infrastrutture digitali, dell'acqua potabile o di altri

servizi essenziali specificatamente individuati dalle autorità nazionali competenti NIS, in conformità del Decreto legislativo 18 maggio 2018 n. 65. Al Referente possono essere demandati gli obblighi di notifica degli incidenti informatici da parte di quei soggetti da cui dipenda la prestazione di un servizio essenziale per gli interessi dello Stato, cosi' come definiti dal Decreto legge 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*" come poi attuato dal DPCM 14 aprile 2021, n. 81.

L'analisi del nuovo Ddl offre lo spunto ad alcune riflessioni. Colpisce innanzitutto che per le misure di rafforzamento della cybersicurezza delle PA (e del Paese in generale) non sia previsto un nuovo capitolo di spesa o nuovo finanziamento: le amministrazioni pubbliche interessate, chiamate a provvedere (si legge nel Ddl) "[…] *all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente*", mentre come noto molti dei progetti cybersecurity interagiscono in programmi già finanziati in ambito PNRR ed appaiono in ogni caso dotati di particolare complessità sia tecnica sia organizzativa, tanto da presupporre necessariamente delle dotazioni finanziarie. Il tema non appare di poco conto perché interagisce evidentemente con le responsabilità gestionali di figure apicali pubbliche, soggette a rischi gestionali erariali.

Dall'altro, il Ddl ripropone ed amplia l'interessante tema della c.d. "compliance integrata" per la tutela dei dati, o meglio del raccordo e legame esistente tra le disposizioni dettate in materia di cybersecurity e la disciplina della tutela dei dati personali, con particolare riferimento al *Regolamento Europeo 679/2016 (GDPR)*, e l'impianto normativo di cui al Decreto Legislativo 8 giugno 2001, n. 231, "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (cd. "Decreto 231"). Ciò tenuto conto che il Ddl propone lo svolgimento di una attività di analisi e valutazione di tutte le aree di rischio per elaborare misure di protezione, policy aziendali e modelli organizzativi e di gestione all'uopo necessari per prevenire in modo sostanziale il verificarsi di eventi criminosi che possono impattare sui dati personali, e quindi sui diritti e le libertà delle persone fisiche interessate.

Sul punto, gia' la Direttiva NIS ha precisato, al considerando 63, che "*in molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti*". La Direttiva NIS2, dal canto suo, rimarca al considerato 108, che "*in molti casi gli incidenti compromettono i dati personali. In tale contesto, le autorità competenti dovrebbero cooperare e scambiarsi informazioni su tutte le questioni pertinenti con le autorità di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE*".

La novella quindi riprende ed amplia il tema della cybersecurity e della privacy anche nel contesto normativo della responsabilità amministrativa degli Enti dipendente da reato, impattando fortemente sull'art. 24-bis del D. Lgs. 231/2001 rubricato "*Delitti informatici e trattamento illecito di dati*".

In un perimetro legislativo in cui il modello GDPR 679/2016 e il modello 231/2001 presentano diversi punti di contatto con riferimento ai doveri di osservanza degli obblighi normativi, occorre segnalare che già oggi l'art. 24 bis del D. Lgs 231/2001 si pone in collegamento con l'articolo 1, comma 11- bis, del decreto-legge 21 settembre 2019, n. 105 recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*", sopra citato.

La fattispecie dei reati informatici di cui all'articolo 24 – bis del Decreto 231 punisce infatti due condotte (una di tipo commissivo ed una di tipo omissivo) accomunate dalla finalità di ostacolare o condizionare i procedimenti ovvero le attività di ispezione e vigilanza di cui al DL n. 105/2019. Il rafforzamento delle misure preventive e di contrasto, nonché l'inasprimento delle pene registrate dall'art. 5 del nuovo Ddl, rendono necessaria una ancora più accurata analisi del rischio ai sensi del D.Lgs 231/2001 con l'individuazione degli interventi da porre in essere e l'adozione di misure tecniche e organizzative puntuali, efficienti e rigorose, volte a contrastare la proliferazione di reati informatici commessi ai danni dell'azienda e/o all'interno della stessa.

Nel quadro, quindi, della definizione di un Modello di organizzazione, gestione e controllo adottato con efficacia preventiva, diventa indispensabile prevedere efficienti e costanti flussi informativi tra il Referente Cybersecurity, ove previsto, che e' il soggetto responsabile del coordinamento di una struttura che si occupa *inter alia* dello sviluppo delle politiche e procedure di sicurezza delle informazioni e della produzione e all'aggiornamento di un piano per la gestione del rischio informatico; l'Organismo di Vigilanza (OdV), che costituisce come noto l'organo che ha il compito di vigilare sulle misure dirette ad evitare il compimento dei reati di cui al Decreto 231, ivi compresi quelli informatici, che possono essere commessi da soggetti apicali, o a questi subordinati, interni all'organizzazione nell'interesse o a vantaggio dell'Ente, e il Data Protection Officier (DPO), che un soggetto super partes, che ricopre un ruolo di controllo interno sulla correttezza delle procedure di gestione dei dati personali, previsto dal GDPR, che svolge altresì una funzione proattiva nei confronti del titolare e del responsabile del trattamento, oltre che dei dipendenti dell'organizzazione, per favorire lo sviluppo di buone pratiche in materia di privacy.

Su quest'ultimo aspetto, rileva sottolineare che dal momento che l'insieme delle fattispecie dei reati informatici indicati nell'art. 24 bis del D.lgs. 231/2001 sono per lo più descrittive sia di illeciti penali che di violazioni di dati personali (data breach), emergono i possibili accostamenti tra l'ODV e la figura del DPO prevista dal GDPR che svolge anche funzioni di advisor e di auditor al fine di evitare violazioni di dati, promuovendo il rispetto delle normative privacy - sia nazionali che europee - nella gestione del trattamento dei dati personali all'interno di un'azienda, con lo scopo di tutelare il titolare di tali dati.

I compiti del DPO e dell'ODV coincidono quando si tratta di prevenire reati informatici che possono simultaneamente, **anche se non necessariamente**, configurarsi come *data breach*, pur non dimenticando che. mentre l'OdV è impegnato a eseguire attività di vigilanza per prevenire la commissione dei delitti informatici (e degli altri reati inclusi nel perimetro del D.lgs. 231/2001) da parte dei soggetti apicali dell'Ente o di soggetti a questi subordinati e nell'interesse o a vantaggio dell'Ente (nella cui nozione si ricomprendono come visto anche le società in house o societa' di servizi pubblici, come identificate dal Ddl cybersecurity); il DPO assiste il proprio titolare dell'organizzazione nel valutare tutte le fonti di rischio che possono essere originate da soggetti malintenzionati e non (che agiscono in maniera volontaria o meno), infrastrutture tecnologiche o eventi naturali.

Pur precisando, per quanto detto, che non sempre e non necessariamente un reato informatico si configura come *data breach*, dal nuovo quadro regolamentare discende un rafforzamento degli ambiti in cui le sfere di competenza di ODV e DPO finiranno col sovrapporsi ed interagire insieme al Referente Cybersecurity, innanzitutto nell'attività di adeguata progettazione dei flussi informativi e dei sistemi di controlli interni ora rafforzati per scongiurare anche la sola insorgenza di eventi lesivi per gli Enti.

Da un punto di vista tecnico/pratico, l'adozione delle misure mitigatorie dei rischi e delle linee guida contemplate nella ISO/IEC 27001:2022 "*Information security, cybersecurity and privacy protection – Information security management systems – Requirements*", ormai alla terza edizione, può senz'altro costituire una valida base di partenza per il percorso comune su cui ODV e DPO saranno ancor più chiamati ad integrarsi, alla quale dovrà affiancarsi l'adozione di protocolli comportamentali e misure di contrasto ad *hoc*, a seguito di processi di analisi e di mappature condivise dei rischi che consentano la puntuale individuazione delle debolezze/falle/vulnerabilità dei processi aziendali, tali da risultare pericolosamente permeabili al perpetrarsi di reati informatici con violazione di dati personali.