Capitolo XII

Protezione dei dati nel settore bancario

di *Giordano Costa e Marc-Frédéric Schäfer**

Premessa

In economia le banche sono spesso definite come aziende orientate all'economia privata, attive nell'ambito del traffico pagamenti, delle operazioni di credito e delle operazioni sui titoli[1]. Nella loro attività raccolgono, a titolo professionale, depositi del pubblico, rispettivamente si rifinanziano presso altre banche e finanziano per conto proprio un numero indeterminato di persone e aziende[2]. Tuttavia, oggi il vero e proprio trasferimento di denaro fisico non ha quasi più importanza. Anzi, l'intero traffico pagamenti ed il commercio di valori mobiliari è svolto elettronicamente. Al più tardi dal momento della liquidazione della banca d'investimento Lehman Brothers è apparso chiaro che il maggior capitale di liquidazione delle banche è investito nei loro impianti di elaborazione di dati. Così la Barclays Bank britannica ha destinato, su un importo complessivo di 1.75 miliardi di dollari, unicamente 250 milioni di dollari per il rilevamento dei campi di attività operativi e 1.5 miliardi di dollari per il rilevamento dei due centri di calcolo[3]. Per questo motivo, dal punto di vista della legge sulla protezione dei dati, le banche possono essere viste come aziende, il cui strumento principale per raggiungere i propri scopi è l'elaborazione dei dati.

* *Giordano Costa, lic. iur., è consulente legale dell'Incaricato federale della protezione dei dati e della trasparenza; esperto in diritto del lavoro e delle assicurazioni sociali Marc-Frédéric Schäfer, Dr. oec. et lic. iur., è consulente legale dell'Incaricato federale della protezione dei dati e della trasparenza; esperto in diritto bancario e assicurativo.*

[1] H. Schmid, *Geld, Kredit und Banken*; edizione Paul Haupt, Bern, Stuttgart, Wien; 2001, pag. 11.
[2] H. Schmid, *op. cit.*, pag. 10.
[3] *Spiegel-Online* del 18 settembre 2008: *Compert-Hardware macht Restwert von Pleitebanken aus*; richiamato il 26 febbraio 2009 al sito http://www.spiegel.de.

Sezione I
Principi fondamentali della Legge sulla protezione dei dati

L'obiettivo della legge sulla protezione dei dati è di proteggere la personalità ed i diritti fondamentali delle persone i cui dati sono oggetto di trattamento (art. 1 della Legge federale sulla protezione dei dati, LPD). La LPD può quindi essere considerata come *lex specialis* sulla protezione generale della personalità di cui all'art. 28 del Codice civile svizzero nell'ambito del trattamento dei dati[4]. Inoltre, la protezione della personalità, per quanto riguarda l'aspetto della protezione dei dati, è ancorata anche negli art.10 cpv. 2 (Diritto alla vita e alla libertà personale) e 13 (Protezione della sfera privata) della Costituzione federale (Cost.). Per rendere concreto il concetto fondamentale della protezione della personalità, perseguito nell'art. 28 CCS, la LPD ha introdotto degli strumenti importanti, sotto forma di principi di trattamento della protezione dei dati (art. 4 segg. LPD), per garantire una protezione sufficiente da lesioni della personalità nel trattamento dei dati personali[5].

1. Applicabilità della LPD

Su questo sfondo, la LPD si applica ai dati personali di persone fisiche e giuridiche, trattati da persone fisiche ed organi della Confederazione (art. 2 LPD). Il trattamento dei dati consiste in una qualsiasi operazione effettuata in connessione con dei dati. La LPD definisce il trattamento con l'elenco non esaustivo delle seguenti attività: la raccolta, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione o la distruzione di dati. Sulla base del principio di territorialità però la LPD è applicabile unicamente per il trattamento dei dati in Svizzera.

Di conseguenza, non appena un dipendente di una banca esegue un bonifico per una persona in Svizzera, egli tratta i dati personali della persona interessata, quindi si applica la LPD. Come dati personali s'intendono tutte le informazioni relative ad una persona identificata o identificabile (art. 3 lett. a LPD). In questo caso è decisivo che esista un riferimento personale tra i dati da trattare ed una persona in particolare, indipendentemente dal fatto che la persona interessata sia effettivamente identificata. È sufficiente che si possa

[4] FF 1988 II 434.

[5] *Commentario relativo alla LPD*, D. Rosenthal all'art. 1 LPD, cif. 2.

prevedere, con una certa probabilità, che la persona che elabora i dati si darà la pena di identificare la persona interessata[6]. Di conseguenza, il solo numero di conto, come pure tutte le informazioni legate ad esso, sono da considerare dati personali, fintantoché nel sistema della banca possono essere collegati ad un nome. Su questo sfondo bisogna supporre che praticamente ogni attività delle operazioni chiave di una banca soggiace alla LPD, e che la banca deve rispettare le prescrizioni sulla protezione dei dati. Inoltre la LPD conosce, oltre ai dati personali semplici, una categoria particolarmente sensibile di dati personali, che la LPD definisce come dati personali degni di particolare protezione. Tra questi vi figurano i dati sulle opinioni o attività religiose, filosofiche, politiche o sindacali, sulla salute, la sfera intima o l'appartenenza ad una razza, sulle misure d'assistenza sociale, come pure i dati sui procedimenti o sulle sanzioni amministrative e penali (art. 3 lett. c LPD).

2. Disposizioni generali di protezione dei dati

I principi generali del trattamento dei dati regolano il quadro giuridico nel quale un trattamento dei dati è permesso secondo la LPD. Come principi del trattamento dei dati l'art. 4 elenca il principio della legalità, il principio della buona fede, il principio della proporzionalità, il principio della finalità ed il principio della riconoscibilità (art. 4 cpv. 1-4 LPD).

Secondo il principio della legalità, un trattamento dei dati non deve infrangere la legge vigente[7]. Questo significa che nella misura in cui lo prescrive la legge, da una parte può essere necessario trattare determinati dati (ad es. registrazione dei dati personali in caso di sospetto di riciclaggio di denaro) e dall'altra può essere vietato trattare determinati dati (ad es. verifica dei movimenti di conto di un candidato ad un posto di lavoro nell'ambito del processo di candidatura; violazione secondo l'art. 328b della Legge federale di complemento del Codice civile svizzero, Libro quinto: Diritto delle obbligazioni CO).

Inoltre il trattamento dei dati deve essere conforme al principio della buona fede e della proporzionalità (art. 4 cpv. 2 LPD). Nella valutazione della proporzionalità la banca deve quindi verificare se il rapporto scopo-mezzi, tra l'obiettivo da raggiungere con il trattamento dei dati ed il trattamento dei dati eseguito a questo proposito, è in armonia[8]. A questo scopo la banca deve

[6] *Basler Kommentar sulla LPD*, U. Belser all'art. 3 LPD, n. 6.

[7] *Basler Kommentar sulla LPD*, U. Maurer-Lambrou/A. Steiner all'art. 4 LPD, n. 6.

[8] *Basler Kommentar sulla LPD*, U. Maurer-Lambrou/A. Steiner all'art. 4 LPD, n. 11.

verificare ogni volta se il trattamento dei dati da parte della banca è oggettivamente necessario. Sarebbe senz'altro esagerato, se una banca per l'apertura di un conto di risparmio dovesse eseguire un intero esame della solvibilità di una persona interessata. Tuttavia, sullo sfondo della lotta contro il riciclaggio di denaro, questo principio va applicato generalmente in modo cauto.

In caso contrario potrebbe sussistere il pericolo che la banca, per motivi di protezione di dati, non raccolga i dati personali che servono per la lotta contro il riciclaggio di denaro e contro il terrorismo internazionale[9].

Secondo il principio della finalità, i dati personali possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge (art. 4 cpv. 3 LPD). A questo proposito è decisivo l'obiettivo del trattamento dei dati. Ad esempio, sotto la lente della protezione dei dati, un'analisi sistematica dei movimenti di conto, per rilevare le attività nel tempo libero delle persone interessate, allo scopo di pianificare misure di marketing, è da considerare problematica. Qualora invece la persona interessata è stata informata di un tale trattamento dei dati e non ha fatto opposizione, questo tipo di trattamento dei dati di regola può essere considerato come non pericoloso.

Per questo motivo, la raccolta di dati personali, e in particolare le finalità del trattamento, devono essere riconoscibili da parte della persona interessata (art. 4 cpv. 4 LPG). Per l'esecuzione di un bonifico, ad esempio, possono essere eseguiti tutti i passi di trattamento dei dati senza che essi siano noti in dettaglio alla persona interessata. Il fatto determinante, in questo caso, è se un comune cittadino deve aspettarsi un tale trattamento dei dati. Nel caso di un bonifico all'interno della Svizzera, un comune cittadino può assolutamente aspettarsi che diverse banche svizzere (inclusa la BNS) siano coinvolte nel trasferimento e trattino di conseguenza i relativi dati. Nel caso di un bonifico in Svizzera di un importo in valuta estera, non ci si può aspettare da un cittadino medio che sappia che il clearing di bonifici in valuta estera deve sempre avvenire nel paese della divisa e che quindi avviene un trattamento dei dati all'estero. Di conseguenza il cliente deve essere informato adeguatamente di questo fatto[10]. Altrettanto sconosciuto ai clienti bancari potrebbe essere il fatto che, a causa della struttura organizzativa, fino ad oggi, tutti i bonifici all'estero sono elaborati presso la SWIFT negli USA[11]. Per rispettare in tali casi il principio della riconoscibilità, la rispettiva banca deve informare attivamente i suoi clienti in merito.

