



Associazione Italiana del Credito al Consumo e Immobiliare

Schema di Decreto Legislativo recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati) - Atto 22 attualmente all'esame delle Commissioni Speciali per l'esame di atti del Governo di Camera e Senato

Giugno 2018

OSSERVAZIONI ASSOFIN

Assofin è l'associazione che riunisce i principali operatori finanziari che operano nei comparti del credito al consumo e del finanziamento immobiliare. Tutte le 65 associate sono emanazione di grandi Società e Gruppi industriali o bancari italiani o stranieri e sono tutte di primaria importanza tanto in termini di attività che di quote di mercato, operando in un mercato importantissimo per il benessere di famiglie e consumatori.

In tale contesto, il recepimento del Regolamento UE 2016/679 è un passaggio legislativo fondamentale per il trattamento dei dati personali nel settore finanziario, sul quale è opportuno un approfondimento per correggere eventuali difficoltà operative che lo schema di decreto legislativo, così come concepito al momento, potrebbe ingenerare.

Le osservazioni di seguito riportate sono quindi il frutto di quanto emerge dall'esperienza operativa che in questi anni il settore bancario e finanziario ha maturato quanto alla disciplina sul trattamento dei dati personali, e riprendono le osservazioni e le criticità già poste all'attenzione del Parlamento dall'Associazione Bancaria Italiana, che con Assofin condivide l'operatività nel settore.

1) Il nuovo impianto normativo nazionale

Lo schema di decreto legislativo, pur mantenendo vigente il Codice Privacy e quindi il D.lgs. n. 196/2003, opera una serie copiosa di abrogazioni di norme che oggi trovano disciplina nel Regolamento UE, le cui disposizioni tuttavia non sono trasferite all'interno del Codice Privacy. Non può non esprimersi qualche perplessità rispetto alla sistematizzazione delle regole privacy nel nostro ordinamento. Dall'impostazione scelta dal legislatore consegue che per avere il quadro della normativa privacy vigente in Italia occorrerà, quanto alle norme primarie, avere a riferimento sia il Regolamento UE (direttamente applicabile) sia il Codice privacy, come emendato. Si suggerisce di riconsiderare l'impianto e di "unificare" in un solo testo la nuova disciplina relativa al Regolamento UE nonché quella contenuta nel Codice privacy, come novellato dallo Schema di D.lgs. in oggetto, per semplificare le norme di riferimento e ricondurle, ove possibile, ad una sorta di "Testo Unico" per gli operatori del settore.

2) Il necessario coordinamento della disciplina nazionale primaria e secondaria con le disposizioni del Regolamento UE

Un aspetto di particolare interesse è costituito dal coordinamento tra la normativa comunitaria (direttamente applicabile nel nostro ordinamento) e quella nazionale, di cui al D.lgs. n. 196/2003, nonché quella "secondaria" emanata dal Garante della privacy nel corso degli anni, nell'ambito di poteri che il legislatore nazionale, nel recepire la Direttiva 95/46/CE, aveva specificatamente attribuito all'Autorità nazionale.

Il mondo bancario e finanziario ha evidenziato l'importanza - in tempi congrui - di una ricognizione puntuale dei Provvedimenti secondari (Provvedimenti generali, Autorizzazioni generali, Codici di deontologia e buona condotta) emanati dal Garante per la protezione dei dati personali in questi anni, che consenta una riflessione approfondita sulla loro compatibilità con il nuovo quadro giuridico.

Il tema è stato in parte affrontato dallo Schema di D. Lgs. in parola nell'ambito delle Disposizioni transitorie.

Con riferimento alle Autorizzazioni generali¹ adottate dal Garante nazionale sino ad oggi, queste ultime hanno rappresentato un importante elemento di “completamento” del quadro normativo nazionale. Infatti, il Codice Privacy italiano prevede espressamente per alcune categorie di dati (ad esempio quelli sensibili²) che il loro trattamento è possibile in presenza di un’apposita autorizzazione rilasciata dal Garante.

Il legislatore nazionale, nello schema di D.lgs., si è occupato opportunamente di rimettere al Garante (entro novanta giorni dalla data di entrata in vigore dello schema di decreto) l’emanazione di un Provvedimento di carattere generale, con il quale l’Autorità individuerà le prescrizioni contenute nelle autorizzazioni generali già adottate che sono ritenute compatibili con il Regolamento o che necessitano di essere aggiornate.

E’ condivisibile l’impostazione seguita dal legislatore, auspicando che non si verifichino situazioni di “vuoto normativo” che potrebbero determinarsi nel caso in cui il Provvedimento generale deputato a stabilire la compatibilità delle autorizzazioni già adottate venga emanato successivamente al termine indicato per la cessazione degli effetti di tali autorizzazioni.

L’impostazione utilizzata per le Autorizzazioni generali però non è stata seguita anche con riguardo ai cd. Provvedimenti Generali. Si tratta di Provvedimenti che – con particolare riguardo al mondo bancario e finanziario – sono stati adottati negli anni dal Garante per prescrivere le misure necessarie o opportune al fine di rendere il trattamento dei relativi dati conforme alle disposizioni vigenti.

Con riferimento a tali Provvedimenti, lo schema di Decreto si limita a prevedere che gli stessi “A decorrere dal 25 maggio 2018 (...) continuano ad applicarsi, in quanto compatibili con il suddetto Regolamento e con le disposizioni del presente decreto”. Così come per le Autorizzazioni generali, si ritiene fondamentale che la verifica di compatibilità rispetto al Regolamento sia anche in questo caso affidata al Garante.

Sempre con riferimento alla disciplina transitoria, un ultimo accenno va fatto alla disciplina relativa alle sorti dei Codici deontologici e in particolare a quello del Codice SIC (Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti). Risulta utile la finestra temporale prevista dallo schema di D.lgs. per allineare al Regolamento UE questo importante Codice, sottoscritto anche da numerose Associazioni dei consumatori.

Questo Codice è stato infatti in grado di disegnare una cornice di regole - seguite dagli intermediari e dai gestori dei cd. SIC dal dicembre del 2004 (anno di emanazione del Codice) – con garanzie importanti per i clienti che richiedono di aprire un rapporto con la banca.

Sebbene Assofin, insieme ad ABI e agli altri sottoscrittori del Codice del 2004, si stia già attivando per aggiornare il Codice, l’attuale panorama normativo è mutato fortemente rispetto al 2004 (anno in cui appunto venne varato il Codice) e si sono inoltre aggiunti nuovi soggetti (assicurazioni, fornitori di servizi di comunicazioni elettroniche) che, oltre alle banche e agli intermediari finanziari, possono accedere ai Sistemi di informazione creditizia (sulla base dell’art. 6-bis del D.L. 13 agosto 2011, n. 141). Anche la legge n. 124/2017 (Legge annuale per il mercato e la concorrenza) ha ulteriormente ampliato l’accesso ai sistemi di informazione creditizia anche ai “soggetti autorizzati a svolgere le attività di vendita a clienti finali di energia elettrica e di gas naturale ai sensi della normativa vigente”. **È per questo motivo che la revisione del Codice prevista dallo Schema di D.lgs. potrà essere l’occasione per estendere anche ai nuovi soggetti il rispetto delle misure già in capo agli intermediari bancari e finanziari, poste a presidio della clientela.**

¹ Le Autorizzazioni generali, previste dall’art. 40 del Codice Privacy e pubblicate nella Gazzetta Ufficiale, consistono in autorizzazioni al trattamento dei dati relative a determinate categorie di operatori o di trattamenti.

² Ai sensi dell’art. 4, comma 1, lettera d) del Codice privacy, sono dati sensibili “i dati personali idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale”.

In questo senso, si auspica l'estensione ad otto mesi dalla data di entrata in vigore del decreto in parola del periodo entro il quale sottoporre al Garante il Codice revisionato.

3) Alcune osservazioni sulle disposizioni contenute nello Schema di Decreto Legislativo

Vi sono poi una serie di previsioni sulle quali si rendono opportune, ad avviso del settore bancario e finanziario, delle integrazioni o modifiche.

A) Limitazioni ai diritti dell'interessato (art. 2-decies)

L'art. 23 del Regolamento prevede che lo Stato membro possa limitare l'esercizio dei diritti dell'interessato (diritto di accesso, di cancellazione, portabilità, etc.) qualora vi siano una serie di condizioni tra cui ad esempio, la difesa, la sicurezza pubblica, la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, etc.

Lo Schema di D.lgs., declinando quanto previsto dal citato art. 23 del Regolamento, indica le situazioni al ricorrere delle quali tali diritti trovano una limitazione.

Posto il richiamo della normativa antiriciclaggio nell'elenco delle situazioni individuate, si segnala tuttavia la necessità di aggiungere anche le disposizioni di contrasto al finanziamento del terrorismo e alla proliferazione delle armi di distruzione di massa.

Considerata, inoltre, la natura e la funzione delle materie elencate e in particolare – per quanto di più diretto interesse del mondo bancario e finanziario – quella sul contrasto del riciclaggio, si ritiene importante che la norma sia formulata in modo tale da non lasciare alla discrezionalità del titolare del trattamento la valutazione sulla possibilità che l'interessato possa esercitare i suoi diritti.

La proposta tende ad assicurare certezza nell'individuazione delle situazioni – dove la tutela dell'interesse pubblico prevale rispetto alla tutela dell'interesse privato – al ricorrere delle quali la norma non consente all'interessato di esercitare i diritti di accesso ai propri dati personali.

B) Attribuzione di funzioni e compiti a soggetti designati (Art. 2-terdecies)

Dal tenore delle diverse disposizioni del Regolamento sembra evincersi che il Responsabile del trattamento³ è una figura "esterna" alla struttura del Titolare⁴, ossia una società o un soggetto cui viene esternalizzato il trattamento dei dati. Ai sensi della previgente normativa, la figura del Responsabile del trattamento poteva coincidere anche con un soggetto interno all'azienda (ad esempio un dipendente) cui veniva affidata, sempre dal titolare, la responsabilità per le attività di trattamento collegate alla sua funzione. Per tale ragione, la figura del "Responsabile interno" è molto utilizzata nell'assetto degli intermediari bancari e finanziari.

Al riguardo, nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali", predisposta dall'Autorità Garante e pubblicata sul suo sito internet, si legge tra le "Raccomandazioni" che, in tema di misure tecniche e organizzative di sicurezza, si ritiene che titolari e responsabili del trattamento "possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante".

³ Da intendersi il soggetto che tratta dati personali per conto del titolare del trattamento.

⁴ E cioè il soggetto che determina la finalità ed i mezzi del trattamento dei dati personali.

Si rendono quindi necessari chiarimenti in ordine alla figura del “Responsabile interno” e alla possibilità che possa ancora essere contemplata all’interno della struttura del Titolare del trattamento, chiarendone l’inquadramento giuridico (che dovrebbe rientrare nell’alveo delle “persone autorizzate al trattamento” come definite oggi dal Regolamento UE) e distinguendolo altresì, sia nelle funzioni che nelle responsabilità e sanzioni, dal responsabile esterno.

C) Sanzioni

Con riferimento all’impianto sanzionatorio, si segnala la necessità di assicurare che non vi siano rischi di sovrapposizione di sanzioni di natura amministrativa e penale e di conseguenza di garantire il rispetto del principio del “*ne bis in idem*”.

Si rileva infatti che con riferimento a diverse fattispecie (tra cui, ad esempio, le violazioni di cui agli articoli 123, 129, 2-quaterdecies, 2-sexies, 2-octies) lo schema di Decreto prevede sia l’applicazione di una sanzione amministrativa (art. 15, comma 1, lettera a), sia l’applicazione di sanzioni penali, al ricorrere degli elementi soggettivi configuranti l’ipotesi di reato (cfr. art. 15, comma 1, lettera b e lettera c).

L’approccio adottato rischia perciò di disallineare la normativa nazionale rispetto a quanto previsto dal Regolamento UE, che all’art. 84, comma 1, dispone che “Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell’art. 83 (...)”.