Trattamento dati: le novità legislative

Focus: il provvedimento del Garante del 12 maggio 2011

Gabriele Faggioli

Clusit, 17 maggio 2012

Considerazioni iniziali

- Il 2011 e il 2012 sono stati caratterizzati da importanti novità nel settore normativo della sicurezza dei sistemi informativi:
- Abolizione decreto Pisanu
- Provvedimento Garante per la protezione dei dati personali 12 maggio 2011 inerente la tracciabilità degli accessi ai dati bancari
- Decreto legge n. 70/2011 “Semestre Europeo - Prime disposizioni urgenti per l'economia” successivamente convertito con legge n° 106/2011
- Decreto Legge n. 201/2011, noto come Decreto Salva Italia, contenente le “Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici”, convertito con la legge del 22 dicembre 2011, n. 214
- Decreto Semplificazioni 5/2012 approvato il 27.01.2012 convertito con la legge 4 aprile 2012 n. 35

Considerazioni iniziali

- **Tra le altre cose le modifiche hanno riguardato:**

- **La nozione di «dato personale» con quindi incidenza sulla applicazione del d.lgs 196/03**

- **L'ambito di applicazione prima, e l'esistenza poi, del Documento Programmatico sulla Sicurezza**

- **La nozione di trattamento per finalità amministrative e contabili**

La liberalizzazione del WIFI

- Con il Decreto Milleproroghe (d.l. 255/10) sono state apportate modifiche di notevole rilievo all'art. 7, I e IV comma, del Decreto Pisanu, nella parte in cui prevedeva obblighi che condizionavano le modalità di installazione e di utilizzo della rete internet nei luoghi pubblici o aperti al pubblico. Ovvero:

  - Nel sistema previgente l'accesso al servizio wi-fi era subordinato all'obbligo di autenticazione dei dati anagrafici riportati sul documento d'identità dell'utente, per monitorare le singole operazioni e per favorire l'archiviazione dei dati acquisiti nel corso della navigazione. **Oggi il predetto obbligo è stato integralmente abrogato a sostegno di una maggiore libertà per l'utente di accedere alla pubblica comunicazione telematica senza alcuna preventiva registrazione dei dati e con minor controllo sulle singole operazioni effettuate.**

  - L'art. 7, I comma, nella vecchia formulazione prevedeva l'obbligo per i gestori di pubblici esercizi o circoli privati di qualsiasi specie - nel quale fossero posti a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni, anche telematiche - di richiedere una preventiva licenza alla questura competente. **In ogni caso oggi tale obbligo è stato ristretto ai soli gestori che offrano la connettività quale attività principale (internet point).**

Il campo di applicazione del d.lgs 196/03

Tabella 1. Regime applicabile da maggio a dicembre 2011

Dati inerenti le persone fisiche		Dati inerenti le persone giuridiche enti e associazioni	
Trattamenti con finalità amministrative e contabili	Semplificazioni (es. non applicazione provvedimento amministratori di sistema)	**Trattamenti con finalità amministrative e contabili**	Disapplicazione integrale d.lgs 196/03 e provvedimenti collegati
Trattamenti senza finalità amministrative e contabili	Applicazione integrale d.lgs 196/03 (es. marketing)	**Trattamenti senza finalità amministrative e contabili**	Applicazione integrale d.lgs 196/03 (es. marketing)

Il campo di applicazione del d.lgs 196/03

Tabella 2. Regime applicabile da fine dicembre 2011

<table>
<tr><th></th><th>Dati inerenti le persone fisiche</th><th colspan="2">Dati inerenti le persone giuridiche enti e associazioni</th></tr>
<tr><td>Trattamenti con finalità amministrative e contabili</td><td>Semplificazioni (es. non applicazione provvedimento amministratori di sistema)</td><td colspan="2" rowspan="2">Disapplicazione integrale d.lgs 196/03 e provvedimenti collegati</td></tr>
<tr><td>Trattamenti senza finalità amministrative e contabili</td><td>Applicazione integrale d.lgs 196/03 (es. marketing)</td></tr>
<tr><td></td><td></td><td>Abbonati</td><td>Applicazione delle regole inerenti il marketing e la data retention</td></tr>
</table>

Il campo di applicazione del d.lgs 196/03

Articolo 4 del d.lgs. 196/2003 (Codice in materie di protezione dei dati personali):

- **b) "dato personale**", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

- c) "**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;

- d) "**dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

- e) "**dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Il campo di applicazione del d.lgs 196/03

Si consideri anche **l'articolo 98 del d.lgs. 30/2005** (Codice della Proprietà Industriale) che con riferimento alle **informazioni segrete** ha stabilito che:

1. Costituiscono oggetto di tutela le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:
   - **a)** **siano segrete**, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;
   - **b)** **abbiano valore economico in quanto segrete**;
   - **c)** **siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.**

2. Costituiscono altresì oggetto di protezione i dati relativi a prove o altri dati segreti, la cui elaborazione comporti un considerevole impegno ed alla cui presentazione sia subordinata l'autorizzazione dell'immissione in commercio di prodotti chimici, farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche.

Il documento programmatico sulla sicurezza

Anno	Previsione
2003-ago 2008	Assenza di deroghe all'obbligo di redazione del Documento Programmatico sulla Sicurezza
Agosto 2008-luglio 2011	Articolo 34 comma 1bis d.lgs 196/03. Per i soggetti che trattano **soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto**, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, **la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione**, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, **di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. Omississ**
Luglio 2011-gennaio 2012	Articolo 34 comma 1bis d.lgs 196/03. Per i soggetti che trattano **soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parent**i, **la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazion**e, resa dal titolare del trattamento ai sensi dell' articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, **di trattare soltanto tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinare tecnico contenuto nell'allegato B)**. Omississ
Gen 2012	**Abrogazione integrale Documento Programmatico sulla Sicurezza**

Il Documento Programmatico sulla sicurezza

- La Legge 4 aprile 2012 n. 35 di conversione del Decreto Legge 9 febbraio 2012 n. 5 prevede, fra l'altro:
- "*Art. 45 Semplificazioni in materia di dati personali 1. ((Al codice in materia di protezione dei dati personali, di cui al decreto legislativo)) 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni: a) all'articolo 21 dopo il comma 1 é inserito il seguente: «1-bis. Il trattamento dei dati giudiziari é altresì consentito quando é effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, ((previo parere del Garante per la protezione dei dati personali,)) che specificano la tipologia dei dati trattati e delle operazioni eseguibili.»; b) all'articolo 27, comma 1, é aggiunto, in fine, il seguente periodo: «Si applica quanto previsto dall'articolo 21, comma 1-bis.»;*
- ***c) all'articolo 34 é soppressa la lettera g) del comma 1 ed é abrogato il comma 1-bis;***
- ***d) nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B sono soppressi i paragrafi da 19 a 19.8 e 26****".*

- Quindi, niente più obbligo di redazione e aggiornamento del DPS né obbligo sostitutivo di autocertificazione.

I trattamenti per finalità amministrative e contabili

- Il provvedimento sugli amministratori di sistema
- Ai sensi dell'art. 154, comma 1, lett. c) del Codice il Garante ha quindi prescritto l'adozione delle misure enunciate ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed **effettuati con strumenti elettronici**, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice), **salvo per quelli effettuati in ambito pubblico e privato a 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):

- Quali sono i trattamenti fuori ambito:
  - Nel provvedimento del 19 giugno 2008 il Garante per la protezione dei dati personali ha emanato un provvedimento contenente "**Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili**" dove si legge: "Diverse *realtà, specie imprenditoriali di piccole e medie dimensioni, trattano dati, anche in relazione a obblighi contrattuali, precontrattuali o di legge, esclusivamente per finalità di ordine amministrativo e contabile (gestione di ordinativi, buste paga e di ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in outsourcing, dipendenti); omississ*"
  - *Oggi: articolo 34 comma 1ter d.lgs 196/03*

I trattamenti per finalità amministrative e contabili

La nozione di trattamento per finalità amministrative e contabili

Articolo 34 comma 1-ter d.lgs 196/03).

Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli **connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati**.

In particolare, perseguono tali finalità le **attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro**.

Considerazioni generali

- **ATTENZIONE!**
- **Non sono abolite le misure minime di sicurezza**
- **Non è abolito l'allegato B al d.lgs 196/03**
- **Permangono le responsabilità penali in caso di mancata adozione delle misure minime di sicurezza**
- **Rimane vigente il provvedimento sugli Amministratori di Sistema**
- **Occorre valutare le clausole contrattuali previste a tutela della riservatezza in caso di outsourcing/cloud**

Il controllo sui lavoratori

- L’articolo 4 dello Statuto dei Lavoratori
  - E’ vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori
  - Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro provvede la Direzione Regionale del Lavoro *omississ*

Applicazione art. 4 comma II S.d.L.

- **La giurisprudenza in materia di controlli difensivi (sentenza Corte di Cassazione n. 4375 del 23 febbraio 2010)**
- **Caso**
  - Ad una lavoratrice, è stato intimato il licenziamento attraverso due distinte contestazioni disciplinari relative ad un utilizzo illegittimo della rete internet aziendale dovuto a ripetuti accessi per esigenze estranee all'attività lavorativa.
  - La lavoratrice ha impugnato entrambi i licenziamenti davanti al Tribunale di Milano, il quale ne ha dichiarato l'illegittimità. Il Tribunale, quanto al primo licenziamento, riteneva che i fatti contestati, sintetizzabili nell'accesso a Internet per ragioni non di servizio in contrasto con il regolamento aziendale del 4-5-2001, **fossero stati rilevati e registrati da un programma di controllo informatico centralizzato (Super Scout), in violazione della L. n. 300 del 1970, art. 4, comma 2, con la conseguente inutilizzabilità dei dati acquisiti**. In ogni caso riteneva violate **le regole di proporzionalità e gradualità delle sanzioni disciplinari**. Quanto, poi, al secondo licenziamento, il giudice riteneva la contestazione tardiva, poiché i fatti contestati erano in parte antecedenti alla prima contestazione disciplinare e in parte una duplicazione dei fatti già contestati e per i mesi precedenti la prima contestazione, sicuramente conoscibili con il programma Super Scout.
  - Avverso la detta sentenza proponeva appello la società datrice di lavoro, deducendo in relazione al primo licenziamento, che **i controlli attuati, in quanto volti contro comportamenti illeciti espressamente vietati dalla società, non erano inibiti dalla L. n. 300 del 1970, art. 4**, e che il comportamento contestato, costituente grave inadempimento degli obblighi aziendali, così come portati a conoscenza della lavoratrice attraverso il regolamento aziendale, giustificava il licenziamento per giusta causa.

Applicazione art. 4 comma II S.d.L.

- **La giurisprudenza in materia di controlli difensivi (sentenza Corte di Cassazione n. 4375 del 23 febbraio 2010)**
- **Caso**
  - La Corte d'Appello di Milano confermava la sentenza appellata e condannava l'appellante al pagamento delle spese. **In sintesi la Corte medesima, riteneva applicabile ai fatti addebitati ed accertati a sostegno del primo licenziamento la L. n. 300 del 1970, art. 4, comma 2, con conseguente indispensabilità di un accordo sindacale o, in mancanza, dell'autorizzazione della Direzione provinciale del lavoro, e concludeva negando qualsivoglia valore probatorio ai dati acquisiti in violazione dell'art. 4 citato, non utilizzabili in causa**. La Corte, poi, ha rilevato la mancanza del nesso di proporzionalità fra gli addebiti e la sanzione in relazione sia alla durata dei collegamenti, **sia all'assoluta mancanza di precedenti contestazioni ad altri dipendenti per fatti analoghi**, sia alla mancanza di precedenti disciplinari in capo alla lavoratrice.
  - Contro tale sentenza la società datrice di lavoro presentava ricorso ritenendo in particolare che, la corte di merito, premesso che "i controlli rivolti a esclusiva finalità di tutela del patrimonio aziendale ricadono al di fuori del campo di applicazione dell'art. 4" citato, avrebbe male interpretato ed applicato il detto articolo, in sostanza "parificando i controlli difensivi a quelli sull'attività lavorativa".

Applicazione art. 4 comma II S.d.L.

- **La giurisprudenza in materia di controlli difensivi (sentenza Corte di Cassazione n. 4375 del 23 febbraio 2010)**
- **Decisione**
- In sintesi, la finalità di controllo a difesa del patrimonio aziendale non è da ritenersi sacrificata dalle norme dello Statuto dei lavoratori.
- Passando a questo punto alla questione di inutilizzabilità, il principio si afferma nei seguenti termini: "gli artt. 4 e 38 dello Statuto dei lavoratori implicano l'accordo sindacale a fini di riservatezza dei lavoratori nello svolgimento dell'attività lavorativa, ma non implicano il divieto dei cd. controlli difensivi del patrimonio aziendale da azioni delittuose da chiunque provenienti. Pertanto in tal caso non si ravvisa inutilizzabilità ai sensi dell'art. 191 c.p.p. di prove di reato acquisite mediante riprese filmate, ancorchè sia perciò imputato un lavoratore subordinata.

Applicazione art. 4 comma II S.d.L.

- **La giurisprudenza in materia di controlli difensivi (sentenza Corte di Cassazione n. 4375 del 23 febbraio 2010)**
- **Decisione**
  - La Corte di Cassazione ha successivamente richiamato la sentenza del medesimo organo (n. 15892/2007) in base alla quale:
    - *"il legislatore ha inteso contemperare l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro, o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi".*
    - *"**L'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore", per cui "tale esigenza" "non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso**".*
  - **In tale ipotesi, si tratta, infatti**, secondo la Corte, comunque **di un controllo c.d. "preterintenzionale" che rientra nella previsione del divieto "flessibile" di cui all'art. 4 citato, comma 2**.

Applicazione art. 4 comma II S.d.L.

- **La giurisprudenza in materia di controlli difensivi (sentenza Corte di Cassazione n. 4375 del 23 febbraio 2010)**
- **Decisione**
  - **Secondo la Corte, sul punto la sentenza impugnata si è attenuta a tali principi e con motivazione congrua e priva di vizi logici ha affermato** che
    - *"**i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento (se non altro, nel nostro caso, sotto il profilo del rispetto delle direttive aziendali)**".*
    - *"**ciò è evidente laddove nella lettera di licenziamento i fatti accertati mediante il programma Super Scout sono utilizzati per contestare alla lavoratrice la violazione dell'obbligo di diligenza sub specie di aver utilizzato tempo lavorativo per scopi personali (e non si motiva invece su una particolare pericolosità dell'attività di collegamento in rete rispetto all'esigenza di protezione del patrimonio aziendale)"***
  - **La Corte si Cassazione ha quindi confermato l'applicabilità al caso di specie l'art. 4, comma 2 citato, negando la utilizzabilità dei dati acquisiti dal citato programma in violazione di tale norma.**

Applicazione art. 4 comma II S.d.L.

02722.12

23 FEB 2012

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

LA CORTE SUPREMA DI CASSAZIONE

SEZIONE LAVORO

Oggetto

licenziamento

R.G.N. 27124/2009

Cron. 2722

Applicazione art. 4 comma II S.d.L.

5.1.- Violazione dell'art. 4 dello statuto dei lavoratori, atteso che il licenziamento è stato fondato su una prova raccolta controllando la posta elettronica del XXXXXX in assenza di previo accordo con le r.s.a. e/o autorizzazione del servizio ispettivo della Direzione provinciale del lavoro e, quindi, in violazione dell'art. 4 in questione, anche in relazione all'art. 8 della CEDU e dell'art. 114 del d.lgs. 30.6.03 n. 196, recante il codice per la protezione dei dati personali.

Applicazione art. 4 comma II S.d.L.

6.- Con il primo motivo è dedotta violazione dell'art. 4 della l. 20.05.70 n. 300, che vieta l'uso degli impianti audiovisivi e delle altre apparecchiature aventi finalità di controllo a distanza dell'attività lavorativa (c. 1) e disciplina le modalità di adozione di impianti ed apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive o dalla sicurezza del lavoro, dai quali può derivare la possibilità di controllo a distanza dei lavoratori (c. 2).

In particolare, la sentenza è contestata nella parte in cui ha ritenuto legittimo il controllo effettuato dal datore sulla posta elettronica aziendale del dipendente, in quanto, non essendo al riguardo regolata alcuna modalità specifica di monitoraggio, tale controllo si porrebbe in contrasto non solo con la norma dello statuto dei lavoratori, ma anche con l'art. 114 del d.lg. n. 196 del 2003 in materia di salvaguardia dei dati personali, che per quanto riguarda la riservatezza del lavoratore negli ambienti aziendali lascia fermo quanto previsto dall'art. 4 suddetto.

Applicazione art. 4 comma II S.d.L.

La possibilità di tali controlli si ferma, dunque, dinanzi al diritto alla riservatezza del dipendente, al punto che la pur insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti "[non] può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore. Tale esigenza … non consente di espungere dalla fattispecie astratta i casi dei cd. *controlli difensivi* ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori quando tali comportamenti riguardino … l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso ove la sorveglianza venga attuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro" (*ivi*). In tale ipotesi, è stato precisato, si tratta di "un controllo c.d. *preterintenzionale* che rientra nella previsione del divieto flessibile di cui all'art. 4, c. 2" (Cass. 23.02.10 n. 4375), così correggendosi una precedente impostazione che riteneva in ogni caso legittimi i c.d. *controlli difensivi*, a prescindere dal loro grado di invasività (Cass. 3.04.02 n. 4746).

Applicazione art. 4 comma II S.d.L.

8.- Nel caso che oggi ci occupa, il giudice di merito non ha accertato quali siano state le concrete modalità attraverso le quali il datore di lavoro ha acquisito il testo dei messaggi di posta elettronica scambiati da XXXXXXti con soggetti estranei al ristretto stretto ambito di diffusione delle notizie delle quali egli era in possesso, poi posti alla base della contestazione disciplinare. Lo stesso giudice, con incontestato accertamento di fatto, ha tuttavia affermato che il datore ha compiuto il suo accertamento *ex post*, ovvero dopo l'attuazione del comportamento addossato al dipendente, quando erano emersi elementi di fatto tali da raccomandare l'avvio di un'indagine retrospettiva.

Applicazione art. 4 comma II S.d.L.

9.- Ad avviso del Collegio, tale fattispecie è estranea al campo di applicazione dell'art. 4 dello statuto dei lavoratori. Nel caso di specie, infatti, il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere. Il c.d. *controllo difensivo*, in altre parole, non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'Istituto bancario presso i terzi.

In questo caso entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale.

Tale situazione, ad una lettura attenta, è già esclusa dal campo di applicazione dell'art. 4 dalla sopra citata giurisprudenza (che già esclude dai *controlli difensivi* vietati quelli aventi ad oggetto la tutela di beni estranei al rapporto di lavoro, v. Cass. n. 15892 del 2007 cit.).

Il primo motivo di ricorso è dunque infondato, in quanto fu correttamente esercitato il potere di controllo attuato *ex post* dal datore di lavoro.

Il provvedimento del Garante Privacy sul tracciamento delle operazioni bancarie

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

A. Perché un provvedimento sulla circolazione e la tracciabilità delle informazioni?

- ESAMINATE le istanze (segnalazioni, reclami e quesiti) **pervenute in tema di trattamento di dati personali della clientela effettuato dalle banche** in ordine ai **temi della "circolazione"** delle informazioni riferite ai clienti all'interno dei gruppi bancari e della **"tracciabilità" delle operazioni bancarie** effettuate da incaricati del trattamento di tali dati (comprese quelle che non comportano movimentazione di denaro – c.d. inquiry);

- RITENUTO di dover definire, in tale contesto, un quadro unitario di misure necessarie e opportune in grado di fornire ulteriori orientamenti utili per gli operatori del settore e i clienti, individuando, a tal fine, i comportamenti più appropriati da adottare;

- Con istanze rivolte all'Autorità, **numerosi interessati hanno dichiarato di essere venuti a conoscenza che dati personali a loro riferiti (in specie, informazioni bancarie), conservati nei data base di alcune banche con le quali avevano instaurato rapporti contrattuali, erano stati oggetto di indebito accesso**, verosimilmente da parte di alcuni dipendenti, i quali, **successivamente, li avrebbero comunicati a terzi che li avrebbero utilizzati per scopi personali** e, segnatamente, in vista di una loro produzione in giudizio (di norma, in separazioni giudiziali e procedure esecutive, in particolare, in pignoramenti presso terzi).

- Il Garante ha svolto una serie di accertamenti propedeutici al provvedimento e ha anche circolarizzato un questionario-tipo

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

A. Perché un provvedimento sulla circolazione e la tracciabilità delle informazioni?

- Il Garante per la protezione dei dati personali ha emanato in data 12 maggio 2011 recante "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie*"

- Il provvedimento si applica **alle banche, incluse quelle facenti parte di gruppi** (disciplinati, in generale, dall'art. 2359 c.c. e, in particolare, dagli artt. 60 e ss. del d.lg. n. 385/1993); **alle società, anche diverse dalle banche purché siano parte di tali gruppi** (di seguito anch'esse denominate "banche"), nell'ambito dei trattamenti dalle stesse effettuati sui dati personali della clientela; a **Poste Italiane S.p.A.** (relativamente all'attività che gli operatori postali possono svolgere nell'ambito dei servizi bancari e finanziari)

- Obiettivo del provvedimento è fornire prescrizioni in relazione al trattamento di dati personali della clientela effettuato al fine di garantire il rispetto dei princìpi in materia di protezione dei dai personali ai sensi del d.lgs. 30 giugno 2003, n. 196 **in ordine ai temi della "circolazione" delle informazioni riferite ai clienti in ambito bancario** e della **"tracciabilità" delle operazioni bancarie effettuate dai dipendenti di istituti di credito** (sia quelle che comportano movimentazione di denaro, sia quelle di sola consultazione, *c.d. inquiry*)
- Restano salve le norme del Codice in materia di trasferimento dei dati all'estero da parte dei titolari del trattamento. In relazione a tale aspetto il Garante si è riservato, qualora se ne dovesse ravvisare la necessità, di intervenire con un successivo provvedimento.
- Il provvedimento non riguarda le modalità con le quali i clienti accedono on line ai servizi bancari (c.d. home banking).

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

Banche/ Società coinvolte

Come indicato dal Provvedimento sono oggetto delle prescrizioni i seguenti soggetti ove stabiliti sul territorio nazionale (art.5 del Codice):
•Banche, incluse quelle facenti parte di gruppi;
•Società, anche diverse dalle banche purchè appartenenti a tali gruppi;
•Poste Italiane S.p.A.

In particolare:
•l'identificazione delle **singole banche** può avvenire tramite **consultazione dell'albo tenuto da Banca d'Italia** relativo alle banche autorizzate in Italia e alle succursali delle banche comunitarie stabilite nel territorio italiano;
•i **gruppi bancari** soggetti al Provvedimento consistono nelle capogruppo e nelle società appartenenti ai gruppi bancari **così come dichiarati a Banca d'Italia**.

Banche di II° livello

Per tali banche, caratterizzate da una clientela composta da altre banche o da soggetti istituzionali, **sono applicabili tutte le indicazioni** definite nel presente documento anche se di **impatto minore**, in quanto **limitate** alle operazioni sui dati bancari di **persone fisiche**, alla luce della recente modifica della definizione di "dato personale"*****

Servizi bancari erogati in modalità "on-line"

Le banche on-line risultano avere un **impatto minore** in quanto le applicazioni in ambito accesso e operations non sono in uso al personale di sportello e sono espressamente escluse dal provvedimento le modalità con le quali i clienti accedono on line ai servizi bancari (cd home banking).
Risultano invece analoghi gli adeguamenti richiesti per le attività di middle e back-office e di controllo interno.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

Key words	Descrizione
Operazione Bancaria	Per Operazioni Bancarie si intendono l'insieme delle operazioni relative alla conduzione dei processi legati alla gestione delle attività *core* della banca, inerenti la raccolta di risparmio da parte del cliente tramite acquisizione di fondi con obbligo di rimborso o operazioni inerenti la gestione del credito nei confronti del cliente e delle attività di controllo interno ad esser connesse. Le Operazioni Bancarie, nell'accezione sopra delineata, possono essere di due tipologie: – Operazioni Dispositive; – Operazioni di Consultazione (Inquiry).
Operazioni Dispositive	Per Operazioni Dispositive si intendono l'insieme di operazioni che comportano una movimentazione economica e/o una variazione patrimoniale, immediata o differita, per conto dei clienti o per conto proprio (e.g. esecuzione bonifico, ordine su mercato, incassi tramite RID, MAV, Bollettini, etc)
Operazioni di Consultazione	Per Operazioni di Consultazione (Inquiry) si intendono quelle operazioni che comportano la possibilità di visualizzare dati della clientela in essere o potenziale, gestiti per l'erogazione di servizi bancari (e.g. visualizzazione saldo di conto corrente, movimenti di conto, etc.)
Dati bancari	Per Dati Bancari si intendono l'insieme dei dati necessari alla conduzione dei servizi bancari riconducibili al singolo cliente (limitatamente alle persone fisiche), gestiti nell'ambito della conduzione delle operazioni bancarie di natura dispositiva e/o di consultazione. Per Dati Bancari si intendono, a titolo esemplificativo: – *Dati relativi a Conti Correnti e Libretti di deposito;* – *Dati relativi a Sistemi di Incasso e pagamento* (E.g. Incasso MAV, RIBA, Bollettini, Bonifici, dati in ambito previdenziale, operatività delle Carte di pagamento, etc); – *Dati in ambito Credito* (E.g. dati relativi a Fidi e garanzie, credito ordinario, anomalo e conto terzi); –*Dati in ambito Finanza* (E.g. Dati su movimentazione portafogli fondi, titoli, gestioni patrimoniali e certificati di deposito); –…

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

Informazioni in ambito e non in ambito

In tal senso, gli **ambiti informativi da prendere in considerazione per l'identifcazione delle attività in perimetro** sono:
Informazioni di business relative a informazioni tecniche e informazioni complementari relative ad accordi e controparti, qualora facciano riferimento a dati bancari della clientela, come precedentemente definiti;
Informazioni operative relative a eventi rapporto, operativi, informativi ed esterni qualora facciano riferimento a dati bancari della clientela, come precedentemente definiti.

Si ritengono ragionevolmente escluse dal perimetro:
Informazioni di business di natura esclusivamente anagrafica qualora non associate univocamente a dati bancari;
Informazioni di business relative ad accordi e controparti qualora non associati a dati bancari;
Informazioni di business tecniche e complementari relative a prodotti/servizi perché riguardanti le caratteristiche degli stessi prodotti/servizi senza alcuna associazione a dati bancari;
Informazioni operative relative ad eventi esterni qualora non associati a dati bancari;
Informazioni operative relative ad operazioni di sintesi per analisi di accordi, analisi di controparti, analisi di prodotti e servizi, posizioni e rischi;
Informazioni di governance relative a regole, configurazioni e processi di governo ad eccezione di eventuali informazioni relative ad attività di controllo interno riferite al singolo cliente (ad esempio informazioni per l'antiriciclaggio).

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

Personale coinvolto

Il Provvedimento cita in diverse sezioni come personale coinvolto i dipendenti e, in generale, gli incaricati al trattamento dei dati della clientela.

