- a seguito della comunicazione di informazioni bancarie a terzi che non siano in alcun modo autorizzati dall'interessato a porre in essere operazioni per suo conto o a conoscere il contenuto della relazione contrattuale in essere con la banca, come, ad esempio, nei confronti:
- del coniuge, cui venga consegnata documentazione bancaria riferita esclusivamente all'altro [16];
- di familiari, contattati talora telefonicamente per comunicazioni dirette ai clienti, ma il cui contenuto venga invece rivelato ingiustificatamente ai primi;
- di professionisti [17] o soggetti legati da un rapporto di lavoro con l'interessato;
- di terzi che, per errore nell'imbustamento o nella spedizione della corrispondenza, divengano destinatari di comunicazioni scritte aventi ad oggetto informazioni bancarie (ad esempio, di estratti conto);
- a seguito della comunicazione di informazioni bancarie presso recapiti non autorizzati, in modo da consentire a terzi di venire a conoscenza di dati riferiti all'interessato (ad esempio, in caso di comunicazioni via *fax*) [18];
- più in generale, per l'inosservanza di misure di sicurezza [19].

3.3. *Comunicazioni dovute o autorizzate.* In numerosi casi è possibile comunicare dati relativi alla clientela senza violare le rilevanti disposizioni in materia di protezione dei dati personali; altre comunicazioni sono anzi doverose in quanto richieste dalla legge. A titolo meramente esemplificativo possono menzionarsi i casi di:

- comunicazioni di informazioni personali per attuare la disciplina in materia di contrasto del riciclaggio [20]. A questo proposito merita rilevare che possono formare oggetto di trattamento da parte della banca non solo informazioni relative a singole transazioni economiche effettuate, ma un novero più ampio di dati personali necessari a rilevare l'anomalia di un'operazione in rapporto alle caratteristiche del cliente [21];
- comunicazioni, per finalità di contrasto finanziario al terrorismo [22] e alla commercializzazione di materiale pedopornografico [23], attualmente nei riguardi dell'Ufficio italiano dei cambi;
- comunicazioni di informazioni personali per l'accertamento e la repressione di violazioni tributarie, nei limiti previsti dalla legge [24]. In quest'ambito, possono essere ricomprese alcune ipotesi quali quelle contenute:
  - nell'ultima parte del menzionato art. 7, comma 6, d.P.R. n. 605/1973, secondo cui *"l'esistenza dei rapporti, nonché la natura degli stessi sono comunicate all'anagrafe tributaria, ed archiviate in apposita sezione, con l'indicazione dei dati anagrafici dei titolari, compreso il codice fiscale"*;
  - nell'art. 32, comma 7, del d.P.R. 29 settembre 1973, n. 600, in materia di disposizioni comuni sull'accertamento delle imposte sui redditi;
  - nella disciplina concernente le comunicazioni verso la *cd.* "anagrafe dei rapporti di conto e di deposito" [25];
- comunicazioni di informazioni, in conformità alla disciplina che regola la materia, alla Centrale rischi della Banca d'Italia [26] e al Servizio centralizzato di rilevazione dei rischi di importo contenuto (Cric) [27] e alla Centrale d'allarme interbancaria (in merito, *v.* infra punto 3.4.);
- comunicazioni (nelle forme previste dalla legge) nei confronti dell'autorità giudiziaria [28] e, nell'ambito di una procedura esecutiva, al creditore procedente (nel rispetto delle vigenti disposizioni in materia di pignoramento presso terzi: artt. 543 ss. c.p.c., come modificati dalla l. 24 febbraio 2006, n. 52) [29];
- comunicazioni a seguito di istanza di accesso alla documentazione bancaria ai sensi dell'art. 119 del testo unico delle leggi in materia bancaria e creditizia (Tub: d.lg. 1° settembre 1993, n. 385; *v.* infra punto 5.2.).

Possono, poi, formare oggetto di comunicazione ai gestori di sistemi (privati) di informazione creditizie, in conformità alla deliberazione del Garante n. 9 del 16 novembre 2004 [30], i dati personali (di contenuto *"negativo"*) necessari per effettuare i trattamenti in conformità al *"codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti"* [31], se preceduti dal preavviso previsto (art. 4, comma 7, del codice di deontologia medesimo) [32].

Possono essere altresì comunicate lecitamente al soggetto garante alcune informazioni personali relative al debitore garantito, nella misura in cui le medesime siano pertinenti rispetto al rapporto di garanzia in essere [33].

3.4. Comunicazioni di dati personali alla Centrale d'allarme interbancaria. L'art. 36 del decreto legislativo n. 507/1999 concernente la depenalizzazione di alcuni reati minori, che ha introdotto nella legge 15 novembre 1990, n. 386 il nuovo art. 10-bis, ha previsto l'istituzione di un archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (la *cd.* Centrale d'allarme interbancaria, di seguito Cai), la cui disciplina di dettaglio è contenuta nel d.m. 7 novembre 2001, n. 458 [34] e nel regolamento del Governatore della Banca d'Italia del 29 gennaio 2002 [35].

Dall'esame delle fattispecie presentate al Garante, anche a seguito dell'esercizio dei diritti previsti dall'art. 7 del Codice (nei confronti sia degli intermediari segnalanti, sia della Banca d'Italia, in qualità di titolari del trattamento) [36], emerge la necessità che gli enti segnalanti prestino la massima cautela nell'accertare l'esattezza e la completezza dei dati personali trattati prima di procedere alla segnalazione (art. 3, comma 2, d.m. n. 458/2001). Ciò, al fine di prevenire l'inserimento nella Cai di nominativi di vittime di furto d'identità (e, comunque, provvedendo con tempestività alle necessarie verifiche e alle eventuali cancellazioni, anche a seguito dell'esercizio del diritto d'accesso da parte dell'interessato) [37], come pure di soggetti che, pur avendo comunicato correttamente alla banca il furto o lo smarrimento di assegni (che devono formare oggetto di successiva e tempestiva segnalazione a cura degli enti segnalanti nel segmento "Pass" della Cai), vengano segnalati in tale archivio a seguito di un'abusiva negoziazione dei medesimi titoli (ad esempio, per mancanza di provvista o per emissione degli assegni in difetto di autorizzazione) [38].

