Registro dei provvedimenti
n. 150 DEL 24.07.2019

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 prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere del Ministero dell'economia e delle finanze;

Visto l'articolo 36, par. 4, del Regolamento (UE) 2016/679, del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche 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, di seguito Regolamento);

Visto il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (decreto legislativo n. 196 del 2003, come modificato dal decreto legislativo 10 agosto 2018, n. 101, di seguito Codice);

Vista la documentazione in atti;

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

Relatore la dott.ssa Augusta Iannini;

PREMESSO

1. Il Ministero dell'economia e delle finanze ha richiesto il parere dell'Autorità su uno schema di decreto legislativo recante modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e 92, recanti attuazione della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015, nonché attuazione della direttiva 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE.

Lo schema di decreto è stato predisposto conformemente alle previsioni di cui all'articolo 31, comma 5, della legge 24 dicembre 2012, n. 234 ai sensi del quale, entro ventiquattro mesi dalla data di entrata in vigore di ciascuno dei decreti legislativi adottati per il recepimento di direttive europee, il Governo può adottare, nell'esercizio della medesima delega legislativa, disposizioni integrative e correttive.

Il parere è richiesto ai sensi dell'articolo 36, par. 4, del Regolamento (UE) 2016/679 e dell'articolo 15 della legge 12 agosto 2016, n. 170 (c.d. "legge di delegazione europea 2015").

Lo schema di decreto, esaminato in sede preliminare dal Consiglio dei ministri lo scorso 1° luglio, contiene le integrazioni e le modifiche che si sono rese necessarie al fine di recepire le osservazioni formulate dalla Commissione europea nell'ambito della procedura di infrazione (n. 2019/2042) con la quale è stato formalmente contestato il non completo recepimento della direttiva (UE) 2015/849 (c.d. "quarta direttiva" antiriciclaggio).

Lo schema contiene, altresì, le disposizioni necessarie ad assicurare il recepimento della direttiva (UE) 2018/843 (c.d. "quinta direttiva" antiriciclaggio), *medio tempore* adottata.

Il Garante ha reso a suo tempo parere sullo schema di decreto legislativo con il quale è stata fornita la prima attuazione della direttiva (UE) 2015/849, che ha introdotto significative modifiche alla vigente disciplina in materia di prevenzione dell'uso del sistema finanziario a fini di riciclaggio e di finanziamento del terrorismo, al fine di allineare la normativa nazionale alle nuove disposizioni introdotte in materia in sede europea (parere n. 125 del 9 marzo 2017, *doc. web* n. 6124534).

L'odierno parere tiene conto anche delle osservazioni rese dal Garante nel provvedimento del 2017, non tutte integralmente recepite.

RILEVATO

2. Con la direttiva del 2015 si è operato un più rigoroso contrasto alla crescente diversificazione del mercato criminale, atteso che i flussi di denaro illecito, compromettendo la stabilità e l'integrità del settore finanziario, rappresentano una concreta minaccia per il mercato interno dell'Unione e dei singoli Stati membri. Considerata la natura mutevole delle minacce costituite dal riciclaggio e dal finanziamento del terrorismo, facilitata dalla continua evoluzione della tecnologia e dei mezzi a disposizione dei criminali, l'adozione di misure di contrasto che consentano di adeguare il sistema di prevenzione a nuove ipotesi di riciclaggio è vista come imprescindibile.

Da ciò l'esigenza di un intervento d'insieme volto a migliorare l'aderenza del quadro normativo nazionale alla nuova disciplina comunitaria, nonché a correggere incongruenze, a chiarire dubbi interpretativi e a rimuovere le difficoltà emerse nel corso degli anni, in sede di applicazione del d.lgs. 21 novembre 2007, n. 231, che resta tuttora la base giuridica che disciplina la materia anche in relazione al trattamento dei dati personali (cfr. art. 6, par. 2 e 3 del Regolamento).

Nondimeno, la Commissione europea nell'ambito di una procedura di infrazione (n. 2019/2042) ha formalmente contestato il non completo recepimento della direttiva (UE) 2015/849 e conseguentemente alcune disposizioni dello schema di decreto intendono recepire le osservazioni rese in proposito dalla Commissione.

Successivamente, è stata adottata la direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 che ha modificato la predetta direttiva (UE) 2015/849. In proposito -si legge nella relazione illustrativa – lo schema di decreto contiene le disposizioni necessarie ad assicurare il recepimento della predetta direttiva, *medio tempore* adottata, per

introdurre talune specifiche e circoscritte modifiche ed integrazioni alla direttiva (UE) 2015/849, senza prevederne l'abrogazione.

