CSA Italy

Responsabilità degli enti per i delitti informatici e trattamento illecito di dati in contesto Cloud Services

---

Settembre 2014

Document Sponsor

Premessa

Obiettivo dello studio è presentare una panoramica degli aspetti connessi al D.Lgs 231/01, relativo alla responsabilità amministrativa degli enti, di principale interesse nel contesto servizi cloud, con particolare riferimento ai rilevanti delitti informatici previsti dal Codice Penale italiano, incluse alcune valutazioni di carattere generale riguardo le applicabili normative Comunitarie in materia di sicurezza informatica, protezione dei dati personali nonché norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi informatici.

Lo studio è rivolto in particolare ai professionisti ed alle organizzazioni che operano in realtà soggette al rispetto del D.Lgs 231/01 e che intendono approfondirne gli aspetti connessi a servizi cloud.

Introduzione

Nell'era del cyberspace il tema della criminalità informatica ha assunto una nuova dimensione ed una rilevanza crescente.

L'incessante diffusione delle tecnologie dell'informazione e della comunicazione per questioni legate principalmente alla riduzione dei costi, all'interoperabilità ed alla standardizzazione ha, da un lato, introdotto nuove opportunità ma, dall'altro, generato il proliferarsi di nuove condotte penalmente rilevanti.

I reati informatici sono facilitati dalla continua evoluzione dello spazio virtuale che consente la delocalizzazione delle risorse e la loro raggiungibilità da ogni luogo e distanza anche, e soprattutto, grazie alla nuova dimensione IT offerta dal Cloud Computing.

Il crimine coinvolge la struttura della tecnologia dell'informazione, compreso l'accesso illegale, l'intercettazione, le interferenze illecite a dati e sistemi, la contraffazione, la frode informatica, il furto di identità digitale e il trattamento illecito dei dati.

Oggigiorno si parla di cybercrime e cybersecurity come inquietanti rischi per lo sviluppo globale, sia per la rilevanza delle infrastrutture critiche informatizzate per l'economia nazionale e la sicurezza, che per l'interazione con le politiche che affrontano la privacy e la protezione dei dati.

In questo scenario si collocano i numerosi interventi legislativi finalizzati, da un lato, a garantire la necessità di tutelare gli interessi legittimi nell'uso e nello sviluppo delle tecnologie informatiche e, dall'altro, a spingere le organizzazioni, sia nel settore pubblico che in quello privato, ad attuare meccanismi interni reali ed efficaci per la salvaguardia della sicurezza delle reti, dei sistemi e dei dati.

Alcuni dei comportamenti che costituiscono una minaccia alla sicurezza informatica, sono stati infatti qualificati all'interno del nostro ordinamento come condotte penalmente perseguibili (es. introduzione di virus informatici, frodi informatiche, sabotaggi, spionaggio, modifica o cancellazione di dati/informazioni, attentati a sistemi informatici che supportano l'erogazione di servizi di pubblica utilità, abusi di privilegi etc..) ed inseriti tra i "reati presupposto" della responsabilità degli enti di cui all'art. 24 bis (Delitti informatici e trattamento illecito di dati) del DLgs. n. 231/2001.

La capacità di garantire la "Regulatory Compliance" e, quindi, diminuire i rischi di commissione dei reati informatici correlati all'utilizzo delle tecnologie ICT, impone:

- L'individuazione delle aree di rischio cd. sensibili in relazione alle "classi di reato presupposto".
- La costruzione di Modelli Organizzativi di gestione e controllo dei rischi che presuppongono:

- l'adozione di misure di sicurezza già espressamente richieste da numerosi previsioni normative (come ad es. il DLgs. 196/2003 ed il Provvedimento del Garante Privacy del 27.11.08);
- l'adozione di misure di sicurezza derivanti da specifiche attività di analisi dei rischi.

Questo studio propone una analisi dello scenario normativo, sia a livello EU che nazionale, di riferimento sulla criminalità e la sicurezza informatica, dal quale mutuare un primo "set" di misure di mitigazione dei rischi ex art. 24 bis del D.Lgs. 231/01 e che deve, dunque, essere tenuto ben presente dagli operatori di servizi basati sul Cloud Computing.

L'attenzione si focalizza in particolare:

- in un'analisi del D.Lgs 231/01 con particolare riferimento alle sue implicazioni in contesti Cloud Computing
- Per quanto riguarda il contesto europeo:
  - sulla proposta di Regolamento EU del 25.1.2012 in materia di Data Protection attualmente in fase di approvazione;
  - sulla recente Direttiva 2013/40/EU, che verrà recepita in Italia entro il 4 settembre 2015;
  - sulla Direttiva 2008/114/EC, recepita in Italia con il decreto legislativo 61/2011 e, successivamente, con la legge n.33/2012;
  - sulla Proposta Direttiva nota come NIS;
  - sul Regolamento UE 611/2013 entrato in 25 agosto del 2013.
- Per quanto riguarda il contesto nazionale:
  - sul DLgs. 196/2003 "Codice in materia di protezione dei dati personale" e relativo Allegato B;
  - sul Provvedimento del 27 novembre del 2008 emanato dall'Autorità Garante in materia di protezione dei dati personali (cd. Provvedimento sugli amministratori di sistema);
  - sulle strategie italiane messe in campo con il D.P.C.M. del 24 gennaio 2013 sul tema della protezione cibernetica e la sicurezza informatica nazionale;
  - sul D.P.C.M. del 27 gennaio 2014 con il quale è stato approvato il "Piano per la protezione cibernetica e la sicurezza informatica".

Le analisi e le considerazioni presentate nello studio riflettono inoltre le impostazioni e le raccomandazioni fornite dal Working Party 29 con la "Opinion 05/2012 on Cloud Computing" del 1° luglio 2012.

Verrà, quindi, proposta una "cross reference map" tra reati informatici presupposto ex art.24 bis del DLgs. 231/01, principi di controllo ICT e misure di mitigazione dei rischi derivanti da quadro normativo analizzato, nonchè una cross reference rispetto ai controlli individuati da Cloud Security Alliance con la sua matrice CCM "Security Control Frameworks For Cloud Providers & Consumers"[1].

[1] https://cloudsecurityalliance.org/research/ccm/

Indice

Si ringrazia

Coordinatore del Gruppo di Lavoro "Legal & Privacy in the Cloud"

Gloria Marcoccio

Autori

Gloria Marcoccio

Giuseppe Serafini

Claudia Ciampi

CSA Staff

Valerio Vertua (coordinatore Comitato Scientifico)

Paolo Foti

Review

Prof. Avv. Giovanni Ziccardi (Comitato Scientifico), Consiglio Direttivo CSA Italy

Document Sponsor

BSI Group Italia

1.0 Panoramica degli aspetti del D. Lgs. 231/01 di principale interesse in contesto cloud services

1.1 Premessa - La trasversalità dell'informatica e della telematica nei processi aziendali, nella commissione e nella prova dei reati presupposto

Un punto di partenza logicamente coerente, ad una ricognizione efficace dei profili giuridici che connettono i principi della responsabilità amministrativa degli enti, di cui al decreto legislativo 231/2001, con i servizi di *Cloud Computing*[2], è dato, a parere di chi scrive, dalla constatazione, da un lato, della trasversalità dell'informatica e della telematica nella maggior parte dei processi aziendali anche decisionali (si pensi per esempio alle decisioni conseguenti all'implementazione di soluzioni di *risk* o vulnerability assessment) e, dall'altro, da un sempre maggiore ricorso, per ragioni di costi, efficienza ed efficacia, a soluzioni di delocalizzazione delle attività di elaborazione e/o di archiviazione dei dati, da parte delle imprese, destinatarie della normativa in esame.

Non vi è, infatti, chi non possa agevolmente constatare che, spesso, la condotta criminale, prevista come fonte di responsabilità dalle disposizioni del decreto legislativo citato, da una parte si può esprimere attraverso strumenti elettronici di elaborazione (pur integrando la fattispecie di un reato c.d. comune) e dall'altra, può essere provata, nei suoi elementi costitutivi, solo facendo ricorso ad operazioni di *digital forensics*[3]; vale a dire, rinvenendo le evidenze, della condotta illecita in sistemi elettronici di elaborazione, sempre più spesso (anche) nella disponibilità, di soggetti terzi (i c.d. *Cloud Service Provider - CSP*), legati all'impresa da vincoli contrattuali di varia natura.

Basti pensare, per fare dei piccoli esempi a quali sarebbero le attività da svolgere per individuare, quando, come e da chi, fossero state compiute condotte, integranti il reato presupposto, di accesso abusivo a sistema informatico o telematico di cui all'art. 615 ter del Codice Penale, sul gestionale della contabilità aziendale, utilizzato in modalità SaaS, al fine di alterarne i dati a vantaggio o nell'interesse dell'ente, piuttosto che, condotte di intercettazione di comunicazioni rilevanti ai sensi dell'art. 617 quater del Codice Penale,

---

2 - Da un punto di vista tecnologico, il principale riferimento per la comprensione del fenomeno "Cloud" è il documento The NIST (National Institute of Standars and Technology) definition of Cloud Computing, Special Publication 800-145 Set. 2011 secondo cui: *"Cloud computing is an evolving paradigm. (...) is a model for enabling ubiquitous, convenient, on demand network acces to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*.

3 - Una definizione di digital forensics coerente con le finalità di questo studio e quella del Digital Forensics Research Workshop del 2001 in base alla quale deve intendersi per digital forensics: *"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and preservation of digital evidence derived from digital sources for the pourpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations". In "Maping the Forensics Standard ISO/IEC 27037 to Cloud Comuting" a cura di Cloud Security Alliance, Incident Management and Forensics Working Group*

perpetrate, da uno dei soggetti da cui promana la responsabilità dell'ente stesso, per procurare un vantaggio a quest'ultimo, acquisendo la disponibilità di informazioni riservate di cui all'art. 98 del Codice in materia di proprietà industriale.

Ebbene, risulta a chi scrive, di intuitiva evidenza, che, in primo luogo, non si potrebbe prescindere, al fine di condurre il giudice ad una valutazione di non riconducibilità della condotta dell'autore del crimine all'ente, da una sistematica verifica dei log degli accessi al gestionale (nel primo esempio), che dovrebbe essere condotta in seguito di operazioni di acquisizione di quei dati, avvenute in modalità tali da preservarne la genuinità e la non alterazione, ma anche, in secondo luogo con ripercussioni non meno importanti, in termini di configurazione del modello di gestione e controllo, da una preventiva organizzazione del flussi di lavoro (i.e. di elaborazione) propri dell'ente, che comprenda sistemi di Identity Access Management e Log Auditing.

1.2 Il Fenomeno della digitalizzazione dei beni e dei rapporti

Ciò chiarito, è ora necessario svolgere, almeno due considerazioni, prima di addentrarci nell'oggetto precipuo di questo studio: la prima, preliminare, di carattere marcatamente giuridico, che attiene in generale al meccanismo di operatività congegnato dal legislatore nella norma che sarà esaminata, per specificare che, essa non sancisce, puramente e semplicemente, la responsabilità amministrativa delle persone giuridiche, come conseguenza del fatto di reato commesso dai soggetti in essa indicati, ma, più propriamente, opera una selezione, assistita dalle garanzie del principio di legalità[4], dei singoli reati dai quali detta responsabilità deriva.

La seconda considerazione è, invece, di carattere meramente fattuale e consegue dalla constatazione della c.d. "*digitalizzazione dei beni e dei rapporti";* si vuol sottolineare, con l'espressione da ultimo impiegata che, ormai, molti dei beni e dei rapporti che prima si caratterizzavano per la loro esistenza nel mondo fisico, si sono spostati, grazie anche anche all'aumentata disponibilità della capacità di elaborazione nella disponibilità dei più, in un ambiente digitale telematicamente interconnesso.

Si pensi, per fare degli esempi, da un lato, al fatto che mentre prima l'attività di creazione intellettuale si svolgeva, sia con riferimento alle opere dell'ingegno, sia con riferimento alle creazioni intellettuali, per lo più, su supporti analogici[5], ora l'intero processo creativo, ivi compresa la prova della data certa[6] da impiegare ai fini dell'attribuzione della paternità di un opera, può svolgersi, interamente mediante strumenti elettronici di elaborazione; e, dall'altro che, sulla falsariga di quanto avvenuto per i beni, anche i rapporti giuridici e gli strumenti economici utili a negoziare ovvero ad acquistare quei beni sono ormai oggetto di digitalizzazione[7], con i vantaggi ed i rischi che ciò comporta.

---

4 - Il Principio di legalità dell'art. 2 del D. Lgs. 231/01 subordina l'applicazione delle misure sanzionatorie ad una previsione legislativa espressa, sia in ordine all'illecito sia in ordine la tipo di sanzione precisando che debba essere entrata in vigore prima della commissione del fatto. Cass. Sez. VI 18 gennaio-12 aprile 2011 N. 14564 in Dir. Pen. Cont. p. 326.

5 - Il foglio di carta che incorporava il progetto o la descrizione dell'invenzione o dell'opera letteraria, piuttosto che il vinile che conteneva l'opera musicale o la pellicola fotografica che conteneva il negativo della fotografia artistica

6 - Non mancano, nemmeno nel nostro paese soggetti che offrono in modalità *SaaS* (*Software As A Service*) strumenti di marcatura temporale.

7 - Ci si riferisce, da un lato, al fatto che prima ancora che con l'esistenza della c.d. moneta elettronica, l'interprete oggi deve confrontarsi con la digitalizzazione dei flussi monetari e del sistema di pagamento con strumenti elettronici e dall'altro, al fatto che la stessa negoziazione di rapporti giuridici avviene mediante le figure ormai note del contratto telematico.

Ciò è tanto vero che la stessa criminalità organizzata si serve, sovente, per finalità di riciclaggio dei proventi delle attività illecite, di strumenti che, da una parte, implicano l'impiego di tecnologie informatiche evolute (ad esempio la compravendita di Bitcoin) e, dall'altra generano, ulteriore profitto illecito attraverso, parimenti, le stesse tecnologie, si pensi ad esempio al *"mining di Bitcoin"* effettuato attraverso la creazione di BotNet[8] ad hoc.

1.3 Il D. Lgs. 231/2001 – Generalità, struttura della responsabilità amministrativa degli enti e trattamento sanzionatorio

Si illustreranno di seguito, senza pretesa di completezza alcuna, prima delle specifiche relazioni intercorrenti tra la norma in esame ed i peculiari rapporti afferenti ad infrastrutture *Cloud Computing*, al solo fine di tracciare un perimetro di nozioni condivise, i tratti generali salienti della disciplina che qui ci occupa, quale risultante dalla vigenza, nel nostro ordinamento delle disposizioni del decreto legislativo 8 giugno 2001 Nr. 231, a seguito delle numerose modificazioni via via intervenute.

Il decreto, la cui adozione deve ricondursi all'ottemperanza del legislatore nazionale a convenzioni internazionali che hanno da tempo imposto meccanismi di imputazione di responsabilità alle persone giuridiche, quali la Convenzione di Bruxelles del 1995 nonché la convenzione OCSE di Parigi del 1997, sulla lotta alla corruzione dei pubblici ufficiali, si caratterizza, come è noto, per avere introdotto, allineando il nostro ordinamento a quello di altri paesi europei, ove la responsabilità delle *societas* ed il conseguente meccanismo sanzionatorio è in opera da tempo, un *tertium genus* di responsabilità, destinata a soggetti diversi dalle persone fisiche[9], conseguente da reato, che coniuga i tratti essenziali del sistema penale e di quello amministrativo.

Si rende, in buona sostanza, responsabile l'ente – senza che si possa parlare di responsabilità oggettiva - prevedendosi la necessità che sussista la c.d. colpa di organizzazione, vale a dire, il deficit organizzativo di non avere predisposto un insieme di accorgimenti preventivi idonei ad evitare la commissione di reati del tipo di quello realizzato[10].

---

8 - Vi sono anche, tra quelli da cui deriva la responsabilità dell'ente, anche i reati informatici, quei reati che, come tali, sono stati codificati, prima con la legge 547/93, poi con la normazione applicativa della convenzione di Budapest sul Cybercrime, a partire dal 2008.

9 - Art. 5 D. Lgs. 231 - *"L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente (...) nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lett. a)"*. In mancanza di una definizione autentica delle funzioni formali di amministrazione, rappresentanza e direzione, si possono utilizzare le norme dettate in altre branche dell'ordinamento così da ricostruire il concetto di amministrazione come legato al potere di gestione e controllo delle risorse materiali dell'ente, il concetto di direzione come legato al potere di gestione e controllo delle risorse umane dell'ente e il concetto di rappresentanza come legato alla formazione, alla manifestazione all'esterno e alla ricezione della volontà dell'ente in relazione agli atti negoziali: si possono così determinare, le cariche rilevanti per il riconoscimento di di soggetto di posizione apicale, indipendentemente dal *nomen juris* utilizzato dall'ente nella sua organizzazione interna (Fattispecie nella quale il Direttore sanitario e il primario di reparto sono stati riconosciuti soggetti apicali). Trib. Riesame Milano (ord), 26 giugno 2008 in Foro ambr., 2008 p. 335

10 - i.e. modelli comportamentali che valutino il rischio reato e siano volti a prevenirlo fissando regole di condotta e predisponendo adeguati controlli.

1.4 Enti destinatari della Norma

In linea generale, si può osservare come, la *ratio* genetica[11] della norma in questione sia da rinvenirsi nell'eliminazione di pericolosi vuoti di responsabilità che, prima della sua entrata in vigore, potevano ravvisarsi - *seppure con i temperamenti previsti, nel caso in cui in cui la persona giuridica fosse civilmente obbligata, o tenuta al pagamento della sanzione pecuniaria - nella maggior parte delle fattispecie di criminalità dei c.d. colletti bianchi.*

Si verificava cioè, che il soggetto, persona giuridica, che, da un punto di vista fattuale e concreto, beneficiava maggiormente delle condotte criminali poste in essere da persone fisiche la cui operatività fosse ad esso riferibile, andasse esente da responsabilità significativa di qualsivoglia natura.

Una analisi, anche solo sommaria, dell'evoluzione, avvenuta nel corso degli ultimi anni, del numero e della tipologia dei c.d. reati reati presupposto *(dalla commissione dei quali ad opera di determinate persone fisiche deriva la responsabilità ulteriore della persona giuridica)*, nella maggior parte espressivi di posizioni protettive di beni giuridici super individuali e sovente, collettivi, induce a ritenere che, attraverso tale specifica normazione, si sia voluto porre in opera un ulteriore, dedicato, strumento di prevenzione generale, al dilagante fenomeno della criminalità d'impresa (più opportunamente, in alcune casi, dell'impresa del crimine[12]). *In tal senso mi pare possa essere sicuramente letta la recente novella legislativa che ha introdotto, tra i reati presupposto quelli c.d. ambientali*[13].

Da un punto di vista interpretativo, un primo dato formale, rilevante, nella individuazione dei limiti applicativi soggettivi, dei meccanismi attributivi di responsabilità, configurati dal sistema del decreto legislativo 231, si rinviene, expressis verbis, nel testo dell'art. 1 che, espressamente, esclude, dal novero dei soggetti nei confronti dei quali tale forma di responsabilità è destinata ad operare, lo Stato, gli Enti Pubblici territoriali, gli altri enti pubblici non economici nonché gli enti che svolgono funzioni di rilievo costituzionale[14].

A contrario, sono quindi da ritenere vincolati dalle disposizioni di legge de quo tutte le persone giuridiche ivi comprese le imprese individuali, ed anche le società ed associazioni prive di personalità giuridica

---

11 - *Amplius* S.M. Corso: Codice della responsabilità “da reato” degli enti annotato con la giurisprudenza. G. Giappichelli Editore, Torino 2012 p. 27.

12 - Nella nuova disciplina vigente per effetto dell'introduzione nel nostro ordinamento del D.Lgs. 231/2001, il fatto-reato commesso dal soggetto inserito nella compagine della societas, in vista del perseguimento dell'interesse o del vantaggio di questa è sicuramente qualificabile come "proprio" anche della persona giuridica e ciò in forza del rapporto di immedesimazione organica che lega il primo alla seconda: la persona fisica che opera nell'ambito delle sue competenze societarie, nell'interesse dell'ente, agisce come organo e non come soggetto da questo distinto; ne la degenerazione di tale attività funzionale in illecito penale è di ostacolo all'immedesimazione - Cass. Sez. VI, 18 febbraio – 16 luglio 2010 nr. 27735, in Resp. Amm, soc. n. 4/2014 p. 164. -.

13 - L’art.2 del D.Lgs. 7 Luglio 2011 n.121, ha in effetti introdotto l’art.25 undecies al D.Lgs. n.231/01 rubricato appunto reati ambientali

14 - Cass. Sez. II, 9 luglio-21 luglio 2010 in Dir. Pen. Proc. 2010 p. 1067 nonché in Riv. Pen n. 6/2011, p.717 Le società a partecipazione mista pubblica e privata, che esercitano una attività di interesse pubblico non sono esonerate dalla disciplina prevista dal d.lgs. n. 231, essendo infatti l'esonero subordinato alla duplice condizione che l'ente medesimo abbia natura pubblicistica e non svolga attività economica, a tale ultima stregua, invece, dovendosi ritenere ascrivibile l'operatività di un ente che sia costituito in forma di società per azioni in considerazione del fatto che, ogni società, proprio in quanto tale, è, infatti costituita per l'esercizio di una attività economica al fine di dividerne gli utili

Ciò chiarito, occorre rilevare ora, che, l'ambito soggettivo ed oggettivo di imputazione all'ente, della responsabilità in commento, risulta, principalmente - *con l'esclusione della responsabilità per il reato commesso nell'interesse esclusivo dei soggetti di seguito indicati, o di terzi e nei limiti di tempo stabiliti dall'art. 3*[15] *del decreto* - dal contenuto degli Artt. 5, 6, 7 del D. Lgs. 231.

In particolare, il paradigma legale di configurazione della predetta responsabilità postula la sussistenza simultanea di almeno due elementi fondamentali, oltre all'avere omesso l'adozione del modello comportamentale di cui si è detto in precedenza, vale a dire: (a). - l'esistenza di un "determinato" rapporto tra l'Ente ed il soggetto agente[16], autore di uno o più reati c.d. presupposto[17]; (b). -la circostanza che, da detto reato, sia derivato un vantaggio[18] per l'ente, ovvero, che tale reato sia stato commesso nell'interesse dell'Ente stesso.

Con riferimento, specificamente, a quanto da ultimo, deve precisarsi che, come è noto ed ampiamente illustrato il giurisprudenza, il concetto giuridico di interesse è sostanzialmente differente da quello di vantaggio, in considerazione del fatto che: il vantaggio è valutabile solo dopo che il reato sia stato portato a compimento[19], mentre l'interesse costituisce la prefigurazione di un indebito arricchimento che sarebbe possibile trarre dalle condotta criminosa ma è indipendente dall'effettiva realizzazione dell'arricchimento.

Per ciò che attiene, invece, l'analisi dei requisiti soggettivi di imputazione della responsabilità all'ente, si può constatare, la configurazione, ad opera del legislatore, nel testo della norma, di un sistema a doppio livello vale a dire, quello afferente i soggetti in posizione apicale[20], individuati alla lettera a) dell'art. 5 e quello dei soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Con riferimento ai soggetti di cui alla lettera a) dell'art. 5, la sussistenza dell'interesse o del vantaggio è sufficiente all'integrazione della responsabilità dell'ente fino a quando sussiste l'immedesimazione organica tra dirigente apicale e l'ente, di tal che, quest'ultimo potrà andare esente da responsabilità, da un lato, se il fatto è commesso dal singolo nell'interesse esclusivo proprio o di terzi, e non sia riconducibile neppure parzialmente all'interesse dell'ente, dall'altro, nel caso in cui non sia più possibile configurare la suddetta immedesimazione, ovvero, infine, allorchè dia prova di avere adottato ed efficacemente attuato, prima della

---

15 - Cfr. Art. 3 d.lgs. 231/2001: *"L'ente non può essere ritenuto responsabile per un fatto che secondo una legge posteriore non costituisce più reato o in relazione al quale non è più prevista la responsabilità amministrativa dell'ente, e, se vi è stata condanna ne cessano l'esecuzione e gli effetti giuridici"*.

16 - Ai sensi dell'art. 26 comma 1 del D.Lgs. 231/2001 pur sussistendo la responsabilità dell'ente: "le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà in relazione alla commissione, nelle forme del tentativo, dei delitti indicati nel decreto.

17 - L'elencazione dei reati presupposto della responsabilità amministrativa, ai sensi dell'art. 2 d. lgs. 231/2001 è tassativa e non è suscettibile di integrazione a mezzo della contestazione di delitti equipollenti o della artificiosa contestazione di elementi costitutivi del del delitto composto. G.u.p. trib. Milano, 3 novembre 2010, in Corr. Merito 2011, p. 285.

18 - Cfr. O. Longo La responsabilità da reato delle persone giuridiche in **filodiritto.com**. Secondo la relazione ministeriale mentre l'interesse caratterizza in modo marcatamente soggettivo la condotta delittuosa della persona fisica e prevede una verifica ex ante, il vantaggio può essere tratto dall'ente anche quando una persona fisica non abbia agito nel suo interesse e prevede una verifica ex post

19 - Cfr. Cass. Sez. II, 20 dicembre 2005 n. 3615.

20 - La nozione di soggetto in posizione apicale nell'ente viene definita dall'esercizio formale di funzioni rappresentanza, amministrazione o direzione, mentre l'esercizio di fatto per essere rilevante deve avere riguardo cumulativamente alle funzioni di gestione e controllo volendosi includere tra i vertici solo quei soggetti che esercitano un penetrante dominio sull'ente.

commissione del fatto, modelli di organizzazione e di gestione idonei ad impedire la commissione di reati del tipo di quello realizzato.

Testualmente, l'art. 6 del D.Lgs. 231/01 dispone che: - Se il reato e' stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che: a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento e' stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi e' stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

Considerazioni specifiche, relativamente agli scopi del presente lavoro, sono da svolgere con riferimento ai soggetti di cui all'art. 5 lettera b, del menzionato articolo 6, vale a dire i soggetto sottoposti alla direzione o alla vigilanza[21] da parte dei soggetti in posizione apicale.

Mentre, come abbiamo visto, vi è, in materia di soggetti che rivestono la posizione apicale, una nutrita giurisprudenza relativamente alla loro individuazione, in concreto, nel tessuto delle compagini societarie oggetto della disciplina, tale disponibilità di riferimenti interpretativi giurisprudenziali non si rinviene a proposito delle altre tipologie di agenti, nè, con riferimento alla individuazione fattuale dei soggetti da ultimo menzionati, soccorre, il testo, invero, ormai datato, della relazione ministeriale [22] di accompagnamento al decreto che qui ci occupa.

1.5 Soggetti in posizione non apicale. Responsabili del Trattamento ed amministratori di sistema

Il linea di principio, si può affermare, che non è necessario che tra l'ente e l'autore del fatto intercorra un rapporto di lavoro subordinato, ma è sufficiente, come dice la norma[23], la sottoposizione ala direzione o alla

---

21 - Cfr. G. De Simone. La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi di imputazione. In diritto penale contemporaneo. p. 28.: "L'estensione della sfera dei possibili autori dell'*Anknüpfungstat* risulta particolarmente opportuna anche in considerazione del fatto che, come attesta la ricerca criminologica, una parte considerevole dei reati d'impresa è acrivibile ai managers in posizione intermedia: sono costoro ad assumere rilevanti decisioni operative e a disporre del bagaglio di informazioni relative alla possibile lesione o messa in pericolo di beni giuridici penalmente tutelati.

22 - Cfr. Rel. Min. al D. Lgs. 231/2001 p. 7 - La seconda categoria di persone fisiche la cui commissione di reati è suscettibile di impegnare la responsabilità amministrativa dell'ente è rappresentata dai c.d. sottoposti. La scelta di limitare la responsabilità della societas al solo caso di reato commesso dai vertici, non si sarebbe rivelata plausibile dal punto di vista logico e politico criminale. Sotto il primo profilo, anche in questo caso, come si è detto, la possibilità di ricondurre la responsabilità all'ente appare assicurata, sul piano oggettivo, dal fatto che il reato sia stato commesso nell'interesse o a vantaggio dell'ente. Sotto il secondo profilo, una diversa opzione avrebbe significato ignorare la crescente complessità delle realtà economiche disciplinate e la conseguente frammentazione delle relative fondamenta operative.

23 - Nella prassi giurisprudenziale, l'interpretazione estensiva è stata condivisa dal G.i.p. del Tribunale di Milano in una nota ordinanza del 27 aprile 2004, con la quale alla società indagata è stata applicata in via cautelare la misura interdittiva del divieto di contrattare con la pubblica amministrazione. Nel caso di specie, si era ipotizzata una responsabilità della Società per fatti di corruzione nei confronti di alcuni funzionari di un altra società, posti in essere p er ottenere l'aggiudicazione di due gare d'appalto (…) Orbene, nel valutare la sussistenza di gravi indizi di responsabilità ai sensi dell'art. 45 d.lgs. 231/2001, il G.i.p. ha ritenuto che rientrassero nella categoria soggettiva individuata dall'art. 5

vigilanza di uno dei soggetti in posizione apicale, il che, come è stato osservato, può accadere per numerose categorie di collaboratori esterni, che si trovino in qualche modo a perdere parte della loro autonomia a favore dell'ente[24].

Non resta quindi che, *de jure condendo*[25], ferme le categorie non controverse dei soggetti da includere tra quelli sottoposti alla direzione o vigilanza dei soggetti in posizione apicale, nei quali possono agevolmente farsi rientrare coloro che sono dipendenti, lavoratori parasubordinati ovvero agenti, tentare una ricostruzione sistematica di tali ulteriori tipologie di collaboratori dell'ente, con specifico riferimento agli schemi, pure atipici, della fornitura di servizi di Cloud Computing.

Quanto da ultimo muovendo, in primo luogo, dal dato letterale normativo costituito dalla soggezione al potere di vigilanza del soggetto generatore di responsabilità dell'ente, ed operando, in secondo luogo, sinteticamente, una verifica, in altre norme di legge, pure applicabili alle obbligazioni negoziali rinvenibili nell'adempimento delle prestazione connaturate ad alcuni modelli di Cloud Service, della sussistenza di tale obbligo di vigilanza.

La constatazione che la maggior parte delle operazioni di elaborazione, sottese all'esecuzione di prestazioni di servizi riconducibili al modello di Cloud Computing, implichi l'effettuazione da parte del Cloud Service Provider di operazioni di trattamento dei dati personali, con riferimento specifico alle disposizioni di cui al decreto legislativo n. 196 del 30 giugno 2003, induce chi scrive a ritenere utile, *ratione materiae*, l'esecuzione della verifica sopra descritta con riferimento al menzionato, ultimo, ambito di operatività legislativa.

Si verificherà, quindi, se, nel contesto di rapporti giuridici, riferibili, da un lato all'effettuazione prestazioni contrattuali rientranti nel genus dei contratti di Cloud Service e, dall'altro, alle operazioni di trattamento di dati personali, siano individuabili, e se si, con quale grado di vincolatività per le parti contraenti, e con quali effetti nelle dinamiche costitutive e di controllo dei modelli organizzativi, posizioni di vigilanza normativamente imposte, che determinino, la necessità, per l'ente, di integrare l'operato del personale del Cloud Service Provider (i.e. fornitore di servizi) all'interno del suo modello organizzativo.

Per sgomberare da subito il campo da equivoci, vale la pena precisare che la verifica in questione non attiene alla possibilità di configurare una qualche rilevanza di condotte penalmente perseguite dal Codice Privacy ai fini dell'attribuzione della responsabilità amministrativa all'ente, bensì, la sussistenza, in forza dell'applicazione delle disposizioni del predetto codice, di posizioni di vigilanza *"funzionale"* in capo all'ente, nei confronti del soggetto *"esterno"* all'ente stesso, sulla base di operazioni di trattamento svolte da quest'ultimo in favore del primo.

Alcuni dati utili allo svolgimento della descritta attività di verifica, possono essere individuati, in primo luogo, nel testo delle indicazioni rilasciate dal Garante Privacy che, espressamente prevede che: (...) l'azienda

---

lett. b), tutte e tre le persone indagate, una delel quali era, per l'appunto, un ex dipendente, consulente esterno della società.

24 - A. Frignani/P.Grosso/G.Rossi, I modelli di organizzazione previsti dal D.Lgs. 231/2001 sulla responsabilità degli enti, in Soc., 2002, p. 153. - Potrebbe essere il caso, ad esempio, degli agenti di commercio, dei concessionari di vendita e dei franchisees, i quali, pur non potendo definirsi subordinati in senso proprio, subiscono compressioni anche significative della loro autonomia in favore dell'ente, e ben possono commettere reati nell'interesse dell'ente stesso; ma nache di altri soggetti, quali consulenti o professionisti comunque esterni all'organigramma aziendale.

25 - Si cercherà, in altre e più semplici parole di costruire il criterio di imputazione soggettiva della responsabilità dell'ente di cui alla lettera b. ultimo inciso dell'art. 5 del d.lgs 231/2001, rinvenendone il presupposto, in norme la cui osservanza implichi, nello svolgimento da parte del terzo, di attività riferibili all'ente, di per sé, un dovere giuridico di vigilanza dell'ente, per esempio, nei confronti di un fornitore di servizi in modalità SaaS.

titolare del trattamento dei dati personali, che trasferisce del tutto o in parte il trattamento sulle "nuvole" deve procedere a designare il fornitore dei servizi cloud "responsabile del trattamento", in secondo luogo, per esempio, nel testo delle condizioni generali di accordo dei servizi cloud di un noto Vendor ove si legge che : *"il Cliente nomina il Vendor*[26] *quale responsabile esterno del trattamento di tali dati ai sensi dell'art. 29 e ss. del D.Lgs. 196/2003"*. Non solo, un altro Vendor, inserisce ad oggi la seguente previsione nelle sue condizioni generali di servizi cloud: *"Qualora per l'erogazione del Servizio, il Vendor, dovesse trattare dati personali di cui è Titolare il Richiedente, il Vendor si impegna ad accettare la nomina a Responsabile del trattamento da parte del Richiedente prima o contestualmente all'inizio del trattamento medesimo. Il vendor si impegna, altresì, a far accettare alla Ditta eventualmente incaricata la nomina a Responsabile da parte del Richiedente, per i trattamenti di competenza"*.

Ciò precisato, vale a questo punto la pena, secondo chi scrive, di verificare se, per esempio in base a quanto previsto dall'art 29 del Codice in materia di protezione dei dati personali possa configurarsi, in capo al titolare del trattamento un obbligo di vigilanza con effetti rilevanti ai fini del d.lgs. 231/2001; a tal fine occorre fare riferimento da una parte a quanto previsto dall'art. 29 da ultimo richiamato che, tuttavia, deve essere letto in correlazione con l'art 4 lett. g). del Codice in materia di protezione dei dati personali.

1.6 I Responsabili del trattamento

Nel sistema del Codice in materia di protezione dei dati personali, organizzato su base gerarchica, il responsabile del trattamento, per espressa previsione legislativa è il soggetto, persona fisica o persona giuridica, preposto dal Titolare al trattamento di dati personali, inoltre, ai sensi, invece, dell'art. 29 commi 4 e 5 del ricordato Codice: *"i compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare"* ed *"il responsabile del trattamento effettua il trattamento attendendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle (…) proprie istruzioni."*

Una prima analisi delle norme sopra riportate consente, ad avviso di scrive, di ritenere configurato, in forza dell'espressa menzione dell'obbligo di vigilare sull'osservanza delle proprie istruzioni, gravante sul titolare del trattamento, il rapporto funzionale descritto nell'art. 5 lett. b del d.lgs. 231/2001, con la conseguenza che, anche nei confronti dei responsabili del trattamento, esterni all'ente, dovranno attuarsi, le cautele organizzative procedimentali e di controllo disegnate dal legislatore.

Occorre però, per definire esattamente, la portata applicativa della affermazione da ultimo effettuata, considerare anche che, molto spesso, la nomina a responsabile esterno è rilasciata, specialmente con riferimento alla fornitura di servizi di Cloud Computing, a società, in persona del loro legale rapp.te. p.t. e non a persone fisiche e ciò potrebbe avere, in concreto, con riferimento alla applicazione delle disposizioni del D. Lgs. 231/01, l'effetto di svuotare il contenuto degli obblighi di vigilanza in considerazione del fatto che, il responsabile, in quanto tale, vale a dire la persona giuridica designata nella qualità dal titolare del

26 - Altri fornitori esteri di servizi Cloud fondano sulla stessa logica il rapporto con il beneficiario delle prestazioni, può leggersi infatti nelle condizioni di licenza di un servizio di archiviazione di e-mail che: *"Partner acknowledges that it (or its customer) is the data controller of any personal data contained within, or associated with emails sent or received any by Mailbox in the course of the VENDOR Services, and that in providing the VENDOR Services, VENDOR is acting as a* ***data processor*** *on behalf of Partner. In processing such personal data, VENDOR* ***will act in accordance with the instructions of Partner****, (...). By using the Services, Customer consents to this processing and storage of an Application and Customer Data. The parties agree that VENDOR is merely a* ***data processor****.*

trattamento non può, per definizione, realizzare, se non attraverso, di nuovo, i propri dipendenti e/o preposti, i reati presupposto da cui sorge la responsabilità dell'ente beneficiario dei servizi[27].

Le conseguenze di questa impostazione rischiano tuttavia di estendere oltre misura la portata applicativa delle disposizioni della lettera b). dell'art. 5 anche se, chi scrive, ritiene che, tale dimensione operativa, di una norma congegnata per attribuire, in questo caso, all'ente, una responsabilità per difetto di vigilanza, non sia incompatibile con la ratio stessa del decreto 231. Naturalmente, la problematica da ultimo rilevata, non trova applicazione laddove, in effetti il responsabile designato sia una persona fisica.

A ben vedere, tuttavia, lo schema negoziale, ed il conseguente criterio di imputazione delle responsabilità ex 231 al contraente beneficiario di servizi di elaborazione, di dati personali, erogati in modalità cloud, potrebbe essere sussumibile, all'interno di una fattispecie riferibile ad un altra figura tipica del sistema delle disposizioni vigenti in materia di protezione dei dati personali, vale a dire quella dell'amministratore di sistema.

1.7 Gli Amministratori di Sistema

La prassi, conosce in effetti situazioni negoziali - prese in considerazione, espressamente dal provvedimento[28] dell'Autorità Garante per la protezione dei dati personali, ove si può leggere che: " Nel caso di servizi di amministrazione di sistema affidati in ***outsourcing*** il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema - nelle quali, un titolare, designa, la persona giuridica dalla quale riceve servizi, in qualità di responsabile del trattamento, e i soggetti, nominativamente individuati, dipendenti di questa, che avranno materialmente accesso ai dati, in qualità di amministratori di sistema.

Occorre ora, per verificare, di nuovo, se la figura dell'amministratore di sistema possa rientrare tra quelle sottoposte alla vigilanza da parte dell'ente, con effetti in punto di attribuzione di responsabilità ex 231, esaminare, nel dettaglio le previsioni del provvedimento relative agli adempimenti posti a carico del titolare del trattamento. In questo ambito, sembrano rilevare le attività, prescritte al titolare del trattamento negi confronti degli amministratori nominati che ne implicano la verifica delle attività; testualmente la lettera e) del provvedimento in esame specifica che: *"L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti[29]"*.

---

27 - Si renderebbe necessario costruire una fattispecie per cui l'ente risponde del fatto di reato commesso, a suo vantaggio e/o nel suo interesse, dai soggetti dipendenti, preposti e/o in posizione apicale, della società nominata nella qualità di responsabile del trattamento, estendendosi, probabilmente, oltre misura, l'imputazione della responsabilità alla persona giuridica.

28 - Cfr. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 - (***G.U. n. 300 del 24 dicembre 2008)*** l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi ***software*** complessi le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

29 - Con riferimento all'estensione degli obblighi di verifica e quindi ad avviso di scrive di vigilanza), Cfr AGPDP [doc.web. n. 1681794] - *"Si ritiene, inoltre, necessario che il titolare effettui le attività periodiche di verifica e controllo previste dal provvedimento del 27 novembre 2008 , come modificato dal provvedimento del 25 giugno 2009, attivando*

Ciò rilevato, occorre ora, nell'ottica di completare il quadro generale dei tratti salienti l'architettura applicativa dell'operato del decreto 231 - che, come detto, non ha inteso strutturare delle fattispecie di responsabilità oggettiva[30] - individuare, quali siano le condizioni che consentono all'ente, di andare esente da responsabilità ovvero di mitigarne gli effetti nel caso in cui la responsabilità vi sia.

La norme di riferimento sono costituite dall'art. 6 con riferimento ai soggetti in posizione apicale e dall'art. 7 con riferimento ai soggetti in posizione non apicale e nel caso di reato commesso da soggetti in posizione non apicale[31], la responsabilità dell'ente resta esclusa dall'adozione, ante factum, di idonei ed efficaci modelli di organizzazione.

L'autorità competente a svolgere le indagini preliminari e ad esercitare l'azione penale nei confronti dell'ente è il pubblico ministero, che, ai sensi dell'art. 59 comma 1 del decreto 231 deve effettuare la contestazione dell'illecito in uno degli atti indicati dall'art. 405 del Codice di Procedura Penale.

La cognizione dell'illecito amministrativo è attribuita allo stesso giudice competente per il reato presupposto (art. 36, comma 1 D. Lgs. 231) che applica le relative sanzioni con un provvedimento giurisdizionale (decreto o sentenza di condanna), emesso all'esito di un procedimento penale, con tutte le garanzie che gli sono proprie[32].

Il successivo articolo 9[33] individua, poi, il trattamento sanzionatorio applicabile nel caso in cui si configuri la responsabilità dell'ente, definendo: sanzioni pecuniarie, interdittive, la confisca nonchè la pubblicazione della sentenza.

La sanzione pecuniaria, che è sempre applicata allorchè sia ritenuta la responsabilità amministrativa dell'ente, è determinata dal Giudice attraverso un sistema basato su quote.Sono previsti casi di riduzione

---

un sistema di audit interno. In particolare, per gli ambiti già consolidati, si ritiene che il titolare effettui i controlli per verificare la rispondenza dell'operato degli Amministratori alle misure organizzative, tecniche e di sicurezza prescritte da questa Autorità".

30 - Con riferimento all'organismo di vigilanza si è osservato che tale organismo, per essere funzionale alle aspettative, non dovrà avere compiti operativi che facendolo partecipe di decisioni dell'attività dell'ente, potrebbero pregiudicare la serenità di giudizio al momento delle verifiche. Al riguardo appare auspicabile che si tratti di un organismo di vigilanza formato da soggetti non appartenenti agli organi sociali, soggetti da individuare eventualmente, ma non necessariamente in collaboratori esterni dotati delle necessarie professionalità. G.i.p. trib. Milano, 20 settembre 2004 in Guida al dir. 47/2004 p. 69.

31 - Art. 7. Soggetti sottoposti all'altrui direzione e modelli di organizzazione dell'ente. 1. Nel caso previsto dall'articolo 5, comma 1, lettera b), l'ente e' responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. 2. In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi. 3. Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonchè al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio. 4. L'efficace attuazione del modello richiede: a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività; b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

32 - Cfr. G. De Simone La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) di imputazione. p. 16 in **penalecontemporaneo.it**

33 - In particolare, le sanzioni interdittive, particolarmente odiose, possono consistere in: interdizione dall'esercizio dell'attività, sospensione o revoca di autorizzazione, licenze o concessioni funzionali alla commissione dell'illecito, divieto di contrattare con la pubblica amministrazione, esclusione da agevolazioni, finanziamenti contributi o sussidi e l'eventuale revoca di quelli già concessi, nonché, infine, il divieto di pubblicizzare beni o servizi.

della sanzione pecuniaria, nelle ipotesi, nelle quali, alternativamente, l'autore del reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne abbia ricavato un vantaggio ovvero ne abbia ricavato un vantaggio minimo, oppure quando il danno cagionato è di particolare tenuità. La sanzione pecuniaria, inoltre, è ridotta, da un terzo alla meta, se, prima della dichiarazione di apertura del dibattimento di primo grado, l'ente ha risarcito integralmente il danno oppure ha eliminato le conseguenze danno se o pericolose del reato, ovvero si è adoperato in tal senso, ovvero è stato adottato un modello idoneo a prevenire la commissione di ulteriori reati.

1.8 Riferimenti legali di base in materia di configurazione dei servizi Cloud

Alla luce di quanto sopra, conviene ora, per delimitare giuridicamente l'ambito di indagine del presente studio, muovere da una definizione di ciò che si intende per Cloud Computing.

Ovviamente, come la maggior parte della materia riferibile al c.d. diritto dell'informatica, il nostro ordinamento, non enuclea, da un punto di vista delle fonti tradizionali, una nozione legale omni-omprenisva di cosa sia il Cloud, di tal che gli stessi paradigmi negoziali che ne disciplinano, allo stato, l'operatività devono essere ricondotti, da un punto di vista interpretativo, a nozioni e schemi contrattuali, che, passando per la nozione di outsourcing, giungono a ricondurre le operazioni riferibili al *modus operandi* che qui ci occupa, nello schema, aperto, dell'appalto di servizi di cui agli artt. 1655 e ss. Codice Civile.

Il tema[34], tuttavia, è stato compiutamente affrontato, con riferimento alle norme in materia di protezione di dati personali applicabili, già dal 2012 ad opera del Gruppo di lavoro[35] art. 29 per la protezione dei dati, e, più recentemente, anche in Italia, ad opera dell'Autorità Garante per la protezione dei dati personali[36].

In particolare, in quest'ultimo documento, si è affermato che nel caso del Cloud Computing, il trasferimento dei dati dai computer locali, nella fisica disponibilità e nel diretto controllo esercitabile dal titolare, verso sistemi remoti, di proprietà di un terzo fornitore del servizio presenta aspetti specifici che necessitano di particolare attenzione.

Tra questi deve rilevarsi, nello specifico, con riferimento alle finalità del presente studio, con riferimento a quanto chiarito sub. 1, relativamente ai soggetti non apicali da cui può derivare la responsabilità dell'ente,

---

34 - Cfr. E. Belisario, “Cloud Computing” in Informatica giuridica, numero 17 eBook Altalex, 2011. - “(…) con particolare riferimento ai sistemi di Cloud Computing di tipologia SaaS ed alla loro riconducibilità al fenomeno dell’*outsourcing*, una parte degli interpreti, ritiene che il contratto che si stipula per l'utilizzo di un sistema di SaaS possa inquadrarsi nello schema dell’appalto di servizi. Dall'altro lato, altri autori, non condividendo la tesi sopra enunciata, sostengono che quello di fornitura di servizi di cloud computing rappresenti una particolare figura di contratto atipico"

35 - Cfr. Parere 05/2012 sul Cloud Computing adottato il 1° luglio 2012 p. 10 Nell'attuale scenario del Cloud Computing, il clienti di servizi di Cloud Computing potrebbero non avere margine di manovra nel negoziare i termini contrattuali dell'uso dei servizi cloud, che in molti casi sono caratterizzati da offerte standardizzate. (Ma) Come affermato nel parere 1/2010 sui concetti di responsabile del trattamento e incaricato del trattamento del gruppo di lavoro articolo 29 “lo squilibrio fra il potere contrattuale di un piccolo responsabile del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla rotezione dei dati personali. Un enfasi particolare va posta (…) sui meccanismi aggiuntivi che si possono dimostrare adeguati per agevolare la due diligence e la responsabilità (quali audit indipendenti di terzi certificati).

36 - Autorità Garante per La Protezione dei Dati Personali, Schede di documentazione, Cloud Computing: indicazioni per l'utilizzo consapevole dei servizi.

che, il fornitore, in base alla tipologia di servizi offerti, assume la responsabilità di preservare la riservatezza, l'integrità o la disponibilità dei dati.

Diventa chiaro, all'interno del quadro obbligatorio poco sopra considerato che, elementi fondamentali, da un lato, della attribuibilità delle condotte del fornitore all'ente in termini di responsabilità amministrativa ex art. 231, e, dall'altro, della attuazione degli obblighi di vigilanza gestione ed organizzazione, siano nei confronti del fornitore del servizio, rispettivamente, l'assetto contrattuale concreto, realizzato al momento dell'acquisto del servizio e la quantità e qualità di sicurezza applicata sui dati personali oggetto di trattamento da parte del fornitore del servizio *cloud* in forza del contratto.

1.9 Relazioni tra l'applicazione di specifici standard di sicurezza informatica e telematica e la responsabilità amministrativa degli enti

In relazione a quanto affermato nel §. 2.1. a proposito dei responsabili del trattamento e degli amministratori di sistema, con specifico riferimento al tema della qualità e quantità di sicurezza informatica e telematica applicata, o da applicare, dall'ente sui propri sistemi e sulle proprie procedure di gestione della sicurezza dei sistemi informativi, al fine di configurare le fattispecie di esonero da responsabilità, sembra opportuno[37], svolgere alcune brevi considerazioni relative alla effettività dei controlli richiesti all'ente stesso, per provare, come suol dirsi, carte alla mano, l'ottemperanza a quel dovere di puntuale preventiva ed ordinata organizzazione degli asset che costituisce fondamento della non attribuzione di responsabilità.

Occorre muovere, per comprendere in quale misura la standardizzazione, nei vari contesti, delle funzioni di gestione della sicurezza di un sistema informativo, vada ad impattare su meccanismi di attribuzione della responsabilità amministrativa, da un dato normativo cogente, espressivo di un generale dovere di diligenza - *imposto sul titolare del trattamento, tutte le volte in cui, ai nostri fini, sia ente* - previsto dall'art. 31[38] del Codice Privacy.

La norma, disciplina, il dovere di sicurezza cui è tenuto il titolare del trattamento, nello svolgimento di operazioni, su dati personali, per le finalità che ne caratterizzano l'operatività, ed ha il merito, secondo chi scrive, in una formulazione, mutuata dalla "vecchia" direttiva sulla *data protection*, da un lato, di esprimere, analiticamente, quali sono i rischi che incombono sui dati ed alla cui prevenzione deve dirigersi l'adozione di qualsiasi processo/procedimento di sicurezza e, dall'altro, di riferire l'adempimento agli obblighi di sicurezza, al parametro dell'***aggiornamento con il progresso tecnico***, rendendo di conseguenza dinamica e, sostanzialmente, inesauribile la realizzazione del dovere medesimo *(proprio come inesauribili ed in continua evoluzione sono le minacce che incombono sui dati).*

37 - Non potendo non constatare, nell'esercizio professionale quotidiano della mia attività lavorativa, una dirimente e preoccupante mancanza di consapevolezza tra gli operatori aziendali, anche di grandi dimensioni ed esercenti attività di rilevante interesse pubblico, prima ancora che economico, delle dinamiche relative ai processi di messa in sicurezza dei sistemi informativi, con riferimento alla documentazione formale delle misure adottate.

38 - Art. 31 (Obblighi di sicurezza) *"I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".*

Inoltre, gli ulteriori riferimenti, alla natura dei dati e alle modalità del trattamento stesso, introducono, nello scenario delle concrete modalità attuative del dovere in questione, alcune variabili, che consentono, l'individuazione, di volta in volta, di specifiche norme (in senso ampio, come sinonimo di standard) comportamentali ed organizzative, relative allo specifico settore in cui il Titolare si trova ad operare.

Ciò detto, diventa evidente, come, la dimostrazione della puntualità della ottemperanza delle prescrizioni dello specifico standard di sicurezza informatica e telematica applicabile al settore in cui opera l'ente, possa costituire (pre)requisito fondamentale della prova della diligenza necessaria a documentare l'effettuazione dei controlli dovuti dall'ente per impedire la commissione dei reati presupposto.

In altre parole, se è vero che la sicurezza informatica e telematica (e quindi, in generale, la prevenzione da utilizzi indebiti dei dati), di uno specifico ambito, ad esempio, quello relativo ai pagamenti con carta di credito è "normata" da una serie di prescrizioni che sono applicabili al quel settore, in forza di vincoli contrattuali, ovvero in forza dei richiami al progresso tecnico ed alla natura dei dati oggetto di trattamento, contenuti nel citato articolo 31 del codice della privacy, sembra ragionevole ritenere, che con specifico riferimento ai reati c.d. informatici propri, previsti dal D. Lgs. 231/2001, occorrerà documentare, l'effettuazione, almeno di tutti quei controlli che lo standard stesso impone con riferimento alla prevenzione delle condotte degli utilizzatori che integrano fattispecie di reato.

Al contrario, la mancanza di misure logiche ed organizzative, apprezzabili e documentate, riferibili alla specifica attività svolta dall'ente, e prescritte dallo standard del settore di riferimento, renderà, ad avviso di chi scrive, assai ardua, se non impossibile, la dimostrazione dell'ottemperanza, da parte dell'Organismo di Vigilanza, al dovere di prevenzione controllo che su di esso incombe con riferimento alla commissione dei reati presupposti.

Con ciò non si vuole (e non si potrebbe), naturalmente, dire che l'ottemperanza allo standard di sicurezza elimini ex es il rischio di commissione dei reati informatici presupposto, ma semplicemente, evidenziare come le prescrizioni dello standard stesso possano essere utilmente impiegate (a prescindere, eventualmente, dalla stessa relativa certificazione) come protocollo operativo nella definizione dei controlli e delle contromisure che l'ente deve adottare per evitare di incorrere nelle ipotesi di responsabilità.

Si pensi, per fare un esempio, rimanendo in tema di standard di sicurezza relativi alle operazioni di elaborazione sui dati dei titolari di carta di credito, con riferimento alla fattispecie di reato di cui all'art. 615 ter del Codice Penale che disciplina l'ipotesi del reato presupposto di accesso abusivo a sistema informatico o telematico, a quanto previsto dal requisito N. 10 dello Standard PCI- DSS39 V.3 che espressamente prevede che debbano essere registrati tutti gli accessi a risorse di rete e dati dei titolari di carta.

Risulta a chi scrive di intuitiva comprensione che, l'osservanza puntuale delle istruzioni[40] di adozione dei requisiti dello standard[41], ben più penetranti e documentabili, di quanto sia dato rinvenire nel corpo del Codice in materia di protezione dei dati personali o nell'allegato B al predetto Codice (che dovrebbero

---

39 - *Payment Card Industry – Data Security Standard* – Si tratta di uno *standard* di sicurezza informatica e telematica, che si sviluppo su 12 requisiti che vincola i soggetti che effettuano operazioni su dati relativi a pagamenti effettuati con carta di credito.

40 - PCI DSS V3, Requisito 10.2.2.. Istruzioni: *"Account con maggiori privilegi, come di amministratore o root, hanno il potenziale di influire in modo significativo sulla sicurezza o sulla funzionalità operativa di un sistema. Senza un registro delle attività eseguite una organizzazione non è in grado di ricondurre ogni questione risultante da un errore amministrativo o dall'uso improprio di privilegi all'individuo o all'azione specifici".*

41 - Considerazioni analoghe possono, naturalmente, essere svolte anche con riferimento allo standard ISO/IEC 27001:2005 relativamente, in generale, ai sistemi di gestione della sicurezza delle informazioni.

costituire il parametro legale di riferimento), assolva ad una funzione preventiva e di esonero da responsabilità assai più elevata che la "mera" osservanza, passiva della semplice disposizione di legge.

1.10 Il problema della dimensione transnazionale dei crimini informatici[42] con riferimento all'art. 4 del D. Lgs. 231/01

Un altro aspetto, parimenti importante, dirimente in alcuni casi, su cui vale la pena di soffermarsi, con riferimento ai principi in materia di responsabilità amministrativa delle persone giuridiche, in ambito Cloud Computing, riguarda, la localizzazione territoriale della *scena criminis* del reato presupposto.

In effetti, un rapido sguardo all'offerta di servizi di *Cloud Computing* "evoluti" consente di constatare, *prima facie*, che i maggiori protagonisti del settore sono localizzati al di fuori del territorio della Repubblica Italiana. Ma non è tutto: talvolta, al problema giuridico sotteso alla localizzazione extra-nazionale (e spesso extracomunitaria) della sede legale del *Cloud Service Provider* si aggiunge l'ulteriore problema "fattuale" della esatta determinazione del luogo ove i dati o le attività di elaborazione, sulle quali insistono le condotte dei reati presupposto,risiedono e/o sono volte.

A ben vedere, assai spesso, il luogo o sovente i luoghi ove sono localizzati i *data center* dei CSP sui quali o mediante i quali si svolgono le attività previste criminose contemplate dal decreto legislativo 231/01, potrebbero non essere soggetti alla legge penale Italiana, in forza di quanto disposto dall'art. 4 del decreto legislativo 231 e dei richiami agli artt. 7, 8, 9 e 10 del Codice Penale.

Tuttavia, l'analisi puntuale della disposizione in commento consente, almeno dal punto di vista del diritto sostanziale e processuale applicabile, ferme le difficoltà probatorie cui si è fatto riferimento e di cui si dirà nel seguito, di "agganciare" la giurisdizione italiana tutte le volte in cui, i soggetti che commettono uno dei reati presupposto, afferiscano ad un ente che abbia la sua sede nel territorio dello Stato a prescindere, nei limiti citati, dal luogo ove il crimine è stato commesso.In particolare, l'art. 4 citato[43], aggiunge, ai già rigorosi criteri di soggezione alla giurisdizione italiana di un reato commesso all'estero, la circostanza, non sempre di facile individuazione, che l'ente abbia sede principale nel territorio dello stato, che il reato sia commesso all'estero da un soggetto funzionalmente legato all'ente, e che non proceda, per lo stesso reato, nei confronti del medesimo soggetto, lo stato del luogo in cui è stato commesso il fatto.

1.11 Corporate Cloud[44] Forensics ed esclusione da responsabilità

La disamina svolta nel § 2 relativa, in particolare, alle condizioni che devono sussistere affinché l'ente possa andare esente da responsabilità amministrativa, ha introdotto da una parte il tema della effettività delle

---

42 - Una definizione utile per le finalità di questo studio di crimine informatico è quella di: *"crimine nel quale un sistema di elaborazione o una sua parte ricopre uno dei seguenti ruoli: – oggetto (ciò include la distruzione o la manipolazione dell'elaboratore, dei dati e dei programmi in esso contenuti e delle relative apparecchiature di supporto) – soggetto (quando l'elaboratore è il luogo, il motivo o la fonte del crimine) – strumento (quando ciò che avviene in relazione all'elaborazione non è di per sé illegale, ma serve a commettere crimini di altro tipo, es. sabotaggio)".*

43 - Cfr. Art. 4 D.Lgs. 231/01 *"Nei casi e alle condizioni previste dagli articoli 7, 8, 9 e 10 del Codice Penale, gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto"*.

44 - Cfr. K. Ruan, Prof. J Carthy, Prof. T. Kechadi, M Crosbie, Centre For Cyvercrime Investigation, University College of Dublin. **Cloud Forensics: An Overview.**

funzioni di controllo dell'osservanza sui contenuti del modello organizzativo di gestione e controllo da parte dell'Organismo di vigilanza e dall'altra, quello della loro prova e/ documentazione.

Si è visto, in particolare, che le lettere c) e d) dell'art. 6 del decreto 231/2001 consentono l'esonero da responsabilità dell'ente, per il reato presupposto, commesso dal soggetto in posizione apicale, solo a condizione che i soggetti autori dell'illecito abbiano commesso il reato eludendo fraudolentemente i modelli di organizzazione e gestione e che, nel contempo, non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

Orbene è di tutta evidenza che, in un ambiente, come quello descritto nel § 2, caratterizzato da un elevato livello di ricorso a tecnologie informatiche e telematiche, ed in particolare in un ambiente *cloud*, sia la prova dell'elusione fraudolenta del modello da parte dell'autore del reato, sia la prova della coerenza dell'esercizio del potere di vigilanza da parte dell'organo preposto, implichino, certamente, un ampio ricorso sia in termini di prevenzione sia in termini di successivo accertamento, a strumenti e tecniche di investigazione digitale[45].

Da un punto di vista preventivo, relativamente alla prova dell'elusione, in considerazione del fatto che, ad avviso di chi scrive, risulta parziale, la configurazione di modelli di gestione e controllo, che non tenga nella debita considerazione l'eventualità di produrre - *in esito ad operazioni di audit, il cui svolgimento è insito nella struttura stessa delle procedure di verifica della applicazione del modello* - evidenze *forensically sound*, vale a dire idonee a fornire ad un giudicante, alla bisogna, prova certa ed incontestabile della condotta omissiva o commissiva di cui si richiede la dimostrazione.

Dal punto di vista del successivo accertamento è addirittura intuitivo pensare al fatto che, sarebbe, non coerente, se non addirittura pericoloso, omettere, nella stesura delle procedure di controllo, di cui può avvalersi l'organismo di vigilanza, nell'esercizio delle sue funzioni, la previsione espressa dell'impiego, di tecnologie e tecniche di investigazione digitale in grado di fornire evidenza adeguata, anche in questo caso dell'azione od omissione da cui in ipotesi potrebbe derivare la responsabilità dell'ente.

Ma non è tutto, la stessa coerenza dell'operato dell'organismo di vigilanza passa attraverso la dimostrazione della genuinità delle evidenze informatiche che, verosimilmente, i membri dell'organismo stesso, porranno a dimostrazione del loro operato. Si vuole dire in altre parole, come accennato in precedenza, che non sembra potersi prescindere da adeguati strumenti informatici di validazione forense dell'evidenza digitale per documentare le circostanze che di volta in volta si renderà necessario provare per le finalità proprie dell'interesse dell'ente ad andare esente da responsabilità.

In linea di principio le attività da ultimo richiamate sono facilmente riconducibili allo svolgimento di operazioni di c.d. *corporate forensics* vale a dire all'impiego, concertato, pianificato e ritualmente eseguito, da parte dell'ente, anche mediante il ricorso al formidabile strumento delle investigazioni difensive di cui all'art. 391 bis e ss del Codice di Procedura Penale, ad operazioni investigazione digitale attuate in conformità con le *best practices* della *digital forensics*, ciò in quanto, se, a bene vedere, le operazioni descritte in precedenza si caratterizzano *ex se* per un elevato livello di difficoltà oggettiva di realizzazione alla luce della sempre maggiore complessità dei sistemi elettronici di elaborazione normalmente impiegati *on premise* dalla maggior parte degli enti soggetti alla disciplina del decreto legislativo 231 in commento, le stesse operazioni diventano, addirittura problematiche, ma non per questo, non effettuabili od eludibili, in

45 - La prova digitale sovente contenuta in un file, ad esempio un file di log, specialmente in ambiente *cloud* è connotata da una estrema volatilità, da una relativa alterabilità, da una elevata latenza, dalla sua possibile localizzazione in sistemi ubicati in paesi soggetti a differenti giurisdizioni e, sovente, strettamente dipendente dal contesto tecnologico (i.e. configurazione dell'elaboratore) ove si genera o si trova.

ambiente *cloud*[46] ove possono profilarsi tutta una serie di difficoltà ulteriori dipendenti dall'ambiente in se considerato – *ostile, per definizione, ad essere cristallizzato in un dato momento*.

In materia, dal punto di vista della specificità tecnica degli argomenti trattati, sembra non eleudibile il riferimento all'operato dell'Incident Management and Forensic Working Group del giugno 2013 dal titolo Mapping the Forensic Standard ISO/IEC 27037 to Cloud[47] Computing

Ciò che sembra emergere dall'analisi del documento[48] sopra richiamato è la constatazione, da una parte ovvia, che l'esecuzione di operazioni di investigazione digitale, in ambiente Cloud, che siano di una effettiva utilità per l'accertatore, sia esso una autorità giudiziaria procedente, ovvero un avvocato, munito dei necessari poteri, correlati, nel caso, come sopra accennato allo svolgimento di attività di investigazione difensiva, non possa prescindere da un certo grado di cooperazione con il fornitore del servizio.

In effetti, se pure è vero, che determinate applicazioni cloud, consentano all'investigatore, in locale, di cercare, ed in caso di esito positivo della analisi, di rinvenire "le tracce delle impronte" sembra invero assai complicato, poter prescindere, nella conduzione di una attività investigativa completa, dalla cooperazione con il Fornitore del servizio, giungendosi così a porre la categoria, assai problematica, della effettuazione, da parte di quest'ultimo di servizi del tipo Forensic-As-A-Service. Quest'ultima categoria di servizi, già praticata,

---

46 - Si veda per approfondire Dykstra, J. Riehl, D. Forensic Collection of Electronic Evidence from Infrastructure-As-A-Service Cloud Computing, Richmond Journal of Law and Technology 19. p.39: "(...) digital forensics for cloud computing brings new technical an legal challenges. Cloud Computing makes forensics different, particularly given the remote nature of the evidence, lack or physical access, an trust required in the integrity and authetnicity. While the goals of the forensic examiner are at the same as before, the non-conventional difficult problems include forensically sound acquisition of remote data, large data volumes, distributed and elastic data, chain of custody, and data ownership. Seizure and acquisition of digital artifacts are the initial steps in the forensics process. Two possible scenario exist: remote investigators could collect forensic evidence themselves from the source, or provider could deliver it. Each scenario requires a differnet degree of trust in data returned. Further, each scenario uses technical implementations to recover the data.

47 - Cfr. pp. 5 e 6 a proposito della nozione di Cloud Forensics: "Whether responding to a security incident, data breach, or in support of litigation, the ill-prepared organization will find itself at a severe (and potentially costly) disadvantage.

48 - Per gli scopi del lavoro che qui ci occupa, ci sembra sembra utile precisare quali sono state le modifiche apportate dal documento sopra citato alla CCM (Cloud Control Matrix) elaborata da Cloud Security Alliance, con riferimento alle operazioni di investigazione digitale. ***(a). - CO-04 Compliance*** *– Contract/Authority Maintenance: Points of contact for applicable regulatory authorities, national and local law enforcement and other legal jurisdictional authorities shall be maintained and regularly updated as per the business need (i.e., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.* ***(b). - DG-05 Data Governance*** *– Secure Disposal: Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.* ***(c). - IS-24 Information Security*** *– Incident Response Legal Preparation: In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures including chain of custody shall be required for preservation and presentation of evidence to support potential legal action subject to the relevant jurisdictions. Upon notification, impacted customers (tenants) and/or other external business relationships of a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.* ***(d). - SA-12 Security Architecture*** *– Audit Logging/Intrusion Detection: Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies through to forensic investigative capabilities in the event of a security breach.*

nel mercato dei servizi cloud, presenta in verità specifici problemi di coerenza con gli schemi legali, rigidi, dell'accertamento di responsabilità amministrativa dell'ente per fato del sottoposto alla vigilanza.

Si vuol dire, in altre parole, che pur rinvenendosi l'ineludibile necessità di poter contare su di una collaborazione proattiva del fornitore del servizio, cloud, nelle dinamiche investigative di fatti di reato rilevanti ex 231 commessi sul cloud, per ciò che attiene, per esempio, il log managament, o la disponibilità di snapshot di istanzeVMWare, piuttosto che le evidenze generate dall'implementazione di soluzioni di Identity Access Management, quest'ultimo potrebbe venire a trovarsi, nella duplice, incompatibile condizione di controllore e controllato, con effetti imprevedibili sui meccanismi di accertamento dei fatti.

2.0 Responsabilità amministrativa degli enti in contesto normativo europeo ed importanza delle misure di sicurezza già previste dalle norme per le aree di rischio in relazione ai delitti informatici

2.1 Contesto normativo EU di riferimento

Le normative emanate dall'Unione Europea assumono una indiscutibile importanza nell'ambito della gestione delle tematiche connesse alla criminalità informatica, alla sicurezza informatica ed alla protezione dei dati, poiché hanno una applicabilità diretta o indiretta sui sistemi legislativi dei paesi Membri dell'Unione Europea.

In tema di sicurezza dei dati è bene tenere presente che l'Europa sta definendo un nuovo **Regolamento sulla data protection** che, quindi, godrà di un'applicazione interna diretta sugli Stati Membri senza che si renda necessario un previo percorso normativo di recepimento e di attuazione ad opera del legislatore interno.

Recentemente la **Direttiva Europea 2013/40/UE** del 12 agosto 2013 relativa agli "Attacchi contro i sistemi di informazione" ha stabilito nuove norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione quando sono commessi su larga scala, e la responsabilità delle persone giuridiche per tale tipologia di reati quando sono commessi a loro vantaggio da soggetti apicali o da dipendenti.

Nell'ambito del contrasto alla criminalità informatica, la **Direttiva 2008/114/EC** dell'8 Dicembre 2008 (recepita in Italia con il Decreto Legislativo 61/2011 e, successivamente, la legge n.33/2012) relativa "all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione", l'Unione Europea ha individuato con il termine "Infrastruttura Critica Europea (ECI)" quella " il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri". La direttiva europea fissa i criteri di individuazione di potenziali ECI e le procedure per la preparazione dei Piani di Scurezza da parte degli operatori/proprietari di infrastrutture critiche.

La recente **Proposta di Direttiva Europea nota come "NIS"** (Directive on Network and Information Security) introduce un obbligo di notifica degli incidenti di sicurezza per gli operatori di infrastrutture critiche e ad altre organizzazioni potenzialmente interessate da attacchi, tra le quali rientrano anche i gestori di servizi di cloud. Tale previsione non solo estende gli obblighi di notifica ad un numero più elevato di soggetti rispetto a quelli già individuati per le "personal data breach notification" (Decreti Legislativi 69/2012 e 70/2012 di attuazione della Direttiva EU 2009/136/EC e Provvedimento del Garante Privacy del 4 aprile 2013 sul "data breach"), ma amplia l'ambito di applicazione degli obblighi di notifica riferendosi agli "Incidenti di sicurezza" (in cui sono ricomprese anche le violazioni di dati personali).

Sul tema è bene anche ricordare che dal 25 agosto del 2013 è entrato in vigore all'interno degli ordinamenti giuridici degli Stati membri UE il **Regolamento UE 611/2013** (notificazione delle violazioni di dati personali nel settore dei servizi di comunicazioni elettroniche accessibili al pubblico) che dovrebbe, dunque, comportare una revisione del sopracitato Provvedimento del Garante Privacy laddove sussistano disallineamenti.

2.1.1 La Proposta di Regolamento Europeo sulla Data Protection

Il 25 gennaio del 2012 l'Unione Europea ha avanzato una Proposta di Regolamento, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione degli stessi all'interno del mercato europeo (regolamento generale sulla protezione dei dati) che , una volta approvata in via definitiva (è stata già approvata in prima lettura il 12 marzo del 2014), andrà a sostituire la Direttiva 95/46/CE ed il Testo Unico Privacy (DLgs. 196/03).

La proposta, infatti, sarà direttamente applicabile in tutti gli stati Membri UE senza bisogno di recepimento (come accade, invece, con le Direttive) e imporrà alle imprese l'adozione di un nuovo modello organizzativo e tecnologico per la tutela dei dati.

Tra i driver della riforma si pongono in primo piano:

- la regolamentazione nuove tecnologie tra cui il Cloud Computing, la Virtualizzazione, le Applicazioni Web e Mobile e la tecnologia Wireless;
- il miglioramento dei trasferimenti internazionali di dati in ambito Globale;
- la necessità di un quadro giuridico più solido e coerente, affiancato da accordi istituzionali ed efficaci misure di attuazione;
- la crescita del mercato interno favorito da una maggiore protezione dei dati personali da parte delle imprese dell'UE.

La proposta di Regolamento ha come focus principale il controllo attribuito all'utente sulla gestione facilitata delle proprie informazioni e la struttura della proposta rispecchia tale obiettivo:

- Principi applicabili al trattamento dei dati p./trasparenza (art. 5).
- Consenso dell'interessato in modo "esplicito" (art. 6).
- Diritto all'oblio e alla cancellazione dei dati online (art. 17).
- Portabilità dei dati da un fornitore di servizi a un altro (art. 18).
- Privacy by Design and by Default (art. 23).
- Obbligo di conservare la documentazione (art. 28).
- Individuazione ed attuazione di misure di sicurezza di mitigazione dei rischi (art.30).
- Notificazione e comunicazione di tutte le violazioni dei dati personali (artt. 31-32).
- Data Protection Impact Analysis (art. 33).
- Obbligatorio il "responsabile alla protezione dei dati" (DPO) per PA e grandi imprese (art. 35).
- Codici di condotta e certificazione (art. 38-39).
- Trasferimento dati all'estero (artt. 40-45).
- Obbligatoria Autorità di controllo in ogni Stato membro (art. 46).
- Comitato Europeo per la protezione dei dati (art. 64).

Di seguito, vengono sintetizzate in tabella le misure organizzative e tecniche più rilevanti introdotte dal nuovo regolamento e che possono, ancorché ancora non cogenti, essere prese in considerazione nell'ambito dell'individuazione delle misure di mitigazione dei rischi ex art.24 bis ai fini della costruzione del Modello organizzativo aziendale.

Proposta di Regolamento UE sulla Data Protection	
Principali misure organizzative e tecnologiche proposte	**Descrizione**
Data Protection Officer (art.35)	Il nuovo ruolo è obbligatorio per il settore pubblico e, nel settore privato per un'impresa con 250 più dipendenti, oppure, quando le attività principali del responsabile del trattamento consistono in trattamenti che richiedono il controllo regolare e sistematico degli interessati.
Privacy by Design (art.23)	L'attuazione del principio si sostanzia nel garantire la privacy e la protezione dei dati fin dalla progettazione, che si sostanzia nell'attuare, in tutto l'intero ciclo di vita delle tecnologie e dei sistemi di business (dalla fase di individuazione, disegno, progettazione e distribuzione, utilizzo e dismissione) tutte le necessarie misure tecnico-organizzative al fine di scongiurare i rischi cui sono esposti i dati personali. L'approccio alla Privacy by Design è caratterizzato da interventi di tipo proattivo piuttosto che reattivo e riguarda i sistemi IT, le pratiche commerciali corrette e la progettazione strutturale e le infrastrutture di rete.
Privacy by Default (art.23)	L'attuazione del principio si sostanzia nell'assicurare la privacy e la protezione dei dati per impostazione predefinita, ovvero mediante l'essenzialità del trattamento dei dati sotto ogni punto di vista. Non è richiesta alcuna azione da parte dell'individuo per proteggere la propria privacy che è, dunque, incorporata nel sistema per default.
Risk Analysis (art.30)	Il nuovo Regolamento prevede che il responsabile del trattamento effettui una formale attività di analisi dei rischi finalizzata all'individuazione ed alla adozione di misure di sicurezza organizzative e tecniche adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi di distruzione accidentale o illegale, perdita accidentale, trattamento illegittimo, la comunicazione, la divulgazione, l'accesso non autorizzati o la modifica dei dati personali.
Privacy Impact Assessment – PIA (art.33)	Il nuovo Regolamento prevede che il responsabile del trattamento effettui una valutazione dell'impatto del trattamento previsto sulla protezione dei dati personali, quando il trattamento, per la sua natura o per il suo oggetto o le sue finalità, presenti rischi specifici per i diritti e le libertà degli interessati.
Data Breach Notification (art.31)	Il responsabile del trattamento nei casi di accertata violazione ai dati personali, deve notificarla (art.31) senza ritardo all'autorità di controllo e, quando possibile, entro le 24 ore. Se la violazione rischia di pregiudicare i dati personali o di attentare alla vita privata dell'interessato, il responsabile del trattamento deve anche comunicarla senza ritardo all'interessato

Il Regolamento (art.39) spinge, inoltre, gli Stati Membri e la Commissione Europea ad incoraggiare, in particolare a livello europeo, l'istituzione di meccanismi di certificazione della protezione dei dati (nonché di sigilli e marchi di protezione dei dati) che consentano agli interessati di valutare rapidamente il livello di protezione dei dati garantito dalle imprese.

2.1.2 La Direttiva Europea 2013/40/UE

La Direttiva Europea 2013/40/UE del 12 agosto 2013 relativa agli "Attacchi contro i sistemi di informazione" stabilisce norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi

di informazione quando sono commessi su larga scala, lasciando margine di autonomia agli Stati Membri per quanto attiene invece gli attacchi di minore gravità.

Il valore della Direttiva risulta comunque ridimensionato nell'ambito del quadro di riferimento nazionale, restando pur fermi i cambiamenti del quadro sanzionatorio che, in certi casi, dovrà invece essere ridefinito.

Al riguardo l'Italia, dotatasi già nel 1993 di una legge organica sui reati informatici, ha recepito la Convenzione di Budapest con Legge 18 marzo 2008, n. 48, apportando modifiche ai titoli XII e XIII del libro II del Codice Penale, ai titoli III del libro terzo e IV del libro quinto del Codice di Procedura Penale, nonché al Decreto Legislativo 8 giugno 2001, n. 231.

Si riporta di seguito la tabella di corrispondenza tra i reati introdotti dalla Direttiva e le fattispecie di reato già disciplinate all'interno del Codice Penale italiano.

Tabella di Cross Reference	
Reati introdotti dalla Direttiva 2013/40/UE	**Reati previsti dal Codice Penale italiano**
Accesso illecito a sistemi di informazione (art.3)	• Accesso abusivo ad un sistema informatico o telematico (art.615-ter c.p.)
Interferenza illecita relativamente ai sistemi (art.4)	• Danneggiamento di sistemi informatici o telematici (art.635 quater c.p.) • Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)
Interferenza illecita relativamente ai dati (art.5)	• Danneggiamento di informazioni, dati e programmi informatici (art.635-bis c.p.) • Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
Intercettazione illecita (art.6)	• Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art.617-quater c.p.)
Strumenti utilizzati per commettere i reati (art.7)	• Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art.615-quater c.p.) • Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico • (art. 615-quinquies c.p.) • Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
Istigazione, favoreggiamento, concorso e tentativo (art.8)	• Istigazione a delinquere (art.614 c.p.) • Favoreggiamento personale (art.378 c.p.) • Concorso di persone nel reato (art.110 c.p.) • Delitto tentato (art.56 c.p.)

Rispetto al quadro sanzionatorio, viene imposta agli Stati l'adozione di Sanzioni effettive, proporzionali e dissuasive, e fissato il limite minimo delle pene detentive massime (art.9) che vengono quantificate in:

- minimo 2 anni per tutti i reati previsti dalla Direttiva (artt. da 3 a 8);
- minimo 3 anni per il reato di cui all'art 7 quando è stato colpito un numero significativo di sistemi di informazione;
- minimo 5 anni per i reati di cui agli artt. 4 e 5, quando sono commessi nell'ambito di un'organizzazione criminale, causano danni gravi o sono commessi ai danni di un sistema di informazione di un'infrastruttura critica.

Viene considerata circostanza aggravante l'aver commesso i reati di cui agli artt. 4 e 5 abusando dei dati personali di un'altra persona allo scopo di guadagnare la fiducia di terzi, in tal modo arrecando un danno al

legittimo proprietario dell'identità, mentre è prevista una esenzione di responsabilità (art.17) per coloro che agiscono senza dolo.

L'art.10 introduce a livello europeo la responsabilità delle persone giuridiche rispetto ai reati sopra menzionati, commessi a loro vantaggio:

- da qualsiasi persona, che agisca a titolo individuale o in quanto membro di un organismo della persona giuridica, e che detenga una posizione dominante in seno alla persona giuridica (basata sul potere di rappresentanza della persona giuridica, sul potere di prendere decisioni per conto della persona giuridica oppure sul potere di esercitare il controllo in seno alla persona giuridica);
- da parte di una persona che opera sotto l'autorità di una persona che detenga una posizione dominante in seno alla persona giuridica, facilitata dalla mancanza di sorveglianza o di controllo da parte di quest'ultima.

La responsabilità delle persone giuridiche non esclude l'avvio di procedimenti penali contro le persone fisiche che siano autori o istigatori o abbiano concorso in uno dei reati di cui agli articoli da 3 a 8.

Detta disposizione appare in linea con quanto già definito dall'art. 24 bis[49] del Decreto Legislativo 8 giugno 2001, n. 231 che prevede la punibilità delle condotte commesse "per conto" dell'impresa, includendo tanto quelle commesse nell'interesse dell'ente quanto quelle commesse nell'interesse (anche esclusivo) di altri soggetti che abbiano procurato vantaggio all'ente medesimo.

2.1.3 La Direttiva 2008/114/EC

La Direttiva 2008/114/CE[50]dell'8 dicembre 2008 (recepita in Italia con il Decreto Legislativo 61/2011 e, successivamente, la legge n.33/2012) fornisce indicazioni per identificare le cd. "infrastrutture critiche europee (ECI)", con specifico riferimento ai settori dell'Energia e dei Trasporti, richiedendo agli Stati Membri di:

- adottare misure atte ad individuare e designare quali infrastrutture debbano essere trattate come critiche;
- definire punti di contatto che consentano un coordinamento a livello UE per quanto attiene la loro sicurezza;
- adottare per ciascuna ECI, la Procedura per il Piano di Sicurezza per gli Operatori (PSO).

Il PSO comporta un'analisi dei rischi basata sulle minacce più gravi, sulla vulnerabilità di ogni elemento e sull'impatto potenziale e deve includere l'individuazione, la selezione e la previsione di priorità per contromisure e procedure, con una distinzione fra "Misure permanenti di sicurezza" e "Misure graduali di sicurezza".

Le prime individuano gli investimenti e gli strumenti indispensabili in materia di sicurezza che si prestano ad essere utilizzati in ogni momento, mentre le seconde possano essere attivate in funzione dei diversi livelli di rischio e di minaccia.

Tra le misure permanenti di sicurezza rientrano:

[49] L'art. 24 bis "Delitti informatici e trattamento illecito di dati" è stato introdotto dalla Legge 18 marzo del 2008 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero".

[50] Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione

- misure di tipo generale, quali quelle tecniche (inclusa l'installazione di strumenti di rilevazione, controllo accessi, protezione e prevenzione);
- misure organizzative (comprese le procedure di allarme e gestione delle crisi);
- misure di controllo e verifica;
- comunicazioni (tra queste rientrano senz'altro le comunicazioni, ai punti di contatto nel singolo Stato Membro, degli incidenti di sicurezza che riguardano reti, sistemi e dati necessari all'operatività ed alla gestione delle infrastrutture critiche);
- crescita della consapevolezza e l'addestramento;
- misure di sicurezza dei sistemi informativi.

2.1.4 La Proposta di Direttiva Europea NIS

L'Unione europea per prevenire gli attacchi informatici, ha presentato il 7 febbraio 2013 una nuova strategia sulla sicurezza informatica che coinvolgerà tutti gli Stati membri, attraverso una "Proposta di Direttiva riguardante le misure volte a garantire un livello elevato e comune di sicurezza delle reti e le informazioni in tutta l'Unione" cd. "NIS Directive" (Directive on Network and Information Security)[51] .

La strategia europea sulla cyber security ha come obiettivo quello di promuovere i valori europei di libertà e democrazia affinché l'economia digitale possa svilupparsi in modo sicuro ed è articolata in cinque priorità[52]:

- conseguire la resilienza informatica;
- ridurre drasticamente la criminalità informatica;
- sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune;
- sviluppare le risorse industriali e tecnologiche per la sicurezza informatica;
- istituire una coerente politica internazionale del ciberspazio per l'Unione europea e sostenere i valori fondamentali dell'UE.

Secondo il "*Piano di sicurezza informatica dell'UE per tutelare l'internet aperta, la libertà e le opportunità nella rete*"[53], questi soggetti dovranno predisporre misure di sicurezza, individuate in base ad apposite analisi dei rischi, e notificare alle competenti autorità nazionali gli incidenti quando questi abbiano impatto significativo sulla sicurezza dei servizi da loro erogati.

E' prevista anche la diretta comunicazione al pubblico nel caso in cui la rivelazione dell'incidente sia ritenuta, da parte dell'autorità, di pubblico interesse.

Tale previsione:

---

[51] Brussels, 7.2.2013 COM(2013) 48 final 2013/0027 (COD) - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. La proposta nasce a seguito di un lungo percorso che ha portato all'attuale formulazione della strategia europea sulla Cyber Security: Brussels, 08.12.2003 n.15895/03 - Brussels, 10.12.2008 n.17104/08 - Brussels, 30.03.2009 n.8375/09 – Brussels, 19.05.2011 n.10299/11.

[52] Brussels, 07.02.2013 IP/13/94 - EU Cyber Security plan to protect open internet and online freedom and opportunity.

[53] Brussels, 07.02.2013 IP/13/94.

- estende gli obblighi di notifica ad un numero più elevato di soggetti rispetto a quelli già individuati per le "personal data breach notification" (Decreti Legislativi 69/2012 e 70/2012 di attuazione della Direttiva EU 2009/136/EC e Provvedimento del Garante Privacy del 4 aprile 2013 sul "data breach");
- amplia l'ambito di applicazione degli obblighi di notifica riferendosi agli "Incidenti di sicurezza" (in cui sono ricomprese anche le violazioni di dati personali);
- spinge verso un cambio di prospettiva della compliance che da passiva, imposta dalle normative e dalla legge, deve diventare attiva ovvero prodotta dalle organizzazioni che dovranno adottare modelli organizzativi di gestione della sicurezza dei sistemi e delle reti, in linea con gli attuali standard di riferimento (come ad esempio quelli rilasciati in tema di Information Security dall'Organizzazione Internazionale ISO).

Gli interventi previsti dalla proposta interessano[54]:

- Il settore dell'energia;
- Il settore dei trasporti;
- Le infrastrutture del mercato finanziario;
- Il settore della produzione forniture idriche;
- Il settore dell'approvigionamento alimentare;
- Gli Internet Exchanges Points.

Nei casi di mancata attuazione degli obblighi di notificazione è prevista l'applicazione di sanzioni "effettive, proporzionate e dissuasive" nel caso d'incidenti di una certa gravità.

2.1.5 Il Regolamento UE 611/2013

Il 25 agosto del 2013 è entrato in vigore all'interno degli ordinamenti giuridici degli Stati membri UE il Regolamento UE 611/2013[55] con l'obiettivo di armonizzare la disciplina della notificazione delle violazioni di dati personali tra gli Stati Membri, attraverso l'introduzione di una procedura uniforme e tempi analoghi di notifica.

In base al Regolamento gli operatori di telecomunicazioni e i fornitori di servizi Internet (Internet Service Provider - ISP), devono comunicare entro 24 ore dal rilevamento del problema (perdita, furto o compromissione dei dati dei loro clienti) i propri dati e le informazioni relative all'incidente alle competenti autorità nazionali (per l'Italia l'Autorità Garante per la Protezione dei dati Personali).

Nel caso in cui alcune di tali informazioni non siano disponibili nell'immediato, deve essere comunque inoltrata entro 24 ore una notifica iniziale contenente solo alcuni dati, ed entro tre giorni da quest'ultima, una seconda notifica contenente le restanti informazioni. In caso di mancata invio della seconda notifica, dovranno essere inviati tutti gli elementi di cui l'azienda è in possesso e presentare una giustificazione motivata per la tardiva notifica.

Il Regolamento prevede altresì un'obbligo di notifica aggiuntiva all'abbonato o ad altra persona nel caso in cui la violazione "rischi di pregiudicare i dati personali o la vita privata" degli stessi. Il Regolamento ha il

[54] Tenendo presente la versione emendata sottoposta postivamente alla prima lettura del Parlamento Europeo il 13 Marzo 2014

[55] Regolamento (UE) N. 611/2013 della Commissione del 24 giugno 2013 sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche.

merito di codificare per la prima volta in modo preciso le circostanze in base alle quali l'eventualità di un tale pregiudizio va valutata.

In Italia l'attuazione del Regolamento dovrebbe comportare una revisione Provvedimento del Garante Privacy del 4 aprile 2013 sul "data breach" laddove sussistano disallineamenti e, comunque, i soggetti giuridici interessati dalla regolamentazione sono chiamati ad operare con attenzione al fine di non incorrere nelle sanzioni previste dal vigente quadro normativo nazionale.

2.2 Lo scenario normativo nazionale

In Italia l'attività normativa nel settore dell'informatica e in particolare dell'applicazione ed utilizzazione delle nuove tecnologie informatiche e telematiche, sia in ambito pubblico che privato, ha avuto nell'ultimo decennio un notevole impulso.

Oggigiorno il quadro normativo nazionale di riferimento in tema di ICT security, tutela dei dati personali e cyber crime è rinvenibile in più atti normativi specifici.

In tema di privacy e data protection, il DLgs. 196/03 ha riordinato ed unificato in un unico Codice la normativa in materia di protezione dei dati personali introdotta in Italia con la Legge 675/96 in recepimento della Direttiva Europea 45/96/CE.

In particolare il Codice fissa una serie di obblighi generali (art.31) e specifici di sicurezza (artt. 33-35 e Allegato B) ed introduce il concetto giuridico di "Rischio", di "Misura idonea" e di "Misura minima".

Sullo stesso piano e sempre con l'obiettivo di tutelare i dati personali, il Provvedimento del 27 novembre 2008, emanato dall'Autorità Garante per la protezione dei dati personali, identifica le misure di sicurezza, organizzative e tecnologiche, che devono essere adottate per la gestione e la verifica delle attività svolte dagli Amministratori di Sistema, dalla quasi totalità dei titolari dei trattamenti di dati personali effettuati con strumenti elettronici, ad eccezione di quelli effettuati in ambito pubblico e privato (realtà di piccole dimensioni) a fini amministrativo-contabili (ad es. gestione di ordinativi, buste paga e di ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in outsourcing, dipendenti).

Riguardo al tema della criminalità informatica, la Legge 48/2008, ratificando la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 23 Novembre 2001, ha apportato modifiche al Codice Penale e di Procedura Penale ed introdotto l'art. 24 bis, rubricato "Delitti informatici e trattamento illecito di dati", nel DLgs. 231/01 con il quale è stata estesa, a vari reati informatici, la responsabilità giuridica delle società e persone collettive nell'interesse delle quali gli stessi sono posti in essere da parte di soggetti apicali e dipendenti.

Sul piano della security, è opportuno tenere presente che il 24 gennaio 2013 l'Italia ha formalizzato la sua strategia nel campo della "Cybersecurity" attraverso il Decreto del Presidente del Consiglio dei Ministri recante "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*".

Tale strategia si è concretizzata in un "Piano per la protezione cibernetica e la sicurezza informatica" approvato con Decreto del Presidente del Consiglio dei Ministri il 27 gennaio 2014.

2.2.1 Il Codice sulla protezione dei dati personali (DLgs. 196/03)

Il Decreto Legislativo del 30 giugno 2003 n.196 in tema di tutela dei dati personali, stabilisce obblighi specifici e generali di sicurezza, che si sostanziano nella necessità, da parte del titolare del trattamento dei dati, di implementare una serie di misure minime di sicurezza identificate direttamente dalla normativa, e di idonee e preventive misure di sicurezza da identificare in base ad una attività di analisi dei rischi.

Per quanto riguarda le misure di sicurezza idonee e preventive, l'art. 31[56] stabilisce che devono essere individuate al fine di proteggere i dati dai:

- rischi di distruzione (riconducibile agli obiettivi di sicurezza della disponibilità e dell'integrità);
- perdita (riconducibile all'obiettivo di sicurezza della disponibilità);
- accesso non autorizzato (riconducibile agli obiettivi di sicurezza della confidenzialità, disponibilità ed integrità);
- trattamento non conforme o non consentito (riconducibile al controllo accessi ed all'integrità dei programmi).

Le misure minime (artt. 33, 34, 35) garantiscono invece quello che la legge definisce appunto il "livello minimo" di protezione dei dati e la loro adozione è "conditio sine qua non" per lo svolgimento delle attività di trattamento. Dette misure devono essere implementate secondo le modalità definite nel Disciplinare Tecnico allegato al Codice (Allegato B) e si applicano sia ai trattamenti effettuati nel settore privato che in quello pubblico.

Le tabelle di seguono proposte, referenziano schematicamente le misure minime di sicurezza previste nell'Allegato B e che risultano di particolare interesse rispetto alla costruzione del Modello organizzativo 231 in termini di loro futura applicabilità nell'ambito della mitigazione dei rischi ex art.24 bis.

Sistemi di autenticazione informatica (da 1 a 11 Allegato B)	
Ambito	**Misure minime di sicurezza previste**
Sistema di identity management	• Utilizzo di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti (art.1)
	•
Credenziali di autenticazione	• Utilizzo sicuro di userid e password (art.2)
	• Utilizzo sicuro dei dispositivi di autenticazione se presenti (smart card, ecc) (art.2)
	• Utilizzo sicuro di chiavi biometriche se presenti (art.2)
	• Assegnazione univoca delle credenziali per l'autenticazione (art.3)
	• Inutilizzabilità di credenziali di autenticazione già assegnati e revocati (art.6)
	• Disattivazione delle di credenziali di autenticazione se non utilizzate da almeno 6 mesi o in caso di perdita della qualità che consentiva l'accesso ai dati personali (art.7 e 8)
Caratteristiche della parola chiave	• 8 caratteri (art.5)
	• Non contiene riferimenti agevolmente riconducibili all'incaricato (art.5)
	• Modificata dall'incaricato al primo utilizzo (art.5)

[56] Art.31 del DLgs. n.196/2003 – "Obblighi di sicurezza – I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

Sistemi di autenticazione informatica (da 1 a 11 Allegato B)	
Ambito	**Misure minime di sicurezza previste**
	• Modificata almeno ogni 6 mesi in caso di trattamento di dati personali (art.5)
	• Modificata almeno ogni 3 mesi in caso di trattamento di dati sensibili (art.5)
Istruzioni organizzative e tecniche	• Utilizzo riservato della password e diligente custodia dei dispositivi di autenticazione (se presenti) (art.4)
	• Utilizzo sicuro della postazione di lavoro durante una sessione di trattamento (art.9)

Sistema di autorizzazione (da 12 a 14 Allegato B)	
Ambito	**Misure minime di sicurezza previste**
Utilizzo sistema di autorizzazione	• Utilizzo di un sistema di autorizzazione Quando per gli incaricati sono utilizzati profili di autorizzazione in ambito diverso (art.12)
Configurazione profili di autorizzazione	• Individuazione e configurazione dei profili di autorizzazione (per ciascun incaricato o per classi omogenee di incaricati) antecedente all'inizio dei trattamenti informatici (art.13)
Verifica dei profili assegnati	• Verifica periodica, almeno annuale, della sussistenza delle condizioni per la conservazione dei profili di autorizzazione (art.14)

Altre misure di sicurezza (da 15 a 18 Allegato B)	
Ambito	**Misure minime di sicurezza previste**
Aggiornamento individuazione ambito trattamento consentito	• Aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati (art.15)
	• Redazione e aggiornamento annuale della lista degli incaricati. La lista può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione (art.15)
Sistemi Antivirus	• Attivazione di idonei programmi antivirus e aggiornamento semestrale (art.16)
Sistemi Anti-Intrusione	• Attivazione di idonei programmi antintrusione e aggiornamento semestrale (art.16)
Programmi per elaboratore	• Aggiornamenti periodici dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (art.17)
	• In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale (art.17)
Frequenza del salvataggio dei dati	• Definizione di istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale (art.18 e 21)

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari (da 20 a 24 Allegato B)	
Ambito	**Misure minime di sicurezza previste**
Sistemi Anti-Intrusione	• Utilizzo di strumenti elettronici atti a proteggere da accessi abusivi (sistemi antintrusione) (art.20)
Istruzioni organizzative e tecniche	• Custodia e uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non autorizzati (art.21)
Utilizzo supporti rimovibili	• Se inutilizzabili, distruzione dei supporti di memorizzazione (art.22)
	• Riutilizzo dei supporti di memorizzazione in altri contesti solo se vi è un previo accertamento della distruzione irreversibile dei dati ivi precedentemente contenuti (art.22)
Accesso ai dati in caso di danneggiamento	• Attivazione di procedure e sistemi di disaster recovery dei dati e dei sistemi (art.23)
Trattamento dati idonei a rivelare stato di salute e vita sessuale	• Procedure atte ad assicurare il trattamento disgiunto dei dati sensibili dagli altri dati personali che permettono di identificare direttamente gli interessati (art.24)
	• Per il trattamento dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, adozione di tecniche di cifratura o utilizzo di codici identificativi o altre soluzioni che rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità (art.24 e 22 c6 DLgs.196/03)
	• Conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale rispetto agli altri dati personali trattati per finalità che non richiedono il loro utilizzo. (art.24 e 22 c7 DLgs.196/03)
	• Protezione e accesso controllato ai locali ove sono trattati i dati relativi all'identità genetica (art.24)
	• Trasporto dei dati relativi all'identità genetica in contenitori muniti di serratura o dispositivi equipollenti (art.24)
	• Trasferimento cifrato dei dati relativi all'identità genetica in formato elettronico (art.24)

Tra le misure minime previste nell'Allegato B era ricompresa anche la tenuta e la conservazione aggiornata di un Documento Programmatico sulla Sicurezza (DPS) che descriveva le azioni poste in essere dall'azienda per contenere, entro limiti accettabili, il rischio di distruzione, anche accidentale (perdita della disponibilità), di accesso non autorizzato (compromissione dell'integrità e della riservatezza), e di trattamento non consentito o non conforme alle finalità della raccolta dei dati personali detenuti e gestiti presso le sedi aziendali.

Ancorché tale misura (art.19) sia stata abrogata con il Decreto Legge n.5/2012, il DPS era e continua ad essere l'unico strumento atto a certificare l'attuazione degli adempimenti normativi cogenti previsti in materia di tutela dei dati personali.

Di conseguenza, la sua compilazione continua ad essere effettuata all'interno delle organizzazioni ed, in ogni caso, se ne raccomanda comunque l'adozione.

2.2.2 Il Provvedimento del Garante Privacy del 27.11.2008

Con il Provvedimento del 27 novembre 2008, il Garante per la protezione dei dati personali ha stabilito che tutte le organizzazioni - private e pubbliche - dovranno registrare e conservare i dati relativi agli accessi degli Amministratori di Sistema sui sistemi da loro gestiti, al fine di agevolare la "verifica sulla loro attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici".

Unica eccezione all'adozione del provvedimento è prevista per le pubbliche amministrazioni e le piccole aziende private che effettuano trattamenti elettronici di dati personali per soli fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008).

Il rispetto delle disposizioni contenute nel Provvedimento, alla cui inosservanza è applicata una sanzione amministrativa che va da un minimo di 30.000 euro a un massimo di 180.000 euro (art. 162 comma 2-ter DLgs. n.196/2003), comporta la necessità di mettere in campo una serie di misure organizzative per garantire la competenza e l'identificazione del personale preposto a ricoprire tale ruolo, e misure tecnologiche per assicurare la tracciabilità degli accessi e consentire l'effettuazione dei controlli periodici imposti dalla normativa.

Di seguito si riporta una tabella riassuntiva delle misure previste dal Provvedimento e che, anche in questo caso, risultano di interesse per la loro applicabilità quali misure di mitigazione dei rischi ex art.24 bis del DLgs.231/01 rispetto alla costruzione del Modello organizzativo.

Provvedimento del Garante Privacy del 27.11.2008	
Ambito	**Misure previste**
Valutazione delle Caratteristiche Soggettive	• L'organizzazione deve incaricare personale di comprovata esperienza, capacità ed affidabilità.
Designazioni Individuali	• La designazione è formale, individuale e reca l'elenco analitico degli ambiti di operatività consentiti.
Elenco degli Amministratori di Sistema	• Tenuta di un elenco aggiornato recante i nominativi degli Amministratori di Sistema con l'elenco delle funzioni ad essi attribuite.
Servizi in outsourcing	• Conservazione degli identificativi degli Amministratori di Sistema che operano nell'ambito dei servizi affidati i outsourcing (elenco aggiornato).
Registrazione degli Accessi	• Registrazione degli accessi e conservazione degli "access log" per un minimo di 6 mesi con garanzia di integrità ed inalterabilità, completezza e possibilità di verifica (prima della cancellazione).
Verifica delle Attività	• Verifica almeno annuale della rispondenza dell'operato degli Amministratori di Sistema alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti in relazione ai trattamenti dei dati personali.

2.2.3 La Direttiva italiana sulla Cyber Security

L'Italia, ritenendo che la minaccia cibernetica costituisce un rischio per la sicurezza nazionale, il *24 gennaio 2013* con Decreto del Presidente del Consiglio dei Ministri recante "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*" ha formalizzato la sua strategia nel campo della "cyber security".

Con questo decreto il nostro paese si pone ai primi posti nella lotta alle minacce cibernetiche e nella protezione del spazio cibernetico o "cyber space" cominciando ad affrontare il problema con un approccio

nazionale, strategico ed accentrato (laddove ad oggi la trattazione di questo tema era affidata prevalentemente ad enti pubblici o soggetti privati) e ponendo le basi per una cooperazione nazionale su più livelli, che coinvolga tutti gli attori pubblici nonché gli operatori privati interessati, ed internazionale sia in ambito bilaterale e multilaterale, sia con l'UE che con la NATO.

Lo "spazio cibernetico" è costituito "dall'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati e utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi"[57]. Vi sono dunque inclusi: internet, le reti di comunicazioni, i sistemi attuatori di processo e le apparecchiature mobili dotate di connessione di rete.

La "minaccia cibernetica" è il "complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia in particolare, nelle azioni di singoli individui o organizzazioni, statuali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi".

La "sicurezza cibernetica" invece è la condizione per cui il cyber-space "risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi"[58].

La nuova strategia nazionale avrà tre scopi principali: individuare le minacce, prevenire i rischi e coordinare una risposta in situazioni di crisi.

Sono tre i livelli d'intervento:

- il primo di indirizzo politico e di coordinamento strategico affidato al "Comitato interministeriale per la sicurezza della Repubblica (CISR)" che si occuperà della elaborazione di un Piano nazionale per la sicurezza dello spazio cibernetico. A sostegno del CISR nel suo compito, verrà istituita presso la Scuola di formazione del DIS un organo dedicato, cui affidare anche compiti funzionali alla promozione e diffusione di una cultura della sicurezza cibernetica;
- il secondo di supporto operativo ed amministrativo a carattere permanente affidato al "Nucleo per la Sicurezza Cibernetica" presieduto dal Consigliere Militare del Presidente del Consiglio, con funzioni di raccordo nei confronti di tutte le amministrazioni ed enti competenti per l'attuazione degli obiettivi e delle linee di azione indicate dalla pianificazione nazionale e che provvederà a programmare l'attività operativa a livello interministeriale e ad attivare le procedure di allertamento in caso di crisi;
- il terzo livello, di gestione delle crisi affidato al "Tavolo Interministeriale di Crisi Cibernetica", con il compito di curare e coordinare le attività di risposta e di ripristino della funzionalità dei sistemi, avvalendosi di tutte le componenti interessate.

Sul piano pratico, la Direttiva prevede anche l'istituzione di un Computer Emergency Response Team nazionale, accanto al già istituito CERT della Pubblica Amministrazione.

L'articolo 11 della Direttiva contiene, infine, indicazioni specifiche per gli operatori privati che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, e che gestiscono le

[57] Articolo 2 lett. h) del D.P.C.M. 24.01.2013

[58] Articolo 2 lett. I) del D.P.C.M. 24.01.2013

infrastrutture critiche a livello nazionale ed europeo, il cui funzionamento si basa su sistemi informatici e di telecomunicazione. Questi dovranno:

- comunicare al Nucleo per la Sicurezza Cibernetica qualsiasi violazione significativa di sicurezza o all'integrità dei loro sistemi informatici utilizzando canali di trasmissione protetti;
- adottare le best practice e le misure finalizzate all'obiettivo della sicurezza cibernetica;
- fornire informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza;
- collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

La sicurezza dello spazio cibernetico, dunque, è articolata su componenti di natura politica, economica, normativa e tecnica, e le principali sfide per il futuro della cyber-security in Italia consisteranno nelle possibilità di partnership tra settore pubblico e privato, indispensabili per la protezione delle infrastrutture critiche estranee alle pubbliche amministrazioni.

2.2.4 Il Piano nazionale per la protezione cibernetica e la sicurezza informatica

Il 27 gennaio 2014 è stata approvato con Decreto del Presidente del Consiglio dei Ministri il "Piano per la protezione cibernetica e la sicurezza informatica".

Il Piano individua undici indirizzi operativi e i relativi obiettivi specifici da conseguire e le relative linee d'azione da porre in essere per dare concreta attuazione al Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico, in linea con quanto previsto dal Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

Tra le linee d'azione, si menzionano:

- il potenziamento del sistema di info-sharing con riferimento alla collaborazione tra i settori pubblico e privato (inclusi i fornitori di servizi), anche per l'individuazione e la riduzione delle vulnerabilità;
- l'adozione di un database integrato per la raccolta delle segnalazioni di incidente e delle contromisure intraprese dai fornitori di servizi e di un sistema integrato per la rilevazione degli allarmi, online incident/intrusion detection, strong authentication;
- il mantenimento di uno schema nazionale per la certificazione dei processi utilizzati dai sistemi informativi, in accordo con lo standard UNI ISO/ IEC 27001:2006;
- l'individuazione di una metodologia di Information Risk Management univoca e condivisa a livello strategico, adottando un modello per le infrastrutture critiche nazionali informatizzate, in accordo con la UNI EN ISO 27005:2011.

2.3 Modello organizzativo DLgs.231/01 e Delitti Informatici

La costruzione del modello organizzativo, idoneo a prevenire la commissione dei delitti informatici e consentire l'esonero dell'ente dalla responsabilità e dalle relative sanzioni pecuniarie ed interdittive, impone:

- la mappatura delle aree di rischio cd. sensibili, riferibili ai servizi interni ed ai servizi erogati alla clientela. Le aree di rischio riguardano sia i servizi interni che i servizi ai clienti;
- l'adozione di misure di mitigazione dei rischi (misure sicurezza fisica, logica ed organizzativa) sia già espressamente richieste dalla legge che derivanti da specifiche attività di analisi dei rischi.

- l'applicazione delle sopracitate misure, all'operatività dei sistemi informatici ed a quella dei destinatari del modello (personale interno e fornitori/consulenti).

La tipica architettura per il Modello organizzativo dovrebbe includere:

- un documento "padre" nel quale sono riportate le predisposizioni/misure/controlli validi nell'ente (misure trasversali);
- tanti documenti "figli" quanti sono i "protocolli" a fronte delle "aree di rischio" individuate (misure verticali).

Le aree di rischio sono individuate tenendo presenti le "classi di reato presupposto" stabilite nel D.Lgs 231/01 (gli articoli 24- 25-duodecies) che risultano applicabili in funzione del tipo di ente, settore di mercato, struttura dell'ente, rapporti internazionali, etc..

Il Protocollo struttura di riferimento per delitti informatici dovrebbe includere:

1. Elencazione dei reati.
2. Aree sensibili individuate per i reati informatici.
3. Sistemi utilizzati per i processi interni dell'ente:
    - Le specifiche aree di rischio;
    - Le possibili condotte illecite;
    - L'individuazione delle strutture organizzative interessate;
    - Le misure a contrasto per le ipotesi di reati informatici;
    - Le regole comportamentali a cura dei Destinatari del Modello;
    - Le modalità di veicolazione delle regole verso Fornitori/Outsourcers.
4. Servizi ai Clienti dell'ente (sviluppo, fornitura, esercizio e manutenzione,…):
    - Il medesimo sviluppo del punto 3
5. Organismo di vigilanza e i delitti informatici.
6. Controlli specifici svolti dall'Organismo.
7. Flussi informativi verso l'Organismo e relative tempistiche/periodicità.

2.4 Rischi ex 24 bis DLgs.231/01 e Misure di sicurezza

In ottica Cloud, il tema della criminalità informatica e della responsabilità delle organizzazioni per delitti informatici e trattamento illecito di dati, assume una dimensione particolarmente rilevante sotto molteplici aspetti.

I maggiori rischi riguardano i reati di accesso abusivo ai sistemi informatici e telematici, con conseguente acquisizione di dati utili alla commissione di ulteriori reati quali il furto di identità, il furto di proprietà intellettuale, lo spionaggio industriale e le estorsioni rivolte alle imprese.

Tali reati sono facilitati dall'alta concentrazione di personale tecnico operante con "account ad elevati privilegi" e dall'elevata quantità di dati presenti sulle infrastrutture informatiche, dalla loro diversa natura e grado di sensibilità.

La definizione e la messa a conoscenza di specifiche deleghe nelle differenti aree dell'organizzazione, attraverso ad esempio la nomina degli amministratori di sistema e dei loro collaboratori specificandone ruolo, poteri e responsabilità risulta essenziale.

Allo stesso modo è di fondamentale importanza definire specifiche politiche di sicurezza e proceduralizzare le attività informatiche e tutte quelle attività da considerarsi a rischio-reato, svolte con l'ausilio o per mezzo di strumenti informatici e telematici (come ad es. la gestione dei documenti informatici, dei dati riservati e sensibili o delle credenziali di accesso ai sistemi).

Molte delle misure di mitigazione dei rischi di commissione dei reati informatici correlati all'utilizzo delle tecnologie ICT, sono mutuabili dal quadro normativo di riferimento in tema di security, data protection e cybercrime analizzato nei precedenti paragrafi.

Sulla base di quanto fin qui esposto viene, quindi, di seguito proposta una "Cross Reference Map" tra:

a. Reati informatici presupposto ex art.24 bis del DLgs. 231/01.
b. Misure di mitigazione dei rischi derivanti da quadro normativo analizzato.

Nell'ambito della schematizzazione, le misure di sicurezza di origine normativa sono state aggregate sulla base dei seguenti Principi di Controllo ICT:

1. Identificazione e separazione dei ruoli.
2. Sistemi autorizzativi (processi, procedure e meccanismi tecnici).
3. Sistemi di controllo degli accessi (processi, procedure e meccanismi tecnici).
4. Tracciamento delle attività svolte sui sistemi/sulla rete.
5. Sicurezza delle Operazioni.
6. Monitoraggio ed esecuzione di verifiche periodiche.
7. Gestione degli incidenti di sicurezza.
8. Formazione, Addestramento e sensibilizzazione del personale.

		Fattispecie di reato ex 24 bis 231/01	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
Principi di controllo	**Rif. Norm.**	**Misure di Sicurezza**	Accesso abusivo ad un sistema informatico telematico (art. 615ter c.p.	Detenzione e diffusione abusiva di codici di accesso sistemi informatici o telematici (art.615quater c.p.)	Diffusione di apparecchiature, dispositivi programmi informatici diretti a danneggiare interrompere un sistema informatico o telematic (art.615-quinquies c.p.)	Intercettazione, impedimento o interruzione illecita comunicazioni informatiche o telematiche(art. 617 quater c.p.	Installazione di apparecchiature atte ad intercettar impedire od interrompere comunicazioi informatiche o telematiche (art.61-quinquies c.p.	Danneggiamento di informazioni, dati e programr informatici (art. 635bis c.p.	Danneggiamento di informazioni, dati e programr informatici utilizzati dallo Stato o da altro en pubblico o comunque di pubblica utilità (art. 61-ter	Danneggiamento di sistemi informatici o telemati (art. 635 quater c.p.)	Danneggiamento di sistemiinformatici o telematici c pubblica utilità (art. 635 quinquies c.p.)	Frode informatica del soggetto che presta servizi certificazione (Art.640 quinquies c.p.	Falsità in un documento informatico pubblico privato (art. 491 bis c.p.)
Identificazione e separazione dei ruoli (SOD)	Provv. GP 27.11.08	La designazione degli AdS è formale, individuale e reca l'elenco analitico degli ambiti di operatività consentiti.	X										
	DLgs.196/03 Allegato B (art 15)	Aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati.	X					X	X	X	X		
	DLgs.196/03 Allegato B (art 15)	Redazione e aggiornamento annuale della lista degli incaricati. La lista può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.	X										
Sistemi autorizzativi (processi, procedure e meccanismi tecnici)	DLgs.196/03 Allegato B (art 12)	Utilizzo di un sistema di autorizzazione quando per gli incaricati sono utilizzati profili di autorizzazione in ambito diverso	X										
	DLgs.196/03 Allegato B (art 13)	Individuazione e configurazione dei profili di autorizzazione (per ciascun incaricato o per classi omogenee di incaricati) antecedente all'inizio dei trattamenti informatici	X										
	DLgs.196/03 Allegato B (art 14)	Verifica periodica, almeno annuale, della sussistenza delle condizioni per la conservazione dei profili di autorizzazione	X					X	X	X	X		
	DLgs.196/03 Allegato B (art 15)	Aggiornamento periodico, con cadenza almeno annuale del profilo autorizzativi di accesso degli incaricati ai dati ed alle apparecchiature						X	X	X	X		
Sistemi di controllo degli accessi (processi, procedure e meccanismi tecnici)	DLgs.196/03 Allegato B (art 1)	Utilizzo di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti	X										
	DLgs.196/03 Allegato B (art 2)	Utilizzo sicuro di userid e password	X	X									
	DLgs.196/03 Allegato B (art 2)	Utilizzo sicuro dei dispositivi di autenticazione se presenti (smart card, ecc)	X	X									X
	DLgs.196/03 Allegato B (art 2)	Utilizzo sicuro di chiavi biometriche se presenti	X	X									
	DLgs.196/03 Allegato B (art 3)	Assegnazione univoca delle credenziali per l'autenticazione	X										
	DLgs.196/03 Allegato B (art 6)	Inutilizzabilità di credenziali di autenticazione già assegnati e revocati	X										
	DLgs.196/03 Allegato B (art 7 e 8)	Disattivazione delle di credenziali di autenticazione se non utilizzate da almeno 6 mesi o in caso di perdita della qualità che consentiva l'accesso ai dati personali	X	X									
	DLgs.196/03 Allegato B (art 5)	Utilizzo di password sicure (8 caratteri, non contenenti riferimenti riconducibili all'incaricato, modificata al primo accesso ed ogni 3/6 mesi)	X	X									

		Fattispecie di reato ex 24 bis 231/01	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
Principi di controllo	**Rif. Norm.**	**Misure di Sicurezza**	Accesso abusivo ad un sistema informatico telematico (art. 615ter c.p.)	Detenzione e diffusione abusiva di codici di accesso sistemi informatici o telematici (art.615quater c.p.)	Diffusione di apparecchiature, dispositivi programmi informatici diretti a danneggiare interrompere un sistema informatico o telematic (art.615-quinquies c.p.)	Intercettazione, impedimento o interruzione illecita comunicazioni informatiche o telematiche(art. 617 quater c.p.	Installazione di apparecchiature atte ad intercettar impedire od interrompere comunicazio informatiche o telematiche (art.61-quinquies c.p.	Danneggiamento di informazioni, dati e programr informatici (art. 635bis c.p.)	Danneggiamento di informazioni, dati e programr informatici utilizzati dallo Stato o da altro en pubblico o comunque di pubblica utilità (art. 65-ter	Danneggiamento di sistemi informatici o telemati (art. 635 quater c.p.)	Danneggiamento di sistemiinformatici o telematici c pubblica utilità (art. 635 quinquies c.p.)	Frode informatica del soggetto che presta servizi certificazione (Art.640 quinquies c.p.	Falsità in un documento informatico pubblico privato (art. 491 bis c.p.)
	DLgs.196/03 Allegato B (art 24)	Protezione e accesso controllato ai locali ove sono trattati i dati relativi all'identità genetica	X					X	X	X	X		
Tracciamento delle attività svolte sui sistemi/sulla rete	Provv. GP 27.11.08	Registrazione degli accessi degli AdS e conservazione degli "access log" per un minimo di 6 mesi con garanzia di integrità ed inalterabilità, completezza e possibilità di verifica (prima della cancellazione).	X	X	X	X	X	X	X	X	X	X	X
Sicurezza delle Operazioni	DLgs.196/03 Allegato B (art 16)	Attivazione di idonei programmi antivirus e aggiornamento semestrale			X			X	X	X	X		
	DLgs.196/03 Allegato B (art 16 e 20)	Attivazione di idonei programmi antintrusione e aggiornamento semestrale	X					X	X	X	X		
	DLgs.196/03 Allegato B (art 17)	Aggiornamenti periodici dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale	X		X			X	X	X	X		
	DLgs.196/03 Allegato B (art 22)	Procedure di custodia e utilizzo dei supporti di memorizzazione dei dati onde evitare accessi non autorizzati e trattamenti non consentiti ai dati sensibili o giudiziari	X										
	DLgs.196/03 Allegato B (art 22)	Se inutilizzabili, distruzione dei supporti di memorizzazione che contenevano ai dati sensibili o giudiziari	X										
	DLgs.196/03 Allegato B (art 22)	Riutilizzo dei supporti di memorizzazione in altri contesti solo se vi è un previo accertamento della distruzione irreversibile dei dati sensibili o giudiziari ivi precedentemente contenuti	X										
	DLgs.196/03 Allegato B (art 23)	Attivazione di procedure e sistemi di disaster recovery dei dati e dei sistemi			X			X	X	X	X		
	DLgs.196/03 Allegato B (art 24)	Procedure atte ad assicurare il trattamento disgiunto dei dati sensibili dagli altri dati personali che permettono di identificare direttamente gli interessati	X			X							
	DLgs.196/03 (art 22 c6) Allegato B (art 24)	Per il trattamento dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, adozione di tecniche di cifratura o utilizzo di codici identificativi o altre soluzioni che rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.	X			X							
	DLgs.196/03 (art 22 c7)) Allegato B (art	Conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale rispetto agli altri dati personali trattati per	X										

		Fattispecie di reato ex 24 bis 231/01	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
Principi di controllo	**Rif. Norm.**	**Misure di Sicurezza**	Accesso abusivo ad un sistema informatico telematico (art. 615ter c.p.)	Detenzione e diffusione abusiva di codici di accesso sistemi informatici o telematici (art.615quater c.p.)	Diffusione di apparecchiature, dispositivi programmi informatici diretti a danneggiare interrompere un sistema informatico o telematic (art.615-quinquies c.p.)	Intercettazione, impedimento o interruzione illecita comunicazioni informatiche o telematiche (art. 617 quater c.p.)	Installazione di apparecchiature atte ad intercettar impedire od interrompere comunicazio informatiche o telematiche (art.61-quinquies c.p.	Danneggiamento di informazioni, dati e programr informatici (art. 635bis c.p.)	Danneggiamento di informazioni, dati e programr informatici utilizzati dallo Stato o da altro en pubblico o comunque di pubblica utilità (art. 61-ter	Danneggiamento di sistemi informatici o telemati (art. 635 quater c.p.)	Danneggiamento di sistemiinformatici o telematici c pubblica utilità (art. 635 quinquies c.p.)	Frode informatica del soggetto che presta servizi certificazione (Art.640 quinquies c.p.	Falsità in un documento informatico pubblico privato (art. 491 bis c.p.)
	24)	finalità che non richiedono il loro utilizzo.											
	DLgs.196/03 Allegato B (art 24)	Trasporto dei dati relativi all'identità genetica in contenitori muniti di serratura o dispositivi equipollenti	X					X	X				X
	DLgs.196/03 Allegato B (art 24)	Trasferimento cifrato dei dati relativi all'identità genetica in formato elettronico	X			X		X	X				X
Monitoraggio ed esecuzione di verifiche periodiche	Provv. GP 27.11.08	Verifica almeno annuale della rispondenza dell'operato degli Amministratori di Sistema alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti in relazione ai trattamenti dei dati personali.	X	X	X			X	X				
Gestione degli incidenti di sicurezza	Reg.UE Data Protection Reg.UE 611/2013 Provv.GP 04.04.13	Notificazione delle violazioni di dati al Garante Privacy (ISP)	X		X		X	X	X				
	Reg.UE 611/2013 Provv.GP 04.04.13	Notificazione delle violazioni rilevanti di dati ai soggetti interessati (ISP)	X		X		X	X	X				
	Direttiva NIS	Notificazione degli incidenti di sicurezza	X	X	X	X	X	X	X	X	X	X	X
	Direttiva 2008/114/CE	Notificazione degli incidenti di sicurezza a ECI	X	X	X	X	X	X	X	X	X	X	X
Formazione, Addestramento e sensibilizzazione del personale	DLgs.196/03 Allegato B (art 4)	Istruzioni organizzative e tecniche sull'utilizzo riservato della password	X										
	DLgs.196/03 Allegato B (art 4)	Istruzioni organizzative e tecniche sulla diligente custodia dei dispositivi di autenticazione (se presenti)	X	X									
	DLgs.196/03 Allegato B (art 9)	Istruzioni organizzative e tecniche sull'utilizzo sicuro della postazione di lavoro durante una sessione di trattamento	X	X									
	DLgs.196/03 Allegato B (art 18)	Istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale			X			X	X	X	X		
	DLgs.196/03 Allegato B (art 21)	Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti	X					X	X				

3.0 Cross reference con la CSA – CCM

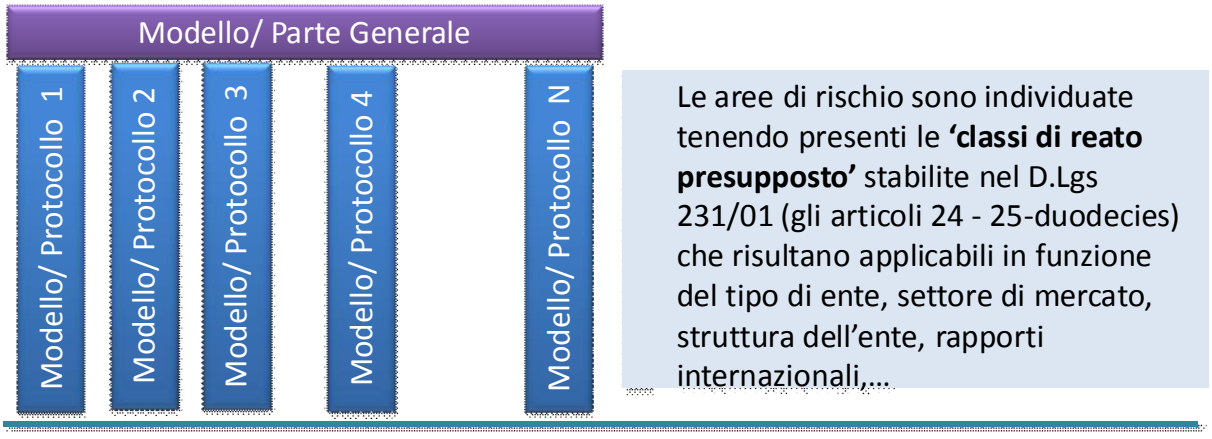
Il quadro di tematiche esposto nei precedenti capitoli evidenzia che per una effettiva efficacia dei cosidetti "modelli 231", in generale ed in particolare nel contesto di servizi cloud computing, assume una importanza fondamentale l'applicazione delle misure di sicurezza già richieste dalla applicabile normative obbligatoria (specifiche prescrizioni di legge come ad esempio quelle derivaneti dalla normativa privacy & protezione dati personali) e dagli standard di riferimento di settore (ISO/IEC 27001, PCI-DSS,…).

Tali misure dovranno trovare riscontri nei rilevanti protocolli per le aree di rischi individuate sempre ai fini della redazione ed attuazione del modello 231.

Caratteristiche essenziali per la costruzione del Modello 231

La tipica architettura per il Modello:

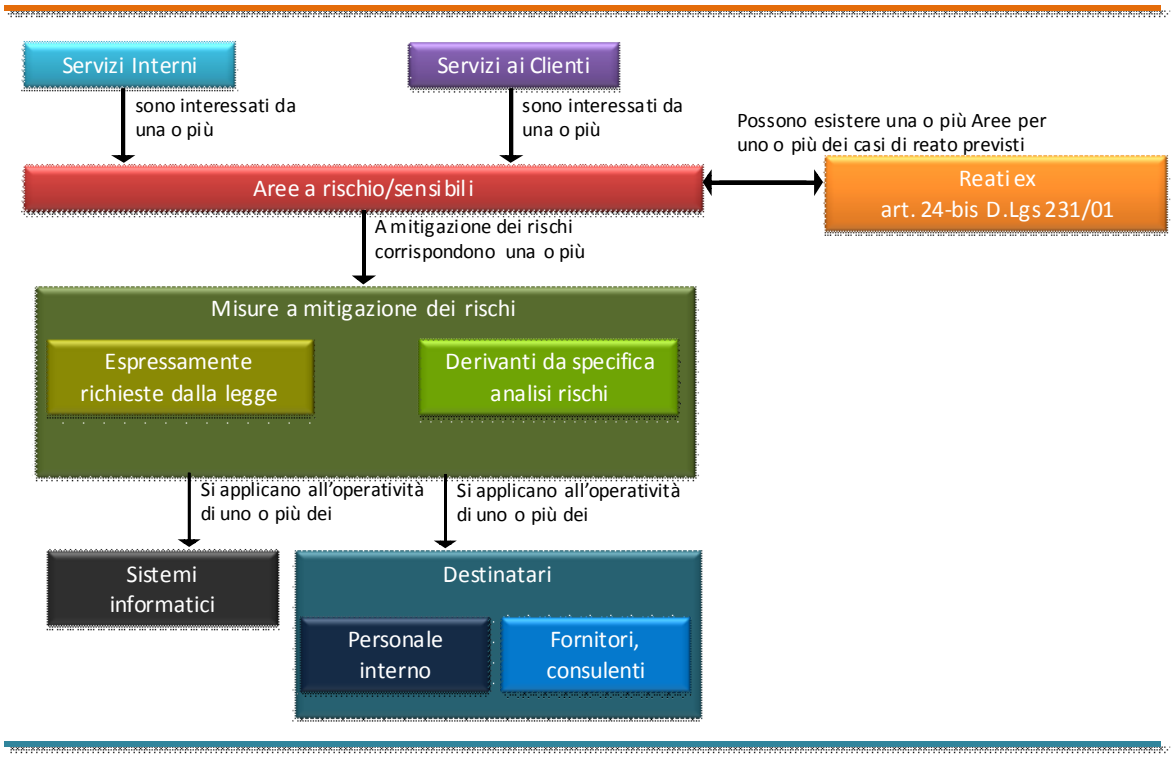
- Un documento 'padre' nel quale sono riportate le predisposizioni/misure/controlli validi nell'ente (misure trasversali)
- Tanti documenti 'figli' quanti sono i 'protocolli' a fronte delle 'aree di rischio' individuate (misure verticali).



Le aree di rischio sono individuate tenendo presenti le **'classi di reato presupposto'** stabilite nel D.Lgs 231/01 (gli articoli 24 - 25-duodecies) che risultano applicabili in funzione del tipo di ente, settore di mercato, struttura dell'ente, rapporti internazionali,…

In particolare per quanto riguarda i delitti informatici, deve sempre essere tentuo presente il contesto di riferimento generale per la possible commissioni dei reati che investe non solo l'organizzazione interna (personale interno, servizi interni quail amministrazione e finanza, gestione del personale, servizi informatici interni,…) ma anche i servizi forniti ai Clienti e il coinvolgimento di fornitori e partner nel business aziendale.

Modello organizzativo Dlgs 231/01 e delitti informatici



In contesto servizi cloud computing, che per un ente possono riguardare sia i suoi servizi interni che quelli esterni erogati ai Clienti, la matrice di controlli realizzata da Cloud Security Alliance rappresenta un affidabile punto di riferimento per individuare le misure da applicare per uno specifico caso di interesse. Si ricorda che tale matrice riporta anche un importante mapping rispetto gli standard internazionali (es. iso 27001, PCI-DSS) linee guida emesse da ben noti enti quali il NIST (National Institute of Technology americano) ed alcune normative.

Per quanto concerne i servizi cloud computing e le responsabilità degli enti in relazione ai delitti informatici è importante evidenziare che i controlli CCM offrono già un'ampia copertura per le misure richieste ai fini del modello 231. Nella attuale ultima versione della matrice CCM, ai fini di questo studio è stata aggiunta una ultima colonna "231" allo scopo di fornire una prima indicazione di copertura, che potrà essere ulteriormente raffinata successivamente indicando come riferimento gli associabili delitti informatici di interesse per i modelli 231 (fonte di requisito primario) oppure le misure di sicurezza derivanti dalle normative applicabil (in tal caso il mapping sarà in riferimento non al requisito primario bensì rispetto ad una particolare contromisura già individuata dalle normative applicabili).

La stima effettuata della copertura "231" offerta dai controlli presenti nella matrice CCM, in termini percentuali e sintetici, è così rappresentabile (secondo sheet dell'incluso file excel).

Modello organizzativo Dlgs 231/01 e controlli CSA-CCM

https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/

Classi di requisiti CSA-CCM	% di requisiti direttamente coinvolti per la conformità al D.Lgs 231/01
Application & Interface Security	50%
Audit Assurance & Compliance	67%
Business Continuity Management & Operational Resilience	25%
Change Control & Configuration Management	20%
Data Security & Information Lifecycle Management	50%
Datacenter Security	89%
Encryption & Key Management	75%
Governance and Risk Management	83%
Human Resources	42%
Identity & Access Management	85%
Infrastructure & Virtualization Security	75%
Interoperability & Portability	0%
Mobile Security	50%
Security Incident Management, E-Discovery & Cloud Forensic	60%
Supply Chain Management, Transparency and Accountability	22%
Threat and Vulnerbility Management	67%