Con l'obiettivo di cogliere la "ratio" del Provvedimento si ritiene che le banche debbano considerare **in perimetro, oltre ai propri dipendenti, anche promotori finanziari, stagisti, interinali, consulenti esterni, personale di società esterne a cui siano affidati in outsourcing servizi che riguardano dati bancari e, in generale, tutti gli incaricati del trattamento** (**tranne** nei casi identificati come "**specificità ed esclusioni**") qualora, sulla base delle definizioni precedentemente fornite, effettuino **operazioni per l'accesso ai dati bancari tramite l'uso interattivo di sistemi.**

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

Dati anagrafici/addizionali/aggregati

Sono **esclusi** dal perimetro **i dati anagrafici o addizionali** raccolti dalle banche in modalità accessoria, se **non associati** ai dati bancari

Sono **esclusi** dal perimetro tutti i dati accessibili solo in **modalità aggregata** e **non riconducibile al singolo cliente**

Sono **esclusi** dal perimetro i **dati di sintesi non riconducibili ai singoli clienti** accessibili traverso gli strumenti di Business Intelligence & Data Mining

Accesso massivo ai dati della clientela

Nel caso di transazioni applicative, che consentono la visualizzazione massiva comunque riconducibile al singolo cliente, *laddove vi siano giustificati vincoli tecnologici*, sarà *sufficiente* **limitare il tracciamento ai dati relativi all'incaricato che ha effettuato la query, alla data/ ora dell'operazione e al dettaglio della richiesta effettuata.**

Uso interattivo dei sistemi

Rispetto a quanto riportato dal Provvedimento relativamente all'**uso interattivo** dei sistemi si precisa che, con tale dicitura, si intende l'**accesso ai dati tramite transazioni applicative che consentono di visualizzare il risultato di una richiesta specifica effettuata dall'incaricato**. Sono quindi **incluse** le richieste di **visualizzazione** di **report massivi** di dati riconducibili al **singolo cliente** secondo i criteri definiti dall'operatore di cui al punto precedente, ma sono invece **escluse**, ad esempio, le visualizzazioni di report massivi effettuati tramite **richieste in modalità automatica/batch.** Per tali casistiche rimangono comunque in vigore tutte le prescrizioni relative alle misure di sicurezza previste dalla normativa vigente.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

Coinvolgimento del personale

E' da considerarsi **esclusa** dal Provvedimento l'**operatività effettuata dal personale delle aree funzionali di Gestione Commerciale, Indirizzo e Controllo e supporto al Business qualora non effettuino operazioni associate ai dati bancari.**

E' da considerarsi **esclusa l'operatività del personale IT limitatamente alle mansioni di amministrazione / gestione dei sistemi informativi in quanto non relativa ad operazioni bancarie secondo le definizioni fornite**.

Tale operatività, relativamente alle attività di amministrazione di basi di dati, di reti, di apparati di sicurezza e di sistemi software complessi risulta inoltre già "controllata" tramite le soluzioni richieste dal precedente provvedimento sugli amministratori di sistema.

Resta inteso che, qualora il personale identificato come amministratore di sistema effettui anche operatività bancaria su dati bancari, tale operatività sia da intendersi inclusa nel perimetro di applicabilità del Provvedimento.

A. Perché un provvedimento sulla circolazione e la tracciabilità delle informazioni?

- Ambito di applicazione
  - Ai sensi dell'art. 60 T. U. B., un "**gruppo bancario**" è composto alternativamente:
    - dalla Banca Italiana Capogruppo e le **società bancarie, finanziarie e strumentali controllate**;
    - dalla Società Finanziaria Capogruppo Italiana e le **società bancarie, finanziarie e strumentali** controllate, se nell'insieme delle società controllate vi è almeno una banca e le società bancarie e finanziarie vi hanno rilevanza determinante.

  - Art. 59 T.U.B. :
    - la **società finanziaria** esercita, in via esclusiva o prevalente, l'attività di assunzione di partecipazioni aventi le caratteristiche indicate dalla Banca d'Italia in conformità alle delibere del CICR.
    - Tra le società finanziarie rientrano anche quegli enti che sono regolarmente iscritti all'Albo degli **Intermediari Finanziari**, previsto dall'art. 106 T.U.B.. Tale norma disciplina **l'esercizio nei confronti del pubblico dell'attività di concessione di finanziamenti sotto qualsiasi forma.**
    - Inoltre, gli **Intermediari finanziari** possono, se autorizzati ai sensi dell'art. 114 nonies TUB, **prestare servizi di pagamento, nonché servizi finanziari** se e in quanto compatibili con la relativa disciplina.
    - **Gli intermediari finanziari possono altresì esercitare le altre attività a loro eventualmente consentite dalla legge, nonché attività connesse o strumentali, nel rispetto delle disposizioni dettate dalla Banca d'Italia.**

A. Perché un provvedimento sulla circolazione e la tracciabilità delle informazioni?

- Ambito di applicazione
  - Ai sensi dell'art. 60 T. U. B., un "**gruppo bancario**" è composto alternativamente:
    - dalla Banca Italiana Capogruppo e le **società bancarie, finanziarie e strumentali controllate**;
    - dalla Società Finanziaria Capogruppo Italiana e le **società bancarie, finanziarie e strumentali** controllate, se nell'insieme delle società controllate vi è almeno una banca e le società bancarie e finanziarie vi hanno rilevanza determinante.

  - Si parla invece di **società strumentali** relativamente all'esercizio, in via esclusiva o prevalente, di attività che hanno carattere ausiliario dell'attività delle società del gruppo, comprese quelle consistenti nella proprietà e nell'amministrazione di immobili e nella gestione di servizi anche informatici.
  - **La natura strumentale è connessa al carattere ausiliario delle società del gruppo:** nella maggior parte dei casi le società strumentali esercitano attività che, in difetto del necessario collegamento funzionale con le attività esercitate del gruppo di riferimento, sarebbero e, nel concreto restano, di tipo industriale, o meglio diverso da quello finanziario.
  - **Va, pertanto, precisato che si attribuisce alla capogruppo una certa discrezionalità nel ravvisare le caratteristiche di strumentalità di tutte le attività, anche diverse da quella bancaria e finanziaria, svolte, indirettamente tramite le sue controllate.**

A. Perché un provvedimento sulla circolazione e la tracciabilità delle informazioni?

- Ambito di applicazione
- **Per società controllate** si intende:
- le società in cui un'altra società dispone della maggioranza dei voti esercitabili nell'assemblea ordinaria (es. la società A possiede il 51% del capitale della società B e dunque dispone della maggioranza dei voti esercitabili nell'assemblea ordinaria di tale società);

- le società in cui un'altra società dispone di voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria (es. la società A possiede il 40% del capitale della società B, nonostante non si tratta di una maggioranza assoluta, però di fatto riesce ad avere un'influenza dominante nell'assemblea ordinaria grazie anche alla presenza di piccoli azionisti che spesso non sono presenti alle assemblee);

- le società che sono sotto influenza dominante di un'altra società in virtù di particolari vincoli contrattuali con essa (es. la società A riesce a controllare di fatto la società B, non in funzione del capitale posseduto dalla prima nella seconda, ma in seguito ad un contratto di esclusiva che lega la società B alla società A.).

A. Perché un provvedimento sulla circolazione e la tracciabilità delle informazioni?

- Ambito di applicazione
- **Sono invece società collegate** quelle società sulle quali un'altra società esercita un'influenza notevole, da presumersi per legge quando può essere esercitato:
  - almeno un quinto dei voti nell'assemblea ordinaria;
  - almeno un decimo dei voti nell'assemblea ordinaria se la società ha azioni quotate in borsa
  - (es. la società B, quotata in borsa, ha un capitale sociale di 500.000 euro, la società A possiede il 15% della società B, l'influenza notevole si presume per legge).

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

B. Oggi gli unici obblighi generalizzati di data retention sono:

- Articolo 132 d.lgs 196/03
  - i dati relativi al traffico telefonico (diversi da quelli trattati a fini di fatturazione) devono essere conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati; **per le medesime finalità, i dati relativi al traffico telematico, esclusi i contenuti delle comunicazioni, devono essere conservati dal fornitore per dodici mesi dalla data della comunicazione** (art. 132 comma 1 D.Lgs 196/2003);
  - i dati relativi alle chiamate senza risposta (prima assoggettati alla medesima disciplina di cui al punto a.), che siano trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, devono essere conservati per trenta giorni (art. 132 comma 1-bis D.Lgs 196/2003).

- Provvedimento del Garante sugli Amministratori di Sistema del 27 novembre 2008
  - Log di accesso, disconnessione e tentativi di accesso degli amministratori di sistema

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

C. La circolazione delle informazioni in ambito bancario

- **La circolazione delle informazioni riferite alla clientela nell'ambito di un gruppo bancario può avvenire** a diversi livelli astrattamente riconducibili a tre distinte tipologie:

  - **1. la comunicazione di dati personali tra banche appartenenti al medesimo gruppo**
  - **2. la circolazione di tali dati tra agenzie o filiali della stessa banca**
  - **3. la circolazione di dati nell'ambito di una stessa agenzia o filiale**

- **1. La comunicazione di dati personali tra banche appartenenti al medesimo gruppo. Due sono state le modalità identificate dal Garante:**

  - in un caso, **tra le agenzie di diverse banche appartenenti al gruppo era prevista una circolarità limitata alle sole operazioni di versamento e prelevamento**, senza avere mai la possibilità di conoscere il saldo contabile o la lista movimenti del conto acceso presso altro istituto del gruppo;
  - in un altro caso, è emerso un **regime di piena circolarità delle informazioni all'interno del gruppo bancario**: la posizione del cliente e i suoi dati bancari erano accessibili dagli operatori di sportello −designati incaricati del trattamento, in ragione delle funzioni svolte e dei profili di autorizzazione ad esse correlati−, senza limitazioni.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

C. La circolazione delle informazioni in ambito bancario

- **2. La circolazione di tali dati tra agenzie o filiali della stessa banca: diverse modalità rilevate dal Garante**
  - **in un caso, i dati dei clienti di una determinata agenzia sono risultati integralmente visibili per gli incaricati della stessa agenzia in possesso di adeguati profili di autorizzazione**, **i quali potevano non solo operare sui conti accesi presso la medesima, ma anche venire a conoscenza dell'esistenza di altri rapporti con lo stesso cliente presso altre agenzie della stessa banca, senza però poterne visualizzare l'effettiva consistenza patrimoniale**. Nell'ambito delle agenzie appartenenti alla stessa banca, gli incaricati abilitati potevano effettuare, su richiesta di clienti titolari di rapporti incardinati presso altra agenzia, talune operazioni bancarie (versamento, prelievo, bonifico, operazioni su titoli, ecc.) con possibilità di ottenere il saldo o la lista dei movimenti solo dopo la corretta effettuazione di una operazione di natura dispositiva;
  - in un altro caso, **gli incaricati non potevano effettuare operazioni di sportello**, ad eccezione dei versamenti in contanti, in filiali diverse da quella presso la quale era gestito il conto corrente di uno specifico interessato. In tale ipotesi, **la banca non operava in regime di circolarità, tranne che per le operazioni di visualizzazione dei dati bancari**, che tutti gli addetti presso una specifica filiale potevano compiere in relazione ai dati bancari anche di clienti di altre filiali;
  - in un ultimo caso, infine, si prevedeva che **i dipendenti operanti all'interno di una filiale potessero accedere ai dati in esame limitatamente ai rapporti accesi presso la filiale medesima**.
- **3. La circolazione di dati nell'ambito di una stessa agenzia o filiale.**
  - E' stato rilevato che, generalmente, **all'interno di una agenzia o filiale di una medesima banca la circolazione dei dati dei clienti avviene solo tra incaricati del trattamento in possesso di specifici profili di autenticazione e autorizzazione**.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

D. Protezione dei dati personali. Assunti di base:

- Ogni banca è autonomo titolare del trattamento
- Il **flusso di dati personali riferiti ai clienti nell'ambito di gruppi** si configura come **comunicazione** a terzi.
- Nell'informativa resa alla clientela, ai sensi dell'art. 13 del Codice, **ogni banca-titolare del trattamento deve indicare che i dati personali della clientela possono essere oggetto di comunicazione ad altri titolari del trattamento** nell'ambito del medesimo gruppo bancario.
- In relazione al profilo del consenso, **la comunicazione di dati è possibile solo ove sia stato acquisito il consenso informato dell'interessato** (art. 23 del Codice) o si sia in presenza di uno dei presupposti di esonero del consenso previsti dall'art. 24 del Codice.
- Al contrario, **il flusso di dati tra diverse agenzie o filiali di una stessa banca costituisce circolazione di informazioni all'interno di un unico titolare del trattamento** e, non configurando un'operazione di comunicazione di dati a terzi, **non richiede il consenso** degli interessato (l'informativa può contenere anche l'indicazione che i dati della clientela potranno circolare tra le agenzie o filiali di ciascuna banca)

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

E. Protezione dei dati personali. Rapporti con gli outsourcer:

- **I sistemi informativi contenenti i dati relativi alla clientela delle banche, mediante i quali vengono registrati gli accessi dei dipendenti a tali dati, sono gestiti da società** (interne o esterne alla compagine di gruppo) **con le quali ciascuna banca stipula appositi contratti di servizio**. Due modelli organizzativi vengono adottati tipicamente:
  - 1. gruppi bancari caratterizzati da una **gestione prevalentemente interna** del sistema informativo […] **affidata a una società di servizio appartenente al gruppo bancario**, che si configura come soggetto terzo Responsabile o, in alcuni casi, Titolare del trattamento dei dati personali […];
  - 2. gruppi bancari/banche caratterizzati da una **gestione prevalentemente esterna del sistema informativo** […] **caratterizzati da un elevato livello di** outsourcing, in relazione alla gestione del sistema informativo. In questo caso, la banca titolare del trattamento, esternalizzando la gestione dei dati, designa il soggetto terzo "responsabile del trattamento".

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

E. Protezione dei dati personali. Rapporti con gli outsourcer:

- **La qualificazione delle società che gestiscono i sistemi informativi quali autonomi "titolari del trattamento"** (con tutte le conseguenze che ciò comporta anche in termini di eventuale responsabilità civile nei confronti degli interessati) **spesso non è conforme alle previsioni del Codice** (e, segnatamente, agli artt. 4, comma 1, lett. f) e g), 28 e 29).
- **È indispensabile che ciascuna banca valuti attentamente se le società di gestione di detti sistemi** (a prescindere dal fatto che si tratti di soggetti interni o esterni alla compagine di gruppo o alla singola banca), **alla luce delle specifiche attività che sono chiamate a svolgere in base ai contratti di servizio**, **possano essere effettivamente considerate quali autonomi titolari o non vadano invece designate quali "responsabili" del trattamento ai sensi dell'art. 29 del Codice**.
- La posizione di "titolare" del trattamento, pur astrattamente riconoscibile anche in capo all'outsourcer, **risulta, tuttavia, ascrivibile solo alla banca nei casi in cui la stessa abbia il potere di**:
  - 1. assumere decisioni relative alle finalità del trattamento;
  - 2. impartire istruzioni e direttive vincolanti nei confronti delle società di gestione dei sistemi informativi, sostanzialmente corrispondenti alle istruzioni che il titolare del trattamento deve impartire al responsabile;
  - 3. svolgere funzioni di controllo rispetto all'operato delle medesime e degli incaricati delle stesse.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

F. Accessi informatici da parte dei dipendenti delle banche ai dati relativi alla clientela e correlato tracciamento delle operazioni poste in essere dagli stessi

- **Le Banche hanno adottato diverse soluzioni in ordine alle caratteristiche tecnologiche dei sistemi informativi con cui vengono tracciate le operazioni bancarie** (sia dispositive, sia di semplice *inquiry*), anche a causa della discrezionalità riconosciuta a ciascuna banca o gruppo bancario nel dare attuazione a quanto previsto nelle "Disposizioni di vigilanza per le banche in materia di conformità alle norme (*compliance*)", adottate dalla Banca d'Italia il 10 luglio 2007.

- **Le Istruzioni di vigilanza definiscono ruolo e responsabilità degli organi di vertice delle banche e prevedono la costituzione della funzione di compliance**, quale elemento integrante del sistema dei controlli interni.

- **La funzione di compliance è preposta al presidio e alla gestione del rischio di incorrere in sanzioni amministrative, perdite finanziarie rilevanti o danni di reputazione** in conseguenza di violazioni di norme imperative o di autoregolamentazione (rischio di compliance).

- Le disposizioni stabiliscono i principali compiti e i requisiti qualitativi minimi della funzione di compliance, le attribuzioni del suo responsabile, le interrelazioni con le altre funzioni aziendali (in particolare con la funzione di controllo interno, c.d. *internal auditing*)

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

F. Accessi informatici da parte dei dipendenti delle banche ai dati relativi alla clientela e correlato tracciamento delle operazioni poste in essere dagli stessi

- La funzione di compliance, preposta al controllo interno nelle banche, è disciplinata dalla legge e da un quadro di norme regolamentari emanate dalla Banca d'Italia mediante apposite istruzioni, in particolare, le Istruzioni di vigilanza in materia di "Organizzazione e controlli interni". **Queste ultime richiedono alle banche di dotarsi di sistemi di monitoraggio dei rischi aziendali e di verifica dell'affidabilità e della sicurezza, anche dei sistemi informativi, istituendo indicatori di anomalie (c.d. *alert*) per orientare successivi interventi di audit**

- **In assenza di disposizioni normative recanti obblighi in materia di tracciabilità delle operazioni bancarie** con riguardo sia all'an sia al quantum della conservazione dei file di log, si rileva che, nell'ambito della discrezionalità riconosciuta alle banche nell'organizzare la funzione di compliance, **tutte le banche sottoposte ad attività ispettiva hanno ritenuto di implementare sistemi di controllo delle operazioni dispositive con finalità di tutela del patrimonio dei clienti e dell'attività bancaria, ma solo alcune di esse sono risultate in possesso di sistemi di tracciamento riguardanti anche operazioni di semplice consultazione (*inquiry*) dei conti correnti o di altri rapporti contrattuali riferiti ai clienti**. Anche in quest'ultimo caso, a causa di tempi di conservazione dei file di log troppo ristretti, tuttavia non è stato sempre possibile risalire ai dettagli di un'operazione di accesso ai dati posta in essere da un incaricato.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

F. Accessi informatici da parte dei dipendenti delle banche ai dati relativi alla clientela e correlato tracciamento delle operazioni poste in essere dagli stessi

- Per questo motivo il Garante, prendendo atto dell'assenza di disposizioni normative in tale ambito, ha ritenuto opportuno prescrivere alcune misure in ordine a:
  - **"tracciamento" degli accessi ai dati bancari** dei clienti
  - **tempi di conservazione** dei relativi file di log
  - **implementazione di alert volti a rilevare intrusioni o accessi anomali ai dati bancari**, tali da configurare eventuali trattamenti illeciti

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

G. Tracciamento delle operazioni

- **Al fine di assicurare il controllo delle attività svolte sui dati dei clienti e dei potenziali clienti da ciascun incaricato del trattamento** (quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento che è tenuto a svolgere) **devono essere adottate idonee soluzioni informatiche**.

- **Oltre alle misure minime di sicurezza**, già prescritte dall'art. 34 del Codice nel caso di trattamento di dati personali effettuato con strumenti elettronici (con particolare riguardo alla necessità di *"protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti […]"* di cui alla lett. e) del citato art. 34), **è necessario implementare misure idonee** (art. 31 del Codice) **che permettano un efficace e dettagliato controllo anche in ordine ai trattamenti condotti sui singoli elementi di informazione presenti nei diversi *database* utilizzati**

- **Tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall'uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente**

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

G. Tracciamento delle operazioni

- **I file di *log* devono tracciare per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni:**
  - il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso
  - la data e l'ora di esecuzione
  - il codice della postazione di lavoro utilizzata
  - il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato
  - la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata (es. numero del conto corrente, fido/mutuo, deposito titoli)

- Le misure di cui al presente paragrafo sono adottate **nel rispetto della vigente disciplina in materia di controllo a distanza dei lavoratori** (art. 4, l. 20 maggio 1970, n. 300), **tenendo altresì conto dei princìpi affermati dal Garante in tema di informativa agli interessati nelle linee guida sull'utilizzo della posta elettronica e di internet**

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

G. Tracciamento delle operazioni

- **Articolo 4 Statuto dei Lavoratori:**
  - E’ vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori
  - Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro provvede la Direzione Regionale del Lavoro omississ

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

H. Conservazione dei log di tracciamento delle operazioni

- **Il periodo di conservazione dei file di log che tracciano gli accessi** varia in base alla tipologia di *log* memorizzato; inoltre, fatta eccezione per quelli che tracciano gli accessi degli amministratori di sistema (per i quali è previsto un periodo minimo di conservazione di 6 mesi), **per gli altri *log* non sono normativamente prescritti tempi di conservazione.** Anche le risultanze istruttorie hanno confermato che i log sono conservati per un periodo variabile (in tal senso è anche la documentazione prodotta dall'ABI, che rileva come i log di accesso ai sistemi informativi siano conservati mediamente per 12 mesi, mentre i log file delle transazioni bancarie sono conservati per un periodo non inferiore a 10 anni)

- Tuttavia, alla luce dell'esperienza maturata in sede ispettiva, **si ritiene congruo stabilire che i *log* di tracciamento delle operazioni di inquiry siano conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione**. Ciò in quanto un periodo di tempo inferiore non consentirebbe agli interessati di venire a conoscenza dell'avvenuto accesso ai propri dati personali e delle motivazioni che lo hanno determinato

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

H. L'implementazione di alert volti a rilevare intrusioni o accessi anomali e abusivi ai sistemi informativi

- **Implementazione di alert**
  - **Deve essere prefigurata da parte delle banche l'attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry eseguite dagli incaricati del trattamento**

  - Anche a tal fine, **negli strumenti di business intelligence utilizzati dalle banche per monitorare gli accessi alle banche dati contenenti dati bancari devono confluire i log relativi a tutti gli applicativi utilizzati per gli accessi da parte degli incaricati del trattamento**

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

I. L'implementazione di alert volti a rilevare intrusioni o accessi anomali e abusivi ai sistemi informativi

- Audit interno di controllo–Rapporti periodici

  – **La gestione dei dati bancari deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento**, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti

  – **L'attività di controllo deve essere demandata a un'unità organizzativa o**, comunque, **a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti**

  – **I controlli devono comprendere anche verifiche a posteriori, a campione, o a seguito di allarme derivante da sistemi di *alerting* e di *anomaly detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento**.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

I. L'implementazione di alert volti a rilevare intrusioni o accessi anomali e abusivi ai sistemi informativi

- Audit interno di controllo–Rapporti periodici
  - **Sono svolte, altresì, verifiche periodiche sulla corretta conservazione dei file di log per il periodo previsto al punto 4.2.2**
  - **L'attività di controllo deve essere adeguatamente documentata** in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

I. L'implementazione di alert volti a rilevare intrusioni o accessi anomali e abusivi ai sistemi informativi

- L'esito dell'attività di controllo deve essere:
  - comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della banca
  - richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza
  - messo a disposizione del Garante, in caso di specifica richiesta

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

L. Informazioni in caso di accessi non autorizzati.

- **Le banche comunicano senza ritardo all'interessato le operazioni di trattamento illecito effettuate - sui dati personali allo stesso riferiti- dagli incaricati**. Tale tempestiva informazione, infatti, in termini generali, può consentire all'interessato l'adozione di appropriate misure e, ove possibile, una minimizzazione dei rischi connessi alla violazione della disciplina di protezione dei dati personali.

- **Le banche comunicano tempestivamente al Garante −fornendo gli opportuni dettagli− i casi in cui risultino accertate violazioni, accidentali o illecite, nella protezione dei dati personali, purché di particolare rilevanza per la qualità o la quantità di dati coinvolti e/o il numero di clienti interessati, dalle quali derivino la distruzione, la perdita, la modifica, la rivelazione non autorizzata dei dati della clientela.**

- Tali comunicazioni costituiscono misura opportuna ai sensi dell'art. 154, comma 1, lett. c) del Codice.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

M. Prescrizioni.

- 1) Misure necessarie:
  - a) Designazione dell'*outsourcer* quale responsabile del trattamento (punto 3.2).
    Quando il trattamento di dati personali dei clienti da parte di outsourcer è svolto restando riservati alle banche i poteri riconosciuti dal Codice solo al titolare (artt. 4, comma 1, lett. f) e 28), e dunque, in concreto, detti poteri, non risultino posti effettivamente in capo all'*outsourcer*, le stesse banche, quali unici titolari del trattamento, devono designare le società operanti in *outsourcing* responsabili ai sensi degli artt. 4, comma 1, lett. g) e 29, commi 4 e 5 del Codice.

  - b) Tracciamento delle operazioni (punto 4.2.1).
    Devono essere adottate idonee soluzioni informatiche per il controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi database. Tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall'uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

M. Prescrizioni.

- 1) Misure necessarie:
  - In particolare, i file di log devono tracciare per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni:
    - il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso;
    - la data e l'ora di esecuzione;
    - il codice della postazione di lavoro utilizzata;
    - il codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato;
    - la tipologia di rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata (es. numero del conto corrente, fido/mutuo, deposito titoli).

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

M. Prescrizioni.

- 1) Misure necessarie:
  - c) Conservazione dei *log* di tracciamento delle operazioni (punto 4.2.2).
  - Il periodo di conservazione dei file di log delle operazioni di inquiry non deve essere inferiore a 24 mesi dalla data di registrazione dell'operazione.

  - d) Implementazione di *alert* (punto 4.3.1).
  - i. Deve essere prefigurata da parte delle banche l'attivazione di specifici *alert* che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry.
  - ii. Negli strumenti di *business intelligence* devono confluire i *log* relativi a tutti gli applicativi utilizzati per gli accessi.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

M. Prescrizioni.

- 1) Misure necessarie:
- e) *Audit* interno di controllo–Rapporti periodici (punto 4.3.2).
  - i. La gestione dei dati bancari deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento.
  - ii. L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti.
  - iii. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di alerting e di anomaly detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sulla corretta conservazione dei file di log per il periodo previsto al punto 4.2.2.
  - iv. L'attività di controllo deve essere adeguatamente documentata e il relativo esito deve essere comunicato ai soggetti indicati al punto 4.3.2.

Il nuovo provvedimento sul tracciamento delle operazioni bancarie

M. Prescrizioni.

- 2) Misure opportune:
  - f) Informativa all'interessato (punto 2.2).
  - L'informativa resa all'interessato ai sensi dell'art. 13 del Codice, potrà contenere anche l'indicazione che i dati della clientela potranno circolare tra le agenzie o filiali di ciascuna banca.

  - g) Informazioni all'interessato (punto 5.1).
  - Le banche comunicano, senza ritardo, all'interessato le operazioni di trattamento illecito effettuate -sui dati personali allo stesso riferiti- dagli incaricati.

  - h) Comunicazioni al Garante (punto 5.2).
  - Le banche comunicano tempestivamente al Garante i casi in cui risulti accertata una violazione, accidentale o illecita, nella protezione dei dati personali, di particolare rilevanza.

- 3) dispone, che le misure di cui al punto 1) del presente dispositivo, siano adottate entro 30 mesi dalla pubblicazione del presente provvedimento sulla *Gazzetta Ufficiale*;

Grazie per l’attenzione...

Per domande o approfondimenti:

gabriele.faggioli@islconsulting.it