3. Lo schema di decreto si compone di 6 articoli.

L'articolo 1, apporta modifiche al Titolo I (Disposizioni di carattere generale) del d.lgs. n. 231/2007, con disposizioni finalizzate, tra le altre, a puntualizzare le categorie di soggetti tenuti all'osservanza degli obblighi antiriciclaggio (comma 1); a definire i compiti e le attribuzioni delle amministrazioni e delle autorità nazionali coinvolte nell'attività di vigilanza, controllo e sorveglianza (comma 2); a rafforzare la collaborazione e lo scambio di informazioni tra le autorità nazionali, nonché la cooperazione internazionale e tra gli Stati membri (comma 3).

L'articolo 2 apporta modifiche al Titolo II (Obblighi) del d.lgs. n. 231/2007, integrando alcune disposizioni relative all'adeguata verifica della clientela ed intervenendo sul regime di accessibilità delle informazioni contenute nel registro della titolarità effettiva delle imprese dotate di personalità giuridica e delle persone giuridiche private, prescrivendo che il pubblico possa accedere alle predette informazioni. Ulteriori prescrizioni disciplinano l'accesso alle informazioni relative alla titolarità effettiva di trust e soggetti giuridici affini.

L'articolo 3 introduce il divieto di emissione e utilizzo di prodotti di moneta elettronica anonimi, mentre l'articolo 4 dispone modifiche al Titolo V del d.lgs. n. 231/2007 in tema di sanzioni e procedure di irrogazione in caso di violazioni. Infine, l'articolo 5 prevede l'obbligo di iscrizione, nel registro degli agenti in attività finanziaria e dei mediatori creditizi, anche dei prestatori di servizi di portafoglio digitale.

Tra gli articoli di particolare interesse sotto il profilo della protezione dei dati personali si segnala, innanzitutto, l'articolo 1, primo comma, lett. *i)*, che - per corrispondere ad una precisa richiesta della Commissione europea - esplicita che il trattamento dei dati personali detenuti ai fini del provvedimento è considerato di interesse pubblico nell'ambito delle garanzie previste dal Regolamento (UE) 2016/679.

Al riguardo occorre considerare che la direttiva (UE) 2015/849 – la quale espressamente cita la necessità di assicurare la protezione dei dati in ossequio alla direttiva 95/46/CE (cfr. art. 41, considerando 41 e 42) – sottolinea che la lotta contro il riciclaggio e il finanziamento del terrorismo è riconosciuta di interesse pubblico rilevante da parte di tutti gli Stati membri (cfr. art. 43).

Il Regolamento (UE) 2016/679 (che è necessario citare nel preambolo del decreto legislativo) ha poi confermato tale assunto, annoverando fra gli *"obiettivi di interesse pubblico generale ..... di uno Stato membro .... un rilevante interesse economico o finanziario...anche in materia monetaria, di bilancio e tributaria"*, la cui salvaguardia consente limitazioni ai diritti degli interessati (art. 23, par. 1, lett. *e)*, Reg.). Inoltre, in base al Codice, *"l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo"*, previsto da norme di legge o, nei casi previsti dalla legge, di regolamento legittima il trattamento di dati relativi a condanne penali o reati (art. 2-*octies*, comma 3, lett. *m)*, Codice).

Di interesse è pure l'articolo 2, comma 3, lett. *a)*, dello schema di decreto che, nell'apportare modifiche all'articolo 39, comma 1, del d. lgs. n. 231/2007, prevede che il

trattamento dei dati personali connesso alle attività di segnalazione e comunicazione sia soggetto alle disposizioni di cui all'articolo 2-*undecies* del Codice.

Sempre all'articolo 2, comma 1, si segnala la lett. *b)* n. 1, in tema di "identità digitale" che, nel modificare l'articolo 19, comma 1, lett. *a)*, n. 2, del d.lgs. n. 231/2007 ed in attuazione di indicazioni contenute nella c.d. "quinta direttiva", precisa che le identità conformi alle regole e-IDAS, rilasciate in altro Paese UE, possano essere accettate, a fini identificativi, solo se caratterizzate da un livello massimo di sicurezza. Le norme, inoltre, ammettono la possibilità per i soggetti obbligati di utilizzare anche identità digitali non rientranti nel circuito e-IDAS, purché sicure e regolamentate dalle autorità ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale.

Infine, l'articolo 2, al comma 1 lettere da *f)* a *i)*, nel modificare gli articoli 21 e 22 del d. lgs. n. 231/2007, interviene, in sintesi, sul regime di accessibilità alle informazioni contenute nel registro delle imprese in tema di titolarità effettiva delle imprese dotate di personalità giuridica e delle persone giuridiche private, prevedendone l'accesso libero. A tal fine, l'articolo 2, comma 1, lett. *h)*, n. 5) dello schema di decreto in esame prevede anche il parere del Garante sul decreto del Ministro dell'economia e delle finanze che dovrà stabilire le modalità di consultazione del predetto registro.

RITENUTO

4. Come già rilevato dal Garante nel parere del 2017 e in precedenti occasioni (cfr. pareri del 12 marzo 2003, doc. *web* n. 1054779, del 12 maggio 2005, doc. *web* n. 1131800 e del 25 luglio 2007, doc. *web* n. 1431012), l'ampiezza della platea dei soggetti tenuti ad obblighi di identificazione della clientela, di registrazione delle operazioni e di segnalazione di operazioni sospette impone una riflessione di fondo sul crescente impatto che la normativa antiriciclaggio assume sempre più in un numero crescente di settori, nonché sulle connesse implicazioni che ne derivano per i diritti delle persone e sul piano della protezione dei dati personali.

La direttiva (UE) 2015/849, al completamento della cui attuazione lo schema di decreto è preordinato, pone l'accento sulla necessità di rispettare i diritti fondamentali delle persone e i princìpi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea, il cui articolo 8 garantisce ad ogni individuo il diritto alla protezione dei dati personali che lo riguardano (considerando 43).

Anche la direttiva (UE) 2018/843 richiama il rispetto dell'attuale quadro giuridico dell'Unione in materia di protezione dei dati, con particolare riferimento al Regolamento (UE) 2016/679 (considerando 38 e 40).

Il predetto Regolamento ha ribadito e rafforzato il richiamo al rispetto del principio di liceità del trattamento (cfr. art. 6, paragrafi 1, lett. *e)*, e 3, lett *b)*), che impone al legislatore di contemperare il diritto alla protezione dei dati con le specifiche esigenze sottese al trattamento, ancorché finalizzato, come in questo caso, a contrastare l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo.

In tale quadro, pertanto, si richiama ulteriormente l'attenzione del legislatore sulla necessità di procedere ad un'attuazione rigorosa in chiave di effettiva necessità, di

proporzionalità e di selettività degli interventi di monitoraggio e prevenzione (art. 5, par. 1, lett. *c*), Reg.), anche in considerazione degli enormi flussi informativi previsti, specie verso l'Unità di Informazione Finanziaria per l'Italia-UIF, e della particolare natura del trattamento.

Ciò premesso, al fine di rendere lo schema di decreto pienamente conforme ai principi e alle regole in materia di protezione dei dati personali previsti dal Regolamento, si svolgono di seguito le seguenti osservazioni.

4.1. Cooperazione dell'UIF con le Unità di altri Paesi (FIU).

L'art. 1, comma 3, lett. c), dello schema in oggetto introduce nel d.lgs. 231/2007 gli artt. 13-*bis* e 13-*ter*, volti a recepire gli artt. 53-56 della direttiva (UE) 849/2015, a seguito dei rilievi sollevati dalla Commissione europea con la nota di costituzione in mora ai sensi dell'art. 258 TFUE n. 2019/2042 – con la quale ha avviato la procedura di infrazione nei confronti dell'Italia per il mancato recepimento completo della direttiva (UE) 849/2015. Le disposizioni di cui si propone l'introduzione, tuttavia, non appaiono pienamente conformi alla disciplina in materia di protezione dei dati personali, in quanto:

- il comma 2 dell'art. 13-*bis*, di cui lo schema in oggetto propone l'introduzione, stabilisce che *"La UIF utilizza le informazioni ottenute dalle altre FIU per lo svolgimento delle attività di cui al comma 1 e per le finalità per cui le predette informazioni sono fornite. Tali informazioni possono essere utilizzate per finalità ulteriori o trasmesse dalla UIF alle autorità nazionali competenti previo consenso della FIU dello Stato che ha fornito le informazioni e nel rispetto degli eventuali limiti o condizioni posti dalla medesima FIU"*. Tale previsione risulta in contrasto con il principio di limitazione della finalità di cui all'art. 5, par. 1, lett. b), del Regolamento, soprattutto tenendo conto che l'art. 54 della direttiva (UE) 849/2015 limita espressamente l'utilizzo delle informazioni al solo svolgimento dei compiti delle FIU previsti dalla medesima direttiva;
- l'art. 13-*bis* non fissa regole specifiche, anche attraverso il rinvio ad una fonte secondaria (cfr. par. 1), in grado di assicurare l'utilizzo di canali protetti di comunicazione, espressamente richiesti dall'art. 56, par. 1, della direttiva (UE) 849/2015 e di cui la Commissione lamentava la mancata attuazione nella nota di avvio della procedura di infrazione. Oggi tali misure sono ancor più necessarie alla luce del principio di integrità e riservatezza e dell'obbligo di garantire un livello di sicurezza adeguato al rischio, di cui agli artt. 5, par. 1, lett. f), e 32 del Regolamento;
- il medesimo art. 13-*bis*, infine, omette di prevedere misure di garanzia specifiche per la tutela dei dati personali, in questo modo non attuando l'art. 56, par. 2, della direttiva (UE) 849/2015 laddove richiede che sia consentito a ciascuna FIU *"di incrociare anonimamente i propri dati con quelli delle altre FIU, assicurando la completa protezione dei dati personali, al fine di individuare in altri Stati membri soggetti che le interessano e rintracciarne proventi e fondi"*.

4.2. L'esercizio dei diritti da parte dell'interessato.

L'articolo 2, comma 3, lett. *a*), dello schema di decreto, nell'apportare modifiche all'articolo 39, comma 1, del d. lgs. n. 231/2007, prevede che il trattamento dei dati personali connesso alle attività di segnalazione e comunicazione sia soggetto alle disposizioni di cui all'articolo 2-*undecies* del Codice, senza alcuna ulteriore specificazione.

Il predetto articolo 2-*undecies* disciplina le limitazioni ai diritti dell'interessato in relazione ad altri interessi meritevoli di considerazione, fra cui anche quelli tutelati in base alle disposizioni in materia di riciclaggio, in applicazione di quanto previsto dal Regolamento (art. 23 Reg.; art. 2-*undecies*, comma 1, lett. *a)*, Codice). Al riguardo, al fine di assicurare maggiore chiarezza alla disposizione in parola si ritiene opportuno sostituire integralmente la locuzione con la seguente: *"In relazione al trattamento di dati personali connesso alle attività di segnalazione e comunicazione di cui al presente comma, i diritti di cui agli articoli da 15 a 22 del Regolamento (UE) 2016/679, del Parlamento europeo e del Consiglio, del 27 aprile 2016, si esercitano nei limiti previsti dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni."*.

4.3. Informazioni sul trattamento agli interessati.

Tra le contestazioni mosse dalla Commissione nella procedura di infrazione vi è la mancata attuazione dell'art. 41, par. 3, della direttiva (UE) 849/2015, laddove impone, ai soggetti obbligati, di fornire ai clienti le informazioni previste dalla disciplina in materia di protezione dei dati personali prima di instaurare un rapporto d'affari o eseguire un'operazione occasionale.

Lo schema in oggetto non prevede alcuna disposizione in proposito, essendo ritenuta sufficiente la vigenza dell'art. 13 del Regolamento, nonché la clausola generale di rispetto del Codice contenuta nell'art. 3, comma 9, del d.lgs. 231/2007, di stile e generica.

Considerato che i principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento, delle sue finalità e della logica applicata al trattamento, ai sensi degli artt. 5, par. 1, lett. a), e 13, del Regolamento, anche in relazione ai dati raccolti presso terzi (art. 14 del Regolamento), si chiede invece di inserire nello schema in oggetto opportune garanzie, mediante l'introduzione di un comma all'interno dell'art. 17 del d.lgs. 231/2007 che rinvii al rispetto del predetto principio di correttezza e trasparenza. Ciò, anche con riferimento ai trattamenti effettuati ai fini di adeguata verifica della clientela attraverso gli indicatori e la valutazione del rischio di cui al precedente punto 1.3.

4.4. Livello di sicurezza dell'identità digitale.

L'art. 19, comma 1, lett. a), n. 2, del d.lgs. 231/2007 viene modificato ad opera dell'art. 2, comma 1, lett. b), n. 1, dello schema in oggetto, prevedendo che anche l'identità digitale posseduta da un cliente e rilasciata in base a sistemi diversi da SPID sia di *"livello massimo di sicurezza"*. Esso però non chiarisce, come invece richiesto dall'Autorità nel citato parere del 2017, che tale livello, con riferimento al sistema SPID, debba attualmente corrispondere al livello 3, in questo modo non garantendo quel livello di sicurezza adeguato al rischio richiesto dall'art. 32 del Regolamento.

4.5. Attuazione del decreto legislativo.

Al fine di assicurare una disciplina omogenea e conforme ai principi in materia di protezione dei dati personali, nell'ambito delle regole o specifiche tecniche da apprestare per l'attuazione del provvedimento è opportuno prevedere espressamente che i diversi decreti o

protocolli di intesa e convenzioni previsti dallo schema di decreto legislativo aventi impatto sulla protezione dei dati siano adottati previo parere del Garante.

5. Come anticipato sopra, i rilievi contenuti nel parere del Garante n. 125 del 9 marzo 2017 sul precedente schema di decreto legislativo in materia di antiriciclaggio in seguito adottato (d.lgs. 25 maggio 2017, n. 90) non sono stati a suo tempo pienamente recepiti.

Pertanto, con riferimento al testo in esame, al fine di apportare quelle correzioni necessarie per rendere il d.lgs. 231/2007 compatibile con il rinnovato quadro normativo in materia di protezione dei dati personali, si svolgono di seguito le seguenti ulteriori osservazioni che tengono conto di quelle contenute nel citato parere e non recepite.

5.1. Garanzie per le comunicazioni di dati personali all'UIF da parte dei soggetti obbligati.

5.1.1. Modalità di comunicazione dei dati.

Premesso che lo schema in oggetto non interviene sulla configurazione dei flussi di dati personali tra i soggetti obbligati e l'UIF, rimane la criticità già rilevata con il parere reso da questa Autorità il 9 marzo 2017 relativa anche alla conseguente costituzione presso l'UIF della banca dati delle segnalazioni di operazioni sospette.

L' art. 6, comma 4, lett. d) del d.lgs. 231/2007, nell'affidare all'UIF il compito di emanare *"istruzioni, pubblicate nella Gazzetta Ufficiale della Repubblica italiana, sui dati e le informazioni che devono essere contenuti nelle segnalazioni di operazioni sospette e nelle comunicazioni oggettive, sulla relativa tempistica nonché sulle modalità di tutela della riservatezza dell'identità del segnalante"*, non contempla l'adozione di garanzie e misure in termini di protezione dei dati personali. Una disposizione di siffatto tenore non appare ancor più conforme alla rinnovata disciplina in materia di protezione dei dati personali che, al contrario, impone che il diritto degli Stati membri, nel prevedere un obbligo legale in capo a titolari del trattamento (art. 6, par. 1, lett. c), del Regolamento), dovrebbe contenere disposizioni specifiche tra cui misure atte a garantire un trattamento lecito e corretto, ai sensi dell'art. 6, par. 3, lett. b), del Regolamento; art. 2-*ter* del Codice). Occorre, quindi, introdurre una disposizione che preveda, tra gli obblighi dell'UIF, anche quelli di individuare misure idonee a garantire la protezione dei dati personali nelle comunicazioni dei dati da parte dei soggetti obbligati all'UIF e sulla tenuta e gli accessi alla banca dati: qualora si intenda rinviare tale disciplina a un apposito atto attuativo, questo dovrà essere adottato, sentito il Garante, ai sensi dell'articolo 36, par. 4, del Regolamento.

5.1.2. Obblighi di adeguata verifica della clientela.

L'art. 18 del d.lgs. 231/2007 non è oggetto di modifica da parte dello schema in oggetto. Restano quindi ferme le criticità già rilevate nel parere del 2017, in base alle quali è necessario che la descrizione degli obblighi di adeguata verifica della clientela debba avvenire in termini precisi e conformi alla direttiva europea, al fine di trattare i soli dati necessari rispetto alle finalità perseguite, con modalità proporzionate, sia per quanto riguarda l'identificazione del cliente o del "titolare effettivo", sia in relazione alla valutazione del "rischio" di riciclaggio e di finanziamento del terrorismo, nel pieno rispetto del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c), del Regolamento. A ciò si aggiunga che il comma 1, lett. a), del medesimo art. 18 comporta, tra tali obblighi di verifica, attività fra le quali è compresa

l'identificazione del cliente e la verifica della sua identità, sulla base di documenti, dati o informazioni ottenuti da una *"fonte affidabile e indipendente"* (art. 18, comma 1, lett. a), dello schema): come evidenziato nel parere reso nel 2017, tale espressione è troppo vaga e deve essere precisata esplicitando che il trattamento dei dati da parte della "fonte" è ammessa solo nel rispetto del principio di liceità, correttezza e trasparenza di cui agli artt. 5, par. 1, lett. a) e 6, par. 1, lett. c), del Regolamento, nonché dell'art. 2-*ter* del Codice.

5.1.3 Indicatori di anomalia e profilo di rischio.

Non risultano oggetto di modifica, da parte dello schema in questione, neanche le disposizioni di cui all'art. 6, comma 4, lett. e), 7, comma 2, lett. a), 15 e 35 del d.lgs. 231/2007, le quali, imponendo ai soggetti obbligati una "profilazione" (adeguata verifica) della clientela, pongono particolari problemi di compatibilità con la disciplina in materia di protezione dei dati personali, non rilevati in sede di espressione del precedente parere poiché nel 2017 il Regolamento non era applicabile.

L'art. 6, comma 4, lett. e), affida all'UIF il compito, *"al fine di agevolare l'individuazione delle operazioni sospette, [di emanare e aggiornare] periodicamente, previa presentazione al Comitato di sicurezza finanziaria, indicatori di anomalia, pubblicati nella Gazzetta Ufficiale della Repubblica italiana e in apposita sezione del proprio sito istituzionale"*; in base all'art. 35, comma 1, i soggetti obbligati utilizzano suddetti indicatori per valutare il sospetto circa le operazioni compiute – anche desumendolo *"dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza conosciuta, in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita"* – e conseguentemente procedono alla segnalazione all'UIF; l'art. 15 stabilisce regole generali in base alle quali i soggetti obbligati effettuano la valutazione del rischio di riciclaggio e finanziamento del terrorismo; infine, l'art. 7, comma 2, lett. a), parametra la frequenza e l'intensità dei controlli e delle ispezione di vigilanza, da parte delle autorità di vigilanza, *"in funzione del profilo di rischio, delle dimensioni e della natura del soggetto obbligato vigilato"*.

Al riguardo, si osserva che la platea dei soggetti obbligati comprende numerose categorie di titolari (operatori finanziari, liberi professionisti, ecc.), cui si aggiungono le pubbliche amministrazioni.

Sulla base delle citate disposizioni i predetti titolari del trattamento sono tenuti a valutare la propria clientela attraverso trattamenti automatizzati consistenti nella profilazione sistematica secondo gli elementi di rischio identificati dall'UIF, i cui esiti saranno resi disponibili alle autorità di vigilanza di settore che devono esercitare i loro poteri di controllo sulla base di un modello *risk based*, determinando la frequenza e l'intensità dei controlli e delle ispezione di vigilanza sulla base dei profili di rischio.

I trattamenti di adeguata verifica della clientela, che presentano un rischio elevato per i diritti e le libertà degli interessati, sono effettuati da soggetti obbligati sulla base di un obbligo legale che deve trovare fondamento in una base giuridica idonea ai sensi del Regolamento (art. 6, parr. 1, lett. c), e 3).

Tale considerazione vale anche per la base giuridica che affida alle autorità di vigilanza di settore il compito di effettuare le attività di controllo attribuendo un profilo di rischio ai soggetti obbligati, anche persone fisiche, per determinare la frequenza e l'intensità dei controlli (art. 6, parr. 1, lett. e), e 3).

Inoltre, tali tipologie di trattamenti, che presentano rischi elevati, comportano una necessaria valutazione di impatto sulla protezione dei dati personali per individuare le opportune garanzie da introdurre a tutela dei diritti e le libertà degli interessati (art. 35 del Regolamento e Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati – WP 248, del 4 ottobre 2017).

L'individuazione di tali misure di garanzia, nel caso di specie, si rende ancor più indispensabile in considerazione del fatto che i soggetti obbligati e le autorità di vigilanza di settore, in qualità di titolari del trattamento, si troverebbero a trattare dati personali in assenza di un'idonea base normativa.

In proposito si osserva, inoltre, che tipologie di trattamento come quelle in esame, suscettibili di introdurre processi decisionali automatizzati, sono consentite solo in presenza di una previsione normativa che precisi misure adeguate a tutela dei diritti e dei legittimi interessi dell'interessato (art. 22, par. 2, lett. b), del Regolamento).

Si rende pertanto indispensabile definire nella base giuridica le misure di garanzia, sia in riferimento alla formulazione degli indicatori di anomalia che alla creazione di profili di rischio. Esse potrebbero essere individuate all'interno dello schema in esame o, più verosimilmente, di un atto attuativo da adottarsi sentito il Garante. Su tale atto sarebbe opportuno, peraltro, effettuare la valutazione di impatto generale ai sensi dell'art. 35, par. 10, del Regolamento, evitando così che tale adempimento ricada sui singoli titolari, quantomeno nei suoi aspetti di carattere generale.

5.2 Banche dati accessibili da parte dell'UIF.

Permangono le medesime criticità, già evidenziate nel parere del 2017, anche con riferimento al comma 6 del già citato art. 6 il quale specifica che, per l'esercizio delle funzioni di cui ai commi precedenti, la UIF si avvale dei *"dati contenuti nell'anagrafe dei conti e dei depositi di cui all'art. 20, comma 4 della legge 30 dicembre 1991, n. 413 e nell'anagrafe tributaria di cui all'articolo 37 del decreto-legge 4 luglio 2006 n. 223..."*. Al riguardo, visto il carattere di revisione organica della disciplina antiriciclaggio anche da parte dello schema in esame, si rafforza la già sottolineata esigenza di riformulare tale periodo, in considerazione delle intercorse modifiche normative che hanno ampliato i dati sui rapporti finanziari conoscibili dall'UIF. In primo luogo, risulta impreciso richiamare l'*"anagrafe dei conti e dei depositi"*, che, seppur disciplinata anche dal d.m. n. 269/2000, su cui il Garante ha espresso il proprio parere in data 18 novembre 1999, per quanto di conoscenza di questa Autorità, non è stata implementata. L'art. 9, comma 6, lett. a), del decreto, definisce, invece, in maniera rispondente al quadro normativo vigente la medesima banca dati oggetto di consultazione *"dati contenuti nella sezione dell'anagrafe tributaria di cui all'articolo 7, commi 6 e 11 del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, come modificato dall'articolo 37, comma 4, del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248"*(c.d. ADR). Inoltre, l'Uif risulta abilitato a consultare, non solo i dati relativi all'esistenza dei rapporti finanziari contenuti nell'apposita sezione Archivio dei rapporti finanziari dell'Anagrafe tributaria, di cui alle predette disposizioni, ma anche i c.d. dati contabili (ad esempio, saldi e giacenza media) (cfr. combinato disposto dagli artt. 7 del d.P.R. 29 settembre 1973 e dell'art. 11 commi 2, 3 e 4 del decreto legge 6 dicembre 2011 n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011 n. 214, e, da ultimo, Provvedimento del Direttore dell'Agenzia delle entrate n. 18269/2015

del 2015). L'ADR, rispetto alla sua prima costituzione, risulta oggi ampliato, sia in termini di tipologia di rapporti oggetto di comunicazione da parte degli operatori finanziari, che di quantità di informazioni relative al rapporto. Pertanto, la corretta formulazione dell'art. 6, comma 6, dovrà riportare gli esatti riferimenti normativi, evidenziando che possono essere consultati anche i dati contabili in aggiunta *"ai dati contenuti nella sezione dell'anagrafe tributaria di cui all'articolo 7, commi 6 e 11 del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, come modificato dall'articolo 37, comma 4, del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248, comprese le informazioni di cui all'art. 11, comma 2, del decreto legge 6 dicembre 2011, n. 201 convertito, con modificazioni, dalla legge 22 dicembre 2011 n. 214"*. Tale esigenza si rende ancor più stringente alla luce del rinnovato quadro giuridico in materia di protezione dei dati personali, che impone come un trattamento di dati personali, necessario per l'esecuzione di un compito di interesse pubblico, sia fondato su una base giuridica chiara e conforme alla disciplina in parola (art. 6, par. 1, lett. e), e par. 3, lett. b), del Regolamento; art. 2-*ter* del Codice) e sia trasparente, con misure appropriate, nei confronti degli interessati (art. 14, par. 5, lett. c)).

5.3. Consultazione dell'archivio SCIPAFI e altre indeterminate procedure di verifica dell'identità.

L'art. 19, comma 1, lett. b), secondo periodo, del d.lgs. 231/2007 non è oggetto di modifica da parte dello schema in oggetto; rimane quindi attuale il rilievo del Garante, avanzato nel parere del 2017, con il quale veniva richiesta l'introduzione di un rinvio a un atto di natura regolamentare che disciplini la consultazione del sistema pubblico per la prevenzione del furto di identità di cui d. lgs. 11 aprile 2011, n. 64 (sistema c.d. SCIPAFI), al fine di effettuare il riscontro sulla veridicità dei dati identificativi forniti dal cliente per adempiere agli obblighi di adeguata verifica. Si rende infatti necessario specificare i presupposti, le categorie di soggetti che vi possono accedere, le procedure di abilitazione dei soggetti obbligati e i dati oggetto di riscontro per la verifica della veridicità dei dati forniti, a maggior ragione sulla base del nuovo quadro giuridico in materia di protezione dei dati personali, secondo cui la base giuridica richiesta dall'art. 6, par. 3, lett. b), del Regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-*ter* del Codice). Si ripropone, dunque, l'introduzione di una disposizione di questo tenore: *"Con decreto del Ministro dell'economia e delle finanze, da adottarsi previo parere del Garante per la protezione dei dati personali, sono individuati i presupposti, le categorie di soggetti che vi possono accedere, nonché il processo di rilascio delle credenziali, i profili di accesso ai dati, le procedure di autenticazione, di registrazione e di analisi degli accessi e delle operazioni per il predetto sistema per la verifica della veridicità dei dati forniti"*.

Anche l'art. 19, comma 1, lett. b), terzo periodo, del d.lgs. 231/2007 non è oggetto di modifica da parte dello schema in oggetto, per cui si continua a registrare la mancata individuazione delle banche dati pubbliche consultabili alternative al sistema SCIPAFI, come già richiesto dal Garante, invece, nel parere del 2017: mantenere questa fonte ulteriore di acquisizione dei dati violerebbe il principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c), del Regolamento, in quanto comporterebbe una duplicazione di flussi di dati, eccedente e non proporzionata, tenendo conto del fatto che già SCIPAFI consente la verifica dei dati con numerose banche dati pubbliche, anche ad accesso riservato. Inoltre, la medesima disposizione non è chiara laddove sembra voler attribuire ai gestori di identità SPID ed EIDAS un ruolo nella verifica dell'identità di soggetti diversi dai richiedenti delle suddette tipologie

di identità digitali: tali gestori non sono infatti certificatori di identità rilasciate in base a qualsiasi sistema conosciuto, ma gestori (e quindi eventualmente certificatori) unicamente di quelle digitali rilasciate in ambito SPID o EIDAS.

5.4. Misure di sicurezza per comunicazione e conservazione dei dati.

L'art. 32, comma 1, del d.lgs. 231/2007, non oggetto di modifica da parte dello schema in parola, prescrive ai soggetti obbligati di *"adottare sistemi di conservazione dei documenti, dati e informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di dati personali"*. Come già rilevato nel parere del 2017, si ritiene opportuno evidenziare che, al fine di rendere il trattamento conforme a quanto stabilito con il Regolamento:

- i soggetti che trattano i dati devono essere scelti dai soggetti obbligati sulla base di elevati requisiti di idoneità soggettiva in termini di affidabilità e competenze, preferibilmente tra coloro che abbiano un rapporto stabile con essi; qualora si tratti di soggetti chiamati ad effettuare un trattamento per conto dei medesimi soggetti, questi devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato (art. 28, par. 1, del Regolamento);
- anche in considerazione delle dimensioni del soggetto obbligato, devono essere adottati meccanismi di cifratura e di sicurezza, rispettivamente finalizzati a proteggere le informazioni contenute nei file e ad assicurare l'integrità del contenuto e a prevenirne alterazioni (art. 32 del Regolamento);
- l'accesso alle informazioni in tutte le fasi del trattamento, anche dopo la cifratura, deve essere circoscritto, per impostazione predefinita, ad un numero il più possibile limitato di persone sottoposte all'autorità del titolare (art. 25, par. 2, del Regolamento);
- qualora i soggetti obbligati decidano di affidare la comunicazione a soggetti esterni, designati responsabili del trattamento o persone sottoposte all'autorità del titolare (artt. 28 e 29 del Regolamento; art. 2-*quaterdecies* del Codice), i dati devono essere loro forniti già cifrati.

5.5. Ruolo assunto dal soggetto esterno.

L'art. 32, comma 3, del d.lgs. 231/2007, non oggetto di modifica da parte dello schema in parola, consente ai soggetti obbligati di avvalersi di un autonomo centro di servizi, ovvero di un soggetto esterno, per la conservazione di documenti, dati e informazioni, *"purché sia assicurato ai soggetti obbligati l'accesso diretto e immediato al sistema di conservazione"*. Con riferimento al ruolo assunto dal centro di servizi rispetto al trattamento dei dati personali, e come già rilevato nel parere del 2017, si ritiene opportuno evidenziare, in conformità al Regolamento, che:

- tale soggetto, che deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato, deve essere preventivamente designato quale responsabile del trattamento ai sensi dell'art. 28 del Regolamento;
- devono essere fornite a tale soggetto adeguate istruzioni, tramite il contratto o altro atto giuridico di cui all'art. 28, par. 3, del Regolamento, e deve vigilare sul trattamento da effettuare, con particolare riguardo alle ipotesi in cui tale soggetto sia designato responsabile

da più soggetti obbligati, al fine di garantire misure di carattere tecnico e organizzativo volte ad assicurare la segregazione dei flussi con ciascun soggetto.

TUTTO CIÒ PREMESSO IL GARANTE

esprime parere nei termini di cui in motivazione sullo schema di decreto legislativo recante modifiche ed integrazioni ai decreti legislativi 25 maggio 2017, n. 90 e 92, recanti attuazione della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015, nonché attuazione della direttiva 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, con le osservazioni di cui ai punti 4 e 5.

Roma, 24 luglio 2019

IL PRESIDENTE

IL RELATORE

IL SEGRETARIO GENERALE