Titolo: Il nuovo DDL Cybersicurezza nel quadro europeo e nazionale. Il possibile *interplay* con la *compliance* 231 e gli obblighi *data protection*. - *Parte 1 – DDL Cybersicurezza e compliance 231*

Autori: Avv. Luca Antonetto (Consigliere e Coordinatore Comitato Studi AODV[231])

Agendadigitale.eu, 22 marzo 2024

1. Premessa

Come testualmente riferito nel comunicato ufficiale del governo n. 66 in pari data il 25 gennaio scorso "*Il Consiglio dei Ministri, …., ha approvato, con la previsione della richiesta alle Camere di sollecita calendarizzazione*[1]*, ….., un* ***disegno di legge che introduce disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale***. [di seguito anche soltanto il "**DDL**" o "**DDL Cybersicurezza**"]

Il testo interviene con modifiche (sostanziali e processuali) in relazione ai 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 per chi li commette, a danno altrui o ad accedere abusivamente a sistemi informatici e/o a intercettare/interrompere comunicazioni informatiche e telematiche.

Inoltre, si rafforzano le funzioni dell'Agenzia per la cybersicurezza nazionale (ACN) e il suo coordinamento con l'Autorità giudiziaria in caso di attacchi informatici, con specifiche procedure

[1] https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-66/24831

volte a rendere più immediato l'intervento dell'Agenzia a fini di prevenzione degli attacchi e delle loro conseguenze e del ripristino rapido delle funzionalità dei sistemi informatici.

Si pone a carico dei soggetti pubblici individuati dalla norma … un obbligo di segnalazione e notifica degli incidenti indicati in apposito provvedimento ACN, con impatto su reti, sistemi informativi e servizi informatici e si disciplina la relativa procedura."

Dal 13 marzo scorso le Commissioni riunite Affari Costituzionali e Giustizia della Camera dei Deputati hanno avviato l'esame del DDL, attualmente ancora in corso.

Come è già stato scritto in questa sede[2] commentando le novità del DDL in materia di reati informatici (pur sbilanciate "*nella direzione di una forte repressione*"), "*rappresenta certamente una positiva novità l'attenzione che il Governo sta rivolgendo al settore dei cyber crimes e della cyber security*". Attenzione imposta da un contesto storico in cui "*la criminalità informatica continua ad evolversi, rapidamente, mettendo in atto tecniche intrusive difficili di contrastare. … Gli attacchi informatici sono aumentati negli anni 2020 e 2021 non solo in termini di vettori e numeri ma anche in termini di impatto*", come rilevato nel corposo *Documento di Approfondimento* recentemente pubblicato da AODV[231], con la collaborazione di Deloitte Legal, su "*La prevenzione dei reati informatici: rischi 231, data protection e misure di compliance*". Quanto all'anno 2022 merita ricordare che, soltanto per l'Italia, "*La Relazione annuale al Parlamento, sulle attività svolte dall'Agenzia per la cybersicurezza nazionale (ACN) in materia di cybersicurezza*" riferisce di oltre "*mille incidenti informatici trattati*"; e si tratta soltanto della punta dell'*iceberg*, considerata la "*intuibile «cifra nera» dei fatti non denunciati …* [per] *ragioni … molteplici: necessità di ripristinare prima possibile la piena funzionalità dell'azienda, timore per il danno reputazionale connesso alla diffusione della notizia … ma anche consapevolezza che l'indagine penale difficilmente si concluderà con successo.*"[3]. Come ricorda il Consiglio Europeo, poi, quella de "*gli attacchi informatici e la criminalità informatica*" rappresenta "*una tendenza destinata a crescere in futuro, visto che si prevede che 41 miliardi di dispositivi in tutto il mondo saranno collegati all'Internet delle cose entro il 2025*"[4].

A livello comunitario l'attenzione risale al 1990, con la *Raccomandazione sulla criminalità informatica del Consiglio d'Europa*, che già presagiva che "*the computer may well become the Achille's heel of the post-industrial society*". Da allora il tessuto normativo europeo e nazionale si è progressivamente infittito delineando un articolato contesto di riferimento, sinteticamente descritto

[2] Abrogazione dell'art. 615 quinquies, modifica dell'art. 617 bis c.p., modifica dell'art. 617 quater c.p., modifica dell'art. 617 quinquies c.p., modifica dell'art. 617 sexies c.p., introduzione dell'art. 623 quater c.p. : circostanza attenuante, modifica dell'art. 629 c.p.: introduzione della fattispecie di estorsione mediante reato informatico: *https://www.agendadigitale.eu/sicurezza/ddl-cyber-security-pene-piu-severe-per-i-reati-informatici-ma-il-giustizialismo-non-basta/*

[3] E. FUSCO, *Riflessioni e proposte in tema di reati cyber*, in *Sistema Penale*, 28/04/2023

[4] https://www.consilium.europa.eu/it/policies/cybersecurity/

nel paragrafo successivo per la migliore comprensione sistematica del DDL, che in tale contesto si innesta.

Al di là di tale premessa sistematica e di una panoramica sul DDL, lo scopo di questo scritto e di quello che seguirà è un duplice *focus* sulle interazioni della *cybersicurezza*, rafforzata dal DDL, con materie contigue, e spesso intrecciate: quindi innanzitutto, in questo articolo, l'interazione la prevenzione dei reati-presupposto informatici *ex* art. 24-*bis* del d.lgs. 231/2001; poi, nel successivo articolo, l'interazione con la *privacy* ex Reg. UE 2016/679, cd. GDPR, in particolare per quanto attiene il ruolo del DPO, le notifiche di violazioni di dati personali e lo stato dell'arte delle misure di sicurezza ai sensi dell'art. 32 GDPR, con un'appendice sugli aspetti civilistici, recentemente portati alla ribalta dalla Corte di Giustizia dell'Unione Europea, con la sentenza 14/12/2023, n. 340/21. In conclusione, si svolgerà una breve analisi del recentissimo documento di indirizzo del Garante della Protezione dei Dati personali, emanato ai sensi dell'art. 57, par. 1, lett. b) e d), del GDPR nonché ai sensi dell'art. 154-bis, c.1, lett. a) del Codice, denominato "*Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*", plastico esempio in cui le esigenze in ambito *cybersecurity*, prevenzione dei reati presupposto in materia d.lgs. 231/2001 devono trovare il corretto bilanciamento con le esigenze di tutela della riservatezza del lavoratore in ambito *data protection*.[5]

Dopo la prima stesura degli articoli, riferita al testo dello "*Schema di disegno di legge recante disposizioni in materia di reati informatici e di rafforzamento della Cybersicurezza nazionale*", come si è detto approvato il 25 gennaio scorso dal consiglio dei Ministri, è sopravvenuto il testo c.d. «bollinato» del "*Disegno di legge*", che ha apportato alcune modifiche, a partire dalla inversione dei due Capi del d.d.l.: in effetti lo "*Schema*" prevedeva al Capo I le "*Disposizioni per la prevenzione e il contrasto dei reati informatici …*", con numerose "*Modifiche*" al codice penale, al codice di procedura penale ed a varie leggi in materia, tra cui, per quanto precipuamente rileva per questo primo articolo, all'art. 5, le "*Modifiche al decreto legislativo 8 giugno 2001, n. 231*"; mentre le "*Disposizioni in materia di rafforzamento della Cybersicurezza nazionale …*" erano previste al Capo II. Nel testo «bollinato», invece, queste ultime sono state anticipate al Capo I, facendo seguire nel Capo II le numerose "*Modifiche*", suddette, con la conseguente rinumerazione di tutti gli articoli ed alcune variazioni di formulazione. Per quanto in particolare rileva per questo primo articolo, le "*Modifiche decreto legislativo 8 giugno 2001, n. 231*" sono passate all'art. 15, con la contestuale importante correzione di un evidente refuso dell'art. 5 dello "*Schema*".

[5] Gli aspetti giuslavoristici del provvedimento del Garante non saranno qui trattati, salvo i richiami necessari allo Statuto dei Lavoratori.

2. **Il contesto europeo e internazionale di riferimento**.

Per quanto attiene il contesto europeo e internazionale in cui si muove il DDL cybersicurezza si rinvia agli articoli già pubblicati su questa sede: https://www.agendadigitale.eu/sicurezza/la-cyber-security-che-verra-levoluzione-normativa-in-italia-e-ue/;
https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/.

3. Le novità del DDL Cybersicurezza.

Dopo aver inquadrato la nuova normativa, si ritiene utile descrivere, in generale, le nuove disposizioni più rilevanti per poi procedere a valutare innanzitutto la possibile interazione di alcune di esse con il d.lgs 231/2001 ("**d.lgs. 231**"), che disciplina la responsabilità amministrativa degli enti.

La maggiore novità è rappresentata da specifiche procedure che mirano a rendere più immediato l'intervento dell'ACN per prevenire attacchi e mitigare le conseguenze, garantendo il rapido ripristino delle funzionalità dei sistemi informatici.

Sulla base di tali premesse sono stati previsti i seguenti obblighi:

1) **L'obbligo di segnalazione e notifica per determinati soggetti pubblici (artt. 8 e 15 dello "Schema" – artt. 1 e 8 del testo «bollinato»)**

Le pubbliche amministrazioni centrali, con le rispettive società in-house, le Regioni e le Province autonome di Trento e Bolzano, i comuni con una popolazione superiore ai 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali, dovranno segnalare tempestivamente all'ACN, e in ogni caso entro 24 ore dalla scoperta dell'incidente, fornendo una notifica completa entro 72 ore dalla stessa data.

gli incidenti informatici subiti aventi impatto su reti, sistemi informativi e servizi informatici. Il mancato rispetto di tali obblighi potrà comportare sanzioni per **importi che variano da 25.000 a 125.000 euro**. Per i dipendenti delle pubbliche amministrazioni, la violazione di queste disposizioni può comportare responsabilità disciplinare e amministrativo-contabile.

2) **Convocazione del Nucleo per la Cybersicurezza (art. 11 - dello "Schema" – artt. 4 del testo «bollinato»).**

Questo nucleo, che potrebbe includere rappresentanti della Procura nazionale antimafia e antiterrorismo, della Banca d'Italia e altri attori, potrà essere convocato per affrontare le questioni più cruciali riguardanti la cybersicurezza nazionale.

3) **Individuazione di un referente per la cybersicurezza (art. 13 – dello "Schema" – artt. 6 del testo «bollinato»)**

Questo professionista, che dovrà essere nominato in seno alle Pubbliche Amministrazioni, avrà il compito di seguire l'iter parlamentare per l'approvazione definitiva della legge, garantendo così un'implementazione efficace e tempestiva delle nuove disposizioni e dovrà essere **basata sulle "qualità professionali possedute",** evidenziando l'importanza di competenze e esperienze specifiche nel campo della sicurezza informatica. Tale figura sarà, inoltre, il **punto di contatto unico dell'amministrazione con l'Agenzia per la Cybersicurezza Nazionale**.

4. DDL Cybersicurezza e D.lgs. 231/2001.

Per quanto riguarda le **interazioni tra il DDL ed il d.lgs. 231/2001**, si rileva innanzitutto che l'art. 1 dello "Schema", divenuto art. 11 nel testo «bollinato» e sempre rubricato "*Modifiche al codice penale*", apporta una serie di "*modificazioni:* [tra altre non di «rilievo 231»] *all'articolo 615-ter* ["*Accesso abusivo di un sistema informatico o telematico*"] *... all'articolo 615-quater* ["*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*"] … *all'articolo 615-quinquies* ["*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*"] … *all'articolo 617-quater* ["*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*"] *... all'articolo 617-quinquies* ["*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*"] *... all'articolo 635-bis* ["*Danneggiamento di informazioni, dati e programmi informatici*"] *... all'articolo 635-ter* ["*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*"] *... all'articolo 635-quater* ["*Danneggiamento di sistemi informatici o telematici*"] *... all'articolo 635-quinquies* ["*Danneggiamento di sistemi informatici o telematici di pubblica utilità*"].

Come è noto, tutti quelli citati costituiscono (anche) reati-presupposto, in quanto richiamati dell'art. 24-*bis* del d.lgs. 231/2001 in materia di "*Delitti informatici e trattamento illecito di dati*".

Peraltro - a parte l'espressa abrogazione de "*l'articolo 615-quinquies*" «compensata» un'introduzione del nuovo "*Art. 635-quater. 1*" (su cui *infra*) - il minimo comune denominatore delle altre

modificazioni citate consiste essenzialmente nell'innalzamento delle pene previste per le persone fisiche autrici dei reati, nell'inserimento di aggravanti e/o nel divieto di attenuanti, per rimodulare più incisivamente il bilanciamento delle circostanze nella punizione delle persone fisiche autrici dei reati (per un'analisi più dettagliata delle modificazioni di ciascuna delle ipotesi di reato elencate, e del relativo impatto punitivo, si rinvia al precedente, puntuale, commento di Agenda Digitale sul tema, sopra citato nella nota 2).

Qualche marginale modifica oggettiva e soggettiva delle fattispecie è prevista dall'art. 1, in particolare: con riferimento all'art. 615-*ter*, n. 2, con l'aggiunta, quanto alla condotta, della "*minaccia*", oltre che dell'"*uso*"; all'art. 615-*quater*, con la sostituzione del più ampio requisito finalistico del "*vantaggio*" a quello attuale del "*profitto*"; all'art. 617-*quater*, con l'estensione dei sistemi informatici o telematici rilevanti e con l'aggiunta tra gli autori di "*chi esercita anche abusivamente la professione di investigatore privato*"; all'art. 635-*ter*, con la ridefinizione del rilievo pubblico dei "*dati e programmi informatici*" di riferimento e con la coerente modifica della rubrica; all'art. 635-*quinquies*, con la ridefinizione delle condotte per rinvio a quelle "*di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi*".

Nel complesso, tali caratteristiche delle modifiche dei citati reati-presupposto informatici, non implicano certo stravolgimenti sotto il profilo degli oneri organizzativi e procedurali delle società e degli enti, sulla cui antitesi, la cd. "*colpa di organizzazione*", è essenzialmente incentrata la loro "*responsabilità amministrativa*" *ex* d.lgs. 231/2001, come riconosciuto dalla giurisprudenza di legittimità più recente, a partire dalla cosiddetta "*sentenza Impregilo bis*" (Cass. Pen., Sez. VI, 23401/2022; cfr., da ultimo, Cass. Pen., Sez. V, 3196/2024).

Allo specifico riguardo può dunque dirsi che anche a fronte delle citate "*modificazioni*" del DDL resteranno sostanzialmente valide le indicazioni del citato *Documento di Approfondimento* di AODV[231], che si propone programmaticamente, e sviluppa sistematicamente nell'arco di 62 pagine, "*di verificare quale sia, nella costruzione del Modello organizzativo 231 e nello sviluppo di un sistema di compliance in materia di data protection, l'attività di risk assessment e i presidi di controllo da porre in essere per contenere l'incremento dei rischi informatici, …, e quale ruolo possa rivestire in concreto l'Organismo di Vigilanza nominato ai sensi del d.lgs. 231/2001*": il tutto con riferimento alle più recenti "*best practices*" del settore ed alle relative misure di sicurezza informatica sia prescrittivo-deontologiche, sia organizzative, sia procedurali, sia tecnico-informatiche.

Lo stesso discorso può valere per il soltanto apparentemente nuovo art. 635-*quater*. 1, introdotto dall'art. 1, lett. p), dello "*Schema*", ora art. 11, l. p) del testo «bollinato», che, in realtà, come si è accennato, di fatto sostituisce l'art. 615- *quinquies*, contestualmente abrogato dall'art. 1, lett. c), del

DDL: infatti la rubrica delle due disposizioni è identica[6], come sono identiche la formulazione della fattispecie, di cui al primo comma, e la relativa pena edittale; rispetto all'attuale art. 615- *quinquies* il «nuovo» art. 635-*quater*. 1 è arricchito di due nuovi commi che, nella logica dell'inasprimento repressivo che ispira tutto il DDL, prevedono aggravanti, rispettivamente "*quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1)*"[7] e "*quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma, primo periodo*"[8]; infine – *last but not least* - cambia la collocazione sistematica della fattispecie, che passa dal novero "*dei delitti contro l'inviolabilità del domicilio*" a quello "*dei delitti contro il patrimonio mediante violenza alle cose o alle persone*" (ma anche tali differenze, di fatto, incidono poco o punto sugli oneri organizzativi e procedurali delle società e degli enti *ex* d.lgs. 231/2001).

4.1 La nuova fattispecie di estorsione mediante reato informatico.

Fa eccezione a quanto sin qui rilevato una vera e propria nuova fattispecie del DDL di apparente maggiore rilievo sostanziale (anche) ai fini prevenzionistici d.lgs. 231/2001.

Si tratta dell'introduzione, ad opera dell'art. 1, lett. l), dello "Schema", ora art. 11, lett. l) del testo «bollinato», della nuova fattispecie di estorsione mediante reato informatico, con l'aggiunta all'art. 629 c.p. ["*Estorsione*"] di un terzo comma, per cui "*Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies, ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5000 a euro 10.000. .....*"

Entrambe le disposizioni da ultimo commentate sono richiamate, come reati-presupposto informatici *ex* art. 24-*bis* del d.lgs. 231/2001, dall'art. 5 dello "*Schema*", ora art. 15 del testo «bollinato», specificamente dedicato alle "*Modifiche al decreto legislativo 8 giugno 2001, n. 231*".

La prima nuova fattispecie è inequivocabilmente richiamata dalla lett. b), della disposizione appena citata, che inserisce un nuovo comma 1-*bis* nell'art. 24-*bis* d.lgs. 231/2001, riferendolo espressamente al nuovo "*delitto di cui all'articolo 629, terzo comma, del codice penale*" (con l'applicazione "*all'ente della sanzione pecuniaria da trecento a ottocento quote*"). La seconda fattispecie è ora inequivocabilmente richiamata dall'art. 15, lett. c), del testo «bollinato», così correggendo il refuso dello "*Schema*" di cui si è fatto cenno in apertura.

---

[6] "*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*."

[7] "*se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, con abuso della qualità di operatore del sistema;*"

[8] "*Qualora i fatti di cui ai commi primo e secondo riguardino 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 ...*"

In effetti l'art. 5, lett. c), dello "*Schema*" sostituiva, nel secondo comma dell'articolo 24-*bis* d.lgs. 231/2001, il riferimento all'abrogato "*art. 615-quinquies*" con l'evidentemente erroneo riferimento all'art. "*615-quater. 1*".

L'ipotesi di un refuso, con la digitazione del numero 1 evidenziato in neretto, al posto del numero 3, era stata immediatamente rilevata e segnalata da AODV[231], considerando che: i) un articolo "*615-quater. 1*" non è previsto né dal codice penale vigente, né da alcuna disposizione del DDL; ii) (come si è già accennato) il DDL, da una parte, abroga "*l'articolo 615-quinquies*", e, d'altra parte, introduce "*dopo l'articolo 635-quater ... il seguente «Art. 635-quater. 1*"; iii) la norma del nuovo art. 635-quater. 1, come si è già detto, risulta sostanzialmente sovrapponibile con quella dell'abrogato art. 615-*quinquies*.

Alla luce della correzione, nel testo «bollinato» del refuso dello "*Schema*", e considerata la prdetta sovrapponibilità del nuovo art. 635-*quater*. 1, all'abrogato art. 6,15-*quinquies*, l'unica novità di sostanziale rilievo ai fini della prevenzione della responsabilità «amministrativa» delle persone giuridiche, risulta alla fin fine quella dell'introduzione del nuovo art. 629, terzo comma, nel novero dei reati-presupposto informatici dell'art. 24-*bis* del d.lgs. 231/2001.

In effetti, per il resto, l'art. 15 del testo «bollinato» (come già l'art. 5 dello "*Schema*") si dedica esclusivamente all'inasprimento delle "*sanzioni pecuniarie*" già previste dall'art. 24-*bis* del d.lgs. 231/2001, elevando l'attuale *range* sanzionatorio del primo comma ("*da cento a cinquecento quote*") al più aspro *range* previsto dall'art. 5, lett. a), del DDL ("*da duecento a settecento quote*"), oltre all'aggiunta di sanzioni interdittive *ad hoc* (richiamando quelle "*previste dall'articolo 9, comma 2, per una durata non inferiore a due anni*") per la nuova fattispecie di estorsione mediante reato informatico.

Quest'ultima nuova fattispecie imporrà senz'altro una specifica considerazione *ex* art. 7, comma 4, lett. a), del d.lgs. 231/2001, insieme alle altre modifiche del DDL di marginale rilievo ai fini della responsabilità «amministrativa» delle società e degli enti, secondo la sequenza canonizzata in materia ed ampiamente illustrata nel citato *Documento di Approfondimento* di AODV[231]: cioè attraverso le consuete fasi della mappatura del rischio-reato, del *risk assessment* di dettaglio, con specifico riferimento ai "*processi c.d. rilevanti (in quanto esposti al rischio-reato)*", e, infine, la "*definizione dei presidi di controllo*", anche alla stregua delle "*best practices di riferimento*".

4.2. Quali presidi di controllo.

Ciò detto, non è agevole identificare "*presidi di controllo*", ovvero misure organizzative e procedurali, ulteriori rispetto a quelle che dovrebbero essere già previsti dal M.O.G. per la prevenzione (della massima parte) dei reati veicolo assunti dal nuovo art. 629, terzo comma, c.p., che,

come si è anticipato, configura la nuova forma di estorsione tramite condotte strumentali, cioè, specificamente, "*mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies*": in effetti - fatta eccezione per l'art. 617-*sexies* - i reati richiamati dal nuovo art. 629, terzo comma, c.p. sono già tutti assunti come reati-presupposto dall'art. 24-*bis* del di legge 231/2001. In altre e più concrete parole, è plausibile che all'esito della considerazione prevenzionistica sopra descritta risultino sufficienti i presidi di controllo già adottati per contenere il rischio dei citati reati veicolo, fatta eccezione per quello dell'art. 617-*sexies*

In effetti l'eccezione sottolineata fa sì che il delitto di "*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*" entri *ex novo* a far parte - sia pure indirettamente, come antecedente necessario - del novero delle fattispecie rilevanti ai fini della prevenzione dei reati-presupposto informatici dell'art. 24-*bis* del d.lgs. 231/2001. Perciò il delitto in questione dovrà essere oggetto di particolare attenzione prevenzionistica, sempre secondo la sequenza canonizzata sopra descritta.

Passando dalla prospettiva del M.O.G. a quella dell'OdV, questi dovrà vigilare sul compimento delle attività sopradescritte, nell'adempimento del suo compito di curare l'aggiornamento del M.O.G. *ex* art. 6, comma 1, lett. b), d.lgs. 231/2001, "*intendendosi tale compito - secondo principio ormai consolidato - come funzione di impulso nei confronti dell'Organo gestorio (unico competente all'approvazione del Modello organizzativo e alle sue modifiche), nonché come funzione di vigilanza sulle azioni di adeguamento di sviluppo dell'organizzazione conseguente alle iniziative raccomandate.*"[9]

5. Conclusioni, anche alla luce della giurisprudenza recente.

In conclusione, se l'attività di adeguamento 231 alla legge che attuerà il DDL non dovranno essere particolarmente innovative ed onerose, la citata "*attenzione che il Governo sta rivolgendo al settore dei cyber crimes e della cyber security*" consiglia di alzare ancor di più la guardia sulla prevenzione dei reati-presupposto informatici, magari anche cogliendo l'occasione per provvedere ad un supplemento di sistematica verifica di idoneità di quanto già fatto in passato nella materia, con un *focus* sulla "*catena di approvvigionamento*" dato che "*la gran parte delle intrusioni avviene attraverso la "«supply chain» aziendale*", come è stato autorevolmente ricordato[10].

Tale verifica si impone anche in considerazione delle indicazioni della attenzione giurisprudenziale ricavabili da una recentissima sentenza di legittimità, Cass. Pen., Sez. V, 26/01/2024, n. 3211, che -

[9] così, per tutti, da ultimo, il *Position Paper* AODV231 su "*Il ruolo dell'OdV nell'ambito del whistleblowing*", 10 ottobre 2023

[10] E. FUSCO, *op. cit.*, p. 2

per la prima volta[11] - si è occupata della responsabilità amministrativa di una società *ex* d.lgs. 231/2001 in riferimento ad una serie di condotte di dipendenti di una società (il "*direttore commerciale e il … responsabile tecnico*") "*riconducibili ad un accesso abusivo al sistema informatico*" *ex* art. 615-*ter* c.p., funzionale "*alla rivelazione di segreti commerciali*" della società datrice di lavoro ad una società concorrente, "*in vista della loro fuoriuscita da*[lla prima] ed al loro successivo formale coinvolgimento nella seconda.

In particolare, da una perizia tecnica era "*emerso che, in periodo di pochi mesi, …, erano stati compiuti una serie di accessi* [al *server* aziendale] *non già allo scopo di svolgere attività in favore della* [società datrice di lavoro] *bensì per operare … su progetti riferibili alla* [società concorrente], *al punto da pervenire a redigere un'offerta … da parte di tale società concorrente ad un cliente della* [società datrice di lavoro] *nonché al fatto che erano stati scaricati negli ultimi giorni di servizio presso queste società una serie di file compatibili solo con una copiatura massiva*."

Riconosciuta nei gradi di merito la sua responsabilità amministrativa *ex* art. 24-*bis* del d.lgs. 231/2001 in relazione al delitto dell'art. 615-*ter* c.p., la società concorrente, ha censurato in Cassazione la "*erronea applicazione dell'art. 5 del d.lgs. n. 231 del 2001 … in quanto i fatti di reato sarebbero stati commessi* [dalle predette persone fisiche] *quando erano ancora alle dipendenze della società* [vittima della rivelazione dei suoi segreti commerciali *ex* art. 623 c.p.], *né essi avrebbero, in quel periodo, potuto essere considerati soggetti addetti contemporaneamente alla gestione al controllo della* [società concorrente] *onde giustificare la responsabilità amministrativa da reato.*".

La Suprema Corte, dopo aver dato una lettura estensiva della "*nozione di «segreti commerciali» oggetto del reato di cui all'art. 623 cod. pen.*", ha accolto il ricorso della società condannata *ex* d.lgs. 231/2001, rinviando la decisione per un nuovo esame, sulla base del rilievo che "*nelle decisioni di merito, considerato che la responsabilità della società ricorrente è correlata a condotte poste in essere dai predetti imputati prima che entrassero a far parte della compagine sociale, avrebbe dovuto essere compiuto un accertamento … sulla possibilità di considerare gli stessi, in virtù dell'art. 5, lett. a), ultima parte, del d.lgs. n. 231 del 2001, «persone che esercitano, anche di fatto, la gestione e il controllo dello stesso»*". In altre parole, la Suprema Corte sconta che i dipendenti/amministratori di una società possano essere **contemporaneamente** considerati anche soggetti di fatto di un'altra società ai sensi della norma citata e che in tale duplice veste possano compiere reati-presupposto nell'interesse o a vantaggio della società di cui sono soggetti di fatto. E nel farlo la stessa pronuncia di legittimità dà una lettura innovativa del requisito dell'esercizio di fatto della gestione e del controllo

[11] in effetti nel pluricitato documento operativo di AODV[231] si dava atto che alla data della sua pubblicazione ("*Giugno 2023*") "*non è dato riscontrare pronunce della suprema corte sulla responsabilità degli enti derivante da … reati informatici. Di conseguenza l'analisi che segue sarà incentrata su una serie di casi pratici che, ancorché abbiano coinvolto le sole persone fisiche imputate, … possono fornire una serie di spunti interessanti anche in tema di responsabilità delle persone giuridiche …*"

di cui all'art. 5, comma 1, lett. a), ultima parte, del d.lgs. 231/2001 (in particolare una lettura estensiva della nozione di "*controllo in via di fatto*").

Quanto sopra sottolineato può essere particolarmente rilevante anche per il caso, considerato dal *Documento di Approfondimento* di AODV[231] con riferimento a Cass. Pen., 25731/2010, del "*possibile concorso tra reato di accesso abusivo e quello di turbata libertà dell'industria o del commercio (ex art. 513 c.p., … a sua volta reato presupposto ex art. 25-bis) in quanto gli imputati avrebbero turbato l'attività economica di una impresa concorrente «a mezzo delle condotte … di cui all'art. 615 ter …»*".

In tema del reato presupposto di accesso abusivo a sistema informatico - nella fattispecie "*aggravato ai sensi del comma terzo dell'art. 615-ter cod. pen.*", trattandosi "*di accesso abusivo alla banca dati del Pubblico Registro Automobilistico*" - merita ricordare anche Cass. pen., Sez. V, Sent., 10/01/2024, n. 1161, che reca una interessante lettura estensiva della "*definizione normativa di «sistema di interesse pubblico»*", da intendersi come "*sistema informatico al servizio di una collettività indifferenziata e indeterminata di soggetti*" senza limitazione "*alle sole ipotesi in cui emergono le «infrastrutture critiche dello Stato»*", dato "*il carattere aperto della previsione …* [che] *permette di ricomprendere anche attività diverse, esse stesse funzionali al perseguimento di un generale interesse di rilevanza pubblicistica, a prescindere dal carattere riservato dei dati contenuti nel sistema informativo (in sé estraneo alla previsione normativa).*"

Questa *nouvelle vague* giurisprudenziale in materia di reati presupposto informatici, concorre a rafforzare l'anticipata opportunità di alzare ancor di più la guardia sulla prevenzione dei reati-presupposto informatici.

Un'altra ragione per farlo, infine, sta nella previsione della magistratura per cui, "*il problema dell'identificazione del colpevole*", tipico della casistica in materia, "*verosimilmente imporrà, quantomeno in prospettiva, di seguire (anche) percorsi alternativi, ragionando sempre di più sulla possibilità di chiamare in causa l'ente, anche in luogo della persona fisica e a mente dell'art. 8 d.lgs. 231/2001.*"[12]

[12] E. FUSCO, *op. cit.*, p. 2