Gli enti segnalanti, oltre a dover effettuare le operazioni di trattamento in modo lecito (osservando quindi anche la disciplina di settore che regola il complessivo funzionamento dell'archivio), devono comportarsi secondo correttezza (art. 11, comma 1, lett. a), del Codice) [39].

La segnalazione è lecita anche in caso di "richiamo" dell'assegno da parte della banca negoziatrice atteso che, nel caso di assegni emessi senza autorizzazione, l'illecito si perfeziona all'atto dell'emissione e, nel caso di assegni emessi senza provvista, al momento della presentazione al pagamento [40].

Limitatamente ai casi di mancato pagamento di un assegno per difetto di provvista (art. 9-*bis* legge n. 386/1990) [41], la segnalazione alla Cai non può essere effettuata se il debitore pone tempestivamente in essere i comportamenti analiticamente indicati all'art. 8 della legge n. 386/1990 [42]. Nel caso in esame, inoltre, l'iscrizione del traente nella Cai non può avvenire se la banca segnalante non ha inviato preventivamente un preavviso di revoca (ai sensi dell'art. 9-bis della legge n. 386/1990), dal ricevimento del quale devono decorrere almeno dieci giorni prima di provvedere all'iscrizione medesima.

Tali presupposti non ricorrono, invece, per quanto riguarda le revoche delle carte di pagamento nella Cai: alla luce della vigente disciplina, infatti, nessuno specifico rilievo è assegnato alla circostanza che l'obbligazione pecuniaria nascente dall'utilizzo di una carta di pagamento sia stata o meno successivamente adempiuta [43].

Le banche sono altresì tenute a segnalare nella Cai i casi di revoca delle carte di pagamento utilizzate per l'acquisto di materiale pedopornografico sulla rete Internet o su altre reti di comunicazioni [44].

3.5. *Benefondi.* Il *cd.* benefondi fa riferimento a una prassi interbancaria che prevede, nell'ambito della negoziazione di assegni tra banche per la realizzazione del credito portato dal titolo, la comunicazione dell'esistenza di una provvista sufficiente in relazione al pagamento di assegni da addebitare sul conto corrente del traente [45]. Le informazioni possono essere fornite dagli istituti di credito nel rispetto dei princìpi generali che la legge prevede per tutti i trattamenti di dati personali svolti dalle banche e secondo le indicazioni riportate nei modelli di informativa distribuiti alla clientela, nei quali può rientrare anche questo tipo di comunicazione alla banca mandataria per l'incasso.

La prassi del benefondi, tuttavia, deve trovare corretta attuazione: le informazioni devono essere fornite ai soli soggetti legittimati all'incasso o alla negoziazione dell'assegno, anziché a terzi non autorizzati; inoltre, le informazioni fornite dalla banca devono essere esatte, aggiornate e non eccedenti rispetto allo scopo per il quale il benefondi è utilizzato, che è relativo alla semplice informazione dell'esistenza o meno sul conto corrente del cliente della banca trattaria dei fondi necessari al pagamento dell'assegno [46].

3.6. *Comunicazione dei dati relativi alla clientela e cessione di sportelli bancari: esonero dall'obbligo di rendere l'informativa.* Un esame più approfondito, sotto i profili della comunicazione dei dati e dell'informativa da rendere alla clientela, merita la fattispecie della cessione di sportelli bancari: essa implica, di regola, limitatamente agli sportelli ceduti, il trasferimento dell'intero compendio di beni, rapporti giuridici attivi e passivi, oltre che dei rapporti contrattuali esistenti a favore della banca cessionaria.

In tale contesto sussistono, come analiticamente indicato di seguito, i presupposti per l'esonero dall'obbligo di rendere l'informativa per la banca cessionaria, la quale potrà pertanto utilizzare modalità più snelle per rendere edotta la clientela in ordine al trattamento dei dati personali correlato alla cessione degli sportelli;

a) *presupposti del trattamento*: bilanciamento degli interessi. La cessione di sportelli bancari, infatti, non esaurisce i propri effetti sul solo piano negoziale, ma determina in pari tempo la comunicazione di dati personali (riferibili, ad esempio, alla clientela, a fornitori, o connessi all'esecuzione del rapporto di lavoro del personale dipendente) dalla banca cedente alla cessionaria, con conseguente applicazione del Codice.
   In relazione a tali operazioni la banca cedente (titolare del trattamento) non provvede, di regola, ad acquisire il consenso degli interessati; deve pertanto verificarsi se sussista un altro fondamento per porre in essere la comunicazione.
   Come è noto, la cessione di innumerevoli rapporti attivi e passivi in corrispondenza del mutamento del centro di imputazione soggettiva dei medesimi (dalla banca cedente a quella cessionaria) trova una disciplina apposita e articolata nell'art. 58 del menzionato Tub, della quale è necessario tener conto in ragione dei riflessi che la stessa può spiegare rispetto ai profili di protezione dei dati personali [47].
   Detta disciplina, infatti, introduce modalità atte ad agevolare, snellendone gli adempimenti, la cessione in blocco di rapporti giuridici, riducendone i costi e preservando in pari tempo i legittimi interessi dei soggetti coinvolti, a vario titolo, nella cessione [48].
   Il *favor* che l'ordinamento riserva alle cessioni "in blocco" di rapporti giuridici in materia bancaria spiega effetti anche sul profilo accessorio della comunicazione dei dati personali che le medesime implicano. Stante la peculiare disciplina approntata dall'ordinamento all'art. 58 del Tub e attesa la natura dei dati trattati (di regola anagrafici o relativi a transazioni di natura economica), i diritti e il legittimo interesse dei soggetti ceduti in ordine al trattamento dei dati che li riguardano non risultano nel caso di specie prevalenti rispetto al legittimo interesse alla comunicazione della banca cedente. Ciò, anche in ragione dell'immutata finalità del trattamento dei dati oggetto della cessione.
   Deve quindi ritenersi integrata la fattispecie prevista nell'art. 24, comma 1, lett. *g*), del Codice sì che, per effetto del presente provvedimento, la comunicazione dei dati personali oggetto della cessione degli sportelli bancari deve ora ritenersi lecita (per le sole finalità sopra menzionate), limitatamente ai dati diversi da quelli sensibili, anche in assenza del consenso degli interessati;
b) *esonero dall'obbligo di rendere l'informativa.* Rispetto alle ipotesi di cessione di sportelli bancari regolata dall'art. 58 del Tub, il cessionario che raccoglie i dati presso il terzo (banca cedente) è comunque tenuto a rendere, al momento della registrazione dei dati, ai soggetti ceduti l'informativa sul trattamento (art. 13, comma 4, del Codice).
   L'informativa, se resa singolarmente a ciascun interessato con la tempistica richiesta dal menzionato art. 13, comma 4 (stante l'elevato numero di soggetti ceduti nelle menzionate operazioni), potrebbe risultare impossibile e, comunque, risulta comportare costi e oneri amministrativi manifestamente sproporzio-

nati rispetto al diritto tutelato, anche perché deve essere fornita in un contesto temporale circoscritto a innumerevoli soggetti, individuati ovvero individuabili per *relationem* grazie alla ricognizione degli sportelli oggetto dell'operazione.
Alla luce di ciò, in via generale e in relazione a ciascuna delle operazioni di cessione di sportelli bancari, il Garante, ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, dichiara che l'impiego dei mezzi necessari a rendere l'informativa singolarmente a ciascuno degli interessati coinvolti nell'operazione risulta sproporzionato rispetto all'interesse che il precetto contenuto nel menzionato art. 13, comma 4, del Codice intende tutelare.
Per queste ragioni l'informativa può essere quindi resa nelle medesime forme previste, seppur a diverso fine, dall'art. 58 del Tub;

c) *misure appropriate.* Tuttavia, come già disposto in passato dall'Autorità [49], è necessario che venga assicurata comunque un'adeguata informativa a vantaggio degli interessati. Occorrono, quindi, misure appropriate a cura delle banche cessionarie che siano parte delle operazioni di cessione di sportelli bancari.

Ciò, dovrà essere assicurato mediante la pubblicazione dell'informativa contenente gli elementi previsti dall'art. 13, commi 1 e 2, del Codice sulla *Gazzetta Ufficiale* della Repubblica italiana, contestualmente alla pubblicazione dell'avviso previsto dal menzionato art. 58.

In applicazione del principio di semplificazione (art. 2 del Codice), i titolari del trattamento non dovranno presentare al Garante una richiesta preventiva di esonero dall'informativa. L'elevato livello di tutela degli interessati (art. 2 *cit.*) dovrà essere, comunque, garantito adottando anche l'ulteriore misura che risulta appropriata (art. 13, comma 5, lett. *c*), del Codice), di seguito indicata: i cessionari dovranno in ogni caso fornire direttamente ai soggetti ceduti gli elementi contenuti nell'art. 13, commi 1 e 2, del Codice, alla prima occasione utile successiva all'avvenuta cessione in blocco (ad esempio, in sede di invio dell'estratto conto). Tale modalità aggiuntiva favorisce una maggiore conoscibilità dell'avvenuta raccolta dei dati presso terzi ad opera della cessionaria [50].

4. Tutela dei propri diritti da parte della banca

L'istituto di credito può utilizzare in sede giudiziaria informazioni relative ai rapporti intrattenuti con la clientela per tutelare i propri diritti nelle controversie con gli interessati, non assumendo valore ostativo, in questa ipotesi, l'impegno di riservatezza assunto in relazione ai servizi prestati, che non può tradursi in un vincolo tale da produrre effetti lesivi nella sfera giuridica della stessa banca e in un limite all'esigenza di difesa giudiziaria dei propri diritti (*cfr.*, al riguardo, art. 24, comma 1, lett. *f*), del Codice).

Il cliente non può infatti pretendere dalla banca un comportamento che si risolva in una lesione dei propri interessi giuridicamente rilevanti e del proprio diritto di difesa.

Tuttavia, i dati che possono essere prodotti in giudizio devono essere solo quelli pertinenti all'esigenza di far valere o difendere un diritto dell'istituto di credito; si deve evitare, ad esempio, l'ingiustificata produzione di interi tabulati (*ad es.*, interi estratti conto) contenenti dati personali (a volte anche riferiti a terzi) non rilevanti per le citate finalità di difesa [51].

5. Esercizio dei diritti previsti dall'art. 7 del Codice

5.1. *Accesso ai dati.* L'art. 7 del Codice obbliga la banca (in qualità di titolare del trattamento) a fornire idoneo riscontro alle richieste di accesso avanzate dagli interessati con riferimento ai dati personali che li riguardano [52].

Tra questi devono essere annoverate anche tutte le informazioni personali relative alle operazioni effettuate dagli interessati, nonché quelle relative alle registrazioni telefoniche degli ordini di negoziazione dagli stessi impartiti [53], come pure le informazioni di carattere personale, eventualmente raccolte dalla banca nell'eseguire ordini di investimento della clientela e idonee a manifestarne obiettivi e propensione al rischio.

L'istanza presentata ai sensi degli artt. 7 e 8 del Codice comporta l'obbligo per la banca di estrapolare dai propri archivi e dai documenti effettivamente conservati i dati personali relativi all'interessato oggetto della richiesta, e di comunicarli allo stesso in modo intelligibile nei modi di cui all'art. 10 del Codice, fornendo se necessario i criteri e i parametri per la comprensione del significato di eventuali codici associati alle informazioni riferite all'interessato medesimo (art. 10, comma 6, del Codice) [54].

In particolare, nel caso in cui l'estrazione dei dati risulti particolarmente difficoltosa, la banca può fornire riscontro alla richiesta dell'interessato anche *"attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti"* (art. 10, comma 4, del Codice) [55], ancorché la disciplina di protezione dei dati non preveda l'obbligo per il titolare del trattamento di esibire o di allegare copia di ogni singolo documento contenente i dati personali dell'interessato [56].

Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi; tali dati, quindi, nel caso di consegna di copia di documentazione che li contenga, debbono essere oscurati [57].

L'esercizio da parte dell'interessato del diritto di accesso ai dati personali che lo riguardano e degli altri diritti previsti dall'art. 7 del Codice è gratuito, salva la previsione contenuta nell'art. 10, commi 7 e 8, del Codice che prevede la possibilità di chiedere all'interessato un contributo spese quando "si determina un notevole impiego di mezzi in relazione alla complessità o all'entità della richiesta" (art. 10, comma 8, del Codice).

5.2. *Accesso ai dati personali ex art. 7 del Codice e accesso alla documentazione bancaria ai sensi dell'art. 119 Tub.* Il diritto di accedere ai dati personali previsto dall'art. 7 del Codice deve essere distinto dal diritto di accesso alla documentazione bancaria previsto dall'art. 119 del Tub [58].

Va al riguardo considerato che quest'ultimo, a differenza di quanto previsto dagli artt. 7 ss. del Codice, riconosce al cliente, a colui che gli succede a qualunque titolo e a chi subentra nell'amministrazione dei suoi beni, il diritto di ottenere copia di atti o documenti bancari (sia che essi contengano dati personali relativi all'interessato, sia nel caso in cui ciò non accada) [59].

Tale diritto non prevede limitazioni rispetto all'ostensibilità delle informazioni contenute nella documentazione richiesta (ivi compresi dati personali relativi a terzi che dovessero esservi contenuti), neanche nelle forme di un parziale oscuramento delle informazioni stesse; il suo esercizio prevede il pagamento delle spese a carico del cliente.

5.3. *Accesso ai dati di defunti (art. 9 del Codice).* La disciplina in materia di protezione dei dati personali prevede che il diritto di accesso ai dati riferiti a persone decedute possa essere esercitato "da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione" (art. 9, comma 3, del Codice) legittimando i soggetti che si trovino in tali condizioni ad esercitare tale diritto in rapporto a dati personali (inclusi rapporti bancari e finanziari) riferibili al defunto.

L'istituto di credito è quindi tenuto a comunicare ai soggetti indicati al menzionato art. 9, comma 3, in modo chiaro e comprensibile informazioni riguardanti la consistenza patrimoniale del defunto, le movimentazioni bancarie, i saldi riferiti ai depositi "al portatore", anche se estinti da terzi successivamente al decesso, nonché la data in cui è stata disposta l'estinzione del conto o il trasferimento del saldo ad altro conto.

Non possono, invece, formare oggetto di comunicazione ai sensi degli artt. 7 e 9, comma 3, del Codice informazioni che siano dati personali riferibili non all'interessato, ma a terzi [60]. Ad esempio, non è conoscibile in base alle norme appena richiamate il nominativo del percettore del saldo di deposito, pur intestato al *de cuius*, in quanto tale informazione riguarda non il cliente deceduto, ma un terzo [61]; ciò, salvo che ricorra un'ipotesi di cointestazione con il defunto [62]. In base, poi, a tale disciplina non può essere accolta la differente richiesta di accesso a dati personali trattati da una banca e riferiti ad una persona

deceduta, se volta a conoscere specificamente e direttamente l'identità della persona delegata dal defunto ad effettuare determinate operazioni bancarie [63].

5.4. *Accesso ai dati personali ex art. 7 del Codice e fallito.* Il diritto d'accesso previsto dall'art. 7 del Codice può essere esercitato dal fallito il quale, per effetto del fallimento, è privato esclusivamente dell'amministrazione e della disponibilità dei suoi beni. A tale proposito, l'amministrazione del patrimonio fallimentare, rimessa al curatore, non riguarda i diritti di natura strettamente personale esercitabili senza autorizzazione o sostituzione del curatore [64].

(1) Allo stato, in base al d.P.R. 14 marzo 2001, n. 144 (Regolamento recante norme sui servizi di bancoposta), adottato in attuazione della delega contenuta nell'art. 40 della l. 23 dicembre 1998, n. 448.

(2) Così, al fine di elevare il grado di sicurezza di beni e persone (segnatamente, del personale dipendente degli istituti di credito e della clientela), le banche possono effettuare trattamenti di dati personali della clientela, nella forma della rilevazione di impronte digitali e di immagini, nei limiti e in conformità alle misure e agli accorgimenti stabiliti nel *Provv.* 27 ottobre 2005, in *www.garanteprivacy.it*, doc. *web* n. 1246675 (pubblicato in *G.U.* 22 marzo 2006, n. 68).

(3) *Cfr. Provv.* 8 marzo 2007, doc. *web* n. 1390872, relativo all'accesso per finalità personali (e non istituzionali) da parte di un funzionario di banca alla Centrale dei rischi della Banca d'Italia e al sistema centralizzato di rilevazione dei rischi di importo contenuto.

(4) In merito, vigente la l. n. 675/1996, l'Autorità (anche a seguito del *Provv.* 28 maggio 1997, doc. *web* n. 40425) si era espressa in termini generali in ordine al rispetto della disciplina relativa all'informativa da rendere alla clientela e alle modalità per raccogliere, ove necessario, il consenso degli interessati: *cfr. Newsletter* 10 maggio 1999.

(5) Allo stato, *v.* art. 2 d.l. 3 maggio 1991, n. 143 (Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio), convertito con modificazioni dalla l. 5 luglio 1991, n. 197 e successivamente modificato dal d.lg. 26 maggio 1997, n. 153. In merito *v.* pure Comitato di Basilea per la vigilanza bancaria (Dovere di diligenza delle banche nell'identificazione della clientela), ottobre 2001.

(6) Art. 7, comma 6, del d.P.R. 29 settembre 1973, n. 605, come sostituito, a far data dal 1° gennaio 2006, dal comma 332 dell'art. 1 l. 30 dicembre 2004, n. 311 e, infine, così modificato dal d.l. 30 settembre 2005, n. 203.

(7) *Cfr. Provv.* 27 ottobre 2005, doc. *web* n. 1189435, relativo all'identificazione della clientela.

(8) *Provv.* 28 maggio 1997, doc. *web* n. 40425, in materia di informativa e consenso della clientela nell'ambito dei servizi bancari.

(9) In merito *v.* le prescrizioni contenute nel regolamento Consob 1° luglio 1998 n. 11522 (Regolamento di attuazione del decreto legislativo 24 febbraio 1998, n. 58, concernente la disciplina degli intermediari), con particolare riguardo all'art. 69.

(10) In particolare, la prassi conosce tre tipologie di tale procedura corrispondenti a diverse esigenze commerciali: Rid utenze, Rid commerciale e Rid veloce. In merito *cfr.* circolare Abi n. 45, serie tecnica O del 6 giugno 1983; *v.* altresì le circolari Abi Prot. SP6014 del 22 dicembre 2004; prot. SP1453 del 29 marzo 2005; prot. SP/003076 del 17 giugno 2005.

(11) *Cfr.* circolari *citt.*

(12) Nel Rid utenze si consente al debitore che vuole avvalersi della procedura per il pagamento del servizio reso da una società di ricevere da quest'ultima il modulo di autorizzazione permanente all'addebito in conto corrente, consegnandolo poi alla banca presso la quale intrattiene il rapporto di conto corrente, ovvero al medesimo creditore; in quest'ultimo caso è essenziale che i moduli riportino *"la indicazione degli estremi completi dell'azienda di credito presso la quale è intrattenuto il conto da addebitare (intestazione e numero filiale, numero dell'agenzia, indirizzo)"*: *cfr.* punto 2.2.1 della menzionata circolare Abi del 6 giugno 1983.

(13) Ciò, è in armonia con il *cd.* segreto bancario che si sostanzia nel dovere della banca di mantenere il riserbo in ordine alle notizie riguardanti i clienti nell'esercizio dell'attività bancaria, rispetto alle quali sussiste un interesse, meritevole di tutela, a che non siano divulgate o comunicate a terzi. Peraltro, come è noto, la Corte costituzionale (sentenza 18 febbraio

1992, n. 51) ha precisato che la tutela del *cd.* segreto bancario, talora desunto dalla clausola generale di correttezza e di buona fede tra banca e cliente (artt. 1175 e 1375 c.c.), non può spingersi "fino al punto di fare di questo ultimo un ostacolo all'adempimento di doveri inderogabili di solidarietà, prima fra tutti quella di concorrere alle spese pubbliche in ragione della propria capacità contributiva (art. 53 della Costituzione), ovvero fino al punto di farne derivare il benché minimo intralcio all'attuazione di esigenze costituzionali primarie, come quelle connesse all'amministrazione della giustizia e, in particolare, alla persecuzione dei reati". *V.* altresì *Provv.* 23 maggio 2001, doc. *web* n. 39821.

(14) *V.* pure art. 1 del codice di comportamento del settore bancario e finanziario adottato dall'Abi.

(15) *Cfr. Provv.* 6 febbraio 2001, doc. *web* n. 40879.

(16) *Cfr. Provv.* 17 settembre 2002, doc. *web* n. 1066132.

(17) Tale è il caso in cui il dipendente aveva divulgato dati su rapporti di conto corrente e di deposito titoli ad un legale esterno il quale, a sua volta, li aveva utilizzati in una controversia tra il cliente e un terzo (si trattava, in concreto, di una controversia relativa all'aumento dell'assegno di divorzio): *Provv.* 23 maggio 2001, doc. *web* n. 39821.

(18) *Cfr. Provv.* 8 marzo 2007, doc. *web* n. 1390910.

(19) *Cfr.* con particolare riguardo allo svolgimento dell'attività di *e-banking*, il *Provv.* 11 novembre 2002, doc. *web* n. 1067296.

(20) *Cfr.* l. 5 luglio 1991, n. 197, con particolare riferimento all'art. 3, comma 7; si prendano pure in considerazione i successivi decreti ministeriali attuativi del 19 dicembre 1991, 26 giugno 1992, 7 luglio 1992 e 7 agosto 1992.

(21) Già nelle *"Indicazioni operative per la segnalazione di operazioni sospette"* (*cd.* "Decalogo"), impartite dalla Banca d'Italia il 12 gennaio 2001 ai sensi dell'art. 3 bis, comma 4, l. 5 luglio 1991, n. 197, punto 2.1. (*cd. know your customer rule*), si precisava che *"il dato oggettivo va integrato con le informazioni sul cliente in possesso dell'intermediario, nel valutare la coerenza e la compatibilità dell'operazione con il profilo economico-finanziario che deve essere dichiarato dal cliente medesimo; particolare attenzione è richiesta qualora risulti che il cliente non svolge attività con rilievo economico. Ingiustificate incongruenze rispetto alle caratteristiche soggettive del cliente e alla sua normale operatività -sia sotto il profilo quantitativo, sia sotto quello degli schemi contrattuali utilizzati- richiedono l'attivazione della procedura di segnalazione"* [...] *"Gli accertamenti bancari e gli ulteriori provvedimenti disposti dall'autorità giudiziaria (misure di prevenzione, rinvii a giudizio, ecc.) sono utilizzati per la valutazione sulla qualità dei clienti così come le notizie di stampa, specie se relative a operazioni finanziarie internazionali irregolari, le comunicazioni pubblicate nella Gazzetta Ufficiale e tutte le altre informazioni desumibili sulla piazza"*.

(22) *V.*, allo stato, il *Provv.* del 9 novembre 2001 dell'Ufficio italiano dei cambi (Istruzioni in materia di contrasto finanziario al terrorismo), pubblicato sulla *G.U.* 15 novembre 2001, n. 266; *v.* anche, in particolare, l'art. 10, d.lg. 22 giugno 2007, n. 109, recante *Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/Ce*, in *G.U.* 26 luglio 2007, n. 172 (disciplina che, tra l'altro, ha abrogato le previgenti pertinenti disposizioni del d.l. 12 ottobre 2001, n. 369, recante *"Misure urgenti per reprimere e contrastare il finanziamento del terrorismo internazionale"*).

(23) *Cfr.* art. 14-*quinquies*, comma 2, della l. 3 agosto 1998, n. 296 come novellata dall'art. 19 l. 6 febbraio 2006, n. 38, recante *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet.*

(24) *Cfr.*, ad esempio, art. 7, comma 6, d.P.R. 29 settembre 1973, n. 605 (*Disposizioni relative all'anagrafe tributaria e al codice fiscale dei contribuenti*) e art. 1, comma 3, d.l. 28 giugno 1990 n. 167 (*Rilevazione a fini fiscali di taluni trasferimenti da e per l'estero di denaro, titoli e valori*), in *G.U.* 30 giugno 1990, n. 151 (e convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 4 agosto 1990, n. 227).

(25) Detta "anagrafe" è stata a suo tempo prevista dall'art. 20, comma 4, della l. 30 dicembre 1991, n. 413 e successivamente regolata con il d.m. 4 agosto 2000, n. 269; *v.* ora d.l. 4 luglio 2006, n. 223, conv., con mod., dalla legge 4 agosto 2006, n. 248); *Provv.* Agenzia delle entrate del 19 gennaio 2007 *"Modalità e termini di comunicazione dei dati all'Anagrafe Tributaria da parte degli operatori finanziari di cui all'art. 7, sesto comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, e successive modificazioni"*.

(26) *Cfr.* del. Cicr 29 marzo 1994; *Provv.* Banca d'Italia 10 agosto 1995; Circ. Banca d'Italia 11 febbraio 1991, n. 139 e successivi aggiornamenti.

(27) *V.*, in particolare, la del. Cicr 3 maggio 1999 (*Istituzione di un archivio accentrato per la rilevazione dei rischi di importo contenuto*) e le Istruzioni della Banca d'Italia (*Sistema centralizzato di rilevazione dei rischi di importo contenuto*), in G.U. 21 novembre 2000, n. 272.

(28) *Cfr.* Cass. 7 agosto 1990, n. 7953; Cass. 27 settembre 2001, n. 12093; Corte app. Milano, 22 luglio 1997, in Giust. civ. 1998, I, 246.

(29) L'art. 547 c.p.c. (come modificato dall'art. 12, l. n. 52/2006) dispone che il terzo pignorato (nel caso in esame, la banca) debba "specificare di quali cose o di quali somme è debitore o si trova in possesso", dandone comunicazione al creditore procedente in conformità alla previsione contenuta nell'art. 543, comma 2, n. 4 c.p.c.

(30) Del. 16 novembre 2004, n. 9 (Bilanciamento di interessi), in *G.U.* 23 dicembre 2004, n. 300 e doc. *web* n. 1070779.

(31) *V.* Del. 16 novembre 2004, n. 8, in *G.U.* 23 dicembre 2004, n. 300, come modificato dall'*errata corrige* pubblicata in *G.U.* 9 marzo 2005, n. 56 e doc. *web* n. 1070713.

(32) In tal senso *v. Provv.* 1° febbraio 2007, doc. *web* n. 1388576; *Provv.* 18 gennaio 2007, doc. *web* n. 1386384; *Provv.* 21 dicembre 2006, doc. *web* n. 1381657; *Provv.* 21 dicembre 2006, doc. *web* n. 1378189; *Provv.* 7 dicembre 2006, doc. *web* n. 1375058; *Provv.* 7 dicembre 2006, doc. *web* n. 1375085; *Provv.* 7 dicembre 2006, doc. *web* n. 1375133; *Provv.* 7 dicembre 2006, doc. *web* n. 1375150; *Provv.* 20 aprile 2006, doc. *web* n. 1289957.

(33) *Cfr. Provv.* 8 ottobre 2003, doc. *web* n. 1132740.

(34) *"Regolamento sul funzionamento dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento"*, pubblicato nella *G.U.* 4 gennaio 2002, n. 3.

(35) Relativo al *"Funzionamento dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento"*, pubblicato in *G.U.* 1° febbraio 2002, n. 27 e successive modificazioni.

(36) *Cfr.* art. 11 d.m. n. 458/2001 e art. 13 del regolamento della Banca d'Italia che (in conformità ai princìpi contenuti nell'art. 7 del Codice) prevede che l'interessato possa accedere "ai dati contenuti nell'archivio che lo riguardano tramite gli enti segnalanti privati o tramite le filiali della Banca d'Italia".

(37) *Cfr. Provv.* 25 gennaio 2007, doc. *web* n. 1387164, in relazione all'inserimento nella Cai di dati personali, solo in parte veritieri, connessi all'emissione di una carta di pagamento non richiesta, né ricevuta dall'interessato.

(38) *V.* in merito *Provv.* 21 dicembre 2006, doc. *web* n. 1378399 (e, in ordine alla medesima vicenda, il successivo *Provv.* 22 febbraio 2007, doc. *web* n. 1391891).

(39) Tenendo in considerazione le circostanze del tutto particolari che in concreto si erano presentate il Garante ha disposto la cancellazione dei dati dall'archivio Cai con *Provv.* 27 settembre 2004, doc. *web* n. 1069074.

(40) *Provv.* 15 febbraio 2005, doc. *web* n. 1148524, che richiama in tal senso le Istruzioni della Banca d'Italia del 21 novembre 2002 e dell'11 luglio 2003.

(41) *Provv.* 17 marzo 2005, doc. *web* n. 1152149.

(42) In particolare il debitore, entro sessanta giorni dalla data di scadenza del termine di presentazione del titolo (dall'art. 9-*bis*, l. n. 386/1990), deve provvedere tempestivamente al pagamento dell'assegno, degli interessi, della penale e delle eventuali spese per il protesto o per la constatazione equivalente e documentare, altresì, l'avvenuto pagamento nelle forme puntualmente previste dal menzionato art. 8: *cfr.* in merito *Provv.* 22 febbraio 2007, doc. *web* n. 1391942; *Provv.* 26 luglio 2005, doc. *web* n. 1157986; *Provv.* 3 marzo 2005, doc. *web* n. 1149190; sulla tempestività delle attività rimesse al debitore *cfr. Provv.* 26 ottobre 2006, doc. *web* n. 1367653.

(43) *Provv.* 19 ottobre 2005, doc. *web* n. 1192373; *Provv.* 4 ottobre 2004, doc. *web* n. 1102353; *v.* ora, d.m. 30 aprile 2007, n. 112 di attuazione della legge 17 agosto 2005, n. 166, recante *"Istituzioni di un sistema di prevenzione delle frodi sulle carte di pagamento"*.

(44) *Cfr.* art. 14-*quinquies*, commi 5 e 6, l. n. 296/1998, *cit.*

(45) In ordine a tale prassi la disciplina in materia di protezione dei dati personali non prevede alcun divieto: *cfr.* Parere del 30 novembre 1998 (in Bollettino n. 6, p. 85 e) doc. *web* n. 39416. In ordine alla legittimità del *cd.* benefondi *v.* pure Cass., 27 novembre 2003, n. 18118; Cass. 10 marzo 2000, n. 2742.

(46) *Cfr.* Cass. 6 giugno 2003, n. 9103; Cass. 7 febbraio 1979, n. 820.

(47) Banca d'Italia, Istruzioni di vigilanza per le banche, tit. III, cap. 5, assume che nella dizione "ramo di azienda", utilizzata dall'art. 58 Tub, possano comprendersi "le succursali e, in genere, ogni insieme omogeneo di attività operative, a cui siano riferibili rapporti contrattuali e di lavoro dipendente nell'ambito di una specifica struttura organizzativa".

(48) Ciò, è stato reso possibile con la previsione di modalità semplificate per notificare la cessione,

consentendo comunque al contraente ceduto di recedere entro tre mesi (dall'avvenuta cessione) dal contratto in presenza di giusta causa (analogamente alla disciplina relativa alla cessione d'azienda di cui all'art. 2558 c.c. e distaccandosi, invece, dai princìpi di diritto comune relativi alla cessione del contratto di cui all'art. 1406 c.c.).

(49) In materia di cessione in blocco e cartolarizzazione dei crediti: *Provv.* 18 gennaio 2007, doc. *web* n. 1392461.

(50) Analoga prescrizione è stata impartita dalla Banca d'Italia, seppure a diverso fine, in relazione alle operazioni di cessione in blocco di rapporti giuridici ai sensi dell'art. 58 del Tub: *cfr.* Banca d'Italia, *Istruzioni di vigilanza per le banche*, tit. III, cap. 5, sez. II.

(51) Restano comunque ferme, ai sensi dell'art. 160, comma 6, del Codice, le autonome determinazioni che l'autorità giudiziaria riterrà di adottare in ordine all'efficacia e all'utilizzabilità di atti e documenti nel procedimento giudiziario.

(52) A tal proposito si vedano altresì le indicazioni già fornite in termini generali dal Garante con le *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati"* (Del. n. 53 del 23 novembre 2006), punto 9.

(53) *Cfr. Provv.* 23 luglio 2004, doc. *web* n. 1099411; *v.* pure, in relazione all'accesso a registrazioni di conversazioni aventi ad oggetto l'acquisto di pacchetti azionari, *Provv.* 19 giugno 2002, doc. *web* n. 1065269; *v.* pure *Provv.* 19 maggio 2005, doc. *web* n. 1151188.

(54) *Cfr. Provv.* 12 marzo 2004, doc. *web* n. 1090100.

(55) *Cfr.* tra gli altri *Provv.* 29 ottobre 2003, doc. *web* n. 1144061; *Provv.* 13 luglio 2006, doc. *web* n. 1321296; *Provv.* 20 dicembre 2006, doc. *web* n. 1376382; *Provv.* 16 marzo 2007, doc. *web* n. 1399446.

(56) *Provv.* 13 luglio 2006, doc. *web* n. 1320699; *Provv.* 23 marzo 2006, doc. n. 1285350.

(57) *Cfr. Provv.* 9 novembre 2006, doc. *web* n. 1366189; *Provv.* 10 dicembre 2003, doc. *web* n. 1053648; *Provv.* 27 dicembre 2001, doc. *web* n. 40987.

(58) *Provv.* 20 luglio 2006, doc. *web* n. 1322844.

(59) *Provv.* 28 settembre 2006, doc. *web* n. 1349798; *Provv.* 1° giugno 2005, doc. *web* n. 1139982; *Provv.* 1° giugno 2005, doc. *web* n. 1139991.

(60) In tal senso *cfr. Provv.* 20 maggio 2004, doc. *web* n. 1098787; Cass., 12 maggio 2006, n. 11004; Circ. n. 229 del 21 aprile 1999, p. 18 e ss.

(61) *Provv.* 27 aprile 2000, doc. *web* n. 1113611.

(62) In tal caso, con *Provv.* 3 aprile 2002, doc. *web* n. 1065256, si è affermato che *"il diritto di accesso ai dati personali conferisce* [...] l*a possibilità di acquisire piena cognizione di tutte le informazioni personali detenute dalla Cassa, permettendo allo stesso di comprendere il loro contenuto, anche attraverso il chiaro richiamo alle generalità dei cointestatari predetti (dati che lo stesso de cuius avrebbe avuto a suo tempo il diritto di conoscere)"*; *v.* pure *Provv.* 8 ottobre 2003, doc. *web* n. 1053855.

(63) *Provv.* 13 novembre 2003, doc. *web* n. 1053654.

(64) Per precedenti in materia *v. Provv.* 9 marzo 2006, doc. *web* n. 1268821, con richiami ulteriori a Cass., 23 luglio 1994, n. 6873 e Cass. 21 aprile 1997, n. 3400; *v.* pure artt. 31, 42 e ss. r.d. n. 267/1942, come modificato, allo stato, dal d.lg. 9 gennaio 2006, n. 5.

42 Linee-guida del Garante per posta elettronica e Internet nel rapporto di lavoro (*)
1 marzo 2007

Registro delle deliberazioni
n. 13 del 1 marzo 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici;

Vista la documentazione in atti;

Visti gli artt. 24 e 154, comma 1, lett. *b*) e *c*) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

PREMESSO

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. *Premessa*

Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Occorre muovere da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);

c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili. [1]

(*) ***G.U.*** **10 marzo 2007, n. 58**
[doc. *web* n. 1387522]
Le note sono in calce al testo

1.2. *Tutela del lavoratore*

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà [2].

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; *cfr.* altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato) [3].

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. *Principi generali*

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del Codice). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. *Discipline di settore*

Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (art. 47, comma 3, lett. *b*) Codice dell'amministrazione digitale) [4].

2.3. *Princìpi del Codice*

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti princìpi:

a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; *par.* 5.2);

b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. *a*), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (*v. par.* 3);

c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. *b*), del Codice: *par.* 4 e 5), osservando il principio di pertinenza e non eccedenza (*par.* 6). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (*par.* 8) ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (*Parere* n. 8/2001, *cit.*, punti 5 e 12).

3. Controlli e correttezza nel trattamento

3.1. *Disciplina interna*

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, secondo comma, Statuto dei lavoratori; allegato VII, *par.* 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di *"uso di attrezzature munite di videoterminali"*, il quale esclude la possibilità del controllo informatico *"all'insaputa dei lavoratori"*) [5].

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. *Linee-guida*

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, *ecc.*) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (*ad es.*, il *download* di *software* o di *file* musicali), oppure alla tenuta di *file* nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (*ad es.*, fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (*ad es.*, le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime –specifiche e non generiche– per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

3.3. *Informativa (art. 13 del Codice)*

All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2..

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art. 4, secondo comma, l. n. 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. *b*), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (*cfr.* artt. 2086, 2087 e 2104 cod. civ.).

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli [6].

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori. È il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di *computer* portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro [7]. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice) [8].

5. Programmi che consentono controlli "indiretti"

5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (*ad es.*, per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (*cd.* controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori [9]. Ciò, anche in presenza di attività di controllo discontinue [10].

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in rela-

zione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati [11], nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori [12].

5.2. *Principio di necessità*

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori (artt. 3, 11, comma 1, lett. *d*) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4).

Dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet [13];
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (*cd. privacy enhancing technologies* - PETs). Le misure possono essere differenziate a seconda della tecnologia impiegata (*ad es.*, posta elettronica o navigazione in Internet).

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; *Provv.* 2 febbraio 2006, *cit.*).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni –reputate inconferenti con l'attività lavorativa– quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (*ad es.*, con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) *Posta elettronica*

Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i *file* allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale) [14].

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta *"in entrata"*) o di quelli inviati da quest'ultimo (posta *"in uscita"*).

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (*ad es.*, *info@ente.it*, *ufficiovendite@ente.it*, *ufficioreclami@società.com*, *urp@ente.it*, *etc.*), eventualmente affiancandoli a quelli individuali (*ad es.*, *m.rossi@ente.it*, *rossi@società.com*, *mario.rossi@società.it*);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; [15]
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (*ad es.*, per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica [16]. In caso di eventuali assenze non programmate (*ad es.*, per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (*ad es.*, l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

6. Pertinenza e non eccedenza

6.1. *Graduazione dei controlli*

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i princìpi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. *Conservazione*

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la *cd.* rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla (*v.* art. 11, comma 1, lett. *e*), del Codice).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. *Datori di lavoro privati*

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (v., in particolare, art. 4, secondo comma, dello Statuto), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.

Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (art. 24, comma 1, lett. *f*) del Codice);
b) in caso di valida manifestazione di un libero consenso;
c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul *cd.* bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo