Pubblicazione Trimestrale

ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Aprile/Giugno

2018

rivista.dirittobancario.it

Rivista di Diritto Bancario | dottrina e giurisprudenza commentata

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

La Rivista di Diritto Bancario seleziona i contributi oggetto di pubblicazione sulla base delle norme seguenti.

I contributi proposti alla Rivista per la pubblicazione vengono assegnati dal sistema informatico a due valutatori, sorteggiati all'interno di un elenco di ordinari, associati e ricercatori in materie giuridiche, estratti da una lista periodicamente soggetta a rinnovamento.

I contributi sono anonimizzati prima dell'invio ai valutatori. Le schede di valutazione sono inviate agli autori previa anonimizzazione.

Qualora uno o entrambi i valutatori esprimano un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche aggiunte e correzioni, la direzione esecutiva verifica che l'autore abbia apportato le modifiche richieste.

Qualora entrambi i valutatori esprimano parere negativo alla pubblicazione, il contributo viene rifiutato. Qualora solo uno dei valutatori esprima parere negativo alla pubblicazione, il contributo è sottoposto al Comitato Esecutivo, il quale assume la decisione finale in ordine alla pubblicazione previo parere di un componente della Direzione scelto ratione materiae.

2018 | 2019

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

SEDE DELLA REDAZIONE

Università degli Studi di Trento, Facoltà di Giurisprudenza, via Verdi 53,
(38122) Trento – tel. 0461 283836

2018 | 2019

GIOACCHINO LA ROCCA

Trattamento dei dati personali e impresa bancaria (Reg. UE 679/2016)

1. *Dati personali e attività bancaria/finanziaria*

Teorici del marketing e sociologi del consumo sono concordi ([1]): la natura delle nostre spese, le esigenze alla cui soddisfazione sono destinati i nostri risparmi disvelano, non solo i nostri rapporti economici, le nostre relazioni, ma anche la nostra personalità, le nostre aspirazioni, il nostro modo di essere. In altre parole, l'analisi dei flussi di pagamento – inevitabilmente raccolti dall'intermediario che svolge il relativo servizio - consente di ricostruire pulsioni, personalità, modo di essere, identità personale, ricerca di identità esibite o dissimulate di un individuo.

Non v'è ovviamente solo il servizio dei pagamenti. Si pensi ad esempio alla recente disciplina della *product governance*: tale disciplina costituisce applicazione del principio generale, secondo il quale gli intermediari finanziari debbono agire sul mercato con l'intento di realizzare al meglio gli interessi dei clienti (v. *considerando* n. 71, Dir. 2014/65). In questa prospettiva, le imprese di investimento che realizzano un determinato strumento finanziario (i c.d. *producers*), debbono mettere a disposizione delle imprese che offrono sul mercato lo strumento (*distributors*), tutte le informazioni necessarie per identificare il mercato di riferimento e la tipologia di clientela, presso i quali lo strumento medesimo può essere distribuito ([2]). Come si vede,

---

* Il lavoro è dedicato al Prof. Roberto Pardolesi.

[1]) V. ad es. KOTHLER, *Marketing management. Analisi, pianificazione e controllo*, quinta edizione italiana interamente rinnovata. Versione italiana a cura di W. G. Scott, Torino, 1991; SASSATELLI, *Consumo, cultura e società*, Bologna, 2004.

[2]) L'art. 16, par. 3, comma 2 e 3 della direttiva stabiliscono: «*Le imprese di investimento che realizzano strumenti finanziari da offrire in vendita alla clientela adottano, esercitano e controllano un processo di approvazione per ogni strumento finanziario e per ogni modifica significativa agli strumenti finanziari esistenti, prima della loro commercializzazione o distribuzione alla clientela. Il processo di approvazione del prodotto precisa per ciascuno strumento finanziario il determinato mercato di riferimento di clienti finali all'interno della pertinente categoria di clienti e garantisce che tutti i rischi specificamente attinenti a tale target siano stati analizzati e che la prevista strategia di distribuzione sia coerente con il target stesso*».

questo istituto, non diversamente sul piano funzionale rispetto alla c.d. «*suitability rule*», mira a far sì che ai clienti appartenenti ad un determinata «categoria» siano «offerti o raccomandati» «prodotti» pertinenti al «target».

È evidente come la *product governance* postuli che, al momento del collocamento, l'impresa di investimento abbia inserito ciascun cliente in una data categoria contraddistinta da un determinato livello di propensione al rischio, con la conseguenza che essa, al pari della "*suitability rule*", richiede necessariamente una profilazione del cliente finalizzata alla prestazione dei servizi di investimento e, dunque, finalizzata alla conclusione ed esecuzione di quei contratti nei quali consiste lo svolgimento di tali servizi.

Altro esempio di profilazione – richiesta, quest'ultima, dalla tecnica bancaria, prima ancora che dalle norme di settore - è quella necessaria per la valutazione del merito di credito, che si esprime soprattutto nella c.d. «istruttoria di fido». Essa è volta a valutare la capacità dell'*accipiens* di restituire le somme in ipotesi ricevute dalla banca. Tale capacità dipende dai flussi di cassa prospettici derivanti dallo svolgimento della sua attività sul mercato in condizioni di concorrenza ([3]). Questa capacità di rimborso, che rappresenta l'elemento di maggiore incertezza, è indagata dalla banca durante la c.d. «istruttoria di fido»: con tale istruttoria la banca mira in sostanza «*a definire la dimensione dei redditi prospettici attesi* [dal soggetto finanziato] *ed il campo di variabilità degli stessi*» ([4]). A tal fine la banca deve necessariamente valutare – come è possibile desumere dall'art. 137 TUB che punisce il reato di «mendacio bancario» - la «*situazione economica, patrimoniale o finanziaria*» del soggetto finanziato. La fonte più importante di informazioni utili a questo fine è proprio il potenziale prenditore dei fondi, come è confermato sempre dall'art. 137 TUB che sanziona "*chi, al fine di ottenere concessioni di credito per sé o per le aziende che amministra, … fornisce dolosamente ad una banca*

[3]) Tutto prende le mosse dall'intuizione di MODIGLIANI, MILLER, *The Cost of Capital, Corporate Finance, and the Theory of Investment*, in «*American Economic Review*», 48 (1958), pp. 261-297, e dagli studi che si sono innestati su questo: v. anche per riferimenti FILOSA, MAROTTA, *Stabilità finanziaria e crisi*, Bologna, 2011, 179 ss.; MALINCONICO, *Il credit risk management del portafoglio prestiti. Da Basilea 1 a Basilea 3*, Milano, 2012, 135.

[4]) MALINCONICO, *op. cit.*, 136.

notizie o dati falsi". Peraltro, il primo comma dell'art. 124-*bis* TUB, a proposito del credito al consumo, avverte che la banca non attinge informazioni solo dall'interessato: «*prima della conclusione del contratto di credito, il finanziatore valuta il merito creditizio del consumatore sulla base di informazioni adeguate, se del caso fornite dal consumatore stesso e, ove necessario, ottenute consultando una banca dati pertinente*». Indicazioni non dissimili si traggono dall'art. 120-*undecies* TUB ([5]), secondo il quale «*prima della conclusione del contratto di credito, il finanziatore svolge una valutazione approfondita del merito creditizio del consumatore, tenendo conto dei fattori pertinenti per verificare le prospettive di adempimento da parte del consumatore degli obblighi stabiliti dal contratto di credito. La valutazione del merito creditizio è effettuata sulla base delle informazioni sulla situazione economica e finanziaria del consumatore necessarie, sufficienti e proporzionate e opportunamente verificate*».

Altro tassello significativo del quadro normativo volto a sottolineare la quantità ed importanza dei dati personali acquisiti nel corso del normale svolgimento dell'attività bancaria finanziaria, è costituito dal par. 6 dell'art. 16 dir. 2014/65, secondo il quale «*le imprese di investimento tengono, per tutti i servizi prestati e tutte le attività e le operazioni effettuate, registrazioni sufficienti atte a consentire all'autorità competente di espletare i propri compiti di vigilanza e … in particolare di verificare che le imprese di investimento abbiano adempiuto tutti gli obblighi, compresi quelli nei confronti dei clienti o potenziali clienti e quelli relativi all'integrità del mercato*». Qui non è ovviamente il caso di soffermarsi sull'importanza sistematica della disposizione per quanto riguarda lo svolgimento dei servizi di investimento sia nei confronti dei clienti già acquisiti, sia nei confronti dei c.d. «prospect» (i non ancora clienti): qui è possibile solo evidenziare come l'estensione della raccolta di dati anche ai «non clienti» è giustificata sul piano del diritto positivodalla parola

[5]) La disposizione, al pari di tutte quelle contenute nel Capo I-bis del Titolo VI del TUB, si applicano al «*contratto di credito con cui un finanziatore concede o si impegna a concedere a un consumatore un credito sotto forma di dilazione di pagamento, di prestito o di altra facilitazione finanziaria, quando il credito è garantito da un'ipoteca sul diritto di proprietà o su altro diritto reale avente a oggetto beni immobili residenziali*» (artt. 120-*quinquies* e 120-*sexies* TUB).

o è finalizzato all'acquisto o alla conservazione del diritto di proprietà su

«*attività*», la quale deve intendersi come insieme di azioni svolte dall'impresa di investimento verso un investitore e dunque comprende anche l'insieme delle relazioni stabilite con una persona che non sia ancora cliente, ossia con la quale sono stati intrattenuti contatti e trattative che non sono esitate nella conclusione di un contratto relativo alla prestazione di servizi di investimento. Orbene, anche tali azioni devono essere oggetto di «registrazione». Qui merita altresì ricordare che per «registrazione» deve intendersi qualsiasi evidenza documentale, risultante da un supporto cartaceo o di altro tipo (v. art. 16, par. 7, comma 1 e 7), che attesti il contenuto del contatto, o del rapporto, o della operazione, intercorsi tra l'impresa di investimento e l'interessato: come si vede, ancora una volta una gran messe di dati personali sono raccolti e detenuti dall'impresa bancaria finanziaria ([6]).

2. *Trattamento dati e attività di impresa nel RGPD*

Se, dunque, le disposizioni passate in rassegna nel precedente paragrafo evidenziano quanto l'attività bancaria/finanziaria presupponga la raccolta e il trattamento di dati personali di persone fisiche, occorre aggiungere immediatamente che il Reg. 679/2016 non si oppone al trattamento dei dati personali nell'ambito dell'esercizio dell'impresa.

[6]) Il quadro normativo delineato nel testo, relativo all'inerenza del trattamento di dati nello svolgimento dell'impresa bancaria/finanziaria, può essere arricchito con l'art. 52-*bis* TUB, secondo il quale «*le banche e le relative capogruppo adottano procedure specifiche per la segnalazione al proprio interno da parte del personale di atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività bancaria. Le procedure di cui al comma 1 sono idonee a: a) garantire la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione; …*»: questa disposizione è qui rilevante perché impone espressamente alla banca di « *garantire la riservatezza dei dati personali*» delle persone fisiche interessate alla vicenda del *whistleblowing*. Da tenere presente anche l'art. 4, n. 14, Reg. 679, che riporta la definizione dei «*dati biometrici*», i quali sono trattati dalle banche per la sottoscrizione dei contratti con la clientela o comunque per il loro riconoscimento: «*dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*».

Come si è già notato in altra occasione, il RGPD focalizza il suo epicentro normativo nel diritto di ciascun individuo, non già alla privatezza della sua vita, quanto piuttosto ad un trattamento dei propri dati «*lecito, corretto e trasparente*»: ciò si desume dell'art. 5, par. 1, lett. a, ed ancor più esplicitamente dal *considerando* n. 1, che richiama espressamente l'art. 8, Carta dei diritti fondamentali UE e l'art. 16 TFUE, mentre il «diritto all'oblio», che corrisponde in definitiva ad un divieto di trattamento, è subordinato alla sussistenza di uno dei motivi elencati nell'art. 19, par. 1, Reg. n. 679 e all'insussistenza di una delle situazioni elencate nel par. 3 dell'art. 17.

Il sistema costruito dal RGPD si delinea nei *considerando* n. 4 e 9. Il primo enuncia espressamente che «*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, … e va contemperato con altri diritti fondamentali*», i quali ultimi sono riportati nello stesso *considerando* e fra di essi vi è il «*diritto di impresa*». Per parte sua il *considerando* n. 9 segnala come preoccupazione del legislatore europeo sia anche quella di disciplinare l'interferenza della protezione dei dati e della sua disciplina con la concorrenza, anzi il *considerando* n. 9 dichiara espressamente che il RGPD trova la sua ragion d'essere anche nella necessità di evitare che il trattamento dei dati personali e la sua disciplina si risolvano in un «*freno all'esercizio delle attività economiche*» all'interno dei Paesi dell'Unione.

In altre parole, nel RGPD echeggia una consapevolezza diffusa, vale a dire che «*i dati … sono diventati il fulcro della produzione. È la definizione stessa di quanto realizzabile dall'impresa ad essere modellata sulla base delle informazioni disponibili sui potenziali acquirenti o beneficiari*» onde ottenere così un vantaggio competitivo spesso irrinunciabile sulla concorrenza ([7]).

[7]) V. per tutti MANTELERO, *il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, in FINOCCHIARO (dir.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 287 ss., 294 s.

