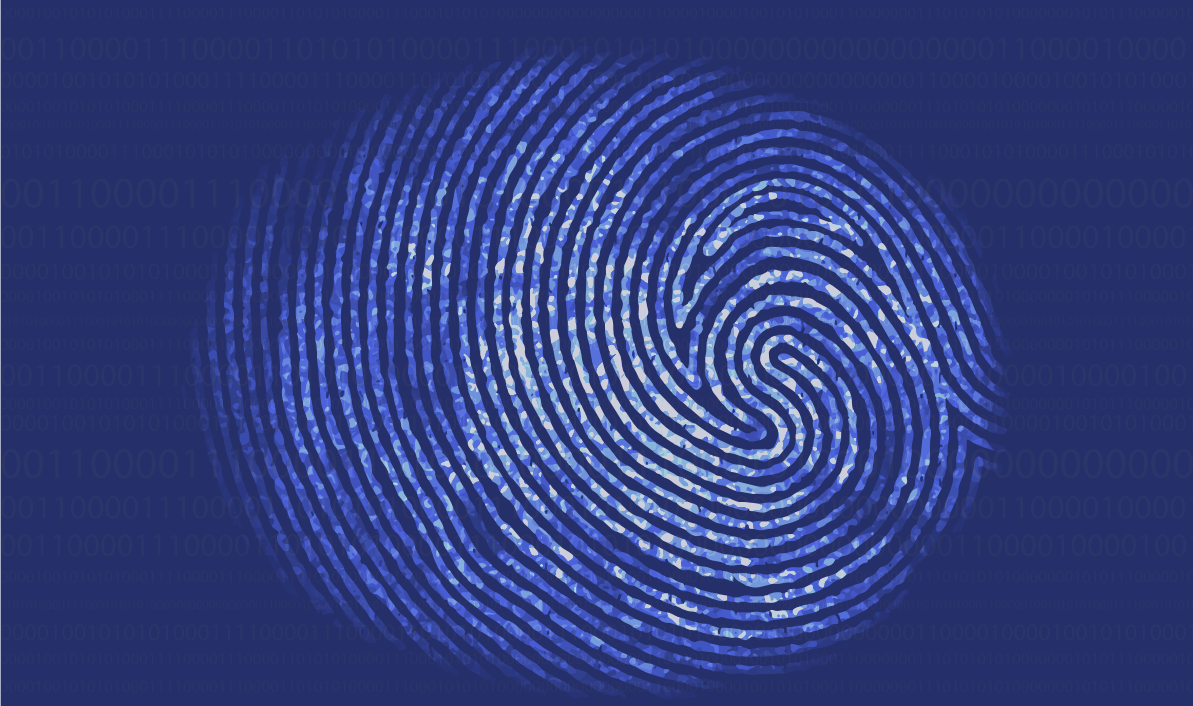
CONSIGLIO NOTARIALE
DI BERGAMO

Identità, privacy e antiriciclaggio: linee guida per notai e professionisti



Venerdì 16 novembre 2018 | Bergamo
Centro Congressi Giovanni XXIII

ATTI DEL CONVEGNO

INTRODUZIONE AI LAVORI

Cari Colleghi, e cari amici delle professioni vicine al notariato,

nella giornata odierna, come sapete, per volontà del Consiglio Notarile di Bergamo, trattiamo argomenti utili alle professioni e di attualità.

Va certamente premesso che la scelta degli argomenti (truffe immobiliari fondate sui furti di identità, nuovi adempimenti in materia di tutela della privacy dei clienti e di antiriciclaggio) è stata *coraggiosa*: non si tratta di argomenti "leggeri"; non è piacevole occuparsene perché *risaltano i profili di responsabilità*, civile e penale, ed anche, come vedremo, disciplinare.

Ma la prospettiva nella quale affronteremo questi temi, difficili, insidiosi sarà diversa: cercheremo, il più possibile, di dare *indicazioni operative* sul "cosa fare in concreto" per prevenire rischi e rispettare le norme.

Il primo argomento, che affronteremo nella mattinata, è quello dei furti di identità e delle truffe in ambito immobiliare. Statisticamente, parliamo di una percentuale infinitesimale rispetto al totale delle transazioni immobiliari. Ma, quando è capitato, l'effetto è stato dirompente. Scoprire che chi ha sottoscritto un atto notarile è un delinquente che ha esibito documenti falsi fa male al notaio, molto male.

Il notariato, è noto a tutti, ha tra le sue funzioni prevalenti la *garanzia di legalità* nell'area negoziale e contrattuale, nei settori connessi alla pubblicità legale (gli immobili e l'Agenzia del Territorio; le imprese, gli altri enti commerciali, le società ed il Registro delle Imprese). Scoprire che si è coinvolti, direi pressocchè sempre in buona fede, in reati di falso è doloroso: gli accertamenti della magistratura e della polizia giudiziaria, come vedremo, tendenzialmente escludono la responsabilità penale, e nella maggior parte dei casi anche quella civile. Ma essere coinvolti, difendersi dalle accuse di responsabilità non piace (per usare un eufemismo).

Quindi oggi ascolteremo dalle voci dei protagonisti di questi accertamenti cosa è accaduto, e rivolgeremo ad essi delle domande per capire cosa, in concreto, si può fare per prevenire simili episodi. Non mancherà un cenno a quanto è accaduto e tuttora accade in Paesi che devono contrastare il fenomeno (dei furti di identità) che si è manifestato in modo rilevantissimo, non sussistendo il sistema di identificazione e controlli di legalità (affidato ai notai) simile al nostro.

Il secondo argomento che proponiamo alla vostra attenzione riguarda l'informativa sul trattamento dei dati, sui diritti che il cliente del notaio ha in relazione al

trattamento, su questo dovere di trasparenza ed informazione: la novità, sul punto, sono rappresentate dal GDPR (la sigla corrisponde alle parole General Data Protection Regulation) che è un regolamento (il numero è 679/2016) attraverso il quale la Commissione Europea intende rafforzare la protezione dei dati personali di cittadini dell'Unione Europea. Il testo è stato adottato il 27 aprile 2016, è efficace a partire dal 25 maggio 2018. In quel documento, e nei documenti che da esso derivano si rafforza l'affermazione dell'obbligo di *informazione* sulle *finalità* del trattamento, sulle sue *modalità* ma anche sui *diritti* che l'interessato ha. Ciò significa, come vedremo, garantire sicurezza, e questa garanzia richiede organizzazione e formazione.

Ma il terzo argomento, l'antiriciclaggio, è senz'altro il più difficile e delicato. Molto ci sarebbe da dire, a seguito dell'adozione delle Regole Tecniche da parte del Consiglio Nazionale del Notariato (e sappiamo che anche gli altri Ordini professionali a noi vicini stanno lavorando per dare indicazioni ai loro iscritti). Mi limiterò a tre osservazioni. La prima: è giusto che i professionisti diano il loro contributo al contrasto alla criminalità, ai fenomeni di riciclaggio e finanziamento del terrorismo: si tratta solo di capire *come* devono farlo e quali sono *i mezzi* a loro disposizione. La seconda: non ha senso non differenziare, a livello normativo, il mondo delle professioni dalle grandi organizzazioni bancarie e finanziarie. Non si può pretendere dal singolo professionista una organizzazione ed un sistema di controlli analogo a quello di una società quotata in borsa. La terza: questo argomento, forse ancora di più, rispetto alla tutela della privacy, richiede una organizzazione negli studi professionali, un sistema di regole interne e di controlli, che richiede impegno e formazione (del professionista innanzitutto e dei collaboratori in seconda battuta). Oggi di questo parleremo, cercando, il più possibile, di dare indicazioni operative.

Ringrazio i relatori per la disponibilità, ed il Consiglio Notarile di Bergamo per il supporto all'iniziativa di formazione: in particolare, il presidente Maurizio Luraghi, i consiglieri Sara Carioni (senza la quale non avremmo avuto questa partecipazione di relatori di alto profilo) e Marco Ruggeri, tutti preziosi nella organizzazione.

Buon congresso a tutti.

Guido De Rosa
responsabile scientifico dell'evento

INDICE

Le truffe immobiliari

pag. 7 Un sommario di giurisprudenza sull'argomento (Cass. civ., sez. 1, n. 28823, 30/11/2017; Tribunale di Nola, Sez. Penale - comp. collegiale, n. 2733, 21/12/2017; Tribunale di Pisa, Sez. Penale - comp. Monocratica, n. 762, 30/04/2012; Tribunale Roma, sez. XIII civile, 05/06/2006; Tribunale di Napoli, sez. GUP, 30/04/2010);

pag. 13 La sentenza 28823/2017 della Corte di Cassazione in versione integrale;

pag. 19 La sentenza del Tribunale di Monza (Tommasi vs Italfondiario) n. 1973/2017 pubblicata il 22/06/2017 RG n. 9329/2014;

La "privacy" negli studi professionali

pag.31 Il DECRETO LEGISLATIVO 10 agosto 2018, n. 101: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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). (18G00129) (GU n.205 del 4-9-2018) in vigore dal 19 settembre 2018;

pag. 87 Gea Arcella, notaio componente commissione informatica del CNN: "Privacy e Notaio", ovvero una introduzione ai temi della tutela della riservatezza, alla funzione notarile, agli obblighi di informazione, al trattamento e alla protezione dei dati;

pag. 91 Gea Arcella, notaio, componente commissione informatica del CNN: Il vademecum su "La protezione dei dati personali nello studio notarile alla luce del Regolamento Europeo (GDPR)";

pag. 105 Roberto Lattanzi, Dirigente del Servizio Studi Autorità Garante della Privacy: il "Diritto alla protezione dei dati di carattere personale" (2010);

pag. 147 Parere 3/2010 sul principio di responsabilità, adottato il 13 luglio 2010, a cura del Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE (organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE);

pag. 167 Garante Privacy: Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 - G.U. n. 287 del 9 dicembre 2008

pag. 173 Garante Europeo Privacy: Parere del 14 aprile 2010, a proposito della Direttiva Europea 95/46/CE, sulla tutela della riservatezza dei dati personali in relazione allo smaltimento di apparecchi elettronici;

INDICE

L'antiriciclaggio

pag. 179 Le regole tecniche adottate dal Consiglio Nazionale del Notariato in attuazione del D.Lgs. 25 maggio 2017 n. 90;

pag. 187 Sara Carioni e Vincenzo Gunnella, notai Componenti della Commissione Antiriciclaggio CNN: il commento alle regole tecniche del CNN alla luce del parere del Comitato di Sicurezza Finanziaria;

pag. 215 Vincenzo Gunnella e Laura Piffaretti, notai Componenti della Commissione Antiriciclaggio CNN: "Le regole tecniche del CNN e le buone prassi organizzative".

CASS. CIV., SEZ. 1, N. 28823, 30/11/2017

«Il Tribunale di Busto Arsizio, sezione distaccata di Saronno, con sentenza del 16 settembre 2008, dichiarava la responsabilità professionale del notaio D.S., condannandolo al risarcimento del danno: il predetto era riconosciuto responsabile della erronea identificazione di tale M.A., mutuatario di una somma erogata da Intesa Sanpaolo s.p.a. per l'acquisto di un immobile. Nell'occasione il Tribunale rilevava che l'identificazione del falso M. - successivamente identificato in A.G. - era stata compiuta dalla segretaria del notaio sulla base di una carta di identità risultata poi contraffatta e che il professionista al momento del rogito non aveva rinnovato la richiesta di esibizione del documento, che nel frattempo era stato sequestrato in occasione del tentativo di aprire presso altra banca un conto corrente a nome M. [...]

Nella fattispecie - spiega l'istante - risultava provato che il notaio D., al momento della formazione dell'atto di cui si controverte, non aveva potuto procedere all'esame del documento d'identità, che era stato già sequestrato dai carabinieri: a quella data, infatti, il professionista disponeva solo della fotocopia del predetto documento, esibito alla coadiutrice dello studio. [...]

Ora, la Corte di appello di Milano ha evidenziato che il notaio aveva raggiunto una propria certezza circa l'identità del comparente sulla scorta di plurimi elementi: il sedicente M. era stato presentato al professionista dai responsabili di un'agenzia immobiliare e da un commercialista da tempo conosciuti; la banca aveva affidato la pratica del mutuo al professionista, incaricandolo di redigere la relazione notarile preliminare e trasmettendo allo stesso controricorrente la documentazione a tal fine necessaria oltre che la bozza del contratto di mutuo nella quale figuravano le generalità false dell'aspirante mutuatario; il finanziamento era stato deliberato dalla banca a seguito di una istruttoria sulla persona del futuro contraente, soggetto che l'istituto di credito per legge aveva l'obbligo di identificare; Intesa aveva comunicato al notaio l'approvazione della delibera del mutuo e l'apertura di un conto corrente a nome dello stesso M.; la stipula degli atti notarili era avvenuta col concorso di varie persone, tra cui lo stesso direttore della banca, che si erano intrattenuti con il sedicente M. in atteggiamenti di familiarità e confidenza; la carta d'identità e il codice fiscale del mutuatario esibiti alla segretaria del notaio, che ne aveva estratto copia, non presentavano alterazioni o altre anomalie tali da giustificare un sospetto di falsificazione. A tale corredo di elementi non vale contrapporre il dato della mancata visione, da parte del notaio, dell'originale del documento di identità, di cui all'epoca lo stipulante non era più in possesso (ma di cui la collaboratrice del professionista aveva in precedenza estratto copia). [...]»