[9] Si veda a questo proposito anche A. Althaus Stämpfli, *Personendaten von Bankkunden*, Stämpfli Verlag AG Bern, 2004, pag. 76.
[10] Si veda http://www.enterag.ch.
[11] Si veda http://www.edoeb.admin.ch.

Secondo il principio dell'esattezza dei dati, la persona che tratta dati personali deve accertarsi della loro esattezza e deve prendere tutte le misure adeguate onde assicurare che dati non pertinenti o incompleti, in considerazione dello scopo per cui sono stati raccolti o elaborati, vengano cancellati o rettificati (art. 5 cpv. 2 LPD). Questo si riferisce soprattutto a fatti, siccome l'esattezza di giudizi sul valore sono molto difficili da valutare[12]. Tuttavia, ad esempio, in occasione di un esame della solvibilità di una persona interessata allo scopo di concedere un credito, va verificato maggiormente se le affermazioni sui fatti, utilizzate per questo esame, siano veramente corrette.

Inoltre, per la banca è consigliabile contrassegnare in modo esplicito nel rispettivo dossier cliente le percezioni e valutazioni soggettive, per indicare, ai sensi dell'esattezza dei dati, che si tratta di valutazioni personali del collaboratore di banca e non di fatti oggettivi.

Secondo il principio della sicurezza dei dati, i dati personali devono inoltre essere protetti contro il trattamento non autorizzato tramite misure tecniche ed organizzative adeguate.

Soprattutto nel traffico pagamenti elettronico, sia tra le banche, sia tra cliente e banca vi sono delle ulteriori esigenze rispetto alla sicurezza dei dati – non per ultimo in forza del segreto bancario[13] -.

Sezione II
La protezione dei dati nel contatto con il cliente in ambito bancario

3. Trattamento di dati personali degni di particolare protezione e profili della personalità

3.1. Considerazioni generali

Nell'ambito dell'erogazione del loro servizio, e allo scopo di impedire il riciclaggio di denaro ed il finanziamento del terrorismo, le banche generalmente non trattano dei dati personali degni di particolare protezione secon-

[12] A. Althaus Stämpfli, *op. cit.*, pag. 76.
[13] Art. 47 della Legge federale sulle banche e le casse di risparmio (LBCR).

do l'art. 3 lett. c LPD. È comunque possibile che, in una relazione d'affari a rischio superiore o nell'ambito di particolari relazioni d'affari, ad es. con persone esposte politicamente, la banca tratti dei dati riguardanti opinioni o attività religiose, filosofiche, politiche o sindacali[14]. In particolare nell'attività di Private Banking, le banche allestiscono spesso un profilo del cliente, da una parte per poter consigliare il cliente in modo migliore e più mirato, e dall'altra per adempiere gli obblighi prescritti dall'art. 7 della Legge federale relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo nel settore finanziario (LRD). Per questo motivo bisogna probabilmente supporre che le banche più caute di principio trattano più dati personali di quelli oggettivamente necessari.

3.2. Particolarità legali

La legge sulla protezione dei dati definisce un profilo della personalità come una compilazione di dati che permette di valutare caratteristiche essenziali della personalità di una persona fisica (art. 3 lett. d LPD). In ambito bancario, in modo particolare nei segmenti di clientela più elevati (Private Banking), sono spesso raccolte delle informazioni sull'attività professionale e commerciale, l'ambiente privato e familiare come pure la situazione di reddito e patrimoniale dei rispettivi clienti bancari[15]. Le informazioni prescritte dalla legge, come le informazioni per l'identificazione del cliente e dell'avente diritto economico – anche se in forma raccolta – prese da sole, difficilmente rappresentano un profilo della personalità. Se però questi dati sono completati da informazioni soggettive sul cliente, note soprattutto al rispettivo consulente, non può essere escluso che rappresentino un profilo della personalità. Non appena però la banca tratta dei profili della personalità o dati personali degni di particolare protezione, devono essere rispettate delle esigenze più elevate.

Oltre al rispetto dei principi del trattamento dei dati, nel trattamento dei profili della personalità e dei dati personali degni di particolare protezione esiste, secondo l'art. 4 cpv. 5 LPD, quando il trattamento di dati personali è subordinato al consenso della persona interessata, l'obbligo che il consenso sia esplicito. Inoltre la banca è soggetta ad un obbligo d'informazione più severo nei confronti della persona interessata (art. 7a LPD). Ciò significa che non è sufficiente che il trattamento dei dati sia riconoscibile per la persona interessata, ma la banca deve informarla attivamente del trattamento dei dati.

[14] A. Althaus Stämpfli, *op. cit.*, pag. 71.
[15] A. Althaus Stämpfli, *op. cit.*, pag. 99.

Questo vale persino nel caso in cui la banca si procura dei dati da terzi (art. 7a cpv. 1 LPD). In tale caso la banca che tratta i dati deve informare la persona interessata al più tardi all'inizio della registrazione dei dati o, se si rinuncia alla registrazione, al momento della loro prima comunicazione a terzi (art. 7a cpv. 3 LPD). L'obbligo d'informazione del detentore della collezione di dati decade però se la registrazione o la comunicazione dei dati è esplicitamente prevista dalla legge, o se l'informazione non è possibile o esige mezzi sproporzionati (art. 7a cpv. 4 LPD). Quest'ultimo caso dovrebbe trovare difficilmente applicazione in ambito bancario, considerando che di regola l'identità ed i dati di contatto della persona interessata dovrebbero essere conosciuti alla banca. Rimane però ancora la domanda, se la LRD rappresenta una base legale sufficiente per esonerare una banca dall'obbligo d'informazione. Secondo l'art. 7 LRD, l'intermediario finanziario deve allestire i documenti relativi alle transazioni effettuate e ai chiarimenti previsti dalla LRD e conservare questi documenti. Gli art. 3 a 11 LRD definiscono l'entità dei chiarimenti necessari in questo caso[16]. Di conseguenza per il trattamento delle informazioni previste in questi articoli cade l'obbligo d'informazione come da art. 7 cpv. 4 LPD. Per quanto riguarda tutte le ulteriori informazioni raccolte e trattate, la persona interessata deve essere tuttavia informata. Lo stesso vale anche se le informazioni registrate sono utilizzate ad un altro scopo, come ad esempio per il miglioramento della consulenza in ambito Private Banking.

Inoltre devono essere notificate le collezioni di dati, se sono trattati regolarmente dati personali degni di particolare protezione o profili della personalità (art. 11a cpv. 3 lett. a LPD) senza che vi sia un obbligo legale (art. 11a cpv. 5 lett. a LPD). Di conseguenza, le banche e gli intermediari finanziari sono esonerati dalla notifica della collezione di dati fintantoché essa è allestita sulla base delle prescrizioni della LRD.

Qualora una collezione di dati personali degni di particolare protezione o profili della personalità è utilizzata anche per altri scopi, oppure qualora vengano raccolte più informazioni di quelle oggettivamente necessarie, la collezione dei dati deve essere di principio notificata all'IFPDT (Incaricato Federale della Protezione dei Dati e della Trasparenza)[17].

[16] *Commentario* sulla LRD, 2003; Thelesklaf, Wyss, Zollinger sull'art. 7 LRD, cif. 3 e 6.
[17] Ulteriori informazioni sulla notifica di collezioni di dati e le rispettive eccezioni si trovano anche nella Sezione IV.

4. Trasmissione di dati all'estero

4.1. Considerazioni generali

A causa dell'intreccio internazionale tra le banche ed il sistema finanziario globale, oggi per una banca è inevitabile trasmettere dei dati all'estero. In questo caso le banche devono considerare degli aspetti speciali della legge sulla protezione dei dati nella gestione di dati che trasmettono all'estero. In particolare, qualora il trasferimento internazionale d'informazioni avviene con paesi che, secondo la LPD, non garantirebbero una protezione adeguata e metterebbero in pericolo la personalità della persona interessata (art. 6 cpv. 1 LPD).

4.2. Prescrizioni legali per una comunicazione di dati all'estero

La LPD regola i principi della comunicazione di dati oltre frontiera soprattutto nell'art. 6 LPD. Secondo questo articolo i dati personali possono essere comunicati all'estero unicamente qualora la personalità della persona interessata non possa subirne grave pregiudizio, dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata (art. 6 cpv. 1 LPD). Siccome oggi la maggior parte degli stati extraeuropei non dispone di un adeguato livello di protezione dei dati, specialmente per le banche attive a livello internazionale si pone la domanda, sotto quali condizioni possono comunicare dei dati all'estero. Gli esempi nei quali delle banche comunicano dei dati all'estero sono molteplici e vanno dall'esecuzione di un bonifico all'estero, attraverso la consulenza di un cliente bancario all'estero (ad esempio, se il consulente bancario s'incontra con il cliente in un albergo all'estero e porta la rispettiva documentazione del cliente), fino allo spostamento della sede o di singoli campi d'attività all'estero.

Nel caso in cui il paese destinatario dei dati personali dispone di un livello di protezione dei dati adeguato secondo l'art. 6 cpv. 1 LPD, i dati possono essere trasferiti senza problemi[18].Sulla sua homepage, l'IFPDT mette a disposizione un elenco dei paesi[19], nel quale è indicato quali stati dispongono di un livello di protezione dei dati adeguato o parzialmente adeguato. Gli stati membri dell'Unione europea dispongono di un livello di protezione adeguato, in particolare grazie alla direttiva 95/46/UE relativa alla tutela delle persone

[18] http://www.edoeb.admin.ch. La trasmissione dei dati all'estero in breve come pure spiegazioni concernenti la comunicazione di dati a carattere personale all'estero secondo la rivista LPD.
[19] http://www.edoeb.admin.ch, Elenco dei Paesi.

fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (direttiva sulla protezione dei dati)[20].

Se una banca invece intende trasferire dei dati personali ad un paese estero che non dispone di una legislazione che garantisce un livello adeguato di protezione, lo può fare soltanto prendendo ulteriori precauzioni. A questo scopo l'art. 6 cpv.2 LPD offre diverse possibilità, le quali saranno enunciate in seguito, con l'aiuto di esempi pratici, soltanto quelle rilevanti per una banca.

Secondo l'art. 6 cpv. 2 lett. b LPD, una banca può trasferire dei dati personali all'estero soltanto se la persona interessata ha dato il suo consenso nel caso specifico. Il consenso deve essere limitato ad una situazione concreta.

La persona interessata, tuttavia, non deve aver dato il suo consenso per ogni singolo trattamento di dati o per ogni singola fase di elaborazione, ma può dare il suo consenso anche per un'intera categoria di trattamenti di dati analoghi, nella misura in cui lo scopo e il destinatario rimangano gli stessi (ad es. ordini permanenti all'estero)[21]. Non è permessa una comunicazione sistematica e regolare di dati per diversi scopi e in diverse situazioni, qualora questa sia giustificata soltanto da un unico consenso nel caso specifico. Affinché un consenso nel caso specifico sia legalmente valido, questo deve essere espresso liberamente e dopo debita informazione (art. 4 cpv. 5 LPD). Ciò significa che la persona interessata deve essere in grado di poter valutare le possibili conseguenze di una trasmissione di dati all'estero, prima di decidere se dare il suo consenso al trattamento dei dati. Si può supporre un consenso implicito, se il trasferimento dei dati all'estero è in relazione diretta con la conclusione o l'esecuzione di un contratto, ed i dati trattati concernono l'altro contraente (art. 6 cpv. 2 lett. c LPD). In ambito bancario, questa eccezione trova applicazione soprattutto nel traffico pagamenti internazionale. Qui bisogna comunque considerare che il cliente deve essere informato sufficientemente sul trattamento dei dati e sulle possibili conseguenze che ne derivano. Per questo motivo le banche informano ad esempio i loro clienti attivamente in merito al fatto che nel caso delle transazioni SWIFT (anche se non è effettuato un bonifico negli USA) è possibile che avvenga una trasmissione dei dati agli USA. Un ulteriore esempio, nel quale la banca ha un obbligo d'informazione, è nel caso di bonifico all'interno della Svizzera, ma in valuta estera. Negli ambienti bancari è noto universalmente che il clearing di un bonifico avviene sempre nel paese della valuta estera. Un comune cliente bancario però di regola non è a conoscenza di questo fatto. Di conseguenza per lui non è riconoscibile che

[20] http://eur-lex.europa.eu.
[21] http://www.edoeb.admin.ch. La trasmissione dei dati all'estero in breve, pag. 5.

nel caso di un bonifico in valuta estera (ad es. in dollari USA) da una banca svizzera ad un'altra banca svizzera, il trasferimento dei dati avviene attraverso l'estero (USA)[22].

Oltre al caso della richiesta di consenso, nel caso specifico, le banche possono trasmettere dei dati all'estero, se garanzie sufficienti, segnatamente contrattuali o all'interno della stessa persona giuridica o società, sulla base di regole comuni di protezione di dati, assicurano una protezione adeguata all'estero (art. 6 cpv. 2 lett. a e g LPD). Di regola le banche applicano questa possibilità ogni volta che una grande entità di dati deve essere trasmessa all'estero e il consenso nel caso specifico non è praticabile. La banca ha l'obbligo di informare l'IFPDT sulle garanzie e le regole di protezione dei dati (art. 6 cpv. 3 LPD). L'IFPDT verifica quindi queste garanzie e regole di protezione dei dati e comunica se esse siano sufficienti. Per facilitare l'elaborazione di garanzie e regole di protezione dei dati, l'IFPDT ha pubblicato sulla sua homepage un contratto tipo[23].

Possono essere inoltre usate come modelli le clausole contrattuali standard[24] dell'UE come pure il Safe Harbor Agreement[25]. Un'applicazione dell'US-Swiss Safe Harbor Frameworks nell'ambito dell'industria finanziaria invece non è possibile, fintantoché la rispettiva azienda negli USA non soggiace alla sfera di competenza della *Federal Trade Commission* (FTC).

5. L'esternalizzazione (outsourcing) del trattamento di dati e la collaborazione con terzi

5.1. Considerazioni generali

Siccome il trattamento dei dati all'interno di una banca è un'attività molto estesa e complessa, spesso sono coinvolti dei partner esterni che erogano diversi servizi. Nella collaborazione con questi partner, la delimitazione tra l'outsourcing di un trattamento di dati (art. 10a LPD) e la comunicazione di dati a terzi spesso non è facile e in pratica crea delle difficoltà. Dato che i due casi, dal punto di vista della legge sulla protezione dei dati, devono essere trattati in modo differente, le aziende devono soddisfare per entrambi delle

[22] Si veda a questo proposito http://www.enterag.ch.

[23] http://www.edoeb.admin.ch; Contratto modello per l'esternalizzazione (outsourcing) di trattamenti di dati all'estero.

[24] http://ec.europa.eu/justice, clausole contrattuali standard per trattamento di dati all'estero.

[25] http://www.edoeb.admin.ch. US-Swiss Safe Harbor Framework.

esigenze diverse. Indipendentemente da questo fatto comunque le banche, nel caso di un trasferimento di dati all'estero, devono sempre adempiere gli obblighi sulla comunicazione di dati personali all'estero secondo l'art. 6 LPD[26].

5.2. Trattamento dei dati da parte di terzi vs. comunicazione dei dati a terzi

Nell'applicazione della legge sulla protezione dei dati, si discute spesso in quali casi una persona sia da considerare un terzo e quando invece no. Di principio, si può supporre che i dipartimenti all'intero di un'azienda non siano da considerare terzi ai sensi della legge sulla protezione dei dati. L'IFPDT al contrario è dell'opinione che ai sensi della legge sulla protezione dei dati, già una società affiliata è da qualificare come terzo rispetto alla casa madre.

Un dipendente dell'azienda che elabora i dati di regola non è considerato come terzo[27]. In particolare la presenza di un rapporto di subordinazione tra la persona che tratta i dati e la persona che svolge in definitiva l'elaborazione dei dati, dà una buona indicazione se si tratti di un terzo oppure no. Se in questo caso si tratta di una persona giuridicamente dipendente, come ad esempio un collaboratore dipendente, di regola questa non è qualificata come terzo[28]. Secondo il punto di vista degli autori, una definizione differente di terzo nel trattamento dei dati da parte di terzi e nella comunicazione di dati a terzi non è opportuna[29].

Il criterio di differenziazione per decidere se si tratta di un trattamento di dati da parte di terzi o di una comunicazione di dati a terzi, può essere dedotto dal trattamento di dati stesso. A questo proposito va verificato se il terzo esegue semplicemente il trattamento di dati, rimanendo vincolato a delle direttive, oppure elabora i dati per interesse proprio o decide sullo scopo ed il contenuto dei dati elaborati. Se una banca consegna ad esempio informazioni sugli indirizzi di clienti ad un terzo, il quale esegue la spedizione di opuscoli pubblicitari per la stessa e utilizza gli indirizzi unicamente per questa spedizione, si è in presenza di un trattamento di dati da parte di terzi (outsourcing; art. 10a LPD). Se invece il terzo utilizza gli indirizzi (con il consenso della banca) anche per la spedizione del proprio materiale pubblicitario, questo potrebbe essere definito comunicazione di dati a terzi. Le difficoltà nella delimitazione possono essere rese più chiare mediante il seguente esempio.

[26] Si veda § 4.2.

[27] D. Rosenthal, Y. Jöhri, *Commentario relativo alla LPD*, D. Rosenthal all'art. 10a LPD, n. 5 segg.

[28] A. Althaus Stämpfli, *op. cit.*, pag. 168.

[29] Anche se a prima vista sembrerebbe utile la costruzione ausiliaria, secondo la quale nel trattamento di dati da parte di terzi, il terzo tratta i dati nella stessa maniera nella quale li tratterebbe il mandante ed il terzo di conseguenza non può essere definito veramente come tale.

Nell'ambito dello sponsoring di un'associazione, la banca intende spedire un'offerta speciale ai membri dell'associazione. A questo scopo l'associazione inoltra alla banca una lista con gli indirizzi dei membri e la incarica di spedire, a nome suo (ad es. su carta intestata all'associazione) un determinato opuscolo pubblicitario informativo. Dal punto di vista della legge sulla protezione dei dati, questa spedizione può essere ancora definita trattamento di dati da parte di terzi (anche se gli indirizzi sono stati trasmessi alla banca). Qualora però un consulente della banca dovesse iniziare, a nome della banca, a contattare le singole persone, alle quali è stato inviato l'opuscolo, con l'obiettivo di acquisire nuovi clienti, si è in presenza di un trattamento di dati nell'interesse della banca per scopi di acquisizione di clientela, ed il trasferimento di dati dall'associazione alla banca andrebbe qualificato come comunicazione di dati a terzi.

5.3. Trattamento di dati da parte di terzi

Se un mandante decide di incaricare un terzo del trattamento di dati, egli può trasmettere i dati al terzo mediante convenzione o per legge, quando i dati sono trattati esclusivamente nella stessa maniera nella quale sarebbe autorizzato a farlo il mandante stesso e nessun obbligo di riservatezza legale o contrattuale lo vieti (art. 10a cpv. 1 LPD). Anche nel trattamento di dati da parte di terzi devono essere rispettati i principi del trattamento di dati[30]. Anche quando un trattamento di dati da parte di terzi non richiede obbligatoriamente il consenso della persona interessata[31], deve perlomeno essere riconoscibile dalla stessa come tale. Inoltre il "trattamento di dati da parte di terzi" non deve provocare un cambiamento non autorizzato dello scopo del trattamento di dati secondo l'art. 4 cpv. 2 LPD. Se il mandante incarica un terzo del trattamento di dati, deve in particolare assicurarsi che il terzo garantisca la sicurezza dei dati (art. 10a cpv. 2 LPD). Inoltre rimane responsabile anche del trattamento di dati da parte di terzi, finché non è in grado di provare di aver fatto tutti gli sforzi ragionevoli per garantire un trattamento di dati conforme alla protezione dei dati. La banca committente può soddisfare quest'esigenza ad esempio tramite obblighi contrattuali del mandante, controlli a campione e – laddove sia possibile – attraverso la scelta di pseudonomizzare dei dati personali prima della trasmissione per l'elaborazione a terzi.

Dove la scelta dei pseudonimi non sia possibile (ad es. nell'outsourcing della

[30] Si veda § 4.2.

[31] Vedi argomentazioni di D. ROSENTHAL, Y. JÖHRI, *Commentario relativo alla LPD*, D. ROSENTHAL all'art. 10a LPD, n. 1

stampa di estratti conto), la trasmissione dei dati deve essere protetta da particolari meccanismi di codificazione. Nell'outsourcing del traffico pagamenti internazionale vanno rispettati i processi prescritti dalle *Special Recommendations* del GAFI (*Financial Action Task Force on Money Laundering* -FATF)[32].

Nel trattamento di dati da parte di terzi, il terzo può far valere gli stessi motivi giustificativi del mandante (art. 10a cpv. 3 LPD). Da questa affermazione si può dedurre che, finché il trattamento di dati da parte del mandante è legale e le premesse degli art. 10a cpv. 1 e 2 LPD sono rispettate, un trattamento di dati da parte di terzi è in ogni caso possibile. Questo può persino avvenire contro l'esplicito desiderio della persona interessata, se, secondo gli art. 12 cpv. 2 lett. b e c LPD in combinazione con l'art. 13 LPD esistono dei motivi giustificativi sufficienti (prevalente interesse pubblico o privato come pure base legale) per un tale trattamento di dati.

5.4. Comunicazione di dati a terzi

Secondo l'art. 3 lett. e LPD, la comunicazione di dati a terzi è un'operazione consueta del trattamento di dati per la quale valgono i principi del trattamento di dati descritti nel capitolo A paragrafo 2. Sussiste inoltre un obbligo di registrazione delle collezioni di dati, se regolarmente sono comunicati dei dati personali a terzi (art. 11a cpv. 3 LPD). Nel seguente capitolo D paragrafo 2 sarà descritto più dettagliatamente l'obbligo di registrazione.

Sezione III
Protezione dei dati sul posto di lavoro in banca

6. Ascolto e registrazione di conversazioni telefoniche

6.1. Considerazioni generali

Il controllo dei dati relativi alle comunicazioni telefoniche come pure l'ascolto e la registrazione dei loro contenuti rappresentano un trattamento

[32] Vedi comunicazione del GAFI "New Anti-Money-Laundering Standards Released" del 20 giugno 2003 sull'argomento "Terrorist Financing" e A. ALTHAUS STÄMPFLI, *Personendaten von Bankkunden*, cit., pag. 158.

di dati ai sensi della LPD. Gli aspetti giuridici di queste misure sono trattati nella pubblicazione dell'IFPDT riguardante la sorveglianza telefonica sul posto di lavoro[33]. Questa ultima costituisce parte integrante del presente testo. Le seguenti considerazioni si limitano all'approfondimento dell'aspetto penale dell'ascolto e della registrazione di conversazioni telefoniche nel settore bancario. In questo settore, tali misure rappresentano una realtà in particolare presso i dipartimenti che si occupano di commercio di titoli quotati in borsa e di marketing telefonico.

6.2. Motivo giustificativo e condizioni

Gli scopi dell'ascolto e della registrazione di conversazioni telefoniche nel settore bancario consistono generalmente nella raccolta e conservazione dei mezzi di prova relativi a negozi giuridici o ad informazioni vincolanti, in singoli casi anche nel controllo della prestazione dell'impiegato. Tali scopi rappresentano generalmente un interesse preponderante della banca e pertanto di per sé già un motivo giustificativo ai sensi dell'articolo 13 cpv. 1 LPD. Dal punto di vista del diritto penale, la legalità dell'ascolto e della registrazione di conversazioni telefoniche è condizionata esclusivamente dall'assenso di tutti gli interlocutori (impiegato e cliente). L'assenso degli interlocutori presuppone dal canto suo una loro sufficiente informazione precedente, che secondo lo scopo perseguito dall'ascolto o dalla registrazione, può assumere forme differenti. L'espressione «informazione sufficiente» serve a precisare che non è necessario annunciare espressamente la registrazione se gli interlocutori possono agevolmente rendersi conto in altro modo che la conversazione sarà registrata[34]. Nel caso dell'ascolto o della registrazione sistematica al fine di raccolta e conservazione dei mezzi di prova relativi a negozi giuridici o ad informazioni vincolanti, non è necessario informarne gli interlocutori ad ogni conversazione. Un'informazione precedente nel contratto di lavoro e, per la clientela, nelle condizioni generali del relativo contratto, è sufficiente. Sufficiente è pure la combinazione tra informazione unica all'impiegato tramite contratto di lavoro e informazione sistematica al cliente tramite riproduzione di un nastro magnetico registrato. Immaginabile è altresì la fattispecie dove più clienti partecipano alla conversazione telefonica con l'impiegato di banca

[33] Cfr. Informazioni dell'IFPDT sulla sorveglianza telefonica sul posto di lavoro, http://www.edoeb.admin.ch.

[34] Rapporto della Commissione degli affari giuridici del Consiglio degli Stati del 2 maggio 2001, FF 2001 2328.

e dove gli uni sono informati contrattualmente, gli altri - non ancora legati da un contratto con la banca - oralmente, da parte dell'impiegato.

Per quanto riguarda l'ascolto o la registrazione occasionale al fine di controllo della prestazione dell'impiegato, questo ultimo va informato perlomeno sul periodo approssimativo (p. es. un mese in particolare) e sulla durata della misura (p. es. due settimane). La durata deve inoltre rispondere a criteri di proporzionalità. Gli altri interlocutori vanno informati ogniqualvolta avviene l'ascolto o la registrazione, tramite riproduzione di un nastro magnetico registrato[35].

6.3. Responsabilità penale

Oltre alle conseguenze civili della violazione della LPD contemplate nella pubblicazione dell'IFPDT citata più in alto, le ipotesi di reato previste agli articoli 179bis (ascolto e registrazione da parte della banca in qualità di parte estranea alla conversazione, p. es. in qualità di datore di lavoro) e 179ter (ascolto e registrazione da parte dell'impiegato di banca quale interlocutore) del Codice penale Svizzero sono realizzate qualora una conversazione non pubblica è ascoltata o registrata senza l'assenso di tutti gli interlocutori. Da sottolineare a questo proposito il fatto che gli articoli 179bis e 179ter CP proteggono il contenuto materiale della comunicazione telefonica, non però i dati relativi alla comunicazione telefonica (p. es. orario, durata, numero digitato)[36].

6.4. Depenalizzazione prevista dall'articolo 179^{quinquies} CP

Secondo l'articolo 179^{quinquies} cpv 1, lit. b, CP non è punibile né secondo l'articolo 179bis cpv. 1 CP né secondo l'articolo 179ter cpv. 1 CP chiunque, come interlocutore o abbonato al collegamento utilizzato registra, in ambito di relazioni commerciali, conversazioni telefoniche vertenti su ordinazioni, su mandati, su prenotazioni o su analoghe operazioni preliminari. Col termine di "abbonato al collegamento" si intendono, nel settore bancario, più specificatamente sia la banca in qualità di parte estranea alla conversazione telefonica, sia il suo impiegato quale interlocutore diretto[37]. Al secondo capoverso dell'articolo 179^{quinquies} CP è previsto che all'utilizzazione ulteriore delle registrazioni

[35] 9. Rapporto di attività dell'IFPDT, § 7.4

[36] Cfr. P. von Ins/P.R. Wyder, in *Basler Kommentar* [Niggli/Wiprächtiger Ed.], Strafgesetzbuch II, articolo 179bis CP N 4, e articolo 179ter CP N 4.

[37] Occorre a questo proposito distinguere ancora gli interlocutori e gli abbonati dai terzi; l'articolo 179^{quinquies} non limita, infatti, la protezione penale contro l'ascolto e la registrazione di conversazioni da parte di terzi inseritisi per esempio abusivamente in una linea telefonica.

conformemente al capoverso 1 sono applicabili per analogia gli articoli 179bis cpv. 2 e 3 CP e 179ter cpv. 2 CP. È opportuno precisare che l'articolo 179quinquies CP libera sia dall'obbligo di ottenere l'assenso, sia da quello dell'informazione precedente dell'interlocutore. L'articolo 179quinquies cpv 1, lit. b, CP rappresenta, infatti, una base legale esaustiva, cioè un motivo giustificativo ai sensi dell'articolo 13 cpv. 1 LPD. Pertanto il principio della trasparenza, rispettivamente della riconoscibilità di un trattamento di dati conformemente alla LPD non è applicabile alla fattispecie prevista all'articolo 179quinquies CP[38]. La depenalizzazione dell'ascolto e della registrazione di conversazioni telefoniche senza informazione precedente e senza assenso di tutti gli interlocutori, prevista all'articolo 179quinquies CP, entra in considerazione unicamente in relazione a mandati, ordinazioni e prenotazioni di massa[39].

L'abbandono dell'obbligo d'informare e di ottenere l'assenso è stato motivato dal fatto che in certe situazioni sarebbe troppo laborioso e richiederebbe troppo tempo segnalare sistematicamente la registrazione agli interlocutori. La depenalizzazione prevista dal legislatore si limita dunque a delle situazioni nelle quali un affare particolare si effettua in massa e dove una certa rapidità è necessaria al suo buon funzionamento. A titolo d'esempio si veda l'attività dell'addetto bancario al commercio di titoli, al traffico telefonico di pagamenti o al marketing telefonico.

La consulenza telefonica al cliente in singoli casi non rappresenta per contro un'operazione di massa. Nel caso in cui durante la stessa conversazione telefonica si offrono servizi sia di consulenza che di conclusione di un contratto, la prima potrà essere registrata solo previa informazione e accordo del cliente, la seconda invece potrà invece essere registrata incondizionatamente.

Per contro, se una prenotazione, ordinazione o mandato di massa porta alla negoziazione e conclusione di un contratto, allora è possibile nonché ragionevolmente esigibile e proporzionato che colui che intende registrare la conversazione ne informi il suo interlocutore[40]. Ciò vale anche nel caso in cui un rapporto contrattuale esiste già tra i due interlocutori. Si rammenta a questo proposito che, trattandosi di un caso d'applicazione dell'articolo 179quinquies CP, l'accordo dell'interlocutore non è necessario.

Il principio della finalità deve essere rigorosamente rispettato. Le registrazioni possono dunque essere utilizzate esclusivamente allo scopo probatorio. Lo sfruttamento di registrazioni effettuate secondo l'articolo 179quinquies cpv 1, lit. b CP, cioè senza l'informazione precedente e senza l'assenso di tutti gli interlocutori, per altri scopi e la loro comunicazione a terzi possono ingaggiare responsabilità sia civili che penali (articolo 179quinquies cpv. 2 CP).

Va infine sottolineato che la nuova normativa contemplata nell'articolo 179quinquies CP segue il principio secondo cui tutti i partecipanti a una conversazione telefonica, siano essi impiegati di banca, interlocutori (clienti) o la banca stessa rispettivamente un suo mandante, possono effettuare registrazioni alle medesime condizioni.

[38] Cfr. analisi dell'articolo 179quinquies CP, http://www.edoeb.admin.ch.
[39] Rapporto della Commissione degli affari giuridici del Consiglio degli Stati, vedi nota 35.
[40] 11. Rapporto d'attività dell'IFPDT, § 8.1.

7. Videosorveglianza

7.1. Considerazioni generali

La videosorveglianza rappresenta un trattamento di dati ai sensi della LPD. Essa è oggetto di diverse pubblicazioni dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), tra le quali le "Informazioni sulla videosorveglianza sul posto di lavoro[41]" e la "Videosorveglianza da parte di persone private"[42]. Queste pubblicazioni approfondiscono la videosorveglianza dal punto di vista della protezione dei dati e costituiscono parte integrante del presente testo. Le seguenti considerazioni intendono approfondire la videosorveglianza nel settore bancario, in particolare dal punto di vista del diritto penale. Nel settore bancario la videosorveglianza si ritrova in particolare presso ingressi, atri, sportelli, camere blindate, nonché, all'esterno dell'edificio, presso i bancomat. La videosorveglianza rappresenta inoltre una realtà in relazione ad attività legate al trasporto o alla manipolazione di valori.

Il presente approfondimento non entra in merito all'impiego della videosorveglianza al fine di controllo della prestazione dell'impiegato. Questa misura non è tipica nel settore bancario.

7.2. Motivo giustificativo e condizioni generali della videosorveglianza

Analogamente a quanto esposto nel capitolo riguardante l'ascolto e la registrazione di conversazioni telefoniche, anche per la videosorveglianza prevale come scopo primario la raccolta e la conservazione di potenziali mezzi di prova relativi a fatti con eventuali ripercussioni sulla responsabilità giuridica delle persone interessate.

[41] http://www.edoeb.admin.ch.
[42] http://www.edoeb.admin.ch.

Generalmente, alla raccolta, conservazione e analisi di videoregistrazioni soggiace dunque un interesse preponderate di sicurezza come motivo giustificativo ai sensi dell'articolo 13 cpv. 1 LPD. Classici esempi di videosorveglianza giustificata da interesse preponderante di sicurezza sono quelle riguardanti la camera blindata o il bancomat. In altri casi, la ponderazione degli interessi in gioco è meno chiara.

La banca rimane inoltre tenuta a garantire alle persone interessate una sufficiente informazione precedente, anche quale deterrente contro eventuali abusi delle videoregistrazioni. La LPD parla a questo proposito di riconoscibilità del trattamento di dati, oppure, analogamente, di principio della buona fede (articolo 4 cpv. 2 e 4 LPD). Da notare a questo proposito che in caso di omissione d'informazione degli impiegati, la scoperta degli autori di un reato tramite un sistema di sorveglianza può comportare per il datore di lavoro la mancata acquisizione dei relativi mezzi di prova in tribunale, potendo la raccolta di dati essere considerata come illecita.

L'informazione precedente può assumere forme differenti, secondo il titolare del diritto alla protezione della personalità, che può essere, nel settore bancario, l'impiegato, il cliente oppure un terzo. Nel caso dell'impiegato, il contratto di lavoro o un suo annesso rappresentano il supporto d'informazione più corrente, anche se une breve informazione scritta, recapitata all'interessato per esempio tramite e-mail, può altresì rappresentare una forma d'informazione precedente sufficiente. Nel caso della sorveglianza della clientela e/o di terzi per contro, lo strumento più efficace e appropriato dell'informazione è rappresentato dal cartello apposto in modo ben visibile nel locale o spazio soggetto a videosorveglianza.

Il coinvolgimento delle rappresentanze del personale nel processo decisionale riguardante l'installazione di un sistema di videosorveglianza è altresì auspicabile, ma non obbligatorio.

7.3. Motivi giustificativi e condizioni per la raccolta e la conservazione

7.3.1. Videoregistrazioni concernenti clienti e terzi. – Si veda a questo proposito le considerazioni contenute nel § 7.2.

7.3.2. Videoregistrazioni concernenti gli impiegati. - Nel caso della sorveglianza degli impiegati di banca a scopo di sicurezza, va riservato espressamente l'articolo 26 dell'ordinanza 3 concernente la Legge federale sul lavoro (OLL 3) [43].

[43] Legge federale sul lavoro, LL.

Con questa disposizione il legislatore svizzero ha voluto inserire nel diritto pubblico del lavoro la protezione della personalità del lavoratore. Non è pertanto possibile derogare a questa disposizione sulla base di accordi di diritto privato, ad esempio mediante una convenzione tra datore di lavoro e impiegato[44]. Secondo questa disposizione, non è ammesso l'uso di sistemi di sorveglianza e di controllo del comportamento dei lavoratori sul posto di lavoro.

I sistemi di sorveglianza e di controllo, se sono necessari per altre ragioni, devono essere concepiti e disposti in modo da non pregiudicare la salute e la libertà di movimento dei lavoratori. Pertanto, la videocamera preposta alla sorveglianza di un atrio di banca, in particolare quello i cui sportelli non sono separati dalla clientela tramite una barriera fisica (ad esempio tramite una vetrata), deve essere posizionata in modo da evitare la sorveglianza sistematica dell'impiegato.

In altre parole, l'impiegato deve essere nella misura del possibile inquadrato solamente eccezionalmente dalle telecamere. Solo così facendo si limitano al minimo i danni alla personalità del lavoratore e si rispetta, oltre alla proibizione della sorveglianza sistematica del comportamento secondo l'articolo 26 OLL 3, anche il principio della proporzionalità dell'articolo 4 cpv. 2 LPD. La *ratio legis* di questa disposizione consiste nella protezione della salute dell'impiegato, la quale potrebbe essere danneggiata in seguito alla pressione che può crearsi dopo un'esposizione prolungata alla videosorveglianza. Nel caso in cui evitare la videosorveglianza sistematica dell'impiegato, quale effetto collaterale di una sorveglianza della clientela, non dovesse essere possibile per ragioni tecniche o organizzative, solo il criptaggio delle immagini degli impiegati nonché una gestione restrittiva delle chiavi di decriptaggio (*Double Key Decryption System*) potrebbero ridurre la pressione dovuta alla sorveglianza prolungata sul posto di lavoro, rendendo così la videosorveglianza sistematica dell'impiegato conforme alla protezione dei dati e della salute[45].

7.4. Motivi giustificativi e condizioni per l'analisi

Sia per le videoregistrazioni concernenti clienti e terzi che quelle riguardanti gli impiegati, valgono le considerazioni al § 7.2.

[44] Indicazioni del Segretariato di Stato, Seco, relative all'art. 26 OLL 3. Cfr. http://www.seco.admin.ch.

[45] Si veda a questo proposito il capitolo 1.7.1 del 15esimo rapporto d'attività dell'IFPDT, dove si è cambiata la prassi in materia di proibizione del controllo sistematico del comportamento sul posto di lavoro grazie soprattutto ai *Privacy Filters*.

7.5. Responsabilità penale

Alla stessa stregua di quanto esposto nel capitolo riguardante l'ascolto e la registrazione di conversazioni telefoniche, anche la videosorveglianza è oggetto di esame dal punto di vista della responsabilità penale. Va premesso che se l'infrazione contemplata all'articolo 179quater CP è commessa nella gestione degli affari di una persona giuridica, per esempio di una banca, la disposizione penale si applica alle persone fisiche che l'hanno commessa.

7.5.1. Responsabilità penale della sorveglianza dei clienti e di terzi. - Secondo la prima frase dell'articolo 179quater CP riguardante la violazione della sfera segreta o privata mediante apparecchi di presa d'immagini, è punibile chiunque, con un apparecchio da presa, osserva o fissa su un supporto d'immagini un fatto rientrante nella sfera segreta oppure un fatto, non osservabile senz'altro da ognuno, rientrante nella sfera privata d'una persona, senza l'assenso di questa ultima. Per quanto riguarda la definizione di sfera segreta o privata, la dottrina e la giurisprudenza forniscono diversi esempi: Intendesi con questo termine per esempio conflitti all'interno della famiglia, comportamenti sessuali o malattie. La protezione dell'articolo 179quater CP viene per contro a cadere allorquando le attività citate si svolgono, rispettivamente sono visibili, in pubblico[46]. Malgrado questi chiari esempi, la separazione tra sfera privata protetta e non protetta solleva questioni complesse. Senza voler entrare nel dettaglio, sia sottolineato a questo proposito che secondo il Tribunale federale, la violazione della sfera privata non è data soltanto nel caso di superamento di una barriera fisica, per esempio allorquando si sorveglia una persona all'interno della propria abitazione tramite videosorveglianza attraverso la finestra, ma anche nel caso di superamento di una barriera giuridico-morale (videosorveglianza di una persona di fronte alla propria abitazione)[47].

Queste considerazioni di dottrina e giurisprudenza non lasciano dubbi sul fatto che l'articolo 179quater CP non si applica alla videosorveglianza di clienti nel settore bancario.

Non del tutto esclusa rimane comunque la possibilità teorica della videosorveglianza al bancomat con raggio d'azione aldilà delle barriere fisiche e/o giuridico-morali previste dal Tribunale federale. In simili casi, l'applicabilità dell'articolo 179quater CP per violazione della sfera privata o segreta di terzi sarebbe ipotizzabile. Una simile violazione del principio della finalità (articolo 4 cpv. 3 LPD) può comportare anche conseguenze sul piano civile.

[46] *Basler Kommentar, cit.*, articolo 179quater CP N 7 e 9, con referenze alla giurisprudenza.
[47] DTF 118 IV 50.

7.5.2. Responsabilità penale in caso di videosorveglianza degli impiegati. - Per quanto riguarda la videosorveglianza degli impiegati con apparecchi ottici, essa non rientra nella fattispecie prevista all'articolo 179quater CP[48]. La videosorveglianza degli impiegati rimane però perseguibile sul piano penale conformemente all'articolo 59 cpv. 1 lit. *a* della legge federale sul lavoro.

8. Accesso e analisi di supporti di dati in caso di sospetto d'infrazione al Codice penale

8.1. Considerazioni generali

Nell'ambito di una procedura penale, la banca in qualità di denunciante si trova in una posizione differente, secondo l'esistenza o meno di un reato dimostrato dai relativi mezzi di prova. Nel caso di esistenza di un reato provato, la banca può denunciare la persona in questione presso le autorità competenti nonché decretare eventuali misure disciplinari o di diritto del lavoro.

Per contro, in presenza unicamente di un sospetto di reato contro una determinata persona o cerchio di persone, la banca in qualità di parte lesa è confrontata alla decisione circa l'opportunità di avviare una procedura penale e di conseguenza al quesito relativo alle sue competenze nell'acquisizione delle prove.

Si tratta in particolare di esaminare se e in quale misura la banca è autorizzata a procedere all'acquisizione, alla conservazione e all'analisi delle prove senza l'intervento delle autorità preposte alle indagini, al fine di verificare se il sospetto è fondato, rispettivamente comprovato, ed eventualmente di avviare una procedura penale in miglior conoscenza di causa. In altre parole trattasi della competenza in materia di acquisizione e analisi di prove.

La questione è di rilevanza pratica, considerato il rischio di non assunzione, da parte dell'autorità giudiziaria competente, di prove raccolte e analizzate in modo illecito, in particolare contrariamente ai principi e alle condizioni della protezione dei dati. A titolo di esempio di reato nel settore bancario sia menzionato il sospetto di violazione del segreto bancario. Classici supporti di prove possono essere i documenti cartacei, la posta elettronica, l'home drive, i CD-Rom, le penne USB, i tabulati con dati riguardanti il traffico telefonico, ecc.

[48] *Basler Kommentar, cit.*, articolo 179quater CP N 10.

L'IFPDT ha trattato della questione nelle sue pubblicazioni[49]. Queste ultime formano parte integrante della presente analisi.

Fatta eccezione per le considerazioni riguardanti il diritto penale, la presente analisi vale ovviamente anche per la raccolta, la conservazione e l'analisi di supporti di dati in caso di sospetto di violazione del diritto privato (p. es. di direttive interne alla ditta) e/o disciplinare.

8.2. Motivo giustificativo e condizioni

L'obbligo del datore di lavoro di proteggere e rispettare la personalità dell'impiegato contemplato agli articoli 328 e ss. del Codice delle obbligazioni (CO) impedisce alla banca la raccolta, l'accesso e l'analisi incondizionati dei supporti di dati privati dell'impiegato. In primo luogo, la LPD condiziona il trattamento di dati all'esistenza di un motivo giustificativo secondo l'articolo 13 LPD. Si impone a questo punto una distinzione fra le condizioni della raccolta di mezzi di prova e quelle riguardanti l'accesso e l'analisi degli stessi.

8.2.1. Motivi giustificativi e condizioni della raccolta di supporti di dati. - Per quanto riguarda la raccolta di mezzi di prova, le basi legali previste dal CO, in particolare gli articoli riguardanti l'obbligo di tenere e conservare i libri di commercio (artt. 957 ss. CO), nonché le disposizioni sulla responsabilità penale dell'impresa, rispettivamente della possibilità di discolparsene tramite relativi mezzi di prova (art. 102 CP), sono sufficienti per giustificarla. Fatta eccezione per l'obbligo di tenere e conservare i libri di commercio, i quali possono essere conservati sist ematicamente da parte della banca, negli altri casi rimane riservato il principio della proporzionalità, che limita la raccolta a dati strettamente pertinenti con gli scopi perseguiti dalla rispettiva base legale.

Pertanto la banca sarà per esempio autorizzata a raccogliere possibili mezzi di prova ai fini dell'art. 102 CP unicamente se in presenza di un sospetto concreto di carente organizzazione interna.

8.2.2. Motivi giustificativi e condizioni dell'accesso e analisi di supporti di dati. - Entrano in considerazione come motivi giustificativi in particolare un interesse preponderante privato o pubblico della banca. Il consenso della persona sospettata all'accesso e all'analisi dei suoi supporti di dati privati è pure ipotizzabile, rappresenta però un motivo giustificativo poco realistico nel contesto specifico.

Quale interesse preponderante v'è soprattutto l'esigenza di appurare e sanzionare la sospetta infrazione penale. Possibili indizi concreti d'infrazione possono essere rappresentati da elementi soggettivi e/o oggettivi della fattispecie in questione, come ad esempio informazioni apparse sulla stampa riguardanti fatti soggetti al segreto bancario. Gli elementi costitutivi d'infrazione devono essere associabili ad una o più persone identificate o identificabili.

Inoltre, l'accesso e l'analisi dei mezzi di prova da parte della banca presuppone l'esistenza di un sospetto concreto d'infrazione. Vaghe sensazioni, impressioni o supposizioni soggettive così come la semplice mancanza di fiducia nei confronti di una o più persone non costituiscono un sospetto concreto.

La buona fede rappresenta pure una condizione fondamentale per la legittimità dell'accesso e dell'analisi di supporti di dati. Questo principio ha come conseguenza in particolare che la banca non può accedere e analizzare supporti di dati privati in conoscenza della loro irrilevanza per lo scopo perseguito.

Le condizioni dell'esistenza di un motivo giustificativo nonché degli elementi concreti di sospetto devono essere adempiute cumulativamente.

Il fatto che l'accesso e l'analisi di supporti di dati privati possa, nel singolo caso, avvenire anche nell'interesse della persona toccata dalla misura (interesse allo scagionamento dal sospetto), non esonera la banca dall'obbligo di adempiere le condizioni succitate.

Per quanto riguarda l'accordo della persona interessata quale condizione all'accesso e all'analisi dei suoi dati personali da parte della banca, esistono tre scenari possibili:

1. La persona interessata, di norma l'impiegato, è previamente informata di essere sospettata di un'infrazione nonché dell'intenzione di accesso ai suoi supporti privati di dati da parte della banca e dà il suo assenso. Con l'assenso la banca evita, in linea di massima, un eventuale ulteriore biasimo per violazione della personalità da parte della persona interessata. Per evitare abusi da parte della banca, si auspica il rispetto del principio dei quattro occhi.
2. L'impiegato non dà il suo assenso. In una simile ipotesi, la responsabilità dell'accesso e dell'analisi è affidata alle autorità competenti in materia d'inchiesta penale. Queste ultime sono tenute a garantire, oltre alla neutralità, anche l'integrità e la confidenzialità dei dati grazie all'ausilio di specialisti del settore, chiamati in gergo tecnico *forensic computing scientists*.

[49] a) Spiegazioni dell'IFPDT concernenti il diritto del datore di lavoro di accedere ai supporti di dati privati di un impiegato in caso di sospetto di reato, cfr. http://www.edoeb.admin.ch.
b) Guida relativa alla sorveglianza dell'utilizzazione di Internet e della posta elettronica sul posto di lavoro, cf. http://www.edoeb.admin.ch.

3. La banca accede ai supporti di dati privati e li analizza senza informazione precedente e assenso della persona interessata e senza far intervenire le autorità competenti. Questo modo di procedere, il più corrente tra i tre stilati in questo capitolo, comporta il rischio dell'esame dell'adempimento delle condizioni d'accesso e di analisi dei supporti di dati da parte del giudice, nel caso in cui ciò fosse esplicitamente richiesto dalla persona interessata o in caso di sospetto, da parte del giudice stesso, di raccolta illecita di mezzi di prova.

Riassumendo, l'accesso e l'analisi dei supporti privati di dati da parte della banca presuppone o l'assenso della persona interessata, o l'intervento delle autorità competenti. Il mancato rispetto di queste regole può ingaggiare la responsabilità della banca per violazione illecita della personalità, se le rispettive condizioni non sono rispettate.

9. Filtraggio dei conti bancari degli impiegati

9.1. Considerazioni generali

Spesso i dipendenti sono obbligati ad aprire e gestire i loro conti bancari privati presso l'istituto bancario per il quale lavorano. Diventando così cliente, la situazione giuridica dell'impiegato di banca si complica. L'implementazione delle misure organizzative adeguate da parte della banca secondo il § 9.6. può risolvere in modo pratico i problemi giuridici.

9.2. Motivo giustificativo e condizioni

Gli interessi fatti valere dalla banca per giustificare questa misura risiedono principalmente nella possibilità di sorvegliare in modo sistematico, tramite filtraggio dei conti bancari con speciali programmi informatici, le transazioni private dell'impiegato e di conseguenza di controllare il rispetto, rispettivamente di sanzionare la violazione, di norme riguardanti ad esempio la proibizione del riciclaggio di denaro sporco (LRD), del commercio interno di azioni o dell'appropriazione indebita (articolo 138 CP).

In singoli casi la banca può fare valere anche altri interessi, come ad esempio quello di una migliore conoscenza dei propri prodotti da parte dell'impiegato attraverso il loro uso sistematico in qualità di cliente.

L'esame dell'esistenza di un interesse preponderante della banca quale

motivo giustificativo (articolo 13 LPD) presuppone un bilanciamento degli interessi in conflitto.

La misura deve inoltre essere proporzionata ed evitare la violazione di altre norme di protezione dei dati e del diritto del lavoro.

In particolare, la banca è tenuta ad informare precedentemente i dipendenti in particolare sull'implementazione della misura, sui suoi scopi e sulla durata di conservazione dei dati nonché a garantire il diritto d'accesso.

9.3. Difficoltà nel bilanciamento degli interessi in conflitto

Gli interessi in conflitto sono, per la banca, in particolare il rispetto delle norme di diritto pubblico citate al § 9.1 e, per l'impiegato, il rispetto della propria personalità, e in particolare della sfera privata, sul posto di lavoro.

Se il bilanciamento degli interessi può tendere a prima vista a favorire gli interessi pubblici della banca, non va sottovalutato il fatto che i dati raccolti tramite filtraggio sistematico dei conti dei collaboratori possono rappresentare, in singoli casi, dei dati sensibili o un profilo della personalità ai sensi dell'articolo 3 lett. *c* e lett. *d* LPD.

Le transazioni bancarie possono, infatti, rivelare, in casi specifici, aspetti della personalità quali la salute, la sfera intima, l'appartenenza politica o religiosa oppure, più segnatamente, il comportamento penalmente reprensibile dell'impiegato. Il bilanciamento degli interessi in conflitto risulta dunque di non facile soluzione.

9.4. Implicazioni del diritto del lavoro

La questione giuridica della liceità del filtraggio dei conti privati degli impiegati di banca si complica oltremodo se si considera che il diritto del lavoro proibisce al datore di lavoro sia di trattare dati non rilevanti per la conclusione o l'esecuzione del contratto di lavoro (articolo 328*b* CO), sia di controllare in modo sistematico il comportamento dell'impiegato (articolo 26 OLL 3).

9.5. Proporzionalità

Il filtraggio dei conti bancari degli impiegati risulta problematico anche dal punto di vista della proporzionalità (articolo 4 cpv. 2 LPD). Infatti, l'attitudine e, di conseguenza, la necessità del filtraggio dei conti possono essere compromesse dalla facilità di raggirare le norme di diritto pubblico in questione. L'impiegato di banca può ad esempio adempiere la fattispecie dell'appropria-

zione indebita tramite conto bancario intestato a terzi. Per di più, questo ultimo può essere gestito presso un altro istituto bancario.

9.6. Soluzione organizzativa

La conformità della sorveglianza sistematica dei conti bancari degli impiegati con la protezione dei dati e con il diritto del lavoro può essere ottenuta implementando misure organizzative adeguate. In particolare, il filtraggio sistematico dei conti privati deve essere affidato esclusivamente a strumenti informatici, e non a persone. Oltre a questa misura, la protezione della personalità degli impiegati di banca durante il filtraggio deve essere rafforzata pseudonimizzando i loro nominativi.

La rispettiva lista di corrispondenza o di reidentificazione, contenente i nominativi relativi ad ogni pseudonimo, va protetta adeguatamente, confidandone la sua custodia a una persona di fiducia all'interno della banca, per esempio al responsabile della protezione dei dati o al rappresentante del personale. Il suo uso da parte della persona preposta all'identificazione di persone, va poi permesso esclusivamente nel caso concreto di segnalazione, da parte del programma informatico, di possibili attività sospette sul conto bancario di uno o più impiegati. I ruoli di conservazione della lista di corrispondenza e di identificazione di persone vanno affidati a persone differenti. Per il resto valgono le considerazioni contenute nel § 8.2.

Sezione IV
Obblighi delle banche quali istituti che trattano dei dati e competenze dell'incaricato federale della protezione dei dati e della trasparenza

10. Obbligo d'informazione delle banche secondo l'art. 8 LPD

Il diritto d'accesso è uno degli strumenti più importanti per far valere i diritti sulla personalità di una persona interessata, perché questo le offre la possibilità di sapere in che modo la sua personalità sia stata violata a causa di un trattamento di dati. Per questo motivo, le aziende sono obbligate a comunicare, ad ogni persona che chiede l'informazione (art. 8 cpv. 1 LPD), tutti i dati che la concernono presenti nella collezione di dati, ivi compreso le informazioni disponibili sulla provenienza dei dati (art. 8 cpv. 2 lett. a LPD).

Inoltre il detentore della collezione di dati deve comunicare lo scopo e se del caso i fondamenti giuridici del trattamento, le categorie dei dati personali trattati, come pure dei partecipanti alla collezione e dei destinatari dei dati (art. 8 cpv. 2 lett. b LPD). La grande importanza che il legislatore attribuisce al richiedente d'informazione è resa evidente anche nella norma penale, secondo la quale chi contravviene agli obblighi previsti dagli articoli 7 e 8–10 LPD fornendo intenzionalmente informazioni inesatte o incomplete, è punito, a querela di parte, con una multa (art. 34 cpv. 1 lett. a LPD). L'informazione è di regola gratuita e scritta, sotto forma di stampato o di fotocopia (art. 8 cpv. 5 LPD). Soltanto se la comunicazione delle informazioni richieste causa un lavoro considerevole oppure le informazioni richieste sono già state comunicate al richiedente nei dodici mesi prima dell'inoltro della domanda, a meno che questi provi un interesse degno di protezione, è possibile stabilire una partecipazione ai costi di al massimo 300 CHF (art. 2 cpv. 1 dell'Ordinanza relativa alla legge federale sulla protezione dei dati, OLPD). Se la persona che ha l'obbligo d'informazione intende applicare una tassa, deve informare il richiedente dell'importo e dargli un termine di dieci giorni per ritirare la sua richiesta (art. 2 cpv. 2 OLPD).

Il detentore di una collezione di dati deve quindi organizzare le sue collezioni di dati in modo tale da poter dare alla persona interessata un'informazione completa entro un termine accettabile (di regola entro trenta giorni; art. 1 cpv. 4 OLPD) sui dati registrati relativi alla persona che inoltra la richiesta. Agli autori non è noto in che misura le richieste d'informazione allo scopo di documentarsi siano utilizzate, in ambito bancario, dalle persone interessate. Secondo l'opinione degli autori però bisogna aspettarsi che in futuro particolarmente i clienti bancari (ma anche dipendenti e terzi) ricorreranno più frequentemente allo strumento della richiesta d'informazione, per ricevere dei giustificativi ed estratti conto, che non sono più in loro possesso.

Prima della concessione di una richiesta d'informazione, il detentore della collezione di dati deve prendere delle misure adeguate al fine di assicurare l'identificazione della persona interessata e proteggere i dati della persona interessata dall'accesso di terzi non autorizzati in occasione della comunicazione delle informazioni[50] (art. 1 cpv. 2 OLPD). Siccome i dati bancari soggiacciono inoltre anche al segreto bancario, al momento della verifica dell'identità del richiedente d'informazioni la banca deve prestare particolare attenzione. Oltre alla verifica dell'identità di clienti che richiedono informazioni (ad es. attraverso una copia del documento di legittimazione), bisogna almeno verificare

[50] http://www.edoeb.admin.ch, Guida per il trattamento di dati personali nel settore privato.

l'indirizzo (sulla base dell'indirizzo registrato nel sistema) come pure la firma (sulla base del cartoncino firme depositato in banca), prima di dare qualsiasi informazione. Comunque, la richiesta di una copia di una carta d'identità o di un passaporto, autenticata da un notaio, di regola è una misura sproporzionata. Per i collaboratori conosciuti personalmente dalla banca valgono delle premesse meno severe.

11. La registrazione di collezioni di dati

L'elenco delle collezioni di dati tenuto dall'IFPDT intende facilitare, alle persone interessate, l'esercizio del loro diritto d'accesso secondo l'art. 8 LPD. In questo elenco possono vedere se e dove sono trattati i dati che eventualmente potrebbero riguardarli[51]. Le persone private devono notificare le collezioni se trattano regolarmente dati personali degni di particolare protezione o profili della personalità; o se comunicano regolarmente dati personali a terzi (art. 11 cpv. 3 LPD). Siccome i dati dei clienti sono protetti di principio dal segreto bancario (art. 47 LBCR), una comunicazione regolare di dati personali avviene piuttosto raramente. Ciononostante, sotto il motto del concetto Allfinanz, potrebbe esistere una comunicazione regolare d'indirizzi a una società affiliata, che ad esempio vende dei prodotti assicurativi. In tale caso la banca, di principio, è obbligata ad annunciare la sua collezione di dati.

Più spesso invece succede, all'interno di una banca, che questa allestisca un profilo della personalità nell'ambito della relazione d'affari, alfine di migliorare la consulenza nell'ambito "Private Banking", e che registri dei dati personali degni di particolare protezione. Anche in tal caso la banca, di principio, è obbligata a registrare le sue collezioni di dati. Sono comunque esonerati da quest'obbligo d'informazione i detentori di collezioni di dati, se i dati sono trattati da una persona privata in virtù di un obbligo legale (art. 11a cpv. 5 lett. a LPD). In particolare nell'ambito della lotta contro il finanziamento del terrorismo e del riciclaggio di denaro, le banche hanno un obbligo legale di conoscere sufficientemente il cliente bancario. Questo permette alle banche di allestire specialmente per questo scopo dei profili della personalità sulla base della LRD. Qualora però questi profili siano utilizzati anche per scopi di marketing o per migliorare la consulenza, l'eccezione non è più data. Un'ulteriore possibilità di essere esonerati dalla registrazione di una collezione di dati, è la designazione di un responsabile della protezione dei dati, il quale vigila in modo indipendente

[51] D. Rosenthal/Y. Jöhri, *Commento relativo alla LPD*, D. Rosenthal, art. 11a LPD, n. 1.

sul rispetto interno delle prescrizioni relative alla protezione di dati e che tiene un elenco delle collezioni di dati. Un'altra possibilità per aggirare l'obbligo di comunicazione, è l'acquisto di un marchio di qualità della protezione dei dati sulla base di una procedura di certificazione secondo l'art. 11 LPD, se il risultato della valutazione è stato comunicato all'Incaricato.

12. Azioni legali secondo l'art 15 LPD

Per far valere i propri diritti di protezione della personalità nei confronti della persona che tratta i dati, la LPD prevede la via dell'azione legale sulla base del diritto privato (art. 15 LPD)[52]. Le azioni legali e le misure cautelari relative alla protezione della personalità si orientano agli articoli 28 fino a 28l del Codice Civile svizzero. L'attore può in particolare chiedere che il trattamento dei dati, segnatamente la loro comunicazione a terzi, sia bloccato oppure che i dati personali siano rettificati o distrutti (art. 15 cpv. 1 LPD). È certamente possibile che una persona interessata notifichi un trattamento di dati illegale all'IFPDT, ma non esiste un diritto rivendicabile legalmente all'intervento da parte dell'IFPDT. Nell'allestimento della LPD, il legislatore ha deciso volutamente che le persone interessate rivendichino attivamente i loro diritti secondo l'art. 15 LPD. Questo però ha come conseguenza che, a causa del rischio di costo e di processo, solo poche persone scelgano la via della procedura civile[53]. I dipendenti tuttavia, sulla base del diritto del lavoro (art. 343k CO) hanno facilitazioni per l'avvio di una procedura legale. Un dipendente interessato può quindi rivolgersi al giudice del suo comune di domicilio o a quello della sede della banca e far valere i suoi diritti con una procedura semplice, rapida e gratuita.

13. Funzione di consulenza e di vigilanza dell'IFPDT

Nell'allestimento della LPD, il legislatore ha scelto un approccio cooperativo. Così ha inserito nella legge un mandato di consulenza dell'IFPDT (art. 28 LPD), e gli ha dato semplicemente la competenza di rilasciare delle raccomandazioni (art. 29 LPD). In questo modo, l'IFPDT è interessato a cercare di raggiungere una soluzione amichevole con il rispettivo detentore della col-

[52] Fatta riserva per particolari regole cantonali per Banche cantonali.

[53] D.Rosenthal/Y. Jöhri, *Commento relativo alla LPD*, D. Rosentha, art. 15 LPD, n. 2.

lezione di dati, prima di pronunciare una raccomandazione che poi verrebbe fatta valere al Tribunale amministrativo federale. Questo processo, dalla raccomandazione fino ad una decisione del Tribunale amministrativo federale, dura di regola almeno un anno.

Nell'ambito della sua funzione di consulenza, l'IFPDT consiglia i privati in materia di protezione di dati (art. 28 LPD). Nel singolo caso la consulenza avviene su richiesta e può essere utilizzata da ogni privato. Per quanto riguarda la forma della consulenza accordata, l'IFPDT è però completamente libero e non esiste un diritto rivendicabile legalmente alla consulenza. Gli argomenti di consulenza comprendono tutte le richieste che possono sorgere in relazione alla LPD e altre norme legali sulla protezione dei dati.

Nell'ambito della sua attività di vigilanza, l'IFPDT può accertare i fatti di sua iniziativa o su richiesta di terzi quando metodi di trattamento possono ledere la personalità di un numero considerevole di persone (ad es. errore di sistema), devono essere registrate collezioni di dati oppure vi è obbligo d'informare secondo l'art. 6 cpv. 3 LPD (art. 29 cpv. 1 LPD). Per adempiere il suo obbligo di vigilanza, l'IFPDT può esigere la produzione di atti, domandare informazioni e farsi presentare trattamenti di dati. È applicabile per analogia l'art. 16 della Legge federale sulla procedura amministrativa concernente il diritto di rifiutare la testimonianza (art. 29 cpv. 2 LPD).

Non gli spettano delle competenze istruttorie, tuttavia una persona privata può essere punita se intenzionalmente fornisce all'incaricato, in occasione dell'accertamento dei fatti (art. 29 LPD), informazioni inesatte o rifiuta di collaborare (art. 34 cpv. 2 LPD). Qualora l'IFPDT, dopo aver accertato i fatti, dovesse constatare che il trattamento di dati non corrisponde alle esigenze legali, può raccomandare di modificare o di cessare il trattamento (art. 29 cpv. 3 LPD). A questo scopo inoltra una raccomandazione a chi tratta i dati. Se una raccomandazione è respinta o non le è dato seguito, questi può deferire la pratica al Tribunale amministrativo federale per decisione (art. 29 cpv. 4 LPD).

In casi urgenti, se le persone interessate rischiano di subire un pregiudizio non facilmente riparabile, l'IFPDT può chiedere provvedimenti cautelari al presidente della corte del Tribunale amministrativo federale competente in materia di protezione dei dati (art. 33 cpv. 2 LPD).

Nei casi d'interesse generale, l'IFPDT può informare il pubblico riguardo ai suoi accertamenti e alle sue raccomandazioni (art. 30 cpv. 2 LPD). In particolare le banche dovrebbero aver sempre presente il diritto d'informazione dell'IFPDT, poiché la pubblicazione di violazioni di dati nei mass media può avere come conseguenza una perdita d'immagine non irrilevante.