Powerful Insights.
Proven Delivery.®

FLASH REPORT

Integrazioni al D.Lgs. 231/2001 a seguito dell'entrata in vigore del Decreto Legge 93/2013

Settembre 2013

Il **17 agosto scorso è entrato in vigore** il Decreto Legge 93/2013 (*"Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province"*), pubblicato sulla Gazzetta Ufficiale 16 agosto 2013, n. 191.

All'art. 9, tale Decreto ha integrato il primo comma dell'art. 24-bis del D.Lgs. 231/2001, ampliando il catalogo dei reati per i quali è prevista la responsabilità amministrativa delle Società e, in particolare:

- frode informatica con sostituzione dell'identità digitale;
- indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento;
- delitti in materia di violazione della *privacy* previsti dal D.Lgs. 196/2003.

Gli effetti del Decreto Legge perderanno efficacia qualora esso non venga convertito in Legge dal Parlamento **entro 60 giorni** dalla pubblicazione in Gazzetta Ufficiale.

I nuovi reati

Le nuove fattispecie rilevanti ai fini del D. Lgs. 231/2001, introdotte lo scorso agosto, sono le seguenti:

a. *Frode informatica con sostituzione dell'identità digitale*

Il Decreto Legge ha provveduto, in primo luogo, ad integrare l'art. 640-ter del codice penale, prevedendo un'aggravante al delitto di frode informatica qualora essa sia realizzata "*con sostituzione dell'identità digitale in danno di uno o più soggetti*".

Si precisa che, prima di quest'ultimo intervento normativo, la frode informatica costituiva una fattispecie rilevante ai sensi del D.Lgs. 231/2001 (art. 24-bis, comma 1) solamente se commessa ai danni dello Stato o di altro Ente pubblico.

Con l'entrata in vigore del Decreto Legge 93 dell'agosto 2013, la frode informatica, se realizzata con sostituzione dell'identità digitale, diventa rilevante, ai sensi del D.Lgs. 231/2001, qualora sia commessa **in danno di qualsiasi soggetto terzo**, ivi inclusa la Pubblica Amministrazione.

b. *Indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento*

La seconda integrazione riguarda i delitti di cui all'art. 55, comma 9 (Sanzioni penali), del Decreto Legislativo 21 novembre 2007, n. 231 (c.d. Decreto Antiriciclaggio).

Tale articolo punisce chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizzi, non essendone titolare, falsifichi o alteri 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 ovvero possieda, ceda o acquisisca tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

protiviti®
Risk & Business Consulting.
Internal Audit.

c. *Delitti in materia di violazione della privacy previsti dal D.Lgs. 196/2003*

L'integrazione relativa ai "delitti (...) di cui alla Parte III, Titolo III, Capo II del Decreto Legislativo 30 giugno 2003, n. 196" (il *Codice in materia di protezione dei dati personali* o *Testo Unico sulla Privacy*[1] - di seguito anche "Codice", "Codice Privacy") riguarda i seguenti reati[2]:

- **trattamento illecito di dati** (art. 167): punisce la condotta di chiunque effettui il trattamento di dati personali in violazione a quanto disposto dal Codice Privacy, articoli 17, 20, 21, 22 (commi 8 e 11), 25, 26, 27 e 45, al fine di trarne profitto per sé o per altri oppure di recare un danno ad altri.

  Esempi di tali condotte sono:

  - impiego di dati personali, tramite sistemi telematici e non, per finalità commerciali, di *direct marketing*, o ricerche di mercato, di Interessati iscritti al Registro Pubblico delle Opposizioni o che hanno negato il consenso al trattamento dei propri dati per tali finalità;
  - trasferimento dei dati personali, senza il consenso espresso degli Interessati, in Paesi extra EU che non offrono un adeguato livello di protezione, diffusione e/o comunicazione di dati sensibili e giudiziari non previsti da espressa disposizione di legge.

- **falsità nelle dichiarazioni e notificazioni al Garante** (art. 168): punibile nel caso in cui si dichiarino o attestino false notizie o circostanze o si producano atti o documenti falsi in occasione di:

  - comunicazioni previste dai commi 1 ed 8 dell'art. 32-bis del Codice a seguito della violazione dei dati personali;
  - notificazioni previste dall'art. 37 del Codice, nel caso in cui il trattamento riguardi, a titolo esemplificativo, dati sensibili registrati al fine di selezionare del personale per conto terzi;
  - comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti.

- **inosservanza di provvedimenti del Garante** (art. 170): commesso da chi, pur essendovi tenuto, non osservi le indicazioni fornite dal Garante:

  - in merito al trattamento di dati sensibili (art. 26, comma 2);
  - in merito al trattamento di dati genetici (art. 90);
  - nei provvedimenti emanati a seguito di ricorso (art. 150, comma 1 e 2);
  - nei provvedimenti di blocco o divieto del trattamento che risulti illecito, emanati a seguito di reclamo (art. 143, comma 1, lettera c).

Le sanzioni 231

Come detto, le novità legislative hanno tutte riguardato il primo comma dell'art. 24-bis del D.Lgs. 231/2001 e, pertanto, come per gli altri reati previsti da tale comma, si applicano:

- **sanzioni pecuniarie**
  - da 100 a 500 quote;
- **sanzioni interdittive**
  - interdizione dall'esercizio dell'attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di pubblicizzare beni o servizi.

Tali sanzioni si aggiungono al quadro sanzionatorio previsto dal Codice Privacy, che nel caso specifico è di tipo **penale**.

[1] Sebbene già prima dell'integrazione dell'agosto scorso l'art. 24-bis del D. Lgs. 231/2001 fosse rubricato *Reati informatici e trattamento illecito dei dati*, non era prevista alcuna fattispecie criminosa relativa alla normativa sulla *privacy*.

[2] Non costituiscono reato-presupposto le contravvenzioni di cui agli artt. 169 (omessa adozione delle misure minime di sicurezza) e 171 (violazione delle disposizioni di cui agli articoli 113,comma 1, e 114).

Considerazioni

La Corte di Cassazione, nella Relazione III/01/2013 del 22 agosto, ha già illustrato e commentato le novità legislative introdotte, effettuando una valutazione in merito al potenziale impatto delle ultime integrazioni al D.Lgs. 231/2001 e giungendo alla conclusione che il maggiore impatto si ha per la configurazione della responsabilità da reato per i delitti in materia di violazione della *privacy:* **"violazione *potenzialmente in grado di interessare l'intera platea delle società commerciali e delle associazioni private soggette alle disposizioni del D.Lgs. 231/2001*"**[3].

Inoltre, si evidenzia che, mentre per il trattamento illecito di dati (art. 167), la configurazione del reato presuppone che il trasgressore ne abbia tratto profitto e che la violazione abbia prodotto un danno a terzi, nel caso dei reati di cui agli art. 168 e 170, è sufficiente il dolo generico in capo all'agente.

Diverrà dunque necessario, da parte degli Enti, l'adeguamento del proprio modello organizzativo mediante un'apposita sezione che preveda:

- il raccordo con il sistema di gestione dei dati e con il modello di *governance* della *privacy* adottati dalla società;
- l'implementazione di un sistema di tutela della *privacy* integrato nel modello organizzativo, qualora non presente;
- l'analisi dell'impianto documentale (e.g. Policy, Procedure, Regolamenti) in materia di *privacy* (D.Lgs. 196/2003 e s.m.i., provvedimenti del Garante Privacy) ai fini dell'individuazione delle aree di miglioramento.

Per tale ragione, un primo spunto operativo potrebbe essere rappresentato dall'esecuzione di attività quali:

- analisi dell'impianto documentale (e.g. Policy, Procedure, Regolamenti) in materia di Privacy;
- individuazione dei soggetti - interni ed esterni - coinvolti nel processo di trattamento dei dati personali;
- analisi volta alla comprensione del modello di gestione della Privacy adottato in azienda.

Tali attività saranno finalizzate all'individuazione dei *gap* esistenti ed all'implementazione di azioni di *remediation*, in termini di misure organizzative e tecnologiche, idonee a garantire la *compliance* alla normativa vigente.

* * *

Protiviti, da anni impegnata nell'assistenza ai propri Clienti su tematiche "231", è in grado di integrare i propri Team con competenze specifiche per l'analisi dei rischi-reato in ambito di frode informatica con sostituzione di identità digitale, indebito utilizzo di carte di credito o di pagamento e delitti in materia di violazione della *privacy* e può quindi assistere la Vostra organizzazione nella gestione degli adempimenti normativi.

Contatti:

Settore Technology Risk

Hernan Gabrieli
hernan.gabrieli@protiviti.it

Antonello Gargano
antonello.gargano@protiviti.it

Settori Bancario e Finanziario

Luca Medizza
luca.medizza@protiviti.it

Luca Salomoni
luca.salomoni@protiviti.it

Settori Industriale e Commerciale

Emma Marcandalli
emma.marcandalli@protiviti.it

Francesco Lanza
francesco.lanza@protiviti.it

Tel.: +39 02 65506301

[3] Per il testo integrale della Relazione si veda: http://www.cortedicassazione.it/Documenti/Relazione_III_01_13.pdf.