ORRICK

Corporate Law Alert

SETTEMBRE 2013

AGGIORNAMENTO NORMATIVO: I NUOVI REATI PRESUPPOSTO EX D.LGS. 231/2001

A cura del Dipartimento italiano Corporate

Alessandro De Nicola
adenicola@orrick.com

Diego Rigatti
drigatti@orrick.com

Con l'articolo 9 comma 2 del D.L. 14 agosto 2013, n. 93 recante "*Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle provincie*" entrato in vigore lo scorso 17 agosto (il "**D.L.**") il Governo ha ampliato il novero dei cd. reati presupposto di cui al D.Lgs. 8 giugno 2001, n. 231 (il "**Decreto 231**"). In attesa della conversione del D.L., si espongono brevemente qui di seguito le novità che impattano sulla disciplina della responsabilità amministrativa degli enti ai sensi del Decreto 231.

Il citato articolo 9 comma 2 del Decreto recita testualmente: "*All'articolo 24-bis comma 1 del decreto legislativo 8 giugno 2001, n. 231 le parole "e 635 quinquies" sono sostituite dalle seguenti: "635 quinquies e 640-ter, terzo comma," e dopo le parole: "codice penale" sono aggiunte le seguenti: "nonché dei delitti di cui agli articoli 55, comma 9, del decreto legislativo 21 novembre 2007, n. 231, e di cui alla Parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196".*

Il legislatore ha dunque stabilito l'introduzione di una serie di nuove fattispecie penali nel Decreto 231 attraverso la modifica dell'art. 24-*bis* comma 1[1].

1. I DELITTI IN MATERIA DI *PRIVACY*

Il D.L. ha introdotto nel catalogo dei reati da cui può scaturire la responsabilità amministrativa dell'ente i delitti in materia di violazione della *privacy* previsti dal D.Lgs. 30 giugno 2003, n. 196 (il "**Codice della *Privacy***")[2],

[1] Per i reati introdotti nel *corpus* del Decreto 231 è prevista a carico dell'ente una sanzione pecuniaria che va da cento a cinquecento quote nonché le sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

[2] Con riferimento all'ambito di applicazione di tali illeciti, bisognerà considerare l'art. 5 del Codice della Privacy, riferito a tutte le disposizioni contenute al suo interno(e dunque comprese anche quelle penali). Ai sensi del comma 1"*Il presente codice disciplina il*

ovvero le fattispecie di trattamento illecito dei dati (art. 167 del Codice della *Privacy*), di falsità nelle dichiarazioni al Garante (art. 168 del Codice della *Privacy*) e di inosservanza dei provvedimenti del Garante (art. 170 del Codice della *Privacy*).

Tale novella, come fatto notare dalla recente relazione della Corte di Cassazione[3], risulta essere di grande impatto, soprattutto per la configurazione della responsabilità da reato degli enti per l'illecito trattamento dei dati, violazione potenzialmente in grado di interessare l'intera platea delle società e delle associazioni private.

Diverrà dunque necessaria da parte degli enti l'adeguamento del proprio modello organizzativo mediante un apposita sezione che preveda un raccordo con il sistema di gestione del trattamento dei dati adottato dalla società ovvero, in assenza di quest'ultimo, un vero e proprio sistema di tutela della *privacy* integrato nel modello organizzativo.

1.2 ILLECITO TRATTAMENTO DEI DATI PERSONALI (ART. 167 CODICE DELLA *PRIVACY*)

Ai sensi del primo comma dell'art. 167 del Codice della Privacy "*Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi*".

Ai sensi del secondo comma, "*Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni*".

La norma tutela il diritto degli interessati alla riservatezza dei dati personali, nonché il diritto a un corretto trattamento di quest'ultimi.

Il delitto in esame è stato costruito con la tecnica del rinvio. Le condotte punibili sono quelle realizzatesi in violazione delle disposizioni richiamate dall'art 167 del Codice della *Privacy* e idonee a procurare un "*nocumento"* nei confronti della persona offesa. Tra queste alcune si riferiscono solamente a soggetti pubblici, come quelle presenti negli articoli 18 e 19 (trattamenti effettuati da soggetti pubblici e principi applicabili in materia di dati

---

trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato" Ai sensi del comma 2 "*Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea …*".