È di questi giorni (maggio 2018) l'intervista al CEO e fondatore di «DoveConviene» pubblicata sulle pagine internet di «Economia & Finanza» di Repubblica (http://www.repubblica.it/economia/rapporti/osserva-italia/trend/2018/05/11/news/il

_digitale_spinge_i_fatturati_del_negozio_fisico-196086026/). «DoveConviene» – come si legge sul sito internet https://corporate.doveconviene.it/ - «*è il brand italiano di "ShopFully International Group", la piattaforma che guida oltre 30*

Tutto ciò non significa che l'impresa possa essere svolta trattando dati personali senza difficoltà. La soluzione del problema posto dalla duplice natura ormai rivestita dall'informazione, che è al tempo stesso - quasi un tassello di un mosaico - rappresentazione di un'espressione della persona umana ed entità dotata di valore economico, è individuata dal legislatore europeo in una prospettiva non lontana da taluni assiomi di fondo della responsabilità civile: qualsiasi attività umana – ed in particolare l'attività imprenditoriale – crea rischi per classi potenzialmente indeterminate di terzi. Il legislatore valuta se il potenziale costo sociale di tali attività sia superato dai potenziali benefici ricavabili sul piano sociale grazie allo svolgimento dell'attività economica e, nell'ipotesi in cui non riscontri tale superamento, vieta lo svolgimento dell'attività ([8]); in altri casi può scoraggiare il compimento dell'attività ponendo a carico di colui che la pone in essere, l'obbligo di risarcire tutti i danni da questa determinati (art. 2050 c.c.); può anche darsi un sistema particolarmente articolato, il quale per un verso – e secondo una regola che può dirsi generale – mira a far sì che l'imprenditore si accolli il costo del rischio da lui stesso creato anche attraverso misure dirette a ridurre i rischi medesimi ([9]), ponendo a

milioni di utenti nel mondo allo shopping nei negozi vicino casa, fornendo tutte le informazioni per un'esperienza smart: promozioni, novità di prodotto, negozi, orari e contatti geolocalizzati in un unico luogo e facilmente accessibili». In tale intervista si individua tra l'altro lo strumento essenziale per coordinare il canale di vendita digitale con quello su internet: «*attraverso la profilazione dell'utente, che ci permette di consigliargli i prodotti che gli interessano maggiormente, proponiamo messaggi ad hoc e geolocalizzati, che si traducono in visite nel negozio. Offriamo la possibilità di sviluppare campagne orientate a generare traffico in negozio e misurarne l'impatto reale sugli ingressi nei punti vendita*»: sono evidenti i molteplici – e potenzialmente invasivi e massivi – trattamenti di dati richiesti dall'esposto piano di marketing.

[8]) V. ad es. art. 112, d.lgs. 206/05: «*il produttore che immette sul mercato prodotti pericolosi … è punito con la pena dell'arresto …*».

[9]) La logica può intravedersi nel fatto che «*le scelte del "che cosa" e del "come" produrre vengono compiute per lo più in base a criteri economici … tali scelte, compiute nell'ambito di singole imprese, hanno anche un valore sociale ove il conto dell'attivo e del passivo dell'impresa rispecchi rispettivamente il valore prodotto e il valore distrutto da essa. Ora è chiaro che del valore distrutto dall'impresa fanno parte non solo le energie lavorative, il materiale impiegato e il logorio delle macchine, ma anche i danni che l'esercizio dell'impresa causa regolarmente a terzi. Perciò occorre concludere che, ove il sistema giuridico non attribuisca all'imprenditore il costo del rischio che egli crea, può accadere che imprese marginali … siano attivi dal punto di vista del singolo imprenditore, laddove dal*

carico dell'imprenditore medesimo i danni che a lui siano «imputabili», salva la prova che «*l'evento dannoso non gli è in alcun modo imputabile*» ([10]).

Tra i rischi determinati dallo svolgimento dell'attività di impresa vi sono quelli che trovano fondamento nel trattamento dei dati personali ad opera dell'impresa medesima. Come già si è accennato, la valutazione costi/benefici sopra indicata è stata effettuata dal legislatore europeo, il quale in linea di massima ha ritenuto socialmente utile lo svolgimento dell'impresa attraverso il trattamento dei dati personali «*a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato*» (lett. *f*, art. 6). Questo rilievo deve essere meglio precisato nel senso che la comparazione costi/benefici connessi all'attività imprenditoriale deve essere condotta caso per caso, tenendo conto delle caratteristiche della concreta attività imprenditoriale e della sua incidenza sulle persone interessate dal trattamento dei dati, ivi comprese le caratteristiche del trattamento stesso, con i bilanciamenti e «contemperamenti» in ipotesi ritenuti necessari, di cui v'è cenno esplicito - cenno peraltro essenziale sul piano sistematico – nel *considerando* n. 4 e nell'art. 6, lett. *f*.

Sul piano generale è necessario sottolineare che nel sistema del RGPD l'analisi costi/benefici sull'opportunità di avviare una data attività imprenditoriale trattando dati personali è rimessa allo stesso imprenditore: sul punto è univoco il *considerando* n. 74 il quale delinea

---

punto di vista sociale siano passivi, distruggendo un valore maggiore di quello che producono, e si mantengano in vita solo in quanto una parte del loro passivo sociale, cioè il costo del rischio da esse introdotto nella società, sia pagato dal pubblico» (TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, 34 s.). Ovviamente, le assonanze con la teoria della responsabilità civile non possono essere estese indiscriminatamente: nell'ambito governato dal RGPD non si tratta di scegliere «i criteri mediante i quali un determinato costo sociale viene lasciato in capo alla vittima o traslato dalla vittima in capo ad altri soggetti» (MONATERI, *La responsabilità civile*, Torino, 1998, 13). Piuttosto nel sistema delineato dal RGPD è necessario individuare e limitare «*i rischi per i diritti e le libertà delle persone fisiche»* determinati dallo specifico trattamento dei dati posto in essere per esercitare una data attività imprenditoriale.

[10]) Così l'art. 82, Reg. 679/2016, che delinea peraltro un sistema particolarmente articolato e meritevole di un autonomo approfondimento. Sull'ambiguità di fondo di tale sistema v. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, in FINOCCHIARO (dir.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 615 ss.

una precisa responsabilità dell'impresa in relazione ai trattamenti svolti nel suo interesse ([11]). Le disposizioni del Regolamento danno seguito a questo principio: l'art. 24, nel delineare la responsabilità del titolare del trattamento, presuppone che quest'ultimo abbia consapevolezza dei «*rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*» in concreto connessi con il trattamento onde adottare «*misure tecniche ed organizzative per garantire … che il trattamento è effettuato conformemente al … regolamento*» e dunque innanzi tutto sia «sicuro» ([12]). La conclusione è rafforzata dall'art. 32: questa disposizione nel suo complesso evidenzia l'articolazione e la complessità dell'analisi costi/benefici, cui è ordinariamente chiamato l'imprenditore intenzionato a servirsi di dati personali. Per parte sua l'art. 35 richiede una specifica analisi, la c.d. valutazione di impatto, in presenza di un «*rischio elevato per i diritti e le libertà delle persone fisiche*» determinato «*in particolare*» dall'«*uso di nuove tecnologie*», «*considerati la natura, l'oggetto, il contesto, la finalità*» del trattamento stesso.

L'impresa bancaria/finanziaria si muove tuttavia su coordinate per certi versi peculiari. Su tale peculiarità ci si è già soffermati in apertura, quando si è evidenziato come nell'attività bancaria/finanziaria il trattamento dei dati personali non costituisce una componente teoricamente rinunciabile anche a costo di impoverire in modo sensibile la redditività dell'impresa. Nell'attività bancaria/finanziaria, infatti, il trattamento dei dati personali si delinea quale condizione imprescindibile per l'esercizio dell'impresa stessa. In proposito mette

[11]) «*E' opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche*».

[12]) Il *considerando* n. 76 offre un quadro sufficientemente analitico della valutazione in ordine ai rischi «*la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*»

conto ribadire ancora una volta che senza informazioni sul cliente non si può effettuare la valutazione di *suitability* dei prodotti finanziari al quale i prodotti medesimi vengono raccomandati o venduti ([13]). E più in generale senza conoscere il profilo del cliente non si può perseguire al meglio l'interesse dello stesso nell'allocazione del suo risparmio, secondo l'imperativo imposto agli intermediari dalle norme apicali di settore, che ha ricevuto recente applicazione con la *product governance*. Come pure senza informazioni sulle persone fisiche non può valutarsi il loro merito di credito.

Non solo: l'impresa bancaria finanziaria consiste nell'esercizio del credito e nella raccolta del risparmio, vale a dire attività essenziali per la salvaguardia e per il corretto funzionamento del sistema economico tanto da essere rilevanti anche sul piano costituzionale. Ne segue che a proposito di essa deve ritenersi assolutamente ultronea l'analisi costi/benefici preventiva che invece – come si è accennato – è in qualche modo necessaria per le altre tipologie di imprese: l'impresa bancaria finanziaria infatti rappresenta una tipologia di impresa della quale, pur con i suoi irrinunciabili trattamenti di dati, il sistema economico non può fare a meno! Questo, tuttavia, come si dirà, non esclude che l'impresa bancaria non debba procedere ad altro tipo di valutazioni.

3. *«Diritti e libertà delle parsone fisiche» vs. «tutela del risparmio»?*

Le specificità esibite dall'impresa bancaria/finanziaria con riguardo al trattamento dei dati non sono circoscritte ai rilievi sopra posti in evidenza. Infatti, i trattamenti di dati che si sono riconosciuti come tipicamente necessitati per l'esercizio dell'impresa bancaria/finanziaria sono evidentemente finalizzati alla profilazione della clientela e degli aspiranti clienti. Questa circostanza assume particolare rilevanza alla stregua dell'art. 35 RGPD, il quale è importante per almeno due motivi: in primo luogo la disposizione contribuisce a precisare una nozione

[13]) Se ne trae recente conferma dalle *Guidelines on certain aspects of the Mifid II suitability requirements* rilasciate dall'ESMA, l'ente di vigilanza sul mercato finanziario europeo, nelle quali si prende atto che gli intermediari utilizzano sistemi automatici o semiautomatici (c.d. robo-advice) per formulare raccomandazioni di investimento o per assumere decisioni di investimento sulla base di profilazioni della clientela realizzate attraverso la raccolta di informazioni.

centrale nel sistema delineato dal RGPD, vale dire la nozione di «*rischio elevato per i diritti e le libertà delle persone fisiche*»; altro aspetto emergente dall'art. 35 cit.(e dai *considerando* che si diranno) – collegato con il precedente e al pari di questo munito di valenza sistematica – è costituito dalla c.d. «valutazione di impatto», la quale – come si accennerà – per un verso non è altro che un particolare esempio di quelle valutazioni sull'opportunità e sui rischi connessi al trattamento dei dati cui l'impresa (e più in generale il titolare del trattamento) è chiamata dal RGPD.

I due aspetti, come si è accennato, sono collegati, nel senso che la nozione di «*rischio elevato per i diritti e le libertà delle persone fisiche*» si precisa meglio in funzione della «valutazione di impatto».

Il «*rischio elevato per i diritti e le libertà delle persone fisiche*» – si desume dal *considerando* n. 75 – può derivare da trattamenti in grado di «*comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo*».

In questa sede non è possibile un approfondimento ulteriore, diretto a comprendere meglio le possibili implicazioni del «*danno fisico, materiale o immateriale*», cui fa riferimento il *considerando*. Per quanto qui più specificamente interessa, occorre prendere atto che i trattamenti di dati necessari per l'espletamento dell'attività bancaria/finanziaria possono determinare i danni sopra descritti. A conferma di questa affermazione sta il paragrafo 3 dell'art. 35, dove la «valutazione di impatto» di cui al par. 1, è richiesta «*in particolare*» ([14]) «*nei casi seguenti: a)una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo*

[14]) Non può non essere colta l'importanza ermeneutica della locuzione «*in particolare*» presente nel paragrafo 3. Essa in primo luogo concorre con l'espressione «di cui al par. 1» a configurare i rischi connessi ai trattamenti elencati nel par. 3 quali espressioni del «*rischio elevato per i diritti e le libertà delle persone fisiche*»; in secondo luogo rende palese che i rischi determinati dai trattamenti elencati nel par. 3 sono solo degli esempi «particolari» di «*rischio elevato per i diritti e le libertà delle persone fisiche*» e non ne esauriscono le possibili tipologie

significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico».

Ciò premesso, deve immediatamente rilevarsi che larghissima parte dei trattamenti di dati effettuati dagli intermediari finanziari rientrano nella lett. a) del riportato paragrafo 3, come d'altra parte è confermato anche dalle recenti *Guidelines* dell'ESMA accennate nella nota 13; in secondo luogo, con riguardo alla lett. b) dell'art. 35, è possibile osservare che attraverso il flusso dei pagamenti – riscontrabile grazie al relativo servizio normalmente esercitato dalle banche anche in esecuzione di un banale contratto di conto corrente - si possono comprendere le convinzioni, la personalità ed il modo di essere delle persone, ossia «*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale*» (art. 9), come pure spesso accade che gli intermediari per motivi di sicurezza trattino «*dati biometrici intesi a identificare in modo univoco una persona fisica*»)(v. ancora art. 9) o che – sempre per motivi di sicurezza – essi pongano in essere quella «*sorveglianza sistematica su larga scala di una zona accessibile al pubblico*» accennata dalla lett. c) dell'art. 35.

Di qui due conclusioni: i trattamenti di dati effettuati nell'ambito dell'attività bancaria/finanziaria sono potenzialmente suscettibili di determinare «*rischi elevati per i diritti e le libertà delle persone fisiche*», con l'ulteriore conseguenza sul piano operativo che, in assenza di un provvedimento di esclusione ad opera dell'autorità di controllo ex art. 35 par. 5, gli intermediari debbono procedere alla «valutazione di impatto», la quale materialmente consiste in un documento avente «almeno» la struttura indicata nel par. 7, art. 35 in esame, ossia essa «*contiene …: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali (*) e dimostrare la*

conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione».

Si è già accennato che la valutazione ex art. 35 Reg. 679 è solo un particolare esempio delle valutazioni richieste al titolare del trattamento, tanto che la dottrina si è interrogata sia sui rapporti tra tale valutazione e quelle previste dagli artt. 24 e 25, sia sui concreti contenuti della valutazione stessa quali sono richiesti dal riportato paragrafo dell'art. 35 ([15]). Nell'ambito della presente riflessione, dedicata ad un primo esame dell'incidenza del Reg. n. 679/2016 sulla *governance* dell'impresa bancaria, può essere maggiormente utile soffermarsi su questo secondo aspetto prendendo le mosse da un esempio concreto. Il cui esame consentirà anche la messa a fuoco di alcune considerazioni di carattere generale. Si può pertanto ipotizzare che l'impresa di investimento o comunque l'intermediario progetti la produzione o la distribuzione di un particolare prodotto finanziario. In questo caso l'intermediario, in applicazione dell'art. 35 RGPD, dovrebbe interrogarsi sulle conseguenti profilazioni della clientela e così procedere alla c.d. «valutazione di impatto». Questa dovrebbe prendere le mosse dai dati e dalla tecnologia che si intendono concretamente utilizzare nella produzione e nella distribuzione del prodotto finanziario. Tutto dovrebbe essere espressamente indicato nel documento destinato a rappresentare la «valutazione di impatto»: in primo luogo dovrebbero indicarsi la «*finalità del trattamento*», che nella specie coincide con «*l'interesse legittimo perseguito dal titolare*»: nella nostra ipotesi si dovrebbe dichiarare che la finalità del trattamento è costituita dalla produzione e/o distribuzione di un nuovo prodotto finanziario, del quale è possibile suppore che, al momento del collocamento, richieda una particolare profilazione della clientela. Tali indicazioni devono essere quanto più complete e dovrebbero mirare in particolare ad illustrare la complessità del prodotto o comunque sottolinearne le caratteristiche che giustificano il trattamento dei dati in concreto posto in essere.

Si apre a questo punto una questione di centrale importanza: nell'ambito delle valutazioni rimesse all'imprenditore dall'art. 35, come pure dagli artt. 24 ss. Reg. n. 679, assume un rilievo cruciale il tema del bilanciamento tra l'interesse del titolare del trattamento e

[15]) Per un primo riferimento in materia v. MANTELERO, *op. cit.*, 307 ss.

l'interesse dell'«interessato» (v. ad es. artt. 5, 17, 18, 21 Reg. 679). In particolare, si richiede espressamente che le misure tecniche ed organizzative assunte dal titolare per trattare i dati siano adeguate alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, pretendendo anche l'adozione di politiche relative alla protezione dei dati se ciò è «proporzionato» rispetto alle attività di trattamento (art. 24). Non va poi tralasciato che, se le valutazioni effettuate dal titolare evidenziassero che il rischio determinato dai trattamenti è particolarmente elevato in assoluto o rispetto all'«interesse legittimo» del titolare, quest'ultimo dovrebbe rinunciare al trattamento in forza della ritenuta prevalenza dei «diritti e delle libertà delle persone fisiche».

Orbene, nel caso dell'impresa bancaria finanziaria la comparazione dei contrapposti interessi del titolare e degli interessati (clienti e potenziali clienti) potrebbe essere meno lineare di quella sopra ipotizzata. In particolare, dovrebbe porsi attenzione alla articolazione che potrebbe assumere in questo caso il quadro dei «diritti e delle libertà delle persone fisiche». Infatti, potrebbe sostenersi con qualche fondatezza che la profilazione effettuata dall'imprenditore bancario/finanziario è diretta a realizzare la migliore allocazione del risparmio delle persone fisiche clienti o potenziali clienti e conseguentemente è volta a dare concretezza non solo all'interesse imprenditoriale dell'intermediario alla raccolta del risparmio presso il pubblico, ma anche all'interesse del cliente e dell'aspirante cliente alla migliore allocazione del risparmio stesso. In altre parole, ci si trova di fronte ad una profilazione, ossia ad un trattamento anche particolarmente incisivo di dati personali, che a ben vedere è volto a salvaguardare valori costituzionalmente protetti ed in particolare a tutelare il risparmio, sulla cui prossimità alla realizzazione delle esigenze di vita del risparmiatore e dunque alla realizzazione effettiva della sua personalità già ci si è a suo tempo soffermati ([16]). È evidente come in questa prospettiva, che comunque costituisce un modello teorico che deve trovare riscontro nella concretezza delle singole fattispecie, risulta meno agevole intravedere una contrapposizione tra «legittimo interesse» del titolare e «diritti e libertà» del cliente o

[16]) V. LA ROCCA, *Autonomia privata e mercato dei capitali. La nozione civilistica di "strumento finaziario"*[2], Torino, 2009, 140 ss.

potenziale cliente, in quanto in questi casi è possibile sostenere (almeno sul piano teorico: come anticipato, il modello deve trovare riscontro nelle singole vicende concrete) che il trattamento, anche quando particolarmente sofisticato ed incisivo, è posto in essere per evitare che la persona fisica subisca «perdite finanziarie» in tutto analoghe a quelle annoverate dai *considerando* n. 75 e 85 tra i possibili danni conseguenti al trattamento dei dati.

Considerazioni non dissimili valgono per le profilazioni preliminari alla concessione del credito: a ben vedere queste profilazioni sono preordinate all'esercizio dell'attività bancaria secondo criteri improntati alla «sana e prudente gestione» della banca elevata dal TUB a paradigma dell'attività bancaria e tale da configurare un principio di ordine pubblico economico, a proposito del quale qui è sufficiente dire che un esercizio dell'attività bancaria non coerente con tale principio porrebbe a carico della banca e del sistema un tale insieme di rischi che comprometterebbe non solo e non tanto l'efficienza del sistema economico, ma la sua stessa permanenza in vita. Qui interessa sottolineare che il trattamento di dati effettuato prima di un'operazione creditizia, o in sede di monitoraggio della stessa nella fase di esecuzione del contratto di credito, certamente consiste nella «*valutazione di aspetti personali ... mediante l'analisi o la previsione di aspetti personali riguardanti ... la situazione economica ... l'affidabilità o il comportamento*» (*considerando* n. 75, Reg. 679/2016) dell'accreditando o dell'accreditato. Analogamente a quanto accade nei servizi di investimento, tale trattamento, peraltro, è volto alla salvaguardia di un interesse che trascende sia quello del titolare, sia quello del cliente o potenziale cliente, in quanto – come si è accennato – è volto a salvaguardare il principio di ordine pubblico economico prima accennato, che in definitiva nella fattispecie si declina nella necessità che la banca assuma le necessarie misure e cautele onde accertarsi che l'eventuale prenditore di fondi sia in grado di sostenere il debito conseguente al finanziamento e non si determini una situazione analoga a quella avveratasi nel caso dei mutui *subprime* (caratterizzata dal finanziamento di massa di soggetti non bancabili e successiva dispersione del rischio in prodotti finanziari distribuiti nel mondo) ([17]),

[17]) A proposito di queste prassi v. il *considerando* n. 3 della direttiva 2014/17/UE, che è stata recepita nel diritto interno negli artt. 120-*quinquies* ss. TUB: «l*a crisi*

il cui richiamo sembra sufficiente a chiarire l'importanza dei profili qui considerati.

Tutto ciò ovviamente non implica affatto che l'intermediario finanziario sia esonerato dalla «*adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default*» ([18]). Le «misure» predette costituiscono, infatti, strumenti volti a contenere il rischio imprenditoriale e si iscrivono in quel processo di internalizzazione (in questo caso delle esternalità negative generate dal trattamento dei dati personali) di rischi e costi dell'attività di impresa cui sopra si è accennato.

4. *Il trattamento dei dati ed i rischi di impresa*

L'inquadramento del rischio connesso al trattamento dei dati tra i rischi di impresa deve essere meglio precisato nel senso che esso costituisce un «rischio operativo». Con riferimento all'attività bancaria la nozione di rischio operativo può essere ricavata da Basilea 4 («*il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di*

---

finanziaria ha dimostrato che un comportamento irresponsabile da parte degli operatori del mercato può mettere a rischio le basi del sistema finanziario, portando ad una mancanza di fiducia tra tutte le parti coinvolte, in particolare i consumatori, e a conseguenze potenzialmente gravi sul piano socioeconomico».

[18]) Sono le parole del *considerando* n. 78, Reg. 679, il quale così prosegue «*tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati*» (e v. anche *considerando* n. 83). L'art. 25 traduce questi principi in precetti precisi.

procedure, risorse umane e sistemi interni, oppure da eventi esogeni») e dalle Disposizioni di Vigilanza della Banca d'Italia cap. 3, all. A, dove si legge che «*l'assunzione di rischi operativi risulta implicita nella decisione di intraprendere un determinato tipo di attività e, più in generale, nello svolgimento dell'attività d'impresa*». Mette conto sottolineare che classificare il rischio connesso al trattamento dei dati tra i rischi operativi è assolutamente coerente con quanto si è sopra rilevato a proposito della strumentalità del trattamento dei dati all'attività di impresa.

Conferme in questo senso possono trarsi anche dalle Disposizioni di vigilanza della Banca d'Italia. In particolare, la conferma della connessione tra trattamento delle informazioni (cioè dei «dati») ad opera della banca, rischio operativo e sistema informativo, si rinviene nella «premessa» del Titolo IV della Parte prima, dedicato alla *governance* bancaria e alla gestione dei rischi, che dedica il Capitolo 4 al sistema informativo: in proposito, si legge che il sistema informativo deve assicurare «*con riguardo al contenimento del rischio operativo, il regolare svolgimento dei processi interni e dei servizi forniti alla clientela, l'integrità, la riservatezza e la disponibilità delle informazioni trattate,* [i quali] *fanno affidamento sulla funzionalità dei processi e dei controlli automatizzati*».

In altre parole i processi ed i controlli automatizzati, che la banca deve normalmente utilizzare per il regolare svolgimento della sua attività, devono garantire – come si legge espressamente nelle istruzioni di vigilanza – la sicurezza dei dati con un'evidente convergenza con le esigenze proclamate dal RGPD. Di questa ovvia interazione tra trattamenti di quantità massive di dati, rischio informatico e rischio operativo vi è ulteriore traccia nello «*Schema della relazione sul governo societario e sulla struttura organizzativa*» (v. *Disposizioni di vigilanza* Parte Prima, Titolo I, Capitolo I, Allegato A), dove è espressamente previsto che quanti richiedano l'autorizzazione all'attività bancaria – dunque prima ancora di avviare l'attività imprenditoriale – abbiano consapevolezza e descrivano alla Banca d'Italia «*le caratteristiche del sistema informativo in relazione alle proprie esigenze operative e al fabbisogno informativo degli organi aziendali per assumere decisioni consapevoli e coerenti con gli obiettivi aziendali e definire il sistema di gestione della sicurezza informatica*». In questo ambito le Disposizioni di vigilanza richiedono

che sia decritto «*il processo di analisi del rischio informatico e la sua interazione con il rischio operativo*» e ci si soffermi sul «*sistema di gestione della sicurezza informatica, con particolare riferimento: alla policy di sicurezza informatica; alle misure adottate per assicurare la sicurezza dei dati e il controllo degli accessi, incluse quelle dedicate alla sicurezza dei servizi telematici per la clientela; alla gestione dei cambiamenti e degli incidenti di sicurezza; alla disponibilità delle informazioni e dei servizi ICT*».

Non è difficile avere conferma della stretta connessione sopra rilevata: le «*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*», ossia un trattamento, oltre che lecito, trasparente e corretto, soprattutto «*sicuro*» (artt. 5 ss. Reg. 679), non potranno che quanto meno corrispondere «*alle misure adottate per assicurare la sicurezza dei dati e il controllo degli accessi, incluse quelle dedicate alla sicurezza dei servizi telematici per la clientela; alla gestione dei cambiamenti e degli incidenti di sicurezza*» richieste dalla Banca d'Italia, con una evidente interazione tra le due normative. In particolare, la convergenza tra le due normative può apprezzarsi attraverso quanto si legge nelle Disposizioni di vigilanza, parte I, tit. IV, Cap. 4, sez. IV, premessa: «*la gestione della sicurezza informatica comprende i processi e le misure volti, in raccordo con la generale azione aziendale per preservare la sicurezza delle informazioni e dei beni aziendali, a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e accountability, appropriata e coerente lungo l'intero ciclo di vita. Obiettivo di tale processo è anche di contribuire alla conformità del sistema informativo alle norme di legge e a regolamenti interni ed esterni. La struttura dei processi e l'intensità dei presidi da porre in atto dipendono dalle risultanze del processo di analisi dei rischi*»: ognuno vede che sono parole che non sfigurerebbero a margine del Reg. n. 679.

5. *Trattamento dei dati personali, Responsabile protezione dati (DPO) e governance dell'impresa bancaria*

L'art. 37, reg. n. 679/2016 prevede che debba essere nominato il Responsabile Protezione Dati quando «*b) le attività principali del*

titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 …». Su queste premesse non possono esservi dubbi che la banca o l'impresa di investimento debbano nominare il Responsabile Protezione Dati: nei paragrafi precedenti si è avuto modo di prendere atto come la banca non possa prescindere dal «*monitoraggio regolare e sistematico*» della clientela e dei potenziali clienti, senza considerare che il trattamento dei dati biometrici (ad es. per le firme dei clienti) può riguardare tutta la clientela della banca.

Si pone a questo punto il problema della collocazione da assegnare al DPO nell'ambito della struttura e della *governance* della banca.

Sotto il primo profilo deve prendersi atto che, alla stregua dell'art. 37 cit. ([19]), il rapporto tra il DPO e la banca può essere disciplinato o da un contratto di lavoro subordinato, oppure da un contratto d'opera professionale. Questo però non significa che, nel caso in cui il rapporto tra banca e DPO sia disciplinato da un contratto di lavoro subordinato, possano effettivamente configurarsi profili di subordinazione gerarchica del DPO nell'ambito della struttura aziendale. Al riguardo deve essere attentamente considerato il par. 3 dell'art. 39, RGPD, secondo il quale «*il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*».

Il primo periodo del riportato par. 3 sembra escludere una subordinazione funzionale del DPO rispetto a qualsiasi altra struttura aziendale, mentre l'ultimo periodo del par. 3 sembra escludere una

[19]) V. par. 6: «*Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi*».

subordinazione gerarchica, dal momento che inserisce il DPO nel primo livello aziendale, ossia tra quanti «*riferiscono al vertice gerarchico*» dell'impresa senza alcun tipo di intermediazione da parte di altre strutture aziendali. In questo senso la disposizione contribuisce a chiarire il *considerando* n. 97, Reg. 679, secondo il quale «*... il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento ...*», escludendo qualsiasi dubbio su come debba essere intesa la relazione di «assistenza» che il DPO è chiamato a svolgere a favore del «titolare del trattamento».

In ogni caso, sia che il DPO sia inquadrato quale lavoratore subordinato, sia che il suo rapporto sia disciplinato da un contratto d'opera, la risoluzione del rapporto tra il titolare del trattamento ed il DPO deve essere attentamente indagata nelle sue reali motivazioni in quanto si deve positivamente escludere che tale risoluzione abbia avuto origine nell'«*adempimento dei propri compiti*» da parte del DPO. Sul punto si apre il problema della tutela che in questo caso spetta al DPO: al riguardo non sembra possibile ipotizzare che il DPO, che abbia subito la risoluzione del rapporto a causa della particolare e giustificata «solerzia», possa fruire di una tutela reale, ossia della reintegrazione nella sua posizione.

Si è anticipato che l'ultimo periodo del par. 3, art. 39, impone un rapporto diretto tra il DPO ed il «*vertice gerarchico del titolare del trattamento*». Non è chi non veda che l'espressione «*vertice gerarchico del titolare del trattamento*» non è univoca, dal momento che può designare tanto il direttore generale, quanto l'amministratore delegato, quanto il consiglio di amministrazione. Ne segue che una concreta determinazione della figura aziendale in cui può intravedersi il «*vertice gerarchico del titolare del trattamento*» deve essere rinviata all'esame delle singole realtà aziendali.

Per quanto riguarda il settore bancario, peraltro, utili indicazioni debbono trarsi dalle Disposizioni di Vigilanza della Banca d'Italia, le quali, quando si soffermano sul «governo societario» delle banche (Parte I, Tit. IV, Cap. 1), pongono la regola – peraltro già presente nel codice civile, che, nell'enunciarla con riferimento al consiglio di amministrazione (v. art. 2381 c.c., laddove impone di assicurare un

assetto organizzativo adeguato alle esigenze dell'impresa), di fatto la prevede a carico dell'organo amministrativo della società a prescindere dalla sua composizione – secondo la quale «*gli organi aziendali devono assicurare il governo dei rischi a cui la banca si espone, individuandone per tempo le fonti, le possibili dinamiche, i necessari presidi*».

Questi aspetti sono meglio precisati nella sezione II del successivo Cap. 4, dove si assegnano all'«*organo con funzione strategica*» compiti che sostanzialmente ripercorrono le incombenze poste dal Reg. 679/2016 a carico del titolare del trattamento. Si legge, infatti, nel par. 2 della predetta sezione II che «*l'organo con funzione di supervisione strategica assume la generale responsabilità di indirizzo e controllo del sistema informativo, nell'ottica di un ottimale impiego delle risorse tecnologiche a sostegno delle strategie aziendali (ICT governance). In tale ambito esso: — approva le strategie di sviluppo del sistema informativo, in considerazione dell'evoluzione del settore di riferimento e in coerenza con l'articolazione in essere e a tendere dei settori di operatività, dei processi e dell'organizzazione aziendale; in tale contesto approva il modello di riferimento per l'architettura del sistema informativo; — approva la policy di sicurezza informatica — approva le linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, software e servizi, incluso il ricorso a fornitori esterni (cfr. Sezione VI); — promuove lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda; — è informato con cadenza almeno annuale circa l'adeguatezza dei servizi erogati e il supporto di tali servizi all'evoluzione dell'operatività aziendale, in rapporto ai costi sostenuti; è informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo. Con specifico riguardo all'esercizio della responsabilità di supervisione della analisi del rischio informatico (cfr. Sezione III), lo stesso organo: — approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico, promuovendo l'opportuna valorizzazione dell'informazione sul rischio tecnologico all'interno della funzione ICT e l'integrazione con i sistemi di misurazione e gestione dei rischi (in particolare quelli operativi, reputazionali e strategici); — approva la propensione al rischio informatico, avuto riguardo ai servizi interni e a quelli offerti alla*

clientela, in conformità con gli obiettivi di rischio e il quadro di riferimento per la determinazione della propensione al rischio definiti a livello aziendale (cfr. Capitolo 3, Allegato C); — è informato con cadenza almeno annuale sulla situazione di rischio informatico rispetto alla propensione al rischio».

Con riguardo al passo appena riportato è opportuno precisare che per «*organo con funzione di supervisione strategica*» deve intendersi il consiglio di amministrazione nel sistema tradizionale del codice del 1942 ed il consiglio di sorveglianza nel sistema dualistico ([20]). In secondo luogo, deve osservarsi che le attività e le valutazioni richieste al titolare del trattamento (quanto meno) dagli artt. 24 e 32, Reg. 679, possono agevolmente comprendersi tra quelli cui deve presiedere l'*organo con funzione di supervisione strategica*. Invero, le misure tecniche ed organizzative «*adeguate*» «*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi*», l'individuazione e l'attuazione di «*politiche adeguate in materia di protezione dei dati*» (art. 24), ed ancora – e sostanzialmente ponendo l'accento sui medesimi aspetti - le «*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*» «*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento*» (art. 32) non sono cosa altra – a ben vedere - rispetto alle attività e alle valutazioni condotte dall'«*organo con funzione di supervisione strategica*» allorché «*approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico, promuovendo l'opportuna valorizzazione dell'informazione sul rischio tecnologico all'interno della funzione ICT e l'integrazione con i sistemi di misurazione e gestione dei rischi (in particolare quelli operativi, reputazionali e strategici); approva la propensione al rischio informatico, avuto riguardo ai servizi interni e a quelli offerti alla clientela, in conformità con gli obiettivi di rischio e il quadro di riferimento per la determinazione della propensione al rischio definiti a livello aziendale*» (v. ancora Disposizioni di vigilanza, cit.), con la conseguenza che, nell'effettuare tali ultime attività, il consiglio di amministrazione (o il consiglio di sorveglianza, o

[20]) V. in proposito le stesse Disposizioni di vigilanza, Parte I, Tit. IV, Cap. 1, Sezione III, par. 1 e 2.

comunque l'organo che alla stregua dello statuto svolge la «*funzione di supervisione strategica*») deve tenere conto anche del «*rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*» e di tale considerazione si deve dare atto nelle relative delibere.

È dunque nello svolgimento di queste attività dell'organo con funzione di supervisione strategica che il DPO deve inserirsi ed esercitare i suoi compiti di controllo e consulenza. Più precisamente, il DPO della banca (o del gruppo, ma in questo caso sarebbero necessarie precisazioni ulteriori, che fuoriescono dal ristretto ambito di queste note) deve necessariamente svolgere, alla stregua dell'art. 38, par. 1, Reg. n. 679, un ruolo attivo nei processi interni che sfociano nelle decisioni relative ai compiti dell'organo con funzione di supervisione strategica elencati nel par. 2, Sez. II, Cap. 4, che si è sopra riprodotto. In ambito bancario, in questi procedimenti deve trovare applicazione la parte dell'art. 39, Reg. cit., in cui si dispone che tra i compiti del responsabile della protezione dei dati vi è quello di «*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati*».

Il ruolo del DPO all'interno della *governance* bancaria non si esaurisce qui. Finora, infatti, si è accennato ai rapporti con l'organo avente funzione strategica, ma – nel raccordo del Regolamento sul trattamento dei dati con la *governance* bancaria e con la normativa di riferimento - occorre tener conto che uno spazio significativo è riservato in quest'ultima all'«*organo con funzione di gestione*», da individuarsi negli amministratori forniti di deleghe o nel direttore generale. Per quanto riguarda più da presso il trattamento dei dati personali, è necessario prendere atto che l'organo con funzione gestoria «*ha il compito di assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficacia ed efficienza) e l'affidabilità del sistema informativo*». In definitiva, tale organo completa nella parte operativa le attività dell'organo con funzione strategica dando concreta esecuzione alle decisioni strategiche assunte dal primo ([21]). In questa

[21]) Cfr. Disposizioni di vigilanza della Banca d'Italia, Cap. 4, sez. II, par. 3: «*l'organo con funzione di gestione ha il compito di assicurare la completezza,*

prospettiva è possibile aggiungere che proprio nell'organo con funzione gestoria deve individuarsi il «titolare del trattamento» chiamato dall'art. 35 Reg. n. 679 ad effettuare la «valutazione di impatto» in presenza di un nuovo trattamento di dati: il testo dell'art. 35 rende evidente che tale valutazione è funzionale a concrete iniziative imprenditoriali di carattere operativo che di per se sfuggono alle competenze dell'organo con funzioni strategiche. Anche in questo caso deve intervenire il DPO (art. 35, par. 2, RGPD).

---

l'adeguatezza, la funzionalità (in termini di efficacia ed efficienza) e l'affidabilità del sistema informativo. In particolare, tale organo:— definisce la struttura organizzativa della funzione ICT (ove presente) assicurandone nel tempo la rispondenza alle strategie e ai modelli architetturali definiti dall'organo con funzione di supervisione strategica; garantisce il corretto dimensionamento quali-quantitativo delle risorse umane;— definisce l'assetto organizzativo, metodologico e procedurale per il processo di analisi del rischio informatico, perseguendo un opportuno livello di raccordo con la funzione di risk management per i processi di stima del rischio operativo;— tranne che nel caso di full outsourcing, approva il disegno dei processi di gestione del sistema informativo, garantendo l'efficacia ed efficienza dell'impianto nonché la complessiva completezza e coerenza, con particolare riguardo ad una funzionale assegnazione di compiti e responsabilità, alla robustezza dei controlli, alla validità del supporto metodologico e procedurale; — approva gli standard di data governance, le procedure di gestione dei cambiamenti e degli incidenti (ove del caso, in raccordo con le procedure del fornitore di servizi) e, di norma con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di business nonché con le strategie aziendali; — valuta almeno annualmente le prestazioni della funzione ICT rispetto alle strategie e agli obiettivi fissati, in termini di rapporto costi / benefici o utilizzando sistemi integrati di misurazione delle prestazioni, assumendo gli opportuni interventi e iniziative di miglioramento; — approva almeno annualmente la valutazione del rischio delle componenti critiche nonché la relazione sull'adeguatezza e costi dei servizi ICT, informando a tale riguardo l'organo con funzione di supervisione strategica; in tale ambito, riscontra la complessiva situazione del rischio informatico in rapporto alla propensione al rischio definita, disponendo allo scopo di idonei flussi informativi concernenti, come minimo, il livello di rischio residuo per le diverse risorse informatiche, lo stato di implementazione dei presidi di attenuazione del rischio (cfr. Sezione III), l'evoluzione delle minacce connesse con l'utilizzo di ICT nonché gli incidenti registratisi nel periodo di riferimento; — monitora il regolare svolgimento dei processi di gestione e di controllo dei servizi ICT e, a fronte di anomalie rilevate, pone in atto opportune azioni correttive; — assume decisioni tempestive in merito a gravi incidenti di sicurezza informatica (cfr. Sezione IV) e fornisce informazioni all'organo con funzione di supervisione strategica in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti».

Nella *governance* bancaria, al pari peraltro di qualsiasi altra impresa esercitata con veste societaria, il collegio sindacale, o più in generale l'organo di controllo ([22]), svolge un ruolo di particolare rilevanza. Per quanto qui interessa, è necessario tener conto che il collegio sindacale è chiamato a valutare l'idoneità e la congruenza degli assetti organizzativi, ivi compresi quelli volti a presidio dei rischi ([23]). In questo ambito rientrano nelle competenze del collegio sindacale anche i controlli sulle procedure volte all'abbattimento dei rischi operativi e quindi le procedure volte alla gestione del rischio connesso al trattamento dei dati. Ne segue che il collegio sindacale è competente a verificare i modi e le forme con i quali la banca dà attuazione al RGPD e che ciò deve avvenire con la collaborazione del DPO anche in applicazione di quanto previsto dal Cap. 3, sez. I, par. 3.2, secondo il quale «*l'organo con funzione di controllo, nello svolgimento dei propri compiti, si avvale dei flussi informativi provenienti dalle funzioni e strutture di controllo interno; le relazioni delle funzioni di revisione interna, di conformità e di controllo dei rischi devono essere direttamente trasmesse dai responsabili delle rispettive funzioni anche all'organo con funzione di controllo*».

Ecco quindi che ben a ragione il DPO, anche grazie alle risorse che potranno essergli state fornite ai sensi del par. 3 dell'art. 38, si colloca tra le strutture interne di conformità e controllo (es. *compliance*, legale, servizi ITC), alle quali pure è tenuto a fornire consulenza (art. 39 lett. A), quando addirittura il DPO non sia chiamato a dirigerli (art. 38, par. 6, Reg. n. 679.

[22]) Le disposizioni di vigilanza rammentano che l'organo di controllo deve individuarsi nel «*collegio sindacale,* [nel] *sistema tradizionale;* [nel] *consiglio di sorveglianza, in quello dualistico;* [nel] *comitato per il controllo sulla gestione, in quello monistico*» (par. 3.1, sez. III, Cap. 1, Tit. IV, Parte I).

[23]) «*I presidi relativi al sistema dei controlli interni devono coprire ogni tipologia di rischio aziendale*» (Cap. 3, sez. I, par. 1).