



Normativa antiriciclaggio e trattamento di dati personali da parte di Poste Italiane S.p.A. - 28 novembre 2013

Registro dei provvedimenti
n. 533 del 28 novembre 2013

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali; di seguito "Codice");

VISTO il d.lgs. 21 novembre 2007, n. 231 ("Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione"), nonché il parere preventivo del Garante del 25 luglio 2007 (in www.garanteprivacy.it; doc. web n. [1431012](#));

VISTI i provvedimenti adottati in tale materia, nel corso del tempo, dalla Banca d'Italia e dagli altri organismi a ciò preposti;

VISTA la segnalazione del 18 settembre 2012 e le successive risultanze istruttorie;

ESAMINATA la documentazione in atti;

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

RELATORE il dott. Antonello Soro;

PREMESSO

1. La segnalazione pervenuta all'Autorità.

Con segnalazione inviata in data 18 settembre 2012 (successivamente integrata il 3 giugno 2013), il sig. XY, già censito nei sistemi informativi di Poste Italiane S.p.A. in qualità di correntista privato, ha lamentato che detta società, in occasione dell'espletamento di alcune operazioni di verifica previste dalla normativa in materia di antiriciclaggio, aveva effettuato un indebito accesso ai suoi dati personali.

Più esattamente il segnalante ha riferito che, in data 23 agosto 2012, si era recato presso l'ufficio postale di Vobbia per effettuare, in nome e per conto del Comune, un versamento di euro 5.162,30 su un conto corrente intestato all'Inps, per procedere all'acquisto di "buoni lavoro (vouchers) da attribuire ad alcuni pensionati" che avevano svolto lavoro occasionale in favore dello stesso Comune. In tale occasione, però, l'operatore di sportello di Poste Italiane S.p.A., anziché limitarsi ad "identificare" l'interessato nella sua qualità di mero esecutore materiale di una specifica operazione da effettuarsi in nome e per conto dell'ente comunale, aveva aperto una procedura informatica volta a "verifica[re] ed analizza[re] ogni rapporto che [costui aveva], come persona privata, con Poste Italiane S.p.A." e, segnatamente, il "conto corrente postale cointestato con il padre per il ritiro della pensione" e la "tessera prepagata tipo «Postepay»".

A detta del segnalante, tali verifiche avevano dato luogo ad una "palese intromissione" nella sua sfera di riservatezza, attesa non solo la loro estraneità rispetto all'operazione richiesta, inerente soltanto al Comune, ma anche in ragione dell'avvenuta documentazione dei poteri rappresentativi conferitigli, di cui, peraltro, era a conoscenza anche la stessa direttrice dell'ufficio postale in virtù del ruolo di consigliere del Comune di Vobbia da costei rivestito; inoltre, l'operazione era stata consentita solo a seguito dell'avvenuto aggiornamento dei suoi dati personali –conservati, ad altro titolo, nel database di Poste Italiane S.p.A.- perché risultati inadeguati a causa dell'intervenuta scadenza del periodo di validità del documento di riconoscimento da lui esibito in occasione dell'apertura del proprio conto corrente.

Alla luce di tali fatti, il segnalante ha chiesto l'intervento dell'Autorità per "ripristinare la necessaria legalità".

2. Il riscontro fornito dalla società.

Con nota del 21 maggio 2013, Poste Italiane S.p.A. ha fatto pervenire le proprie osservazioni sulla vicenda, rappresentando di aver predisposto sulla propria "rete" informatica, in adempimento agli obblighi in materia di antiriciclaggio, "un blocco procedurale a sportello" per le operazioni di importo superiore a 5.000 euro ("con riferimento sia alle posizioni sprovviste di adeguata verifica per le quali occorre il «recupero» dei dati, sia per le posizioni anagrafiche «cd. incomplete o incorrette»"), comportante la sottoposizione a controllo non solo dell'effettivo titolare del rapporto, ma anche di colui che intervenga quale "mero esecutore di un'operazione anche occasionale".

In particolare, la società ha sostenuto che la normativa sul contrasto del riciclaggio richiederebbe "un articolato e complesso sistema di processi, applicativi informativi e controlli a carattere «trasversale»", che giustificerebbe "l'estensione delle procedure per il recupero delle informazioni necessarie [...] ai soggetti operanti anche non in qualità di titolari o facoltizzati ad operare sul rapporto movimentato" (come, nel caso specifico, il segnalante); tali operazioni, da effettuarsi in occasione del "primo contatto utile" (art. 22 d.lgs. n. 231/2007), sarebbero coerenti sia con la necessità di svolgere un "controllo costante del rapporto continuativo" facente capo all'interessato (art. 18 del d.lgs. n. 231/2007), sia con il contenuto dell'attività di "riciclaggio", la quale può estrinsecarsi anche attraverso "tentativi di trasformazione, trasferimento, conversione di fondi e provviste finanziarie, mediante l'alterazione dei ruoli, dei poteri, delle facoltà" di tutti coloro che, a vario titolo, siano coinvolti in operazioni finanziarie.

Ciò premesso, la società ha confermato che le menzionate procedure di "adeguata verifica" erano state avviate anche nei confronti dell'odierno segnalante, il quale era stato identificato anche per accertare la sua posizione di semplice esecutore di un'operazione occasionale da effettuarsi in nome e per conto dell'ente rappresentato; in tale occasione, il sistema, avendo riconosciuto in capo all'interessato la qualità di "cliente di Poste Italiane" (in ragione dei dati anagrafici già presenti, quale privato correntista, nel database informatico della società), all'esito delle verifiche aveva subordinato la conclusione dell'operazione anche "all'aggiornamento della data di scadenza del documento di identità" ivi memorizzato, consentendone il perfezionamento solo a "variazione anagrafica" avvenuta.

3. Le valutazioni dell'Autorità.

Il procedimento ha ad oggetto un presunto indebito accesso ai dati personali del segnalante (in qualità di correntista privato di Poste Italiane S.p.A.) verificatosi in occasione di una richiesta di versamento su conto corrente inoltrata dall'istante in nome e per conto del Comune di Vobbia.

Preliminarmente, si rileva che la società non ha contestato di aver effettuato specifiche verifiche sulla tessera "Postepay" del segnalante e sul conto corrente postale intestato a lui e al suo genitore, sicché, almeno sul piano storico, i fatti possono ritenersi pacifici tra le parti.

Nel merito della questione, invece, si osserva quanto segue.

La normativa in materia di antiriciclaggio prevede che i soggetti destinatari delle relative disposizioni adottino idonei e appropriati sistemi e procedure, anche per dare corretta attuazione agli obblighi in tema di adeguata verifica della clientela (c.d. customer due diligence: art. 3, comma 1 del d.lgs. n. 231/2007); tali misure, in ogni caso, debbono comunque rispettare le garanzie e le prescrizioni stabilite dalla normativa in materia di protezione dei dati personali (cfr. art. 3, comma 2 del d.lgs. n. 231/2007) e debbono anche risultare "proporzionate" al rischio di riciclaggio dei proventi di attività criminose o di finanziamento del terrorismo, il quale va rapportato, tra l'altro, al tipo di cliente e alle caratteristiche della concreta operazione che si intende effettuare (art. 3, comma 3 del d.lgs. n. 231/2007).

I presupposti, il contenuto e le modalità di adempimento dei predetti obblighi sono individuati dagli artt. 15 e ss. del menzionato decreto. In particolare, gli intermediari finanziari sono tenuti –tra l'altro- a identificare e a verificare l'identità dei clienti sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente (art. 18, comma 1, lett. a) del d.lgs. n. 231/2007), quando:

- eseguono operazioni occasionali comportanti trasmissione o movimentazione di mezzi di pagamento di importo superiore a una certa soglia;
- vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione di un cliente.

In ogni caso, in conformità a quanto già statuito dal richiamato art. 3, comma 3 del decreto, il corretto assolvimento degli obblighi di adeguata verifica della clientela presuppone un "approccio basato sul rischio", che tenga conto del tipo di cliente e di operazione richiesta, da effettuarsi sulla base di alcune istruzioni fornite dalle preposte autorità di vigilanza e di taluni criteri generali indicati all'art. 20, comma 1 del decreto stesso (sul punto, vedi: 1) le Istruzioni fornite da Banca d'Italia con il "Provvedimento recante disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del decreto legislativo 21 novembre 2007, n. 231" del 3 aprile 2013 – applicabili a decorrere dal 1° gennaio 2014–, con il correlato comunicato stampa dell'11 aprile 2013; 2) sul piano più generale, il "Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'art. 7 comma 2 del Decreto Legislativo 21 novembre 2007, n. 231" del 10 marzo 2011, nonché i chiarimenti forniti dal Ministero dell'Economia e delle Finanze con nota del 17 dicembre 2008, prot. n. 116098; 3) il "Provvedimento recante gli indicatori di anomalia per gli intermediari" del 27 agosto 2010; 4) il "Provvedimento recante disposizioni attuative per la tenuta dell'archivio unico informatico e per le modalità semplificate di registrazione di cui all'art. 37, commi 7 e 8, del decreto legislativo 21 novembre 2007, n. 231", del 3 aprile 2013, anch'esso applicabile dal 1° gennaio 2014); 5) riguardo al trattamento dei dati personali, il Parere del Garante del 25 luglio 2007).

Pertanto, alla luce del quadro normativo, non vi è dubbio che la corretta identificazione degli utenti –ivi compresi i "semplici" esecutori materiali di operazioni occasionali effettuate per conto terzi- e la verifica della loro identità costituiscano, anche in considerazione delle gravi sanzioni applicabili in caso di inadempimento (artt. 55 e 56 del d. lgs. n. 231/2007), obblighi ineludibili a carico dei soggetti tenuti alla relativa osservanza, tra cui figura anche Poste Italiane S.p.A. (art. 11, comma 1, lett. b), del d.lgs. n. 231/2007).

Nondimeno, tali obblighi, come già rilevato, devono essere concretamente assolti commisurando il relativo adempimento al grado di rischiosità associato al tipo di cliente, all'operazione che si intende effettuare, al rapporto avviato o alla prestazione professionale richiesta (in tal senso, v. già il Parere del Garante del 25 luglio 2007).

Ad avviso di questa Autorità, nel caso in questione il criterio dell'"approccio basato sul rischio" risulta essere stato disatteso da Poste Italiane S.p.A., la quale, in occasione dell'espletamento dei controlli richiesti dalla normativa vigente, ha effettuato verifiche (comportanti anche il trattamento dei dati personali dell'interessato) obiettivamente eccedenti in rapporto al "profilo di rischio" a costui concretamente associabile e al tipo di operazione richiesta (v., in argomento, anche i chiarimenti resi dal Ministero dell'Economia e delle Finanze in data 19 dicembre

Infatti, l'esiguo importo dell'operazione, l'avvenuta documentazione dei poteri rappresentativi esercitati dall'istante in favore del Comune, la conoscenza personale del cliente da parte della direttrice dell'ufficio postale, la natura pubblica dell'ente rappresentato e la motivazione sottesa all'occasionale operazione (acquisto di semplici "vouchers" da assegnare ad alcuni pensionati), costituiscono circostanze da rendere non solo inopportuno, ma addirittura eccedente lo svolgimento di un così penetrante controllo sui rapporti privatamente intrattenuti dall'interessato con la stessa società; ne consegue che il connesso trattamento di dati personali effettuato nell'occasione da Poste Italiane S.p.A., oltre a non essere conforme al principio di necessità (art. 3 del Codice), è risultato eccedente anche in rapporto alla finalità (pur lecita) perseguita dalla società (art. 11, comma 1, lett. d) del Codice), la quale avrebbe potuto ben essere raggiunta, se non già attraverso l'attuazione degli "obblighi semplificati" di adeguata verifica delineati dall'art. 25 dello stesso d. lgs. n. 231/2007, osservando modalità di verifica meno pervasive.

In considerazione di tali rilievi risulta quindi necessario, alla luce di quanto previsto dagli artt. 143, comma 1, lett. c), 144 e 154, comma 1, lett. d), del Codice, prescrivere a Poste Italiane S.p.A. di astenersi dal trattare, in occasione di future operazioni finanziarie che dovessero essere effettuate dal sig. XY in nome e per conto del Comune di Vobbia, le informazioni personali riferibili al segnalante relative a rapporti negoziali privatamente intrattenuti dal medesimo con la stessa società, a meno che ciò non risulti effettivamente giustificato dal rilevamento di un concreto rischio valutato ai sensi dell'art. 20, co. 1 del d. lgs. n. 231/2007.

Inoltre, in ragione dell'elevato numero di utenti che si avvalgono quotidianamente dei servizi postali e finanziari forniti dalla società, ai sensi degli artt. 143, comma 1, lett. b), 144 e 154, comma 1, lett. c) del Codice, si ritiene di dover prescrivere a Poste Italiane S.p.A. di adottare opportune misure formative e tecnico-organizzative idonee a prevenire, nell'ambito dell'espletamento dei doverosi controlli richiesti dalla normativa in materia di antiriciclaggio, operazioni di trattamento dei dati personali dei clienti non conformi al criterio dello "approccio basato sul rischio" fissato dal citato art. 20 del d. lgs. n. 231/2007.

TUTTO CIO' PREMESSO, IL GARANTE:

- dichiara l'illiceità del trattamento dei dati personali del sig. XY, effettuato da Poste Italiane S.p.A. in data 23 agosto 2013;
- ai sensi degli artt. 143, comma 1, lett. b) e c), 144 e 154, comma 1, lett. c) e d) del Codice, prescrive a Poste Italiane S.p.A. di astenersi dal trattare, in occasione di future operazioni finanziarie che dovessero essere effettuate dal sig. XY in nome e per conto del Comune di Vobbia, le informazioni personali riferibili al segnalante relative a rapporti negoziali privatamente intrattenuti dal medesimo con la stessa società, a meno che ciò non risulti effettivamente giustificato dal rilevamento di un concreto rischio valutato ai sensi dell'art. 20, co. 1 del d. lgs. n. 231/2007;
- ai sensi degli artt. 143, comma 1, lett. b), 144 e 154, comma 1, lett. c) del Codice, prescrive alla società di adottare opportune misure formative e tecnico-organizzative idonee a prevenire, nell'ambito dell'espletamento dei doverosi controlli richiesti dalla normativa in materia di antiriciclaggio, operazioni di trattamento dei dati personali dei clienti non conformi al criterio dell'"approccio basato sul rischio" fissato dall'art. 20 del d. lgs. n. 231/2007.

Ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 28 novembre 2013

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia