Luglio 2018

GDPR, Cyber security e reati informatici nelle istanze di riforma del D.Lgs. 231/2001

Maurizio Fedele, giurista d'impresa presso il Credito Fondiario SpA di Roma

Sommario[*]: 1. Whisteblowing. Sistemi di segnalazione di illeciti – 2. Ruolo dell'Organismo di Vigilanza - 3. Sistemi Whistleblowing e GDPR – Direttiva (UE) 2016/679 - 4. Cyber security integrata: GDPR, reati informatici e Direttiva NIS

Sulla consolidata esperienza dei MOG – Modelli di Organizzazione e Gestione della responsabilità parapenale delle imprese previsti dal D.Lgs. 2131/2001 è in corso un importante dibattito di organizzazioni imprenditoriali e ordini professionali (Confindustria, ABI, CNCDEC, Ordine Forense, ASSONIME). Partendo dalle incombenze immediate di adeguamento alle collegate normative in materia di whisleblowing, GDPR e Cyber Security (Direttiva NIS) – è possibile avviare una più ambiziosa istanza di riforma organica del dettato normativo che, ponendo rimedio alla sedimentazione e superfetazione normativa, consenta una efficiente e sostenibile mitigazione dei rischi derivanti dal D.Lgs. 231/2001 fondata su un principio di *"prevenzione mediante organizzazione" più comprehensive possibile, capace di inglobare sinergicamente tutte le più rilevanti funzioni aziendali in un opportuno contesto di Enterprise Risk Management* ".

1. Whistleblowing. Sistemi di segnalazione di illeciti

L'istituto del c.d. "whistleblowing", anche prima della Legge 179/2017, non era sconosciuto alle società dotate di MOG ex D.Lgs. 231/2001. È quanto si ricava da una lettura attenta dell'art. 6, comma 2, del Decreto 231, secondo il quale l'ente non risponde se, tra le altre cose, sono stati previsti "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*".

Ai nostri fini, occorre delineare un quadro generale delle normative che prescrivono incombenti di segnalazione di illeciti, accostandole, laddove possibile, ai rischi di

[*] Nel presente contributo, ampi richiami alla tesi di F. Ribera, Privacy: il nuovo Regolamento Europeo e le convergenze con il modello organizzativo ex d.lgs. 231/2001, discussa per il Master Universitario di Secondo Livello in Diritto d'Impresa dell'Università Luiss Guido Carli, AA 2016-2017, inedita

incorrere nella fattispecie di reati rilevanti per il Decreto 231 – qui di seguito indicati tra parentesi [ ] :

- in attuazione all'art. 52-bis del Testo Unico Bancario (TUB), Banca d'Italia con l'11.mo aggiornamento della sua Circolare n. 285/2013 sulle Disposizioni di Vigilanza per le banche, ha prescritto "*sistemi interni di segnalazione delle violazioni ... di atti o fatti che possano costituire una* ***violazione di norme disciplinanti l'attività bancaria*****"** già adottati dalle aziende del sistema bancario con procedure approvate dagli organi di supervisione strategica [*Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza* – art. 25-ter – art. 2638, comma 1 e 2 c.c.];

- inoltre, Banca d'Italia ha pubblicato moduli per le segnalazioni di **violazioni normative e irregolarità di natura gestionale** di dipendenti e collaboratori degli intermediari vigilati o da altri non dipendenti o collaboratori "*utili per le sue funzioni di vigilanza e attiva*" [come sopra];

- con il D.Lgs. 90/2017 il Legislatore ha recepito la Direttiva 2015/849/UE (IV Direttiva Antiriciclaggio) che, tra le altre cose, modifica l'art. 48 del D.Lgs.231/2007 prevedendo che i destinatari della disciplina sono tenuti a istituire "*procedure per la segnalazione al proprio interno […] di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo*" [*Riciclaggio, autoriciclaggio* – art. 25-octies; *Reati con finalità di terrorismo o eversione dell'ordine democratico* – art. 25-quater] ;

- la legislazione in materia di sicurezza sul lavoro (v. art. 20 D.Lgs. 81/2008) pone una serie di obblighi a carico dei lavoratori, tra cui l'obbligo di segnalare immediatamente al datore di lavoro attraverso il Responsabile dei Lavoratori per la Sicurezza le anomalie presenti in attrezzature, sostanze, materiali e dispositivi, anche ove non siano fonte di pericolo incombente per i lavoratori [Reati di omicidio colposo o lesioni colpose commessi in violazione di norme antinfortunistiche, tutela igiene e salute sul lavoro – art. 25-septies];

- in recepimento delle Direttive MiFUD II e MiFIR, l'art. 4-undecies del TUF prevede che gli intermediari finanziari e assicurativi "*adottano procedure per la segnalazione … di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta, nonché del regolamento (UE) 596/2014*" ("Regolamento MAR") [Reati abuso di mercato, c.d. insider trading -- art. 25-sexies];

- da ultimo, l'art. 2 della Legge 179/2017 ha aggiunto tre nuovi commi all'art. 6 del D.Lgs. 231/2001 per cui tutte le società dotate di MOG 231 lo debbono implementare con un sistema di segnalazione "*a tutela dell'integrità dell'ente … di condotte illecite, rilevanti ai sensi del presente decreto*…" [tutte le fattispecie di reato rilevanti per il D.Lgs. 231/2001**]**.

In effetti, con specifico riferimento al sistema bancario, sono attesi interventi chiarificatori del Legislatore e delle Autorità di vigilanza, in particolare sui seguenti punti:

"- come garantire la riservatezza del segnalante nel «canale alternativo» (quali modalità informatiche sono necessarie?);

- se uno o entrambi i canali debbano direttamente pervenire all'OdV (l'art. 6 comma 2 lett. d) è chiaro invece nello stabilire che gli obblighi di informazione sinora vigenti sono previsti «nei confronti dell'OdV»);

- se possano essere utilizzati per le segnalazioni da parte di soggetti esterni all'organizzazione dell'ente (fornitori, partner, consulenti, ecc.);

- se si debba trattare di canali separati da quelli utilizzati per la segnalazione di illeciti rilevanti ai fini di altre normative;

- come siano gestibili le inevitabili interconnessioni tra ii diversi canali (es. con le segnalazioni ai sensi dell'art. 48 del D. Lgs. n. 231/2007 per le quali è prescritto uno "specifico canale di segnalazione, anonimo e indipendente")".[1]

2. Ruolo dell'Organismo di Vigilanza

Secondo autorevoli orientamenti espressi in un Tavolo di lavoro tra le organizzazoni di settore e gli ordini professionali "*ancorché il nuovo comma 2-bis, invece, non menzioni esplicitamente il destinatario delle segnalazioni, è lecito ipotizzare che possa essere coinvolto l'OdV ... potrebbe ritenersi che il nuovo requisito previsto dalla norma sia rispettato anche nel caso in cui i sistemi di whistleblowing già esistenti all'interno dell'organizzazione siano strutturati in maniera libera, purché si garantisca che la segnalazione giunga all'Organismo di Vigilanza. In altri ordinamenti le segnalazioni possono essere gestite addirittura da soggetti terzi esterni all'organizzazione, specializzati nella fornitura di questo particolare servizio...*".

Sul punto, converge anche Confindustria, secondo la sua nota "*La disciplina del whistleblowing*"[2], l'O.d.V. non è individuato come destinatario esclusivo, ma appare indispensabile che sia sempre destinatario autonomo e indipendente delle segnalazioni. Soluzione in grado di realizzare con efficacia le finalità della nuova disciplina, di salvaguardare l'integrità dell'ente e tutelare il segnalante, difficilmente ottenibili se, invece, le segnalazioni venissero recapitate a soggetti nei cui confronti il segnalante abbia una posizione di dipendenza funzionale o gerarchica ovvero ovvero a soggetti che abbiano un potenziale interesse correlato alla segnalazione.

[1] Intervento di F. Palisi - Ufficio Ordinamento Finanziario, *I sistemi interni di segnalazione in ambito bancario* al seminario "Luci e ombre del whistleblowing" tenuto dall'ABI il 12.3.2018

[2] Nota illustrativa "*La disciplina del whistleblowing*" di Confindustria, Gen. 2018, in http://www.lavorosi.it/fileadmin/user_upload/PRASSI_2018/Confindustria-disciplina-del-whistleblowing.pdf

È dunque necessario prevedere un coinvolgimento costante, contestuale e concorrente dell'O.d.V. fin dal primo ricevimento della segnalazione per scongiurare il rischio che il flusso di informazioni generato dai sistemi di whistleblowing sfugga al controllo dell'Organismo di Vigilanza. Infatti, è importante considerare che tutte le diverse forme di segnalazione degli illeciti già viste sub. par. 1:

- hanno una sistematica e oggettiva attinenza a rischi di incorrere nella responsabilità para-penale del Decreto 231;

- sono inoltre parte integrante dei flussi di informazione che debbono pervenire all' Organismo di Vigilanza e del più ampio MOG di cui l'Organismo è tenuto a verificare il funzionamento.

3. Sistemi Whistleblowing e GDPR – Direttiva (UE) 2016/679

Tra gli interventi da integrare nelle procedure aziendali del WB, come si vedrà al successivo par. 4, vi è anche la conformità alla disciplina del Regolamento (UE) 2016/679, nelle forme in cui sarà regolato dal prossimo decreto legislativo di adeguamento della normativa nazionale al GDPR[3]

Per questa materia, risulta di notevole importanza il profilo della **differenza fra anonimato e riservatezza** dell'identità del segnalante. Confindustria, nella nota illustrativa precitata, precisa che "*il profilo della riservatezza dell'identità del segnalante è diverso da quello dell'anonimato*". Sul punto, anche l'Autorità Nazionale Anticorruzione (ANAC) chiarisce che la rivelazione dell'identità del denunciante (si ritiene, protetta e riservata) è indispensabile proprio per assicurare una sua tutela adeguata[4].

Le oscillazioni circa il corretto inquadramento della normativa a tutela del segnalante, anche nel settore privato, potrebbero essere state risolte a livello europeo. Infatti, per garantire l'identità del segnalante e tutelare lo stesso da forme di ritorsione, lo scorso 23 aprile, la Commissione Europea ha adottato una proposta di direttiva, attualmente al vaglio del Parlamento e del Consiglio UE, per la protezione di coloro che denunciano violazioni del diritto UE[5]

[3] V. Iter parlamentare Atto Governo N. 22, Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, in http://www.camera.it/leg18/682?atto=022&tipoAtto=Atto&idLegislatura=18&tab=1#inizio

[4] Determinazione ANAC n. 6 del 28 aprile 2015 – "Linee Guida in materia di tutela del dipendente pubblico che segnala illeciti"

[5] Sulla nuova direttiva europea, nel sito Commissione europea, vedasi *Protezione degli informatori: la Commissione stabilisce nuove norme a livello dell'UE,* 23.4.2018 - https://ec.europa.eu/italy/news/20180423_protezione_informatori_nuove_norme_it

L'art. 1 della proposta contiene l'elenco delle materie di diritto dell'Unione a cui lo standard minino comune di tutela dei whistleblowers dovrà applicarsi. A titolo esemplificativo rientrano: appalti pubblici, servizi finanziari, riciclaggio di denaro e finanziamento del terrorismo, sicurezza dei prodotti, sicurezza dei trasporti, tutela ambientale, sicurezza nucleare, sicurezza degli alimenti e dei mangimi e salute e benessere degli animali, salute pubblica, protezione dei consumatori. L'art. 4 introduce l'obbligo di predisporre un meccanismo di segnalazione degli illeciti e di follow-up delle denunce sia nel privato, per tutte le imprese con più di 50 dipendenti o con un fatturato annuo superiore ai 10 milioni di euro**.**

4. Cyber security integrata: GDPR, reati informatici e Direttiva NIS.

Esiste una vasta letteratura sui problemi di sicurezza che storicamente caratterizzano lo scenario dell'ICT - Information and Communications Technology. Da alcuni anni la casistica delle intrusioni e degli attacchi informatici ha assunto dimensione planetaria e complessità crescente in relazione alla diffusione e agli sviluppi tecnologici dell'ICT, in particolare dei data base, della trasmissione dati, dell'elaborazione a distanza (cloud e informatica distribuita) e dei social network (da ultimo, caso Facebook –Cambridge Analytica). Tra le normative di contrasto a queste patologie della comunicazione c'è il GDPR, nel Regolamento (UE) 2016/679. L'articolo 4 – Definizioni recita testualmente:

Ai fini del presente regolamento s'intende per:

*(…) 12) «**violazione dei dati personali**» [c.d. data breach]: la violazione di sicurezza che comporta accidentalmente o in **modo illecito** la **distruzione**, la **perdita**, la **modifica**, la **divulgazione non autorizzata** o l'**accesso** ai dati personali trasmessi, conservati o comunque trattati*;

Il termine "*data breach*" si traduce nella normativa nazionale come **trattamento illecito dei dati** che, secondo le linee guida del Gruppo di lavoro ex art. 29 ("WP29") adottate il 6 febbraio 2018 ai sensi degli artt. 33 e 34 del GDPR, si verifica in tre categorie di eventi sia accidentali che illeciti:

– "*Confidentiality breach*", divulgazione o accesso non autorizzato a dati personali;

– "*Availability breach*", alterazione di dati personali;

– "*Integrity breach*", modifica di dati personali.

Nel Decreto legislativo 8 giugno 2001, n. 231 l'articolo 24-bis, D.lgs. n. 231/2001, non a caso rubricato "*Delitti informatici e **trattamento illecito di dati***" sono annoverati i reati rilevanti di **accesso abusivo** ad un sistema informatico o telematico (art. 615-ter c.p.), **detenzione e diffusione abusiva di codici di accesso** a sistemi informatici (art.615-quater c.p.), interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.), **danneggiamento** di informazioni, dati e programmi informatici (art. 635-bis c.p.), danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.).

Seppur in maniera incompleta dopo il fallito tentativo di introdurre con il D.L. n. 93/2013 tutti i reati previsti dal previgente Codice privacy nel novero dei reati presupposto del Decreto 231, alcune fattispecie strettamente legate ai profili della protezione dei dati in ambito aziendale, oggi configurano per esse, come per le altre figure di reato ulteriori profili di punibilità a carico dell'ente con elevate sanzioni pecuniarie (sino ad euro 774.550,00) e, nelle ipotesi delittuose più gravi, anche interdittive dell'attività con confisca. Appare cioè evidente che le casistiche di "data breach", ovvero trattamento illecito dei dati previste dal Regolamento (UE) 2006/679, dalla Legge di delegazione europea e infine dagli articoli dal 167 a 172 dello schema di decreto legislativo all'esame del Parlamento, appaiono sovrapponibili alle fattispecie dei delitti informatici e trattamento illecito di dati degli artt. 24 e 24-bis, e forse anche dagli artt. 25-quater [Delitti con finalità di terrorismo o di eversione dell'ordine democratico] e 25-quinquies comma 1 lett. c [Delitti contro la personalità individuale] del D.Lgs. 231/2001.

Rafforza tali considerazioni l'emanazione del D.Lgs. 65/2018 (in vigore dal 24.6.2018) in attuazione della Direttiva (UE) 2016/1148 - cosiddetta **Direttiva NIS - Network and Information Security** - recante misure che stabiliscono un livello comune di sicurezza di reti e sistemi informativi nell'U.E., disciplinando in modo organico e trasversale la materia della **cyber security** con misure tecnico-organizzative per ridurre il rischio di incidenti informatici, per la continuità dei servizi essenziali (energia, trasporti, salute, finanza, ecc.) e dei servizi digitali (motori di ricerca, servizi cloud, piattaforme di commercio elettronico).[6]

5. Conclusioni

Dalle considerazioni sopra svolte, senza pretesa di esaustività, risulta evidente come sia veramente auspicabile un intervento normativo di armonizzazione e coordinamento del coacervo di norme che disciplinano i sistemi di segnalazione, la cyber security di dati, sistemi e reti e i modelli di prevenzione degli illeciti nelle aziende. L'elemento unificante, risolutore della evidente stratificazione normativa in materia, può muovere da una *ratio* che il Legislatore ha già elaborato, e che si ritrova nella locuzione già usata all'art. 2-bis, lettera a) della Legge 179/2017: "***a tutela dell'integrità dell'ente***".

In attesa di ciò, le società che abbiano adottato Modelli di Organizzazione e Gestione ex D.Lgs. 231/2001 e i loro Organismi di Vigilanza hanno la necessità di:

- aggiornare i MOG e le procedure interne per implementare un sistema che, supportato da adeguate piattaforme informatiche, permetta di istituire efficienti "canali" di

[6] V. iter e documentazione parlamentare dello schema di decreto legislativa di attuazione della direttiva (UE) 2016/1148 in http://www.camera.it/leg17/682?atto=520&tipoatto=Atto&leg=17&tab=1 , e A.C. Messina, *Incidenti informatici contenuti*, in Italia Oggi, 4.6.2018 – anche in ordine alle modifiche alla Convenzione 108/1981 sulla protezione degli individui rispetto al trattamento automatizzato dei dati personali

comunicazione previsti sia dalla Legge 179 che in vario modo dalle normative sopra descritte;

- strutturare tali "canali" garantendo il costante coinvolgimento degli Organismi di Vigilanza ex Decreto 231 nonchè la riservatezza e la tutela dei segnalanti da eventuali atti discriminatori o ritorsivi;

- introdurre opportune misure di riservatezza e tutela, attualmente carenti, anche per coloro che siano invece soggetti passivi o comunque contestati dalle segnalazioni;

- provvedere all'integrazione del un "nuovo" sistema di whistleblowing, coordinato con tutti quelli già implementati ai sensi delle normative di settore che già li prevedono (es: quello ex art. 52 – bis TUB per le banche) in un sistema uniforme e di facile comprensione per i possibili whistlebowers.

Ad avvalorare le istanze di riforma organica del D.Lgs. 231/2001 sta anche la considerazione che il concetto di "*tutela dell'integrità dell'ente*" ha certamente un perimetro di rischi legali, giudiziari, sanzionatori e reputazionali enormemente più vasto e insidioso di quello, pur ampio, sanzionato nel catalogo dei reati ex D.Lgs. 231/2001 e presidiato dagli Organismi di Vigilanza. Una valutazione questa che muove da un oggettivo confronto fra diversi corpus normativi incidenti (GDPR, Whisleblowing, reati informatici, Cyber security) e tra le tipologie di rischi da presidiare a seconda del settore economico in cui operano le aziende.