[3] Relazione n. III/01/13

diversi da quelli sensibili e giudiziari), e negli artt. 20, 21, 22 (trattamento di dati sensibili e giudiziari effettuato da soggetti pubblici).

Le violazioni riferibili ai soggetti privati sono invece quelle di cui all'art. 23 (che disciplina la prestazione del consenso al trattamento dei dati), art. 123 (trattamento dei dati relativi al traffico), art. 126 (trattamento dei dati relativi all'ubicazione), art. 130 (comunicazione indesiderate), ovvero le violazioni commesse in applicazione delle disposizioni di cui all'art. 129 (elenchi abbonati), art. 17 (trattamento che presenta dei rischi specifici); art. 25 (divieto di comunicazione e di diffusione di dati); artt. 26 e 27 (garanzie per i dati sensibili o giudiziari da parte di privati), e art. 45 (trasferimenti vietati all'estero).

Ai fini della sussistenza dell'elemento soggettivo, per l'integrazione del delitto di cui all'art. 167, è richiesto nell'agente il dolo specifico, consistente nel "*fine di trarne per sé o per altri profitto o di recare ad altri un danno".*

La fattispecie di cui all'art. 167 del Codice della *Privacy* costituisce senza dubbio una delle disposizioni centrali dell'interna normativa sulla *privacy* e pertanto sarà in grado di interessare l'intera platea degli enti privati soggetti alle disposizioni del Decreto 231.

1.3 FALSITÀ NELLE DICHIARAZIONI E NOTIFICAZIONI AL GARANTE (ART. 168 DEL CODICE DELLA *PRIVACY*)

La fattispecie di cui all'art. 168 del Codice della privacy punisce la condotta di "*chiunque, nelle comunicazioni di cui all'articolo 32-bis, commi 1 e 8, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi … salvo che il fatto costituisca più grave reato … omissis ".*

Il delitto in esame tutela il corretto svolgimento della funzione di vigilanza e dell'attività svolte dal Garante. La norma consente un'applicazione particolarmente estensiva, sebbene anche in quest'ipotesi l'art. 168 richiami ulteriori disposizioni presenti nel Codice della Privacy, quali quelle di cui all'art. 32-*bis*[4], (adempimenti conseguenti ad una violazione di dati personali), e all'art. 37 (notificazione del trattamento)[5].

---

[4] Art. 32-*bis*, commi 1 e 8 del Codice della Privacy (Adempimenti conseguenti ad una violazione di dati personali). 1. "*In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione al Garante*". 8. "*Nel caso in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico affidi l'erogazione del predetto servizio ad altri soggetti, gli stessi sono tenuti a comunicare al fornitore senza indebito ritardo tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti di cui al presente articolo*".

[5] Ai sensi dell'art. 37 del Codice della Privacy (Notificazione del trattamento) la notifica al garante va effettuata solamente qualora il trattamento riguardi alcune tipologie di dati quali: a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica; b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della

Ai fini della sussistenza dell'elemento soggettivo, per l'integrazione delitto di cui all'art. 168, è sufficiente il mero dolo generico in capo all'agente.

1.4 INOSSERVANZA DEI PROVVEDIMENTI DEL GARANTE (ART. 170 DEL CODICE DELLA *PRIVACY*)

La norma punisce "*chiunque essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c)*".

Più precisamente l'articolo 170 del Codice della Privacy punisce l'inosservanza dei provvedimenti del Garante emessi in materia di dati sensibili (art. 26 comma 2), di dati genetici (art. 90), in materia di blocco del trattamento (art. 143, comma 1, lettera c), e in materia di provvedimenti conseguenti alla presentazione del ricorso (art. 150, commi 1 e 2).

A differenza di quanto previsto a proposito di trattamento illecito dei dati (art. 167 Codice della *Privacy*), per l'integrazione del delitto in commento non è richiesto il verificarsi di alcun "*nocumento*"nei confronti della persona offesa. Ciò comporta un'anticipazione della soglia di punibilità alla mera inosservanza di quanto stabilito dal Garante della *Privacy*.

Assumerà dunque fondamentale importanza il rispetto dei provvedimenti emessi dal Garante della *Privacy*, sopratutto in tema di trattamento dei dati del lavoratore (anche per i c.d. controlli difensivi), di uso di internet e della posta elettronica, di amministratore di sistema.

Sarà anche necessario per le società e gli enti privati procedere a una revisione delle modalità di gestione delle segnalazioni interne di potenziali illeciti (c.d. *whistleblowing*)[6], dal momento che quest'ultime potrebbero contenere dati personali, magari anche sensibili e giudiziari.

---

spesa sanitaria; c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale; d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti; e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie; f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti. L'elencazione non è tassativa, dal momento che il Garante può individuare con proprio provvedimento altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità di trattamento o della natura dei dati personali.

[6] Il termine "*whistleblower"* indica quel lavoratore che denuncia al datore di lavoro, anche in forma anonima, un proprio collega o superiore, scoperto a commettere un illecito. Il Decreto 231 ha indotto molte società a introdurre specifiche procedure interne per la raccolta e la gestione di segnalazioni (anche in via anonima) di possibili illeciti, al fine di attivare tempestivamente l'intervento degli organi preposti al controllo delle eventuali infrazioni commesse (primo fra tutti l'Organismo di Vigilanza previsto dal Decreto 231).Già nel passato l'Autorità Garante non aveva mancato di segnalare a Parlamento e Governo l'opportunità di un intervento normativo per disciplinare i sistemi di segnalazione (cd. "*whistleblowing*"), dati gli evidenti profili di interferenza di tale fenomeno con la disciplina di protezione dei dati. Cfr. doc. web n. 1693019 sul sito istituzionale www.garanteprivacy.it.

2. LA FRODE INFORMATICA COMMESSA TRAMITE SOSTITUZIONE DELL'IDENTITÀ DIGITALE

È stato innanzitutto introdotto nel catalogo dei reati presupposto la nuova aggravante ad effetto speciale del delitto di frode informatica di cui all'art. 640-*ter* comma 3 del codice penale, fattispecie inserita nel codice penale dal medesimo D.L., al comma 1 dell'articolo 9. Il delitto in oggetto andrà ad integrarsi qualora la frode informatica venga commessa con sostituzione dell'identità digitale in danno di uno o più soggetti. Con tale norma il legislatore ha voluto dunque implementare la tutela dell'identità digitale, punendo più severamente le frodi realizzate mediante l'accesso abusivo ad un sistema informatico attuato attraverso l'indebito utilizzo dell'identità digitale altrui.

Per quanto riguarda gli effetti di tale nuovo reato sui modelli organizzativi adottati dagli enti ai fini della prevenzione della responsabilità amministrativa, le società dovranno procedere ad un riesame dei presidi esistenti nei propri modelli e, in particolare, di quelli posti a tutela del corretto uso delle apparecchiature *hardware* e *software* in possesso del personale, generalmente presenti nei modelli a seguito dell'introduzione dei cd. reati informatici all'art. 24-*bis* del Decreto 231 da parte della Legge 18 marzo 2008, n. 48.

3. L'INDEBITO UTILIZZO, LA FALSIFICAZIONE, L'ALTERAZIONE E LA RICETTAZIONE DI CARTE DI CREDITO O DI PAGAMENTO

Con l'articolo 9 del D.L. è stato altresì introdotto nel novero dei reati 231 il reato di indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento di cui all'art. 55 comma 9 del D.Lgs. 21 novembre 2007, n. 231. [7]

L'introduzione di questo reato quale presupposto della responsabilità amministrativa degli enti implica la necessità di integrare i presidi attualmente previsti dalla parte speciale per la prevenzione dei reati cd. di riciclaggio introdotti dall'art. 25-*octies* del Decreto da parte del D.Lgs. 21 novembre 2007, n. 231. Tale integrazione dovrà essere preceduta da un approfondito *assessment* che si renderà necessario soprattutto per le società operanti nel settore dell'*e-commerce* e per le società finanziarie.

[7] Articolo 55 comma 9 Decreto Legislativo 231/2007 (c.d. Legge Antiriciclaggio): Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi