Approfondimenti

Febbraio 2020

Responsabilità penale e responsabilità degli enti nel d.l. sulla cyber security

Avv. Fabio Federico, Partner, DFS Avvocati Penalisti

1. I contenuti essenziali del decreto

Obiettivo dichiarato (all'art. 1, comma 1) del d.l. 105/2019, convertito dalla l. 133/2019, è quello di "*assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici… da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento delle attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale*".

Per realizzare questa finalità, il decreto, all'**art. 1, comma 1**, ha istituito il cd. **perimetro di sicurezza nazionale cibernetica** (da qui in avanti, semplicemente il "perimetro"), ha previsto, a carico dei soggetti che vi rientreranno, alcuni obblighi e ha attribuito determinate funzioni di vigilanza alla Presidenza del Consiglio dei Ministri (rispetto ai soggetti pubblici) e al Ministero dello sviluppo economico (rispetto ai soggetti privati).

Quanto agli **obblighi**, in estrema sintesi, il **comma 2b)** impone ai soggetti rientranti nel perimetro di elaborare e trasmettere annualmente alle autorità preposte (cioè alla Presidenza del Consiglio dei Ministri e al Ministero dello sviluppo economico) l'elenco delle reti, dei servizi informativi e dei sistemi informatici impiegati (aventi le caratteristiche indicate al comma 1).

Il **comma 3a)** prevede l'obbligo, per i medesimi soggetti, di comunicare al gruppo di intervento per la sicurezza informatica (CSIRT) tutti gli eventuali incidenti riguardanti quelle medesime reti, quei medesimi servizi e quei medesimi sistemi.

Il **comma 6a)**, infine, riguarda le ipotesi di affidamento (sempre da parte degli stessi soggetti) di forniture di beni e di servizi relativi sempre alle stesse reti, agli stessi sistemi e agli stessi servizi: in questo caso, vige l'obbligo di comunicazione al Centro di Valutazione e Certificazione Nazionale (CVCN), indicando altresì il rischio associato alla fornitura.

Quanto alla **vigilanza**, per quel che stabilisce il **comma 6c)**, essa è prevista con riferimento al rispetto di ciascuno degli obblighi di cui si è detto sopra, nonché dei procedimenti correlati.

La violazione di quegli obblighi e l'ostacolo alla vigilanza delle autorità preposte sono presidiati nella maggior parte dei casi da **sanzioni amministrative** e, nelle ipotesi residuali che ci si appresta a descrivere, da **sanzioni penali**, nonché, nel caso degli enti, *ex* **d.lgs. 231/2001**.

Il **comma 9**, infatti, contiene un'elencazione di violazioni che danno luogo all'applicazione di sanzioni amministrative; la gamma di ipotesi include (tra le altre cose) anche "*il mancato adempimento degli obblighi di predisposizione delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b)*"; "*il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera a)* (cioè la notifica degli incidenti, ndr)"; "*la mancata comunicazione di cui al comma 6, lettera a)* (cioè la comunicazione delle informazioni dovute in caso di affidamenti, ndr)".

Il **comma 11**, invece, punisce con la reclusione da uno a tre anni (ma il decreto legge prevedeva una pena massima di cinque anni, che è stata ridotta in sede di conversione) "*chiunque, allo scopo di ostacolare o di condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b) o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a) o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6, lettera c), od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto*".

Il **comma 11 *bis***, infine, prevede che, "*all'art. 24 bis, comma 3, del decreto legislativo 8 giugno 2001, dopo le parole: 'di altro ente pubblico', sono inserite le seguenti: 'e dei delitti di cui all'articolo 1, comma 11, del decreto legge 21 settembre, n. 105*": nella sostanza, è stato ampliato il catalogo dei reati presupposto della responsabilità a carico degli enti, con una nuova ipotesi punita con la sanzione pecuniaria fino a quattrocento quote (anche in questo caso, si segnala che l'attuale formulazione della norma consegue alle modifiche apportate in sede di conversione, dal momento che il decreto legge aveva originariamente collocato questa fattispecie al di fuori del d.lgs. 231/2001, cui non era stata apportata alcuna modifica, il che era stato motivo di critica in sede di primi commenti e aveva indotto il Servizio studi della Camera e del Senato a segnalare l'"*opportunità di inserire tale reato nell'ampio catalogo dei reati presupposto già contemplato dal decreto legislativo n. 231 del 2001*"[1]).

[1] Il riferimento è a SASSI, *Sicurezza cibernetica e responsabilità ex d.lgs. 231/2001: la nuova fattispecie del d.l. 105/2019*, consultabile *online* al sito *quotidianogiuridico.it*; Servizio Studi del Senato e della

2. Il reato previsto dall'art. 1, comma 11

Come sempre accade ogni volta che il legislatore introduce una nuova fattispecie di reato o di responsabilità a carico degli enti, il decreto legge 155/2019 ha fin da subito attirato l'attenzione degli addetti ai lavori: giuristi, ma anche imprese, preoccupate di dover ridefinire la propria politica interna di contrasto e di prevenzione dei reati, per non incorrere in sanzioni.

A maggior ragione, ciò è avvenuto nel caso di specie, dal momento che il decreto ha ad oggetto una materia – quella dei rischi correlati all'impiego delle moderne tecnologie cibernetiche – che, come si sa, rappresenta una priorità e un'urgenza dei nostri tempi, tant'è vero che, al tentativo di farvi fronte, negli ultimi anni sono stati dedicati diversi atti e provvedimenti normativi, non solo in ambito nazionale, ma anche e soprattutto a livello internazionale, europeo e non[2].

Cionondimeno, allo stato, per quel che riguarda il reato di cui si discute (ma non solo), tutto è ancora avvolto da grande indeterminatezza.

Il punto, infatti, è che i requisiti essenziali della nuova fattispecie sono ancora in gran parte da definire per mezzo di decreti e di regolamenti da adottare nel corso dei prossimi mesi e, perciò, vi è già stato chi ha qualificato la norma come "*vera e propria norma*

Camera dei Deputati, Dossier 30 settembre 2019, *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*, consultabile *online* al sito *camera.it*

[2] A titolo di mero (e non esaustivo) esempio, tra i più recenti si possono ricordare il *G7 declaration on responsible States behavior in cyberspace*, il *G7 actions for enhancing cybersecurity for business* e, in ambito comunitario, il Regolamento 679/2016 e la Direttiva 1148/2016 (cd. 'Direttiva NIS', acronimo di *Network and Information Security*): sono tutti atti finalizzati, appunto, alla tutela di specifici profili di sicurezza informatica. In particolare, quella che ha più specifica attinenza con le questioni disciplinate dalla legge in commento è la Direttiva NIS che ha, infatti, affrontato per la prima volta a livello europeo proprio il problema delle misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, rivolgendo la sua attenzione direttamente agli operatori, ai fornitori e ai fruitori di servizi informatici in settori nevralgici. Come è noto, ne è conseguito un decreto legislativo, d.lgs. n. 65/2018, che ha imposto l'adozione di misure tecnico-organizzative adeguate alla prevenzione degli incidenti informatici da parte di un novero di soggetti – operatori di servizi essenziali (OSE) e fornitori di servizi digitali (FSD) – operanti in otto settori determinati: energia, trasporti, banche, mercati finanziari, fornitura e distribuzione di acqua potabile, infrastrutture digitali, servizi digitali (quali motori di ricerca, servizi *cloud* e piattaforme di commercio elettronico). Nello stesso periodo in cui sono state emanate le linee guida per gli OSE in ambito NIS (cioè a luglio del 2019), ha poi visto la luce lo schema del disegno di legge sfociato appunto nel d.l. n. 105/2019. Si tratta, per certi versi, di due normative complementari: mentre l'obiettivo della Direttiva NIS e del conseguente d.lgs. 65/2018 è rafforzare la tutela dei servizi civili, cioè quelli i cui malfunzionamenti potrebbero causare danni alla popolazione e al tessuto produttivo, l'obiettivo del d.l. 105/2019 è tutelare tutti quei servizi e relativi operatori pubblici e privati che svolgono un ruolo cruciale per gli interessi dello Stato e i cui malfunzionamenti potrebbero creare pregiudizi per la sicurezza nazionale. Su questi temi cfr., *ex plurimis*, AGNINO, *Cyber security: le novità della legge n. 133/2019*, consultabile *online* al sito *ilpenalista.it*; GIUSTOZZI, *Così il Perimetro di sicurezza nazionale rafforzerà le difese cyber dell'Italia*; v. pure Servizio Studi del Senato e della Camera dei Deputati, cit.

penale in bianco", manifestando "*qualche perplessità alla luce del principio di legalità stabilito dall'art. 25, comma 2, Cost. e dall'art. 7 Convenzione E.D.U.*"[3].

Guardando, ad es., ai **soggetti** che potranno rispondere del nuovo reato, si può ad oggi affermare che la nuova fattispecie abbia previsto un'ipotesi di **reato proprio**, poiché solo coloro che rientreranno nel perimetro saranno assoggettati agli obblighi sopra brevemente riepilogati e alla vigilanza delle preposte autorità, quindi solo loro potranno porre in essere le condotte incriminate.

Chi sono, però, nello specifico?

L'art. 1 si limita a dire che, nel perimetro, saranno ricomprese "*amministrazioni pubbliche, enti e operatori pubblici e privati*", ma affida una più precisa indicazione a un decreto del Presidente del Consiglio dei Ministri, da adottare entro quattro mesi dall'entrata in vigore della legge di conversione.

Quello che è certo è che, in parte, coincideranno coi soggetti destinatari degli obblighi previsti dal d.lgs. 65/2018, cioè i cd. OSE e FSD (v. nota n. 2) e con quelli destinatari delle norme del d.lgs. 259/2003 (codice delle comunicazioni elettroniche): lo prevede il comma 8, che detta i criteri di coordinamento tra gli obblighi imposti dai diversi decreti a carico di un nucleo comune di destinatari.

Anche riguardo alla **condotta**, la norma in commento sconta, ad oggi, una certa genericità: è vero ed è chiaro, infatti, che è sanzionata la violazione di determinati obblighi, secondo determinate modalità (il rilascio di informazioni false o l'omissione di informazioni dovute e l'ostacolo alle funzioni di vigilanza); tuttavia, ancora una volta, i criteri da rispettare per effettuare le comunicazioni previste dal decreto – di fondamentale e intuitiva importanza per stabilire se vi sia stata o meno una violazione – non sono stati individuati e la loro determinazione è rimessa, come sopra, alla normativa secondaria, per cui bisognerà ancora attendere[4].

Al netto di ciò, si possono comunque svolgere un paio di rilievi.

Primo: si tratta di un reato a forma vincolata; la condotta ostativa, cioè, rileva soltanto se posta in essere secondo certe modalità.

Ciò significa che comportamenti ostativi, diversi dal rilascio di informazioni false o dall'omissione di informazioni dovute, non essendo previsti dalla norma, non rilevano.

---

[3] SASSI, *ibidem*.

[4] I criteri per la compilazione degli elenchi di cui al comma 2, lett. b), infatti, dovranno essere individuati dal medesimo decreto del Presidente del Consiglio dei Ministri che – come detto, entro quattro mesi dall'entrata in vigore della legge di conversione – specificherà chi siano i soggetti ricompresi nel perimetro, mentre quelli per le comunicazioni in caso di affidamenti, di cui al comma 6, lett. a), saranno individuati, entro dieci mesi dall'entrata in vigore della legge di conversione, da un regolamento da adottare ai sensi dell'art. 17, comma 1, l. 23 agosto 1988, n. 400.

Quindi, alcune condotte – quali l'occultamento di documenti, la loro distruzione, ecc. – si collocano al di fuori dell'ambito del penalmente rilevante nonostante la loro intrinseca valenza fuorviante, specie rispetto all'esercizio delle funzioni di vigilanza, che avrebbe forse potuto beneficiare di più ampia tutela.

A questo proposito, è quasi automatico fare un parallelismo (e sottolineare le differenze) con l'art. 2638 c.c. che, nel punire l'ostacolo alle funzioni di vigilanza esercitate nei confronti delle società, incrimina anche l'ostacolo frapposto "*con altri mezzi fraudolenti*", diversi dall'esposizione di fatti materiali non rispondenti al vero.

Secondo rilievo: come detto, il testo della norma fa riferimento soltanto ai procedimenti di formazione degli elenchi (di cui al comma 2, lett. b)), ai procedimenti di affidamento (di cui al comma 6, lett. a)) e alla funzione di vigilanza (di cui al comma 6, lett. c)); non è punito il rilascio di informazioni false o l'omissione di determinate informazioni al CSIRT in caso di incidenti.

Non è detto, tuttavia, che tali ultime condotte siano del tutto irrilevanti (penalmente), se l'eventuale incidente sia oggetto di inchiesta da parte delle autorità preposte alla vigilanza, dal momento che, come detto, la vigilanza è esercitata **anche** rispetto agli obblighi di informazione previsti in caso di incidenti.

In altri termini, le medesime false informazioni rilasciate e/o le medesime informazioni omesse che, se rivolte al CSIRT, non hanno alcuna valenza penalmente, potrebbero invece averla se rivolte alla Presidenza del Consiglio dei Ministri o al Ministero dello sviluppo economico (in sede ispettiva e di vigilanza).

Se così fosse, tuttavia, la norma presenterebbe quantomeno profili di irragionevolezza, dal momento che, in caso di incidente, tutelerebbe in maniera del tutto difforme (e meno severa) l'ipotesi in cui la condotta fuorviante sia indirizzata verso il soggetto dotato dei poteri e delle competenze tecniche per intervenire nell'immediatezza (cioè il CSIRT) rispetto all'ipotesi in cui le medesime condotte siano indirizzate verso gli ispettori (che solitamente intervengono a maggior distanza di tempo dall'evento, quando i suoi effetti sono ormai irreversibili e si tratta, ormai, soltanto di accertare le responsabilità).

Quanto all'**elemento soggettivo**, il reato è a **dolo specifico**: la condotta rileverà solo ed esclusivamente se finalizzata a ostacolare il monitoraggio da parte delle preposte autorità.

Non basta, quindi, il consapevole rilascio di informazioni non vere né è sufficiente la consapevole omissione di informazioni, ma è richiesto un *quid pluris*, cioè l'intento di fuorviare.

Il disvalore penale sta tutto lì: non già e non tanto nella condotta materiale, che attenta in concreto alle finalità perseguite dal decreto e che, in alcuni casi ("*il mancato adempimento degli obblighi di predisposizione delle reti, dei sistemi informativi e dei*

servizi informatici di cui al comma 2, lettera b)" e "*la mancata comunicazione di cui al comma 6, lettera a)*", cfr. comma 9), è già presidiata da responsabilità amministrativa, bensì nell'elemento soggettivo che l'accompagna, che notoriamente pone difficili questioni probatorie.

La funzione del dolo specifico, del resto, è tipicamente selettiva: in una gamma condotte materiali assolutamente identiche, e produttive in concreto di identiche conseguenze, attribuisce rilevanza solo e soltanto a quelle che siano state poste in essere con un certo intento soggettivo dell'agente.

Ai fini dell'integrazione del reato, comunque, non è necessario che l'obiettivo perseguito sia raggiunto: si tratta, infatti, di un **reato di pericolo** e il fatto che debba trattarsi di informazioni (false o omesse) '***rilevanti***' induce a ritenere che – nonostante il requisito non sia espressamente richiesto dalla norma – si tratti di pericolo concreto.

Quanto al **trattamento sanzionatorio**, come detto, il reato è punito con la reclusione da uno a tre anni, a seguito della scelta del legislatore al momento della conversione, allorché ha mitigato il massimo edittale che prima arrivava fino a cinque anni.

Sul **piano processuale**, ciò ha comportato che il reato non consenta l'applicazione di misure coercitive (applicabili solo qualora la pena massima prevista sia superiore nel massimo a quattro anni e, per la custodia cautelare in carcere, non inferiore a cinque anni).

Inoltre, dal momento che la pena massima è inferiore a quattro anni di reclusione, è prevista la citazione diretta dinnanzi al Tribunale monocratico.

3. La responsabilità a carico delle persone giuridiche prevista dall'art. 1, comma 11 *bis*

Il comma 11 *bis* si colloca su una linea di perfetta continuità col percorso intrapreso dal legislatore nell'ormai lontano 2008, quando introdusse nel d.lgs. 213/2001 l'art. 24 *bis*, inserendo per la prima volta, tra i reati presupposto della responsabilità degli enti, anche quelli cd. informatici.

Come per tutti gli altri reati presupposto, anche in questo caso vale ovviamente il rilievo per cui sarebbe utopistica la pretesa di un controllo, da parte dell'ente, tanto capillare da azzerare completamente il rischio che certe condotte vengano poste in essere, anche perché le possibilità di controllo e di prevenzione vanno pur sempre contemperate con coi diritti dei controllati (tutelati dalle norme sulla privacy e dallo Statuto dei lavoratori[5]).

Ad ogni buon conto, alla luce della nuova normativa le imprese saranno chiamate a implementare i propri modelli prevedendo misure idonee a gestire i nuovi rischi che

[5] Su questi temi, cfr. *ex plurimis* DEZZANI – DELL'AGNOLA, *La prevenzione dei reati informatici nel rispetto dei diritti del lavoratore*, in *Resp. amm. soc. enti*, 2009, f. 3, pp. 133 ss..

potranno conseguire alla violazione degli obblighi sanzionati penalmente dal comma 11.

In breve: si tratterà di rivedere e di aggiornare i modelli esistenti in maniera tale che, anche rispetto al reato previsto dal comma 11, la politica aziendale preveda e attui tutto quanto nelle sue possibilità per prevenirne la commissione.

In particolare, sul versante operativo, i modelli dovranno prevedere:

- un adeguato programma di formazione del personale, con riferimento alla materia disciplinata dalla legge in commento;
- l'attribuzione di ruoli e di responsabilità nell'ambito dei diversi settori dell'organizzazione, in relazione ai rischi conseguenti alla violazione degli obblighi presidiati da sanzione penale dal comma 11;
- adeguati flussi informativi verso l'OdV, tali da consentire allo stesso di individuare le anomalie suscettibili di approfondimento;
- l'introduzione di procedure di rilevazione e di gestione del rischio di trasmissione di informazioni false, di omissione di informazioni dovute o di ostacolo alle funzioni di vigilanza da parte della Presidenza del Consiglio dei Ministri o del Ministero dello sviluppo economico;
- l'individuazione, all'interno di ciascuna impresa, delle cd. attività sensibili che, rispetto al reato previsto dal comma 11: saranno tutte quelle che comportano un ruolo e una responsabilità nell'elaborazione degli elenchi di cui si è più volte detto, nonché nella loro trasmissione alle preposte autorità, nell'elaborazione delle comunicazioni in caso di affidamenti e nella gestione dei flussi informativi con la Presidenza del Consiglio dei Ministri e con il Ministero dello sviluppo economico;
- l'aggiornamento delle regole di comportamento, sia sotto il profilo dei divieti, sia sotto il profilo degli obblighi di condotta, sia sotto il profilo della vigilanza interna a che la condotta dei vertici aziendale sia rispettosa delle nuove regole.

Anche il Codice Etico e il Codice Disciplinare dovranno essere implementati: il primo mediante l'esplicitazione dell'impegno al rispetto dei principi sottesi alla nuova normativa, il secondo mediante la previsione di sanzioni specifiche per i trasgressori dei principi espressi nel Codice Etico e dei protocolli riguardanti le comunicazioni che l'ente dovrà effettuare.

Ciò detto, vi è da chiedersi, per concludere, quanto in concreto questa nuova fattispecie sia destinata a trovare spazio.

Non solo perché è presumibile che, nel perimetro, saranno inclusi prevalentemente soggetti pubblici, cui, come è noto, non si applicano le disposizioni previste dal d.lgs. 231/2001 (per l'esclusione prevista dall'art. 1, comma 3), ma anche per quanto detto al punto precedente: il legislatore ha delimitato la fattispecie del reato presupposto mediante alcuni accorgimenti (la forma vincolata della condotta e il dolo specifico), che hanno circoscritto a monte, riducendole a situazioni residuali, le ipotesi di rilevanza penale.

Quindi, se non tutte le forme di ostacolo ai procedimenti previsti dai commi 2 e 6 e alle funzioni di vigilanza daranno luogo a responsabilità penale (v. quanto detto sopra a proposito dell'occultamento e della distruzione di documenti), a maggior ragione non daranno luogo a ipotesi di responsabilità a carico degli enti, che presuppone un requisito/filtro ulteriore, cioè che il reato sia stato commesso "*nel suo* (cioè dell'ente, ndr) *interesse o a suo vantaggio*"; "*l'ente non risponde*" per comportamenti di chi abbia "*agito nell'interesse esclusivo proprio o di terzi*" (art. 5 d.lgs. 231/2001).

La società è, infatti, rimproverabile per il fatto di reato commesso dal dipendente se – e solo se – questo sia frutto di una politica aziendale che consenta che gli interessi dell'impresa siano perseguiti mediante la commissione di reati. Viceversa, un reato commesso da un dipendente o da un apicale infedele, del tutto estraneo agli interessi dell'impresa, e magari persino dannoso per essa, non può che restare rimproverabile alla sola persona fisica.

Perciò, da un lato, ai fini dell'integrazione della fattispecie penale, assume rilevanza centrale l'intento ostativo dell'agente; dall'altro lato, ai fini dell'integrazione dell'illecito da parte dell'ente, assumono rilevanza centrale il suo interesse o il suo vantaggio.

Non è detto che, in concreto, i due presupposti siano sempre consequenziali.

Si possono ipotizzare, infatti, casi in cui l'agente intenda ostacolare le procedure e la vigilanza non già nell'interesse o a vantaggio dell'ente, ma per suo esclusivo personale tornaconto.

Ad es., può ipotizzarsi il caso in cui, in occasione di una verifica, uno dei vertici aziendali intenda fuorviare le attività ispettive affinché non emergano sue precedenti condotte, magari suoi precedenti illeciti professionali, nei confronti dell'ente.

In situazioni simili, difficilmente potrà dirsi (anzi, lo si dovrà escludere) che la condotta – ancorché integrante tutti i presupposti previsti dal comma 11 – sia stata tenuta nell'interesse o a vantaggio dell'ente, che è invece doppiamente danneggiato dal comportamento fraudolento del suo esponente: prima, dalle sue originarie mancanze o dai suoi originari illeciti e, poi, per essere stato esposto al rischio di un procedimento *ex* d.lgs. 231/2001.

È prevedibile, comunque, che i requisiti dell'interesse e del vantaggio verranno rapportati ai risparmi di spesa sottesi alla condotta incriminata e, quindi, ai risparmi per l'adozione delle misure tecniche e preventive che l'inclusione nel perimetro comporta.

Perciò, la previsione di questa nuova ipotesi di responsabilità a carico degli enti rappresenta senz'altro uno stimolo, per le imprese, ad un serio impegno per la promozione della sicurezza.

Naturalmente, questi temi, così come tutti i precedenti, potranno essere oggetto di maggiori e più concreti approfondimenti quando i vari atti normativi, da cui dipende l'operatività della legge in commento, saranno emessi.