TRIBUNALE DI NOLA, SEZ. PENALE - COMP. COLLEGIALE, N. 2733, 21/12/2017

ESTRATTO IMPUTAZIONE: «**A)** delitto p.p. dall'art. 110-640, 61 n. 7 c.p. poiché in concorso con persone allo stato non identificate, mediante artifici e raggiri consistiti nello stipulare presso la concessionaria MIRA spa di Cercola il contratto di finanziamento n. 3807096 del 21.12.2009 dell'importo di euro 12.067,00 per l'acquisto dilla FIAT

Panda tg. (omissis), a nome dell'ignaro D.E. nato a Napoli il (omissis), e utilizzando documenti d'identità, tessera sanitaria e busta paga contraffatti, apparentemente intestati al D.E.; **[...]** quindi, in data 13.7.2010 formalizzavano e trascrivevano, anchecon atto notarile, e presso l'agenzia HERMES s.n.c. di Pomigliano d'Arco, un ulteriore passaggio di proprietà da M.G. a S.F., Zio del D.A., il quale - su richiesta di quest'ultimo e ignaro della provenienza illecita del veicolo - accettava di intestare a se stesso l'autovettura, che sarebbe stata in realtà destinata al D.A. stesso e a sua madre A.P., ove l'auto veniva effettivamente rinvenuta e sequestrata.»

Estratto motivazione:

«Infine la medesima automobile Fiat Panda recante targa (omissis) veniva venduta il 13.7.2010 da M.G. a S.F. presso la società Hermes s.n.c. di C.M. sita in Pomigliano D'Arco alla via R. (verbale cit. p.32 nonché copia dei registi dell'agenzia pratiche auto di Castello di Cisterna in cui emerge che in data 13.7.2010 il committente "S.F." faceva richiesta di trasferimento di proprietà in suo favore, nonché certificato PRA, atto di trasferimento di proprietà con CDP e visura PRA in atti), mediante formalizzazione del trasferimento con atto pubblico a firma del notaio P. (in atti).

Il ricorso all'atto pubblico si era necessario stante lo stato di analfabeta della M.

La circostanza indicata veniva peraltro confermata, come anticipato, da C.G., socio della società Hermes snc che si era occupata del passaggio di proprietà dal M. al S. (cfr. dichiarazione, sul punto acquisite ex art. 493, III comma c.p.p.) nonché dal notaio P., che aveva stipulato l'atto di trasferimento tra la M. e il S. (vedi infra).

Il C., invero, precisava che - stante il fatto che la M. era analfabeta - l'atto di vendita era stato stipulato davanti al notaio P. con studio in C. e non mediante autentica presso lo sportello telematico della società, come invece è prassi. Presso il notaio la M. era stata accompagnato da un giovane, P.V., notaio che aveva curato l'atto di trasferimento dell'automobile che ci occupa dalla M. al S., confermava in dibattimento la circostanza dello stato di analfabetismo della M. tanto che la sottoscrizione del contratto era avvenuta alla presenza di due testimoni (cfr. atto notarile, in atti).»

Tribunale di Pisa, Sez. Penale - comp. Monocratica, n. 762, 30/04/2012

Estratto imputazione: « a) del reato di cui all'art. 110, 624,61 n. 2 e 11 c.p. per essersi, in concorso tra loro, impossessati della patente di guida di R.C. e di un assegno bancario in bianco n. ...-07 tratto sul c/c N. 8205 della Carisap di Ascoli Piceno [...]

b) del reato di cui agli art.110-477-482 C.P., 61 n. 2 c.p., per avere, in concorso tra loro e con soggetto allo stato ignoto, alterato la patente di guida di R.C. cui sostituivano, allo scopo di commettere il reato di cui al capo c), la foto[...]

c) del reato di cui all' art. 110 - 48 - 479 c. p. per avere, in concorso tra loro e con soggetto allo stato ignoto , indotto il Notaio R.R. a compiere falsità ideologica in atti pubblici e segnatamente ad attestare falsamente di avere ricevuto la dichiarazione di R.C. il quale nominava C.B. suo procuratore generale, mentre in realtà presso il notaio si presentava (esibendo la patente di guida del R. che era stata alterata mediante sostituzione della foto) e sottoscriveva detta procura soggetto diverso dall' interessato, accompagnato da R.A., che aveva preventivamente preso contatti con il notaio e presenziava alla lettura del documento.

d) del reato di cui agli artt. 110 c.p. 640 c.p. , 61 n. 7 c.p. , per essersi in concorso tra loro e con soggetto allo stato ignoto, procurati un ingiusto profitto con artifizi e raggiri

consistiti nel determinare in stato di incapacità . Carlo (tramite l'assunzione di rilevanti quantità di benzodiazepina) e ponendo in essere le condotte meglio descritte ai superiori capi di imputazione, così svuotavano il patrimonio della P.O. attraverso:

- l'emissione a favore del figlio R.A. dell'assegno bancario n.

...-07 tratto sul c/c N. ... della Carisap di Ascoli Piceno

dell'importo di euro 50.000/00 ;

- la sottoscrizione di una falsa Procura Generale a favore di C.B. (moglie da cui aveva divorziato nel 1989), redatta avanti al notaio R. di S.G., la quale procedeva a gravare di ipoteche tutti gli immobili di proprietà della P.O. a garanzia dei seguenti debiti: mutuo dell'importo di euro 1.800.000/00 acceso alla società Dolomiti S.r.l. con amministratore unico R.A., mutuo importo di euro 1.100.000/00 acceso alla società Dolomiti S.r.l., apertura di credito 1.117.000,62 acceso dalla associazione Italiana di Turismo Sociale per l'Europa.»

Estratto motivazione:

«apprendeva che risultava da lui emesso un assegno in favore del figlio Andrea e rilasciata una procura generale in favore della C.; che nulla sapeva sia dell'assegno che dell'atto notarile in favore della ex moglie, negando tassativamente di averli sottoscritti; che successivamente scopriva che sugli immobili di sua proprietà erano state accese tre ipoteche a garanzia di due mutui (uno dell'importo di un milione ed ottocentomila euro, l'altro di un milione e centomila euro) e di una apertura di credito in favore di società riconducibili ai figli ed all'ex moglie (la Dolomiti s.r.l. e l'Associazione Italiana Turismo Sociale per l'Europa); che, fatto ritorno ad Ascoli Piceno, gli veniva diagnosticato un meningioma. Il teste ha poi disconosciuto come proprie le sottoscrizioni apposte in calce all'assegno ed alla procura generale che gli sono stati mostrati dal P. M. e non si è riconosciuto nella fotografia apposta sulla patente di

guida a lui intestata, che gli è stata mostrata in fotocopia (e che fu sequestrata presso lo studio del notaio R., dove fu rinvenuta allegata alla procura generale), mentre ha riconosciuto come propria la fotografia della carta di identità, che ebbe a recuperare per mezzo del suo legale (al quale fu consegnata dalla figlia Chiara che la aveva rinvenuta in quel di Udine, dove la stessa vive, in circostanze a dir poco sospette). [...]

R. A., il notaio che redasse la procura generale in favore della C., ha dichiarato che tale geometra B. (poi escusso come teste di riferimento), tecnico con cui spesso collaborava, gli telefonò dicendogli che un suo conoscente aveva il padre in precarie condizioni di salute (...si trovava in pessime condizioni di salute, mi sembra addirittura terminali, così mi fu detto - cfr. verbale stenotipico dell'udienza del 14/6/11, fol. 34) e che per tale motivo voleva conferire una procura generale alla moglie; che, a fronte della sua disponibilità a recarsi in ospedale per raccogliere la volontà del malato, gli fu riferito che non ce ne era necessità, in quanto il paziente sarebbe uscito dall'ospedale proprio per la redazione della procura; che vennero nel mio studio tre persone, di cui il R. o sedicente tale, accompagnato dalla moglie e dal figlio e che procedetti alla identificazione attraverso la presentazione che il geometra B. mi aveva fatto del figlio e, quindi, il figlio che mi presentò il padre e poi con l'esibizione di un documento di identità ... del R., cioè di colui che avrebbe dovuto sottoscrivere la procura (cfr. verbale stenotipico dell'udienza del 14/6/11, foll. 35, 36); che la persona che aveva di fronte era la stessa effigiata nella fotografia apposta sulla patente di guida di cui fu fatta la fotocopia, poi allegata all'atto pubblico. [...]

Per i fatti di cui al capo C), inoltre, a carico degli imputati vi è anche la copia della patente di guida allegata alla procura generale e sequestrata nello studio del notaio, che prova in maniera inequivoca che presso lo studio del notaio R. i due imputati si recarono con un'altra persona che spacciarono per il R.C. (la foto sul documento non è quella del R. ed il pubblico ufficiale ha riferito di averlo identificato sulla base di due elementi: la dichiarazione di R.A. - a sua volta presentato al notaio da un suo collaboratore - che glielo indicò come il proprio padre ed il documento esibito, che recava una foto corrispondente alle fattezze della persona che il pubblico ufficiale aveva di fronte).»

Tribunale Roma, sez. XIII civile, 05/06/2006

Estratto motivazione:

« Il contratto stipulato tra l'acquirente di un veicolo a motore usato e l'imprenditore che cura gli aspetti amministrativi del trasferimento di proprietà è un contratto atipico misto, la cui causa partecipa tanto del mandato, quanto del contratto d'opera. Secondo la sua struttura socialmente tipica, l'acquirente assume l'obbligo del pagamento di un corrispettivo in denaro (obbligo nella specie assolto dall'attrice: cfr. all. 4 al fasc. attoreo), mentre l' "agenzia" assume l'obbligo principale di individuare il notaio cui affidare l'autentica della sottoscrizione del venditore e curare l'annotazione al P.R.A. del trasferimento di proprietà. [...]

Nel caso di specie, il convenuto P. ed i suoi incaricati (del cui operato egli risponde, ai sensi dell'art. 1228 c.c.) sono colposamente venuti meno a tale obbligo.

Essi infatti, con l'uso dell'ordinaria diligenza, avrebbero potuto agevolmente accertare:

(a) l'effettiva proprietà del veicolo, attraverso l'accesso alla banca dati telematica del P.R.A.;

(b) la falsità grossolana della carta d'identità esibita dal venditore, recante sulla prima facciata l'indicazione del comune di Roma quale ente rilasciante, e nella II facciata l'indicazione del comune di Verona;

(c) la falsità grossolana della carta di circolazione, recante tali errori di ortografia ("*famigliare*"; "*istallazzione*") da dovere indurre quanto meno un sospetto in un soggetto che professionalmente si dedica alla trascrizione delle vendite di autoveicoli.

La truffa di cui è stata vittima l'attrice è stata dunque colposamente agevolata dalla convenuta del convenuto, per quanto detto resosi inadempiente agli obblighi di buona fede scaturenti dal contratto di prestazione d'opera stipulato con l'attrice.

7. La domanda nei confronti di G.C..

Il notaio G.C. era stato incaricato, da (o su richiesta di) M.P., di autenticare la sottoscrizione apposta dal sedicente venditore del veicolo sulla dichiarazione di vendita necessaria per la trascrizione, ai sensi dell'art. 13 r.d. 29.7.1927 n. 1814.

Nell'assolvere tale incarico, il notaio ha dichiarato (cfr. all. 2, foglio 2, fascicolo attoreo) di "essere certo della identità personale" della persona che ha dichiarato essere D.F.

Nel rendere interrogatorio libero, il convenuto ha dichiarato di avere esaminato, prima di sottoscrivere la suddetta dichiarazione un solo documento d'identità del venditore.

Ciò posto *in* facto, si rileva *in iure* che la condotta del notaio è stata assai lontana dalle regole della diligenza professionale, per le ragioni che seguono.

7.1. Nel caso di specie è pacifico che al momento dell'autentica il notaio non avesse affatto la "conoscenza personale" del venditore, e quindi non poteva avere contezza della loro identità.

La sua condotta è stata dunque gravemente colposa perché, in assenza di tale certezza, si è limitato ad accertare l'identità del sottoscrittore sulla base della sola esibizione di una carta d'identità. Quest'ultima infatti è un documento agevolmente falsificabile, non di rado falsificato, e sovente falsamente redatto su moduli "in bianco" trafugati alle amministrazioni comunali.

Deve dunque escludersi che, sulla base dell'esame di questo solo documento, il notaio possa dirsi "certo" dell'identità di chi lo esibisca. In tal senso si è pronunciata la S.C., secondo la quale la certezza del notaio in ordine all'identità personale delle parti, in difetto di conoscenza personale, non può essere fondata sul solo esame di una carta d'identità, od altro documento equipollente, atteso che l'art. 49 della legge 16 febbraio 1913 n. 89 prescrive che il notaio raggiunga un sicuro convincimento in proposito con la valutazione di "tutti gli elementi" all'uopo idonei, contemplando, in caso contrario, il ricorso a due fidefacienti. Pertanto, ove manchino altri elementi, sia pure di tipo presuntivo, idonei a corroborare le risultanze della carta d'identità, l'esame di quest'ultima non può ritenersi sufficiente all'osservanza del suddetto obbligo professionale, trattandosi del resto di documento d'identificazione a fini di polizia, privo di forza certificatrice generale (esattamente *in terminis*, Cass., 17-05-1986, n. 3274, in Foro it., 1987, I, 171).»

Tribunale di Napoli, sez. GUP, 30/04/2010

Estratto motivazione:

« L'inchiesta bancaria appurava, altresì, che l'inizio dei rapporti bancari con molti dei soggetti intestatari dei mutui era coinciso con la concessione dei mutui ipotecari e che tutte le pratiche erano state istruite dal direttore ed i mutui deliberati da lui stesso, benché quattro di queste fossero di competenza di altro Ufficio centrale (Centro mutui di Milano); ma quel che più conta è il fatto che i beneficiari dei mutui avevano prelevato l'intera somma riconosciuta nell'immediatezza della concessione e non avevano onorato le rate in scadenza con autonoma provvista.

A proposito di tali pratiche di mutuo gli ispettori sottolineavano che 132 di esse erano state iniziate tramite la mediazione con la banca della srl Euroassinvest di Be.Sa., che era stato autorizzato sempre da S. ad usare le postazioni di lavoro di dipendenti per operare nelle relative procedure informatizzate. Altro dato molto interessante ma che non sembra aver avuto la dovuta attenzione nel corso dell'indagine è data dal fatto che 132 contratti di mutuo erano stati stipulati dal notaio D., che tra l'altro li aveva redatti con diversi contraenti inesistenti all'anagrafe ed i cui documenti di identità sono risultati falsi; tali soggetti erano tutti riconducibili a G. [...]

[...] vi fu emissione e/o richiesta di assegni circolari da parte di G. per oltre 120mila euro, la cui provvista proveniva, attraverso complessi movimenti ben descritti in atti, da conti intestati a detti soggetti; è interessante notare che anche un pagamento in favore del notaio D. fu effettuato con provvista rinveniente dal mutuo concesso nel predetto modo illecito a Ca.Ma.»

Archivio selezionato: Sentenze Cassazione civile

Autorità: Cassazione civile sez. I

Data: 30/11/2017

n. 28823

Classificazioni: NOTAIO E ARCHIVI NOTARILI - Responsabilità

LA CORTE SUPREMA DI CASSAZIONE

SEZIONE PRIMA CIVILE

Composta dagli Ill.mi Sigg.ri Magistrati:

Dott. AMBROSIO Annamaria - Presidente -

Dott. DI MARZIO Mauro - Consigliere -

Dott. NAZZICONE Loredana - Consigliere -

Dott. FALABELLA Massimo - rel. Consigliere -

Dott. DOLMETTA Aldo Angelo - Consigliere -

ha pronunciato la seguente:

SENTENZA

sul ricorso 14689/2013 proposto da:

Intesa Sanpaolo S.p.a., derivante dalla fusione per incorporazione della Sanpaolo Imi S.p.a. nella Banca Intesa S.p.a., in persona del legale rappresentante pro tempore, elettivamente domiciliata in Roma, Largo di Torre Argentina n.11, presso lo studio dell'avvocato Martella Dario, giusta procura speciale per Notaio avv.

A.B. di (OMISSIS);

- ricorrente -

contro

D.S., elettivamente domiciliato in Roma, Largo di Torre Argentina n. 11, presso lo studio dell'avvocato Lazzaretti Andrea, che lo rappresenta e difende unitamente agli avvocati D'Ippolito Fabio Giacomo, Mendolia Carmelo, giusta procura a margine del controricorso;

- controricorrente -

e contro

R.A.P.;

- intimato -

avverso la sentenza n. 4023/2012 della CORTE D'APPELLO di MILANO,

depositata il 11/12/2012;

udita la relazione della causa svolta nella pubblica udienza del

28/09/2017 dal cons. FALABELLA MASSIMO;

udito il P.M., in persona del Sostituto Procuratore Generale DE

AUGUSTINIS UMBERTO che ha concluso per il rigetto del ricorso;

udito, per la ricorrente, l'Avvocato Dario Martella che ha chiesto

l'accoglimento del ricorso;

udito, per il controricorrente, l'Avvocato Fabio Giacomo D'Ippolito

che ha chiesto il rigetto.

Fatto
FATTI DI CAUSA

1. - Il Tribunale di Busto Arsizio, sezione distaccata di Saronno, con sentenza del 16 settembre 2008, dichiarava la responsabilità professionale del notaio D.S., condannandolo al risarcimento del danno: il predetto era riconosciuto responsabile della erronea identificazione di tale M.A., mutuatario di una somma erogata da Intesa Sanpaolo s.p.a. per l'acquisto di un immobile. Nell'occasione il Tribunale rilevava che l'identificazione del falso M. - successivamente identificato in A.G. - era stata compiuta dalla segretaria del notaio sulla base di una carta di identità risultata poi contraffatta e che il professionista al momento del rogito non aveva rinnovato la richiesta di esibizione del documento, che nel frattempo era stato sequestrato in occasione del tentativo di aprire presso altra banca un conto corrente a nome M..

2. - In sede di gravame la pronuncia di prime cure era parzialmente riformata dalla Corte di appello di Milano. Questa, con sentenza pubblicata l'11 dicembre 2012, per quanto qui rileva, escludeva la responsabilità colpevole del notaio e rigettava le domande risarcitorie proposte nei confronti dello stesso in relazione all'erronea attestazione dell'identità dello stipulante M.A.. Il giudice dell'impugnazione osservava come la L. n. 89 del 1913, art. 49 (legge notarile), nel testo novellato con L. n. 333 del 1976, più non prevedesse la necessità che la certezza circa l'identità personale della parte stipulante costituisse "un risultato da ottenersi personalmente ed esclusivamente dal notaio" e che, inoltre, l'apprezzamento circa la responsabilità del professionista in ordine all'effettiva corrispondenza tra generalità dichiarate e generalità effettive andasse condotto avendo riguardo non solo all'esame del documento d'identità, ma anche sulla scorta della valorizzazione di altri elementi di fatto e di natura presuntiva - purchè gravi, precisi e concordanti - che avessero avuto un rilievo nella formazione del convincimento del notaio stesso. Sulla base di tali rilievi, la Corte distrettuale operava una ricognizione della complessiva situazione di fatto e giungeva alla conclusione che l'identificazione di M. da parte del notaio D. era stata conseguita senza che potesse ravvisarsi, da parte di quest'ultimo, la violazione delle regole di diligenza, prudenza e perizia professionale.

3. - La pronuncia è oggetto del ricorso per cassazione che Intesa Sanpaolo fonda su di un unico, articolato, motivo. Resiste con controricorso D.S..

Diritto
RAGIONI DELLA DECISIONE

1. - Il motivo denuncia violazione ed errata applicazione della L. n. 89 del 1913, art. 49 come modificato dalla L. n. 333 del 1976, nonchè degli artt. 1227, 2699 e 2703 c.c.. Deduce la banca che era compito del notaio rogante provvedere alla identificazione delle parti contrattuali prendendo visione dell'originale del documento d'identità dei contraenti o, in difetto di pregressa conoscenza personale degli stessi, avvalendosi di testimoni per la verifica dei dati dichiarati: all'opposto, il professionista non aveva proceduto alla identificazione dei soggetti stipulanti il contratto di mutuo. Ricorda, in particolare, la ricorrente che, ai fini dell'identificazione dei contraenti, non potesse prescindersi all'esame dall'originale della carta d'identità o di altro documento equipollente: in altri termini, il professionista era tenuto ad operare un tale riscontro anche a seguito della modificazione della disciplina introdotta la L. n. 89 del 1913, cit. art. 49. Nella fattispecie - spiega l'istante - risultava provato che il notaio D., al momento della formazione dell'atto di cui si controverte, non aveva potuto procedere all'esame del documento d'identità, che era stato già sequestrato dai carabinieri: a quella data, infatti, il professionista disponeva solo della fotocopia del predetto documento, esibito alla coadiutrice dello studio. La sentenza è inoltre censurata avendo riguardo all'applicazione dei criteri operanti in materia di concorso del fatto colposo del creditore. In particolare è contestato che il notaio non fosse tenuto a verificare l'identità del contraente per aver prestato affidamento nei rapporti di conoscenza palesatisi, in occasione del rogito, tra i funzionari dell'agenzia immobiliare e della banca e il sedicente M.. In altri termini, non era possibile, ad avviso della ricorrente, porre sullo stesso piano le eventuali negligenze che sarebbero state poste in atto dall'istituto bancario dalle più gravi mancanze di cui si era reso responsabile il professionista nella identificazione del mutuatario.

2. - Il motivo è infondato.

Il testo vigente della L. n. 89 del 1913, art. 49 è il seguente:

"Il notaio deve essere certo dell'identità personale delle parti e può raggiungere tale certezza, anche al momento della attestazione, valutando tutti gli elementi atti a formare il suo convincimento.

"In caso contrario il notaio può avvalersi di due fidefacienti da lui conosciuti, che possono essere anche i testimoni".

Il testo dell'articolo risulta mutato rispetto alla versione originaria:

"Il notaro deve essere personalmente certo dell'identità personale delle parti.

"In caso contrario deve accertarsene per mezzo di due fidefacienti da lui conosciuti, i quali possono essere anche i testimoni".

La modificazione del testo normativo si deve alla L. n. 333 del 1976, art. 1 che ha ridimensionato il dato della conoscenza personale delle parti per il notaio tenuto alla loro identificazione. Infatti, nell'attuale versione non compare più l'avverbio "personalmente" (collegato alla certezza in ordine all'identità delle parti); nel testo della disposizione vigente è inoltre precisato che la sicurezza circa l'identificazione possa conseguirsi anche al momento dell'attestazione: il che vale ad escludere la necessità del dato della pregressa conoscenza personale della parte da parte del notaio; infine, la norma novellata conferisce rilievo a "tutti gli elementi atti a formare il (...) convincimento" del professionista: con ciò chiarendo che l'acquisizione di una certezza sulla identità della parte non dipenda - o comunque possa non dipendere, in concreto - dalla conoscenza personale che il notaio abbia di quel soggetto (la quale può anche mancare) e che detta acquisizione sia anzi determinata da fatti o situazioni che non sono definibili in via astratta e generale, ma che è necessario accertare di volta in volta.

In tal senso, questa Corte è venuta affermando che il cit. art. 49 vada interpretato nel senso che il

professionista, nell'attestare l'identità personale delle parti, deve trovarsi in uno stato soggettivo di certezza intorno a tale identità, conseguibile, senza la necessaria pregressa conoscenza personale delle parti stesse, attraverso le regole di diligenza, prudenza e perizia professionale e sulla base di qualsiasi elemento astrattamente idoneo a formare tale convincimento, anche di natura presuntiva, purchè, in quest'ultimo caso, si tratti di presunzioni gravi, precise e concordanti (Cass. 10 maggio 2005, n. 9757; analogamente, nel senso che il notaio non è responsabile dei danni che taluno subisca per effetto della discordanza tra identità effettiva e identità attestata del comparente, se l'identificazione sia il risultato di un convincimento di certezza raggiunto anche al momento dell'attestazione, sulla base di una pluralità di elementi che, comunque acquisiti, siano idonei a giustificarlo secondo regole di diligenza, prudenza e perizia professionale: Cass. 10 agosto 2004, n. 15424).

Ora, la Corte di appello di Milano ha evidenziato che il notaio aveva raggiunto una propria certezza circa l'identità del comparente sulla scorta di plurimi elementi: il sedicente M. era stato presentato al professionista dai responsabili di un'agenzia immobiliare e da un commercialista da tempo conosciuti; la banca aveva affidato la pratica del mutuo al professionista, incaricandolo di redigere la relazione notarile preliminare e trasmettendo allo stesso controricorrente la documentazione a tal fine necessaria oltre che la bozza del contratto di mutuo nella quale figuravano le generalità false dell'aspirante mutuatario; il finanziamento era stato deliberato dalla banca a seguito di una istruttoria sulla persona del futuro contraente, soggetto che l'istituto di credito per legge aveva l'obbligo di identificare; Intesa aveva comunicato al notaio l'approvazione della delibera del mutuo e l'apertura di un conto corrente a nome dello stesso M.; la stipula degli atti notarili era avvenuta col concorso di varie persone, tra cui lo stesso direttore della banca, che si erano intrattenuti con il sedicente M. in atteggiamenti di familiarità e confidenza; la carta d'identità e il codice fiscale del mutuatario esibiti alla segretaria del notaio, che ne aveva estratto copia, non presentavano alterazioni o altre anomalie tali da giustificare un sospetto di falsificazione.

A tale corredo di elementi non vale contrapporre il dato della mancata visione, da parte del notaio, dell'originale del documento di identità, di cui all'epoca lo stipulante non era più in possesso (ma di cui la collaboratrice del professionista aveva in precedenza estratto copia). Deve rilevarsi, in proposito, che la Corte territoriale, nel valorizzare i molteplici elementi di cui si è detto, ha applicato correttamente la norma di cui al cit. art. 49: come si è visto, infatti, questa non predetermina le prove che debbano essere prese in considerazione ai fini del convincimento del notaio circa l'identità della parte, ma impone che il professionista abbia maturato detto convincimento nel rispetto delle regole di diligenza, prudenza e perizia professionale e sulla base di qualsiasi elemento astrattamente idoneo a formare tale convincimento. Non può d'altro canto considerarsi determinante, ai fini del giudizio vertente sulla correttezza dell'operato del notaio, il dato della mancata esibizione dell'originale del documento di identità da parte dello stipulante al momento del rogito, visto che il documento stesso (che il notaio visionò solo in copia) non presentava alterazioni o anomalie, secondo quanto insindacabilmente accertato dal giudice del merito; su di un piano logico, dunque, detta evenienza rende la mancata acquisizione dell'originale non decisiva, in quanto consente di escludere che l'esibizione del detto documento avrebbe indotto il professionista a constatare la falsità delle generalità di M.: generalità, è bene ribadire, che apparivano al notaio incontestabilmente autentiche anche sulla base dei diversi elementi individuati dalla Corte di appello, e che si sono in precedenza menzionati.

E a quest'ultimo proposito occorre aggiungere che la censura basata sul concorso del fatto colposo del creditore non coglie nel segno. Infatti, la Corte di merito non ha inteso fare applicazione dell'art. 1227 c.c., essendosi piuttosto limitata ad attribuire rilievo a una serie di evidenze che non potevano non confermare l'odierno controricorrente nel convincimento circa la corretta identificazione della parte interessata alla stipula del contratto di mutuo. Tra i fattori che possono concorrere a formare la certezza richiesta dalla norma, possono senz'altro ricomprendersi, oltre ai documenti di riconoscimento, il comportamento delle parti, la natura dell'affare e le indicazioni fornite da terzi nella veste di testimoni informali e non di fidefacienti (Cass. 10 agosto 2004, n. 15424, in motivazione); ma non è di certo escluso che tra tali elementi siano da annoverare pure le indicazioni fornite dall'altro contraente (nella specie la banca che mai dubitò, prima del rogito, della identità di

M.A.).

3. - Il ricorso va dunque respinto.

4. - Le spese di giudizio seguono la soccombenza.

PQM
P.Q.M.

La Corte rigetta il ricorso; condanna parte ricorrente al pagamento delle spese processuali, liquidandole in Euro 7.000,00 per compensi, oltre alle spese forfettarie nella misura del 15 per cento, agli esborsi liquidati in Euro 200,00, ed agli accessori di legge; ai sensi del D.P.R. n. 115 del 2002, art. 13, comma 1 quater inserito dalla L. n. 228 del 2012, art. 1, comma 17 dà atto della sussistenza dei presupposti per il versamento, da parte del ricorrente, dell'ulteriore importo a titolo di contributo unificato pari a quello dovuto per il ricorso.

Così deciso in Roma, nella Camera di Consiglio della sezione prima civile, il 28 settembre 2017.

Depositato in Cancelleria il 30 novembre 2017

N. R.G. 9329/2014

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

Tribunale di Monza

Seconda Sezione

Il Tribunale, nella persona del Giudice dott. Caterina Caniato ha pronunciato la seguente

SENTENZA

nella causa civile di I Grado iscritta al n. r.g. **9329/2014** promossa da:

ITALFONDIARIO S.P.A. [P.IVA 00880671003] nella sua qualità di procuratore di Intesa Sanpaolo s.p.a. ed in persona del procuratore dott. Stefano Benetollo giusta procura conferita dall'amministratore delegato e legale rappresentante *pro-tempore* e rappresentata e difesa dagli avvocati Emanuele Cirillo e Francesco Cirillo presso il cui studio elegge domicilio in Monza, via Vittorio Emanuele II n. 36

PARTE ATTRICE

CONTRO

ENRICO TOMMASI [C.F. TMMNRC61R24H703D] rappresentato e difeso dall'avvocato Andrea Cristiano M. Minotti presso il cui studio elegge domicilio in Monza, via Teodolinda n. 2

PARTE CONVENUTA

CONCLUSIONI

Le parti all' udienza di precisazione delle conclusioni hanno concluso richiamandosi agli atti depositati in via telematica che vengono di seguito riprodotti.

FOGLIO DI PRECISAZIONE DELLE
CONCLUSIONI PER LA BANCA ATTRICE
La difesa di Italfondiario S.p.A., che agisce quale procuratore di Intesa Sanpaolo S.p.A., dichiara di non accettare i contraddittorio relativamente a eventuali nuove domande proposte da controparte e precisa le conclusioni come segue:
Voglia l'Ill.mo Sig. Giudice Unico del Tribunale di Monza, ogni contraria istanza, sia istruttoria che di merito, deduzione ed eccezione respinta; emesse tutte le declaratorie del caso, così statuire:
1) accertata la responsabilita' del Notaio Tommasi per violazione degli artt. 49 e segg. della Legge Notarile, condannarlo al pagamento di Euro 137.547,75.-, oltre le rate maturate e maturande del mutuo, gli interessi di mora ed ogni altra somma dovuta al momento del pagamento ai sensi delle norme contrattuali e di legge sui finanziamenti di credito fondiario a titolo di risarcimento del danno causato a Intesa Sanpaolo S.p.A.
2) con vittoria di spese, diritti ed onorari di causa.
Salvis juribus.

CONCLUSIONI PER PARTE CONVENUTA
Voglia l'Ill.mo Tribunale adito, contrariis reiectis e previa ogni più opportuna statuizione, respingere le domande attoree in quanto infondate in fatto e diritto.
Con vittoria delle spese e dei compensi di giudizio

Concisa esposizione delle ragioni di fatto e di diritto della decisione

L'Italfondiario s.p.a. ha adito questo Tribunale citando in giudizio il dott. Enrico Tommasi al fine di accertare e dichiarare la responsabilità dello stesso per aver violato gli artt. 49 e seguenti della legge notarile; per l'effetto, condannare il convenuto a risarcire i danni arrecati, a causa della sua negligenza consistente nell'errata identificazione del soggetto mutuatario - sig.ra Rolandi Rossella -, per un importo di €137.547,75 oltre alle rate maturate e maturande del mutuo, agli interessi di mora e ogni altra somma dovuta.

Si è costituito tempestivamente in giudizio il convenuto contestando la propria responsabilità in ordine a quanto previsto dalla legge notarile vigente.

Questo giudice ritiene doveroso disporre la trasmissione integrale in copia degli atti di causa e della presente sentenza alla Procura della Repubblica territorialmente competente in ordine all'accertamento e all'eventuale esercizio dell'azione penale con riguardo ai reati di sostituzione di persona (art. 494 c.p.) perché ignoti avrebbero indotto in errore l'Italfondiario s.p.a. e il dott. Tommasi sulla propria identità al fine di ottenere un vantaggio ingiusto consistente nell'erogazione di un mutuo per un valore pari a € 115.000,00 e di possesso e fabbricazione di documenti di identificazione falsi (art. 497 bis c.p.) perché la carta di identità con n. AH 8947153 rilasciata dal comune di Monza risulta contraffatta.

In fatto

La domanda di parte attrice trae origine da un contratto di mutuo stipulato, presso i locali della banca, con la sig.ra Rolandi Rossella innanzi al notaio Enrico Tommasi in data 22.12.2006 registrato a Desio in data 28.12.2006 n°10029/17 ed iscritto a Lecco in data 02.01.2007 n°65/19 (Doc. n°2 parte convenuta). La somma che la banca ha erogato a titolo di mutuo è pari a €115.000,00 – deliberata da Italfondiario s.p.a. il 18.12.2006 – e per l'accreditamento di tale importo è stato aperto il c/c n. 6152750341/38 intestato a nome della mutuataria (Come risulta dal contratto di mutuo – Doc. n°2 parte convenuta).

Contestualmente al contratto di mutuo, la mutuataria ha sottoscritto un contratto di compravendita col sig. Bido Paolo avente ad oggetto l'acquisto di un immobile sito in Valbrona. Su di esso grava garanzia ipotecaria iscritta presso l'agenzia del territorio nella sezione pubblicità immobiliare in data 02.11.2007 da parte dello stesso notaio (Doc. n°6 parte attrice).

Dall'inadempimento del soggetto mutuatario è seguita una diffida di messa in mora da parte della banca, attrice nell'odierno giudizio, per mezzo della quale ha intimato alla signora il versamento del residuo ancora dovuto. Successivamente, l'Italfondiario s.p.a. ha notificato un atto di precetto per la riscossione delle somme non pagate, ma la notificazione non ha avuto esito positivo dal momento che il destinatario è risultato irreperibile (Doc. n°8 parte attrice).

Considerata l'irreperibilità della mutuataria, la banca – per mezzo del suo legale – ha trasmesso a mezzo fax al Comune di Valbrona (la sig.ra ha dichiarato all'atto della compravendita di voler stabilire entro diciotto mesi dal 28.12.2006 la propria residenza nel comune di Valbrona (pag. 334 Doc. 3 parte convenuta) conferma della residenza della sig.ra Rolandi. Il Comune ha dato risposta negativa in data 18 febbraio 2009 con atto su carta intestata, sottoscritto dall'ufficiale delegato all'anagrafe e protocollato con n. 821 (*"In riferimento alle Vs. richieste si comunica che entrambi i nominativi in oggetto risultano sconosciuti all'anagrafe di questo Comune"*).

Successivamente l'istituto di credito ha chiesto informazioni al Comune di San Giorgio a Cremano poiché dalla documentazione risultava essere il luogo di nascita della mutuataria. L'ufficio avrebbe risposto con questa dicitura "NON ANAGRAFATO" (Doc. 10 parte attrice); della provenienza di questa comunicazione non si è certi visto il modo anomalo della sua trasmissione: la risposta sarebbe stata scritta direttamente sul fax del legale della banca senza che la stessa venisse riportata su un apposito modulo in carta intestata e senza l'indicazione del numero di protocollo, con firma del funzionario e timbro illeggibili.

Inoltre, la banca ha inoltrato una richiesta al Comune di Monza per sapere se avesse rilasciato la carta di identità della sig.ra Rolandi. L'ufficio anagrafe in data 26 febbraio 2009 ha risposto che la carta di identità è risultata contraffatta e che la signora è sconosciuta all'anagrafe (*"Con la presente, si comunica che la Carta d'identità della persona nominata in oggetto risulta essere stata contraffatta, in quanto il numero di serie sopra indicato non appartiene al Comune di Monza; inoltre il nominato in oggetto è sconosciuto a questa Anagrafe"* Doc. 14 parte attrice).

L'incertezza sull'identità del soggetto mutuatario ha portato l'Italfondiario s.p.a. ad agire nei confronti del notaio perché su di lui incombeva l'obbligo di accertare, con un grado di diligenza qualificato, l'effettiva identità delle parti contraenti.

In diritto

L'art. 49 L.N. stabilisce che *"il notaio deve essere certo dell'identità personale delle parti e può raggiungere tale certezza, anche al momento della attestazione, valutando tutti gli elementi atti a formare il suo convincimento. In caso contrario il notaio può avvalersi di due fidefacienti da lui conosciuti, che possono essere anche i testimoni"*.

La norma non individua la documentazione che il notaio è obbligato a richiedere per accertare l'identità delle parti né l'attività da svolgere per raggiungere questo fine, ma di contro impone al professionista alcune regole di giudizio.

Egli deve raggiungere tale certezza mediante la valutazione di tutti gli elementi necessari e diretti a formare il suo convincimento *"anche di natura presuntiva purché si tratti di presunzioni gravi, precise e concordanti"* (Cass., Sez. III, sentenza del 10 maggio 2005 n°9757 (RV. 581307). Nel fare ciò il notaio è tenuto a rispettare le regole della diligenza, della prudenza e della perizia ai sensi dell'art. 1176 2° comma c.c. connesse alla peculiare attività svolta. Solo nel caso in cui non si è formata una sicurezza sull'identità personale delle parti, il professionista ha la facoltà di avvalersi di due fidefacienti da lui conosciuti in qualità anche di testimoni.

La giurisprudenza è concorde nel ritenere integrata la possibile negligenza e quindi la responsabilità dei danni causati il professionista che si avvalga della sola carta di identità o di documento equipollente per l'identificazione dei soggetti partecipanti all'atto (Cass., Sez. III, sentenza del 12 maggio 2017 n°11767). Tale orientamento si fonda sulla facilità di

contraffazione del documento di identità e sulla difficoltà di riconoscere una sua alterazione in assenza di evidenti segni di abrasione (Sul punto Cass., Sez. I, sentenza del 17 maggio 1986 n°3274 (Rv. 446262 - 01) *"tale certezza, in difetto di conoscenza personale, non può essere fondata sul solo esame di una carta d'identità, od altro documento equipollente, ancorché formalmente ineccepibile perché privo di segni esteriori che ne evidenzino la falsità"* conf. Cass., Sez. III, sentenza del 10 maggio 2005 n°9757 (RV. 581307) e Cass., Sez. III, sentenza del 12 maggio 2017 n°11767).

Trattandosi di un'obbligazione di mezzi e in virtù del principio della vicinanza della prova, incombe sul professionista provare di aver tenuto un comportamento diligente nell'esecuzione della prestazione, mentre l'attore rimane onerato di provare il titolo del proprio credito.

Venendo all'esame del caso di specie, sulla base dei principi sopra riportati, il Tribunale ritiene che il notaio Enrico Tommasi non abbia violato gli obblighi derivanti dalla legge notarile concernenti l'identificazione del soggetto mutuatario.

L'Italfondiario s.p.a. ha affermato nei propri atti difensivi (Pag. 5 atto di citazione) di non sapere quali siano gli accertamenti che il notaio abbia condotto per formare il proprio convincimento in ordine all'identità delle parti.

Parte convenuta abbia assolto il proprio *onus probandi* dimostrando il rispetto, nell'esercizio delle proprie funzioni, delle regole di diligenza, prudenza e perizia.

Innanzitutto, il dott. Tommasi ha provato di aver formato il proprio convincimento sulla base oltre che della esibizione della carta di identità da parte della mutuataria, anche di ulteriori dati provenienti dalla pubblica amministrazione: il certificato di residenza rilasciato dall'ufficio anagrafe di Monza (Doc. 5 parte convenuta art. 183 VI comma n°2 cpc) e la certificazione di attribuzione del codice fiscale da parte dell'Agenzia delle Entrate (Doc. 4 parte convenuta art. 183 VI comma n°2 cpc).

Il certificato di residenza e l'attribuzione del codice fiscale risultano corrispondenti alla realtà e non presentano vizi o anomalie evidenti tali da far insorgere nemmeno in un professionista il dubbio che possano essere falsi. Infatti, il certificato di residenza è stato rilasciato su carta

intestata del comune di Monza, è stato firmato dal funzionario dell'ufficio anagrafe ed è stato timbrato; invece, la certificazione di attribuzione del codice fiscale indica l'ufficio competente, la "banda" con scritto il codice fiscale e la firma del funzionario. L'autenticità non è contestata dall'attore che precisa solo che la documentazione avrebbe dovuto essere prodotta prima della stipula del contratto di mutuo (pag. 1 terza memoria istruttoria).

La circostanza che questi documenti siano stati richiesti dal professionista contestualmente alla sottoscrizione del contratto di mutuo è stata confermata dalla teste Landa Emiliana: *"A seguito della causa, ho recuperato il fascicolo e vi ho rinvenuto sicuramente il certificato di residenza in originale e la copia del certificato di attribuzione del codice fiscale"*; inoltre, il teste ha dichiarato che il notaio chiede per prassi l'originale della carta di identità: *"Il Notaio al momento del rogito chiede di prassi l'originale"*.

Non vi è motivo di dubitare di tale testimonianza. Tra l'altro il certificato anagrafico risulta rilasciato in data 9 ottobre 2006, quindi circa due mesi prima della sottoscrizione del contratto ed è quindi più che verosimile che il Notaio, che lo ha prodotto, lo abbia all'epoca verificato.

Infine, la parte convenuta ha formato il proprio convincimento anche sulla base di elementi presuntivi dotati nel caso di specie del grado di gravità richiesto. Il dott. Tommasi ha ipotizzato che Italfondiario s.p.a. avesse accertato preventivamente l'identità della mutuataria dal momento che gli istituti di credito sono obbligati *ex lege* a svolgere un'attività istruttoria circa l'identità della clientela prima dell'erogazione di somme di denaro e dell'apertura di conti correnti. Per di più, questa fase preliminare è avvenuta in un periodo antecedente alla sottoscrizione del contratto di mutuo: la delibera di approvazione del mutuo, come riportato nell'accordo redatto dal dott. Tommasi, è del giorno 18 dicembre 2006 (pag. 342 Doc. 2 parte convenuta), mentre il contratto è stato sottoscritto in data 28 dicembre 2006.

L'onere gravante sugli istituti di credito è sancito dal d.lgs. 231/2007 che impone ai *"(...) destinatari delle disposizioni in esso previste, i quali adottano idonei e appropriati sistemi e procedure in materia di obblighi di adeguata verifica della clientela (...)"* (art.3), agli "(…) *intermediari finanziari e gli altri soggetti esercenti attività finanziaria di cui all'articolo 11* (tra cui le banche) *osservano gli obblighi di adeguata verifica della clientela in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale*

degli stessi ed, in particolare, nei seguenti casi: a. quando instaurano un rapporto continuativo; b. quando eseguono operazioni occasionali, disposte dai clienti che comportino la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro (...)" (art. 11 comma 4).

Il d.lgs. 231/2007 ha dato attuazione alla direttiva 2005/60/CE che è ancora in vigore (pur se abrogata ai sensi dell'art. 66 della direttiva 2015/849/UE , tuttavia è in vigore sino al 26 giugno 2017 e comunque la nuova direttiva non modifica nella sostanza l'impostazione di quella precedente, prescrivendo sempre adeguate verifiche nei confronti della clientela. Infatti, l'art. 11 dir. 2015/849/UE *"Gli Stati membri assicurano che i soggetti obbligati applichino le misure di adeguata verifica della clientela nelle circostanze seguenti: quando instaurano un rapporto d'affari; quando eseguono un'operazione occasionale che sia di importo pari o superiore a €15.000, indipendentemente dal fatto che l'operazione sia eseguita con un'unica operazione o con diverse operazioni che appiano collegate (...)"* e l'art. 9 par. 1 dir. 2005/60/CE *"Gli Stati membri impongono che la verifica dell'identità del cliente e del titolare effettivo avvenga prima dell'instaurazione del rapporto d'affari o dell'esecuzione della transazione"*. In ogni caso è rimessa alla valutazione dell'ente *"decidere se far ricorso a registri disponibili al pubblico contenenti informazioni sui titolari effettivi, chiedere ai loro clienti i dati pertinenti ovvero ottenere le informazioni in altro modo (...)* (considerando n°10).

I citati atti comunitari sono applicabili anche ai notai. Tuttavia il Tribunale, come sopra motivato, non ritiene che parte convenuta abbia violato tale normativa in quanto il dott. Tommasi ha fatto affidamento sul fatto che il mutuo fosse stato erogato in data antecedente alla sottoscrizione del contratto ed aperto il conto corrente su cui accreditare la somma e tali fatti lo hanno indotto a ritenere certa l'identità della signora, stante l'obbligo di una previa verifica della sua identità da parte della banca, considerata anche l'entità della somma mutuata.

Il dott. Tommasi non è responsabile del danno subito da Italfondiario dal momento che egli ha utilizzato la diligenza qualificata richiesta nell'esecuzione della sua prestazione. Infatti, l'obbligo *ex lege* degli enti creditizi di effettuare una preventiva verifica del cliente e la

delibera di approvazione avvenuta in data antecedente, integrati dalla richiesta di esibizione della carta di identità, certificato di residenza e di attribuzione del codice fiscale sono elementi idonei a formare il convincimento di un professionista sull'identificazione del soggetto partecipante all'atto.

Ad abundantiam, è applicabile al caso di specie il principio sancito dall'art. 1227 c.c. che esclude il risarcimento per il creditore che non abbia utilizzato l'ordinaria diligenza nell'evitare i danni che avrebbe potuto impedire. Infatti, se la banca avesse effettuato correttamente un controllo della propria clientela, a cui era tenuta non solo per legge ma soprattutto in presenza di un cliente non abituale, avrebbe potuto apprendere prima dell'approvazione del mutuo che l'identità del soggetto non fosse corrispondente alla realtà e così evitare il danno oggetto del presente giudizio.

Si rigetta integralmente la domanda di parte attrice perché infondata per i motivi esposti in narrativa.

Sulle spese

In virtù del principio disciplinato all'art. 91 c.p.c., le spese seguono la soccombenza e vengono poste a carico di parte attrice e liquidate come da dispositivo.

La liquidazione delle spese legali è subordinata all'applicazione dei nuovi parametri previsti con DM 55/2014 che prevede la suddivisione in scaglioni in base al valore della causa e della fase processuale. Inoltre, tiene conto della natura della controversia, del numero e dell'importanza delle questioni trattati; nonché del pregio dell'opera prestata e dei risultati conseguiti (art. 4, c. 1) e dando applicazione al principio per cui nei giudizi per pagamento di somme il valore della controversia viene determinato sulla scorta della somma effettivamente attribuita alla parte vincitrice, e non della somma domandata (art. 5).

Alla luce di questi criteri, si liquidano le spese come da tariffa a cui vanno aggiunti onorari e spese. Le somme sono così ripartite:

a. Fase di studio della controversia: € 2.430,00
b. Fase introduttiva del giudizio: € 1.550,00

c. Fase istruttoria e/o di trattazione: €4.000,00

d. Fase decisionale: € 4.050,00

TOTALE: **€ 12.030,00**

P.Q.M.

Il Tribunale, definitivamente pronunciando, ogni diversa istanza ed eccezione disattesa o assorbita, così dispone:

1. Rigetta la domanda di Italfondiario s.p.a. perché infondata;
2. Dispone la trasmissione di tutti gli atti di causa e della presente sentenza alla Procura della Repubblica presso il Tribunale di Monza per l'accertamento dei reati di sostituzione di persona (art. 494 c.p.) e di possesso e fabbricazione di documenti di identificazione falsi (art. 497 bis c.p.) o altre fattispecie che riterrà di ravvisare;
3. Condanna altresì Italfondiario s.p.a. a rimborsare a Enrico Tommasi le spese di lite, che si liquidano in €12.030,00 per compensi, oltre a rimborso spese generali nella misura del 15% ed oltre a i.v.a. e c.p.a. se dovute come per legge.

Monza, 12 giugno 2017

Il Giudice

dott. Caterina Caniato

DECRETO LEGISLATIVO 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129)

(GU n.205 del 4-9-2018)

Vigente al: 19-9-2018

Capo I
Modifiche al titolo e alle premesse del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87 della Costituzione;

Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017, e in particolare l'articolo 13, che delega il Governo all'emanazione di uno o piu' decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

Vista la legge 24 dicembre 2012, n. 234, recante norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Visto il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

Visto il 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

Vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati;

Vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

Visto il decreto legislativo 18 maggio 2018, n. 51, recante attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 21 marzo 2018;

Acquisito il parere del Garante per la protezione dei dati personali, adottato nell'adunanza del 22 maggio 2018;

Acquisiti i pareri delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione dell'8 agosto 2018;

Sulla proposta del Presidente del Consiglio dei ministri e dei Ministri per gli affari europei e della giustizia, di concerto con i Ministri per la pubblica amministrazione, degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze e dello sviluppo economico;

E M A N A

il seguente decreto legislativo:

Art. 1

Modifiche al titolo e alle premesse
del decreto legislativo 30 giugno 2003, n. 196

1. Al titolo del decreto legislativo 30 giugno 2003, n. 196, dopo le parole «dati personali» sono aggiunte le seguenti: «, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE».

2. Alle premesse del decreto legislativo 30 giugno 2003, n. 196, dopo il terzo Visto sono inseriti i seguenti:

«Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017» e, in particolare, l'articolo 13, che delega il Governo all'emanazione di uno o piu' decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

Vista la legge 24 dicembre 2012, n. 234, recante norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Visto il 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);».

Capo II
Modifiche alla parte I del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

Art. 2

Modifiche alla parte I, titolo I, del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte I, titolo I, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica del titolo I e' sostituita dalla seguente: «Principi e disposizioni generali»;

b) prima dell'articolo 1 e' inserito il seguente Capo:

«Capo I (Oggetto, finalita' e Autorita' di controllo)»

c) l'articolo 1 e' sostituito dal seguente:

«Art. 1 (Oggetto) . - 1. Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito «Regolamento», e del presente codice, nel rispetto della dignita' umana, dei diritti e delle liberta' fondamentali della persona.»;

d) l'articolo 2 e' sostituito dal seguente:

«Art. 2 (Finalita'). - 1. Il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento.»;

e) dopo l'articolo 2 e' inserito il seguente:

«Art. 2-bis (Autorita' di controllo). - 1. L'Autorita' di controllo di cui all'articolo 51 del regolamento e' individuata nel Garante per la protezione dei dati personali, di seguito «Garante», di cui all'articolo 153.»;

f) dopo l'articolo 2-bis sono inseriti i seguenti Capi:

«Capo II (Principi) - Art. 2-ter (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri). - 1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento e' costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e' ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione e' ammessa quando e' comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e puo' essere iniziata se e' decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalita' sono ammesse unicamente se previste ai sensi del comma 1.

4. Si intende per:

a) "comunicazione", il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 2-quater (Regole deontologiche). - 1. Il Garante promuove, nell'osservanza del principio di rappresentativita' e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti

previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformita' alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. Lo schema di regole deontologiche e' sottoposto a consultazione pubblica per almeno sessanta giorni.

3. Conclusa la fase delle consultazioni, le regole deontologiche sono approvate dal Garante ai sensi dell'articolo 154-bis, comma 1, lettera b), pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportate nell'allegato A del presente codice.

4. Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceita' e la correttezza del trattamento dei dati personali.

Art. 2-quinquies (Consenso del minore in relazione ai servizi della societa' dell'informazione). - 1. In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni puo' esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della societa' dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di eta' inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, e' lecito a condizione che sia prestato da chi esercita la responsabilita' genitoriale.

2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi.

Art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante). - 1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

a) accesso a documenti amministrativi e accesso civico;

b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini

italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita';

c) tenuta di registri pubblici relativi a beni immobili o mobili;

d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;

e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;

f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonche' documentazione delle attivita' istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attivita' di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonche' l'accertamento delle cause di ineleggibilita', incompatibilita' o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo;

i) attivita' dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;

l) attivita' di controllo e ispettive;

m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

n) conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

o) rapporti tra i soggetti pubblici e gli enti del terzo settore;

p) obiezione di coscienza;

q) attivita' sanzionatorie e di tutela in sede amministrativa o giudiziaria;

r) rapporti istituzionali con enti di culto, confessioni religiose e comunita' religiose;

s) attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

t) attivita' amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse

quelle correlate ai trapianti d'organo e di tessuti nonche' alle trasfusioni di sangue umano;

u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumita' fisica;

v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

aa) tutela sociale della maternita' ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonche' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva.

3. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-septies.

Art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute). - 1. In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformita' alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.

2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 e' adottato con cadenza almeno biennale e tenendo conto:

a) delle linee guida, delle raccomandazioni e delle migliori

prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;

b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;

c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

3. Lo schema di provvedimento e' sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni.

4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da adottare relativamente a:

a) contrassegni sui veicoli e accessi a zone a traffico limitato;

b) profili organizzativi e gestionali in ambito sanitario;

c) modalita' per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute;

d) prescrizioni di medicinali.

5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalita' del trattamento e possono individuare, in conformita' a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati e' consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalita' per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonche' le eventuali altre misure necessarie a garantire i diritti degli interessati.

6. Le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute per finalita' di prevenzione, diagnosi e cura nonche' quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanita'. Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del regolamento, o altre cautele specifiche.

7. Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, e' ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo.

8. I dati personali di cui al comma 1 non possono essere diffusi.

Art. 2-octies (Principi relativi al trattamento di dati relativi a condanne penali e reati). - 1. Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorita' pubblica, e'

consentito, ai sensi dell'articolo 10 del medesimo regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le liberta' degli interessati.

2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonche' le garanzie di cui al medesimo comma sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante.

3. Fermo quanto previsto dai commi 1 e 2, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza e' consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:

a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento;

b) l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;

c) la verifica o l'accertamento dei requisiti di onorabilita', requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;

d) l'accertamento di responsabilita' in relazione a sinistri o eventi attinenti alla vita umana, nonche' la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attivita' assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

f) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

g) l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza;

h) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosita' sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;

i) l'accertamento del requisito di idoneita' morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;

l) l'attuazione della disciplina in materia di attribuzione del rating di legalita' delle imprese ai sensi dell'articolo 5-ter del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni,

dalla legge 24 marzo 2012, n. 27;

m) l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo.

4. Nei casi in cui le disposizioni di cui al comma 3 non individuano le garanzie appropriate per i diritti e le liberta' degli interessati, tali garanzie sono previste con il decreto di cui al comma 2.

5. Quando il trattamento dei dati di cui al presente articolo avviene sotto il controllo dell'autorita' pubblica si applicano le disposizioni previste dall'articolo 2-sexies.

6. Con il decreto di cui al comma 2 e' autorizzato il trattamento dei dati di cui all'articolo 10 del Regolamento, effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalita' organizzata, stipulati con il Ministero dell'interno o con le prefetture-UTG. In relazione a tali protocolli, il decreto di cui al comma 2 individua, le tipologie dei dati trattati, gli interessati, le operazioni di trattamento eseguibili, anche in relazione all'aggiornamento e alla conservazione e prevede le garanzie appropriate per i diritti e le liberta' degli interessati. Il decreto e' adottato, limitatamente agli ambiti di cui al presente comma, di concerto con il Ministro dell'interno.

Art. 2-novies (Trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale). - 1. Le disposizioni degli articoli 2-sexies, 2-septies e 2-octies del presente decreto legislativo recano principi applicabili, in conformita' ai rispettivi ordinamenti, ai trattamenti delle categorie di dati personali di cui agli articoli 9, paragrafo 1, e 10 del Regolamento, disciplinati dalla Presidenza della Repubblica, dal Senato della Repubblica, dalla Camera dei deputati e dalla Corte costituzionale.

Art. 2-decies (Inutilizzabilita' dei dati). - 1. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall'articolo 160-bis.

Capo III (Disposizioni in materia di diritti dell'interessato) - Art. 2-undecies (Limitazioni ai diritti dell'interessato). - 1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;

b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;

c) all'attivita' di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) alle attivita' svolte da un soggetto pubblico, diverso dagli

enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalita' inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonche' alla tutela della loro stabilita';

e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

f) alla riservatezza dell'identita' del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

2. Nei casi di cui al comma 1, lettera c), si applica quanto previsto dai regolamenti parlamentari ovvero dalla legge o dalle norme istitutive della Commissione d'inchiesta.

3. Nei casi di cui al comma 1, lettere a), b), d) e) ed f) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio dei medesimi diritti puo', in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalita' della limitazione, per il tempo e nei limiti in cui cio' costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), e) ed f). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalita' di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonche' del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facolta' di cui al presente comma.

Art. 2-duodecies (Limitazioni per ragioni di giustizia). - 1. In applicazione dell'articolo 23, paragrafo 1, lettera f), del Regolamento, in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonche' dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalita' previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento.

2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento possono, in ogni caso, essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalita' della limitazione, nella misura e per il tempo in cui cio'

costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari.

3. Si applica l'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.

4. Ai fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonche' i trattamenti svolti nell'ambito delle attivita' ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attivita' amministrativo-gestionale di personale, mezzi o strutture, quando non e' pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.

Art. 2-terdecies (Diritti riguardanti le persone decedute). - 1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualita' di suo mandatario, o per ragioni familiari meritevoli di protezione.

2. L'esercizio dei diritti di cui al comma 1 non e' ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della societa' dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.

3. La volonta' dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto puo' riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.

4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.

5. In ogni caso, il divieto non puo' produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonche' del diritto di difendere in giudizio i propri interessi.

Capo IV (Disposizioni relative al titolare del trattamento e al responsabile del trattamento) - Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati). - 1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilita' e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorita'.

2. Il titolare o il responsabile del trattamento individuano le modalita' piu' opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorita' diretta.

Art. 2-quinquiesdecies (Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico). - 1. Con riguardo

ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del Regolamento, il Garante puo', sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento e' tenuto ad adottare.

Art. 2-sexiesdecies (Responsabile della protezione dei dati per i trattamenti effettuati dalle autorita' giudiziarie nell'esercizio delle loro funzioni). - 1. Il responsabile della protezione dati e' designato, a norma delle disposizioni di cui alla sezione 4 del capo IV del Regolamento, anche in relazione ai trattamenti di dati personali effettuati dalle autorita' giudiziarie nell'esercizio delle loro funzioni.

Art. 2-septiesdecies (Organismo nazionale di accreditamento). - 1. L'organismo nazionale di accreditamento di cui all'articolo 43, paragrafo 1, lettera b), del Regolamento e' l'Ente unico nazionale di accreditamento, istituito ai sensi del Regolamento (CE) n. 765/2008, del Parlamento europeo e del Consiglio, del 9 luglio 2008, fatto salvo il potere del Garante di assumere direttamente, con deliberazione pubblicata nella Gazzetta Ufficiale della Repubblica italiana e in caso di grave inadempimento dei suoi compiti da parte dell'Ente unico nazionale di accreditamento, l'esercizio di tali funzioni, anche con riferimento a una o piu' categorie di trattamenti.».

Capo III
Modifiche alla parte II del codice in materia di protezione dei dati personali di cui decreto legislativo 30 giugno 2003, n. 196

Art. 3

Modifiche alla rubrica e al titolo I della parte II, del decreto legislativo 30 giugno 2003, n. 196

1. La rubrica della parte II del decreto legislativo 30 giugno 2003, n. 196, e' sostituita dalla seguente: «Disposizioni specifiche per i trattamenti necessari per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nonche' disposizioni per i trattamenti di cui al capo IX del regolamento».

2. Al titolo I della parte II, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) prima del titolo I, e' inserito il seguente:

«Titolo 0.I (Disposizioni sulla base giuridica) - Art. 45-bis (Base giuridica). - 1. Le disposizioni contenute nella presente parte sono stabilite in attuazione dell'articolo 6, paragrafo 2, nonche' dell'articolo 23, paragrafo 1, del regolamento.»;

b) all'articolo 50, e' aggiunto, in fine, il seguente periodo: «La violazione del divieto di cui al presente articolo e' punita ai sensi dell'articolo 684 del codice penale.»;

c) all'articolo 52:

1) al comma 1, le parole: «per finalita' di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica,» sono soppresse;

2) al comma 6, le parole «dell'articolo 32 della legge 11 febbraio 1994, n. 109,» sono sostituite dalle seguenti: «dell'articolo 209 del Codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50,».

Art. 4

Modifiche alla parte II, titolo III,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo III, del decreto legislativo 30 giugno 2003, n. 196, l'articolo 58 e' sostituito dal seguente:

«Art. 58 (Trattamenti di dati personali per fini di sicurezza nazionale o difesa). - 1. Ai trattamenti di dati personali effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, sulla base dell'articolo 26 della predetta legge o di altre disposizioni di legge o regolamento, ovvero relativi a dati coperti da segreto di Stato ai sensi degli articoli 39 e seguenti della medesima legge, si applicano le disposizioni di cui all'articolo 160, comma 4, nonche', in quanto compatibili, le disposizioni di cui agli articoli 2, 3, 8, 15, 16, 18, 25, 37, 41, 42 e 43 del decreto legislativo 18 maggio 2018, n. 51.

2. Fermo restando quanto previsto dal comma 1, ai trattamenti effettuati da soggetti pubblici per finalita' di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, si applicano le disposizioni di cui al comma 1 del presente articolo, nonche' quelle di cui agli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51.

3. Con uno o piu' regolamenti sono individuate le modalita' di applicazione delle disposizioni di cui ai commi 1 e 2, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies, anche in relazione all'aggiornamento e alla conservazione. I regolamenti, negli ambiti di cui al comma 1, sono adottati ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, e, negli ambiti di cui al comma 2, sono adottati con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta dei Ministri competenti.

4. Con uno o piu' regolamenti adottati con decreto del Presidente della Repubblica su proposta del Ministro della difesa, sono

disciplinate le misure attuative del presente decreto in materia di esercizio delle funzioni di difesa e sicurezza nazionale da parte delle Forze armate.».

Art. 5

Modifiche alla parte II, titolo IV,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo IV, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) all'articolo 59:

1) alla rubrica sono aggiunte, in fine, le seguenti parole: «e accesso civico»;

2) al comma 1, le parole «sensibili e giudiziari» sono sostituite dalle seguenti: «di cui agli articoli 9 e 10 del regolamento» e le parole «Le attivita' finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.» sono soppresse;

3) dopo il comma 1 e' aggiunto il seguente: «1-bis. I presupposti, le modalita' e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.»;

b) l'articolo 60 e' sostituito dal seguente:

«Art. 60 (Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale). - 1. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento e' consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, e' di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalita' o in un altro diritto o liberta' fondamentale.»;

c) all'articolo 61:

1) alla rubrica sono aggiunte, in fine, le seguenti parole: «e regole deontologiche»;

2) i commi 1 e 2 sono sostituiti dai seguenti:

«1. Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da piu' archivi, tenendo presenti le pertinenti Raccomandazioni del Consiglio d'Europa.

2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli di cui agli articoli 9 e 10 del regolamento, che devono essere inseriti in un albo professionale in conformita' alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 2-ter

del presente codice, anche mediante reti di comunicazione elettronica. Puo' essere altresi' menzionata l'esistenza di provvedimenti che a qualsiasi titolo incidono sull'esercizio della professione.».

Art. 6

Modifiche alla parte II, titolo V,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo V, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) l'articolo 75 e' sostituito dal seguente:

«Art. 75 (Specifiche condizioni in ambito sanitario). - 1. Il trattamento dei dati personali effettuato per finalita' di tutela della salute e incolumita' fisica dell'interessato o di terzi o della collettivita' deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-septies del presente codice, nonche' nel rispetto delle specifiche disposizioni di settore.»;

b) la rubrica del Capo II e' sostituita dalla seguente: «Modalita' particolari per informare l'interessato e per il trattamento dei dati personali»;

c) l'articolo 77 e' sostituito dal seguente:

«Art. 77 (Modalita' particolari). - 1. Le disposizioni del presente titolo individuano modalita' particolari utilizzabili dai soggetti di cui al comma 2:

a) per informare l'interessato ai sensi degli articoli 13 e 14 del Regolamento;

b) per il trattamento dei dati personali.

2. Le modalita' di cui al comma 1 sono applicabili:

a) dalle strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie e dagli esercenti le professioni sanitarie;

b) dai soggetti pubblici indicati all'articolo 80.»;

d) all'articolo 78:

1) alla rubrica la parola «Informativa» e' sostituita dalla seguente: «Informazioni»;

2) al comma 1, le parole «nell'articolo 13, comma 1» sono sostituite dalle seguenti: «negli articoli 13 e 14 del Regolamento»;

3) al comma 2, le parole «L'informativa puo' essere fornita» sono sostituite dalle seguenti: «Le informazioni possono essere fornite» e le parole «prevenzione, diagnosi, cura e riabilitazione» sono sostituite dalle seguenti: «diagnosi, assistenza e terapia sanitaria»;

4) il comma 3, e' sostituito dal seguente: «3. Le informazioni possono riguardare, altresi', dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto.»;

5) al comma 4, le parole «L'informativa» sono sostituite dalle

seguenti: «Le informazioni» e la parola «riguarda» e' sostituita dalla seguente «riguardano»;

6) al comma 5:

6.1. le parole «L'informativa resa» sono sostituite dalle seguenti: «Le informazioni rese»;

6.2. la parola «evidenzia» e' sostituita dalla seguente: «evidenziano»;

6.3. la lettera a) e' sostituita dalla seguente: «a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformita' alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, e' manifestato liberamente;»;

6.4. sono aggiunte, in fine, le seguenti lettere: «c-bis) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221; c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.»;

e) all'articolo 79:

1) la rubrica e' sostituita dalla seguente: «(Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie)»;

2) il comma 1 e' sostituito dal seguente: «1. Le strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie possono avvalersi delle modalita' particolari di cui all'articolo 78 in riferimento ad una pluralita' di prestazioni erogate anche da distinti reparti ed unita' della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate.»;

3) al comma 2, le parole «l'organismo e le strutture» sono sostituite dalle seguenti: «la struttura o le sue articolazioni» e le parole «informativa e il consenso» sono sostituite dalla seguente: «informazione»;

4) al comma 3, le parole «semplificate di cui agli articoli 78 e 81» sono sostituite dalle seguenti: «particolari di cui all'articolo 78»;

5) al comma 4, la parola «semplificate» e' sostituita dalla seguente «particolari»;

f) l'articolo 80 e' sostituito dal seguente:

«Art. 80 (Informazioni da parte di altri soggetti). - 1. Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento, oltre a quanto previsto dall'articolo 79, possono avvalersi della facolta' di fornire un'unica informativa per una pluralita' di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di altri soggetti pubblici, diversi da quelli di cui al predetto articolo 79, operanti in ambito sanitario o della protezione e sicurezza sociale.

2. Le informazioni di cui al comma 1 sono integrate con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attivita' amministrative effettuate per motivi di interesse pubblico rilevante che non richiedono il consenso degli interessati.»;

g) all'articolo 82:

1) al comma 1, le parole da «L'informativa» fino a «intervenire» sono sostituite dalle seguenti: «Le informazioni di cui agli articoli 13 e 14 del Regolamento possono essere rese»;

2) al comma 2: le parole da «L'informativa» fino a «intervenire» sono sostituite dalle seguenti: «Tali informazioni possono altresi' essere rese», e la lettera a) e' sostituita dalla seguente: «a) impossibilita' fisica, incapacita' di agire o incapacita' di intendere o di volere dell'interessato, quando non e' possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato;»;

3) al comma 3, le parole da «L'informativa» fino a «intervenire» sono sostituite dalle seguenti: «Le informazioni di cui al comma 1 possono essere rese» e le parole «dall'acquisizione preventiva del consenso» sono sostituite dalle seguenti: «dal loro preventivo rilascio»;

4) al comma 4, le parole «l'informativa e' fornita» sono sostituite dalle seguenti: «le informazioni sono fornite» e le parole da «anche» fino a «necessario» sono sostituite dalle seguenti: «nel caso in cui non siano state fornite in precedenza»;

h) dopo l'articolo 89 e' inserito il seguente:

«Art. 89-bis (Prescrizioni di medicinali). - 1. Per le prescrizioni di medicinali, laddove non e' necessario inserire il nominativo dell'interessato, si adottano cautele particolari in relazione a quanto disposto dal Garante nelle misure di garanzia di cui all'articolo 2-septies, anche ai fini del controllo della correttezza della prescrizione ovvero per finalita' amministrative o per fini di ricerca scientifica nel settore della sanita' pubblica.»;

i) all'articolo 92:

1) al comma 1, le parole «organismi sanitari pubblici e privati» sono sostituite dalle seguenti: «strutture, pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie»;

2) al comma 2, lettera a), le parole «di far valere» sono sostituite dalle seguenti: «di esercitare», le parole «ai sensi dell'articolo 26, comma 4, lettera c),» sono sostituite dalle seguenti: «, ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento,» e le parole «e inviolabile» sono soppresse;

3) alla lettera b), le parole «e inviolabile» sono soppresse.

Art. 7

Modifiche alla parte II, titolo VI,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo VI, del decreto legislativo 30 giugno 2003, n. 196, l'articolo 96 e' sostituito dal seguente:

«Art. 96 (Trattamento di dati relativi a studenti). - 1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonche' le istituzioni di alta formazione artistica e coreutica e le universita' statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalita' e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalita'.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresi' ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.».

Art. 8

Modifiche alla parte II, titolo VII,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo VII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica e' sostituita dalla seguente: «(Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici)»;

b) l'articolo 97 e' sostituito dal seguente:

«Art. 97 (Ambito applicativo). - 1. Il presente titolo disciplina il trattamento dei dati personali effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ai sensi dell'articolo 89 del regolamento.»;

c) l'articolo 99 e' sostituito dal seguente:

«Art. 99 (Durata del trattamento). - 1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici puo' essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi

scopi per i quali i dati sono stati in precedenza raccolti o trattati.

2. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, e' cessato il trattamento nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del Regolamento.»;

d) all'articolo 100:

1) al comma 1, le parole «sensibili o giudiziari» sono sostituite dalle seguenti: «di cui agli articoli 9 e 10 del Regolamento»;

2) al comma 2, le parole da «opporsi» fino alla fine del comma, sono sostituite dalle seguenti: «rettifica, cancellazione, limitazione e opposizione ai sensi degli articoli 16, 17, 18 e 21 del Regolamento»;

3) dopo il comma 4, e' aggiunto il seguente: «4-bis. I diritti di cui al comma 2 si esercitano con le modalita' previste dalle regole deontologiche.»;

e) la rubrica del Capo II e' sostituita dalla seguente: «Trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica»;

f) all'articolo 101:

1) al comma 1, le parole «per scopi storici» sono sostituite dalle seguenti: «a fini di archiviazione nel pubblico interesse o di ricerca storica» e le parole «dell'articolo 11» sono sostituite dalle seguenti: «dell'articolo 5 del regolamento»;

2) al comma 2, le parole «per scopi storici» sono sostituite dalle seguenti: «a fini di archiviazione nel pubblico interesse o di ricerca storica»;

g) all'articolo 102:

1) la rubrica e' sostituita dalla seguente: «(Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica)»;

2) il comma 1 e' sostituito dal seguente: «1. Il Garante promuove, ai sensi dell'articolo 2-quater, la sottoscrizione di regole deontologiche per i soggetti pubblici e privati, ivi comprese le societa' scientifiche e le associazioni professionali, interessati al trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica.»;

3) al comma 2 sono apportate le seguenti modificazioni:

3.1 l'alinea e' sostituito dal seguente: «2. Le regole deontologiche di cui al comma 1 individuano garanzie adeguate per i diritti e le liberta' dell'interessato in particolare:»;

3.2 alla lettera a), dopo la parola «codice» sono inserite le seguenti: «e del Regolamento»;

3.3 alla lettera c) le parole «a scopi storici» sono sostituite dalle seguenti: «a fini di archiviazione nel pubblico interesse o di ricerca storica»;

h) l'articolo 103 e' sostituito dal seguente:

«Art. 103 (Consultazione di documenti conservati in archivi). - 1.

La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati dichiarati di interesse storico particolarmente importante e' disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 e dalle relative regole deontologiche.»;

i) la rubrica del Capo III e' sostituita dalla seguente: «Trattamento a fini statistici o di ricerca scientifica»;

l) all'articolo 104:

1) alla rubrica, le parole «per scopi statistici o scientifici» sono sostituite dalle seguenti: «a fini statistici o di ricerca scientifica»;

2) al comma 1, le parole «scopi statistici» sono sostituite dalle seguenti: «fini statistici» e le parole «scopi scientifici» sono sostituite dalle seguenti: «per fini di ricerca scientifica»;

m) all'articolo 105:

1) al comma 1, le parole «per scopi statistici o scientifici» sono sostituite dalle seguenti: «a fini statistici o di ricerca scientifica»;

2) al comma 2, le parole «Gli scopi statistici o scientifici» sono sostituite dalle seguenti: «I fini statistici e di ricerca scientifica», le parole «all'articolo 13» sono sostituite dalle seguenti: «agli articoli 13 e 14 del regolamento» e le parole «, e successive modificazioni» sono soppresse;

3) al comma 3, le parole «dai codici» sono sostituite dalle seguenti: «dalle regole deontologiche» e le parole «l'informativa all'interessato puo' essere data» sono sostituite dalle seguenti: «le informazioni all'interessato possono essere date»;

4) al comma 4, le parole «per scopi statistici o scientifici» sono sostituite dalle seguenti: «a fini statistici o di ricerca scientifica», le parole «l'informativa all'interessato non e' dovuta» sono sostituite dalle seguenti: «le informazioni all'interessato non sono dovute» e le parole «dai codici» sono sostituite dalle seguenti: «dalle regole deontologiche»;

n) l'articolo 106 e' sostituito dal seguente:

«Art. 106 (Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica). - 1. Il Garante promuove, ai sensi dell'articolo 2-quater, regole deontologiche per i soggetti pubblici e privati, ivi comprese le societa' scientifiche e le associazioni professionali, interessati al trattamento dei dati per fini statistici o di ricerca scientifica, volte a individuare garanzie adeguate per i diritti e le liberta' dell'interessato in conformita' all'articolo 89 del Regolamento.

2. Con le regole deontologiche di cui al comma 1, tenendo conto, per i soggetti gia' compresi nell'ambito del Sistema statistico nazionale, di quanto gia' previsto dal decreto legislativo 6 settembre 1989, n. 322, e, per altri soggetti, sulla base di analoghe garanzie, sono individuati in particolare:

a) i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal medesimo decreto legislativo n. 322 del 1989, siano effettuati per idonei ed effettivi

fini statistici o di ricerca scientifica;

b) per quanto non previsto dal presente codice, gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione e diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza e alle modalita' per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato, tenendo conto dei principi contenuti nelle pertinenti raccomandazioni del Consiglio d'Europa;

c) l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare direttamente o indirettamente l'interessato, anche in relazione alle conoscenze acquisite in base al progresso tecnico;

d) le garanzie da osservare nei casi in cui si puo' prescindere dal consenso dell'interessato, tenendo conto dei principi contenuti nelle raccomandazioni di cui alla lettera b);

e) modalita' semplificate per la prestazione del consenso degli interessati relativamente al trattamento dei dati di cui all'articolo 9 del regolamento;

f) i casi nei quali i diritti di cui agli articoli 15, 16, 18 e 21 del Regolamento possono essere limitati ai sensi dell'articolo 89, paragrafo 2, del medesimo Regolamento;

g) le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire alle persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies;

h) le misure da adottare per favorire il rispetto del principio di minimizzazione e delle misure tecniche e organizzative di cui all'articolo 32 del Regolamento, anche in riferimento alle cautele volte ad impedire l'accesso da parte di persone fisiche che non sono autorizzate o designate e l'identificazione non autorizzata degli interessati, all'interconnessione dei sistemi informativi anche nell'ambito del Sistema statistico nazionale e all'interscambio di dati per fini statistici o di ricerca scientifica da effettuarsi con enti ed uffici situati all'estero;

i) l'impegno al rispetto di regole deontologiche da parte delle persone che, ai sensi dell'articolo 2-quaterdecies, risultano autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile del trattamento, che non sono tenute in base alla legge al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.»;

o) l'articolo 107 e' sostituito dal seguente:

«Art. 107 (Trattamento di categorie particolari di dati personali). - 1. Fermo restando quanto previsto dall'articolo 2-sexies e fuori dei casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di dati di cui all'articolo 9 del Regolamento, quando e' richiesto, puo' essere prestato con modalita' semplificate,

individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-septies.»;

p) l'articolo108 e' sostituito dal seguente:

«Art. 108 (Sistema statistico nazionale). - 1. Il trattamento di dati personali da parte di soggetti che fanno parte del Sistema statistico nazionale, oltre a quanto previsto dalle regole deontologiche di cui all'articolo 106, comma 2, resta inoltre disciplinato dal decreto legislativo 6 settembre 1989, n. 322, in particolare per quanto riguarda il trattamento dei dati di cui all'articolo 9 del Regolamento indicati nel programma statistico nazionale, le informative all'interessato, l'esercizio dei relativi diritti e i dati non tutelati dal segreto statistico ai sensi dell'articolo 9, comma 4, del medesimo decreto legislativo n. 322 del 1989.»;

q) all'articolo 109, comma 1, le parole «della statistica, sentito il Ministro» sono sostituite dalle seguenti: «di statistica, sentiti i Ministri»;

r) l'articolo 110 e' sostituito dal seguente:

«Art. 110 (Ricerca medica, biomedica ed epidemiologica). - 1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non e' necessario quando la ricerca e' effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformita' all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed e' condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non e' inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalita' della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le liberta' e i legittimi interessi dell'interessato, il programma di ricerca e' oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.»;

s) l'articolo 110-bis e' sostituito dal seguente:

«Art. 110-bis (Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici). - 1. Il Garante puo' autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del

Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attivita' quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalita' della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le liberta' e i legittimi interessi dell'interessato, in conformita' all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza.

3. Il trattamento ulteriore di dati personali da parte di terzi per le finalita' di cui al presente articolo puo' essere autorizzato dal Garante anche mediante provvedimenti generali, adottati d'ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell'ulteriore trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati. I provvedimenti adottati a norma del presente comma sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana.

4. Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attivita' clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attivita' di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.».

Art. 9

Modifiche alla parte II, titolo VIII,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo VIII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica e' sostituita dalla seguente: «Trattamenti nell'ambito del rapporto di lavoro»;

b) l'articolo 111 e' sostituito dal seguente:

«Art. 111 (Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro). - 1. Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato

nell'ambito del rapporto di lavoro per le finalita' di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalita' per le informazioni da rendere all'interessato.»;

c) dopo l'articolo 111 e' inserito il seguente:

«Art. 111-bis (Informazioni in caso di ricezione di curriculum). - 1. Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalita' di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non e' dovuto.

d) la rubrica del Capo II e' sostituita dalla seguente: «Trattamento di dati riguardanti i prestatori di lavoro»;

e) la rubrica del Capo III e' sostituita dalla seguente: «Controllo a distanza, lavoro agile e telelavoro»

f) all'articolo 113, sono aggiunte, in fine, le seguenti parole: «, nonche' dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276.»

g) la rubrica dell'articolo 114 e' sostituita dalla seguente: «Garanzie in materia di controllo a distanza»);

h) all'articolo 115:

1) la rubrica e' sostituita dalla seguente: «(Telelavoro, lavoro agile e lavoro domestico)»;

2) al comma 1, le parole «e del telelavoro» sono sostituite dalle seguenti: «del telelavoro e del lavoro agile»;

i) all'articolo 116, comma 1, le parole «ai sensi dell'articolo 23» sono sostituite dalle seguenti: «dall'interessato medesimo».

Art. 10

Modifiche alla parte II, titolo IX,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo IX, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica e' sostituita dalla seguente: «Altri trattamenti in ambito pubblico o di interesse pubblico»;

b) la rubrica del Capo I e' sostituita dalla seguente: «Assicurazioni»;

c) all'articolo 120:

1) al comma 1, le parole «private e di interesse collettivo (ISVAP)» sono soppresse;

2) al comma 3, sono aggiunte, in fine, le seguenti parole: «di cui al decreto legislativo 7 settembre 2005, n. 209».

Art. 11

Modifiche alla parte II, titolo X,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo X, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) all'articolo 121:

1) la rubrica e' sostituita dalla seguente: «(Servizi interessati e definizioni)»;

2) dopo il comma 1, e' aggiunto il seguente:

«1-bis. Ai fini dell'applicazione delle disposizioni del presente titolo si intende per:

a) «comunicazione elettronica», ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad uncontraente o utente ricevente, identificato o identificabile;

b) «chiamata», la connessione istituita da un servizio di comunicazione elettronica accessibil e al pubblico che consente la comunicazione bidirezionale;

c) «reti di comunicazione elettronica», i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) «rete pubblica di comunicazioni», una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;

e) «servizio di comunicazione elettronica», i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) «contraente», qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) «utente», qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) «dati relativi al traffico», qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) «dati relativi all'ubicazione», ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) «servizio a valore aggiunto», il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) «posta elettronica», messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.»;

b) all'articolo 122, comma 1, dopo la parola «con» e' soppressa la parola «le» e le parole «di cui all'articolo 13, comma 3» sono soppresse;

c) all'articolo 123:

1) al comma 4, le parole «l'informativa di cui all'articolo 13» sono sostituite dalle seguenti: «le informazioni di cui agli articoli 13 e 14 del Regolamento»;

2) al comma 5, le parole «ad incaricati del trattamento che operano ai sensi dell'articolo 30» sono sostituite dalle seguenti: «a persone che, ai sensi dell'articolo 2-quaterdecies, risultano autorizzate al trattamento e che operano» e le parole «dell'incaricato» sono sostituite dalle seguenti: «della persona autorizzata»;

d) all'articolo 125, comma 1, e' aggiunto, in fine, il seguente periodo: «Rimane in ogni caso fermo quanto previsto dall'articolo 2, comma 1, della legge 11 gennaio 2018, n. 5.»;

e) all'articolo 126, comma 4, le parole «ad incaricati del trattamento che operano ai sensi dell'articolo 30,» sono sostituite dalle seguenti: «a persone autorizzate al trattamento, ai sensi dell'articolo 2-quaterdecies, che operano» e le parole «dell'incaricato» sono sostituite dalle seguenti: «della persona autorizzata»;

f) l'articolo 129 e' sostituito dal seguente:

«Art. 129 (Elenchi dei contraenti). - 1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorita' per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 4, e in conformita' alla normativa dell'Unione europea, le modalita' di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del

pubblico.

2. Il provvedimento di cui al comma 1 individua idonee modalita' per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per finalita' di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale nonche' per le finalita' di cui all'articolo 21, paragrafo 2, del Regolamento, in base al principio della massima semplificazione delle modalita' di inclusione negli elenchi a fini di mera ricerca del contraente per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonche' in tema di verifica, rettifica o cancellazione dei dati senza oneri.»;

g) all'articolo 130:

1) al comma 1, e' aggiunto, in fine, il seguente periodo: «Resta in ogni caso fermo quanto previsto dall'articolo 1, comma 14, della legge 11 gennaio 2018, n. 5.»;

2) al comma 3, le parole «23 e 24» sono sostituite dalle seguenti: «6 e 7 del Regolamento» e le parole «del presente articolo» sono soppresse;

3) al comma 3-bis, le parole «all'articolo 129, comma 1,» sono sostituite dalle seguenti: «al comma 1 del predetto articolo,» e le parole «di cui all'articolo 7, comma 4, lettera b)» sono sostituite dalle seguenti: «di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale»;

4) al comma 3-ter:

4.1 alla lettera b), le parole «codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 12 aprile 2006, n. 163» sono sostituite dalle seguenti «codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50»;

4.2 alla lettera f), le parole «di cui all'articolo 7, comma 4, lettera b)» sono sostituite dalle seguenti: «di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale»;

4.3 alla lettera g), le parole «23 e 24» sono sostituite dalle seguenti «6 e 7 del Regolamento»;

6) al comma 5, le parole «all'articolo 7» sono sostituite dalle seguenti: «agli articoli da 15 a 22 del Regolamento»;

7) al comma 6, le parole «dell'articolo 143, comma 1, lettera b)» sono sostituite dalle seguenti: «dell'articolo 58 del Regolamento»;

h) all'articolo 131, la rubrica e' sostituita dalla seguente: «(Informazioni a contraenti e utenti)»;

i) all'articolo 132:

1) al comma 3, secondo periodo, le parole «, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante» sono soppresse ed e' aggiunto, in fine, il seguente periodo: «La richiesta di accesso diretto alle comunicazioni telefoniche in entrata puo' essere effettuata solo quando possa

derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397; diversamente, i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalita' di cui all'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.»;

2) al comma 5, le parole «ai sensi dell'articolo 17» sono sostituite dalle seguenti: «dal Garante secondo le modalita' di cui all'articolo 2-quinquiesdecies» e le parole da «nonche' a:» a «d)» sono sostituite dalle seguenti: «nonche' ad»;

3) dopo il comma 5, e' aggiunto il seguente: «5-bis. E' fatta salva la disciplina di cui all'articolo 24 della legge 20 novembre 2017, n. 167.»;

l) dopo l'articolo 132-bis sono inseriti i seguenti:

«Art. 132-ter (Sicurezza del trattamento). - 1. Nel rispetto di quanto disposto dall'articolo 32 del Regolamento, ai fornitori di servizi di comunicazione elettronica accessibili al pubblico si applicano le disposizioni del presente articolo.

2. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta, ai sensi dell'articolo 32 del Regolamento, anche attraverso altri soggetti a cui sia affidata l'erogazione del servizio, misure tecniche e organizzative adeguate al rischio esistente.

3. I soggetti che operano sulle reti di comunicazione elettronica garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati.

4. Le misure di cui ai commi 2 e 3 garantiscono la protezione dei dati relativi al traffico ed all'ubicazione e degli altri dati personali archiviati o trasmessi dalla distruzione anche accidentale, da perdita o alterazione anche accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti, nonche' garantiscono l'attuazione di una politica di sicurezza.

5. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia e' definita dall'Autorita' per le garanzie nelle comunicazioni secondo le modalita' previste dalla normativa vigente.

«Art. 132-quater (Informazioni sui rischi). - 1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, mediante linguaggio chiaro, idoneo e adeguato rispetto alla categoria e alla fascia di eta' dell'interessato a cui siano fornite le suddette informazioni, con particolare attenzione in caso di minori di eta', se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio e' al di fuori dell'ambito di applicazione delle misure che il fornitore stesso e' tenuto ad adottare a norma dell'articolo 132-ter, commi 2, 3 e 5, tutti i possibili rimedi e i relativi costi presumibili. Analoghe

informazioni sono rese al Garante e all'Autorita' per le garanzie nelle comunicazioni.».

Art. 12

Modifiche alla parte II, titolo XII,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte II, titolo XII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica e' sostituita dalla seguente: «Giornalismo, liberta' di informazione e di espressione»;

b) all'articolo 136, comma 1:

1) all'alinea, dopo le parole «si applicano» sono inserite le seguenti: «, ai sensi dell'articolo 85 del Regolamento,»;

2) alla lettera c), la parola «temporaneo» e' soppressa, dopo la parola diffusione e' inserita la parola «anche» e le parole «nell'espressione artistica» sono sostituite dalle seguenti: «nell'espressione accademica, artistica e letteraria»;

c) l'articolo 137 e' sostituito dal seguente:

«Art. 137 (Disposizioni applicabili). - 1. Con riferimento a quanto previsto dall'articolo 136, possono essere trattati i dati di cui agli articoli 9 e 10 del Regolamento anche senza il consenso dell'interessato, purche' nel rispetto delle regole deontologiche di cui all'articolo 139.

2. Ai trattamenti indicati nell'articolo 136 non si applicano le disposizioni relative:

a) alle misure di garanzia di cui all'articolo 2-septies e ai provvedimenti generali di cui all'articolo 2-quinquiesdecies;

b) al trasferimento dei dati verso paesi terzi o organizzazioni internazionali, contenute nel Capo V del Regolamento.

3. In caso di diffusione o di comunicazione dei dati per le finalita' di cui all'articolo 136 restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'articolo 1, paragrafo 2, del Regolamento e all'articolo 1 del presente codice e, in particolare, quello dell'essenzialita' dell'informazione riguardo a fatti di interesse pubblico. Possono essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico.»;

d) all'articolo 138, comma 1, le parole «dell'articolo 7, comma 2, lettera a)» sono sostituite dalle seguenti: «dell'articolo 15, paragrafo 1, lettera g), del Regolamento»;

e) la rubrica del Capo II e' sostituita dalla seguente: «Regole deontologiche relative ad attivita' giornalistiche e ad altre manifestazioni del pensiero»;

f) l'articolo 139 e' sostituito dal seguente:

«Art. 139 (Regole deontologiche relative ad attivita' giornalistiche). - 1. Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione da parte del Consiglio nazionale dell'ordine dei giornalisti di regole deontologiche relative al trattamento dei dati di cui all'articolo 136, che prevedono misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quanto riguarda quelli relativi alla salute e alla vita o all'orientamento sessuale. Le regole possono anche prevedere forme particolari per le informazioni di cui agli articoli 13 e 14 del Regolamento.

2. Le regole deontologiche o le modificazioni od integrazioni alle stesse che non sono adottate dal Consiglio entro sei mesi dalla proposta del Garante sono adottate in via sostitutiva dal Garante e sono efficaci sino a quando diviene efficace una diversa disciplina secondo la procedura di cooperazione.

3. Le regole deontologiche e le disposizioni di modificazione ed integrazione divengono efficaci quindici giorni dopo la loro pubblicazione nella Gazzetta Ufficiale della Repubblica italiana ai sensi dell'articolo 2-quater.

4. In caso di violazione delle prescrizioni contenute nelle regole deontologiche, il Garante puo' vietare il trattamento ai sensi dell'articolo 58 del Regolamento.

5. Il Garante, in cooperazione con il Consiglio nazionale dell'ordine dei giornalisti, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio e' tenuto a recepire.

Capo IV
Modifiche alla parte III e agli allegati del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

Art. 13

Modifiche alla parte III, titolo I,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte III, titolo I, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) prima del Capo I e' inserito il seguente:

«Capo 0.I (Alternativita' delle forme di tutela) - Art.140-bis (Forme alternative di tutela). - 1. Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, l'interessato puo' proporre reclamo al Garante o ricorso dinanzi all'autorita' giudiziaria.

2. Il reclamo al Garante non puo' essere proposto se, per il medesimo oggetto e tra le stesse parti, e' stata gia' adita l'autorita' giudiziaria.

3. La presentazione del reclamo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorita' giudiziaria tra le stesse

parti e per il medesimo oggetto, salvo quanto previsto dall'articolo 10, comma 4, del decreto legislativo 1° settembre 2011, n. 150.»;

b) al capo I, le parole «Sezione I - Principi generali» sono soppresse;

c) l'articolo 141 e' sostituito dal seguente:

«Art. 141 (Reclamo al Garante). - 1. L'interessato puo' rivolgersi al Garante mediante reclamo ai sensi dell'articolo 77 del Regolamento.»;

d) dopo l'articolo 141, le parole «Sezione II - Tutela amministrativa» sono soppresse;

e) l'articolo 142 e' sostituito dal seguente:

«Art. 142 (Proposizione del reclamo). - 1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonche' gli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto.

2. Il reclamo e' sottoscritto dall'interessato o, su mandato di questo, da un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle liberta' degli interessati, con riguardo alla protezione dei dati personali.

3. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale mandato, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.

4. Il Garante predispone un modello per il reclamo, da pubblicare nel proprio sito istituzionale, di cui favorisce la disponibilita' con strumenti elettronici.

5. Il Garante disciplina con proprio regolamento il procedimento relativo all'esame dei reclami, nonche' modalita' semplificate e termini abbreviati per la trattazione di reclami che abbiano ad oggetto la violazione degli articoli da 15 a 22 del Regolamento.»;

f) l'articolo 143 e' sostituito dal seguente:

«Art. 143 (Decisione del reclamo). - 1. Esaurita l'istruttoria preliminare, se il reclamo non e' manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento puo' adottare i provvedimenti di cui all'articolo 58 del Regolamento nel rispetto delle disposizioni di cui all'articolo 56 dello stesso.

2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessita' degli accertamenti.

3. Il Garante decide il reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento. In presenza di motivate esigenze istruttorie, che il Garante comunica all'interessato, il reclamo e' deciso entro dodici mesi. In caso di attivazione del procedimento di cooperazione di cui all'articolo 60 del Regolamento, il termine rimane sospeso per la durata del predetto

procedimento.

4. Avverso la decisione e' ammesso ricorso giurisdizionale ai sensi dell'articolo 152.»;

g) l'articolo 144 e' sostituito dal seguente:

«Art. 144 (Segnalazioni). - 1. Chiunque puo' rivolgere una segnalazione che il Garante puo' valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento.

2. I provvedimenti del Garante di cui all'articolo 58 del Regolamento possono essere adottati anche d'ufficio.»;

h) all'articolo 152, il comma 1 e' sostituito dal seguente: «1. Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonche' il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo regolamento, sono attribuite all'autorita' giudiziaria ordinaria.».

Art. 14

Modifiche alla parte III, titolo II,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte III, titolo II, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica e' sostituita dalla seguente: «Autorita' di controllo indipendente»;

b) l'articolo 153 e' sostituito dal seguente:

«Art. 153 (Garante per la protezione dei dati personali). - 1. Il Garante e' composto dal Collegio, che ne costituisce il vertice, e dall'Ufficio. Il Collegio e' costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti devono essere eletti tra coloro che presentano la propria candidatura nell'ambito di una procedura di selezione il cui avviso deve essere pubblicato nei siti internet della Camera, del Senato e del Garante almeno sessanta giorni prima della nomina. Le candidature devono pervenire almeno trenta giorni prima della nomina e i curricula devono essere pubblicati negli stessi siti internet. Le candidature possono essere avanzate da persone che assicurino indipendenza e che risultino di comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche o dell'informatica.

2. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parita'. Eleggono altresi' un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

3. L'incarico di presidente e quello di componente hanno durata settennale e non sono rinnovabili. Per tutta la durata dell'incarico

il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attivita' professionale o di consulenza, anche non remunerata, ne' essere amministratori o dipendenti di enti pubblici o privati, ne' ricoprire cariche elettive.

4. I membri del Collegio devono mantenere il segreto, sia durante sia successivamente alla cessazione dell'incarico, in merito alle informazioni riservate cui hanno avuto accesso nell'esecuzione dei propri compiti o nell'esercizio dei propri poteri.

5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attivita' di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382. Il personale collocato fuori ruolo o in aspettativa non puo' essere sostituito.

6. Al presidente compete una indennita' di funzione pari alla retribuzione in godimento al primo Presidente della Corte di cassazione, nei limiti previsti dalla legge per il trattamento economico annuo omnicomprensivo di chiunque riceva a carico delle finanze pubbliche emolumenti o retribuzioni nell'ambito di rapporti di lavoro dipendente o autonomo con pubbliche amministrazioni statali. Ai componenti compete una indennita' pari ai due terzi di quella spettante al Presidente.

7. Alle dipendenze del Garante e' posto l'Ufficio di cui all'articolo 155.

8. Il presidente, i componenti, il segretario generale e i dipendenti si astengono dal trattare, per i due anni successivi alla cessazione dell'incarico ovvero del servizio presso il Garante, procedimenti dinanzi al Garante, ivi compresa la presentazione per conto di terzi di reclami richieste di parere o interpelli.»;

c) l'articolo 154 e' sostituito dal seguente:

«Art. 154 (Compiti). - 1. Oltre a quanto previsto da specifiche disposizioni e dalla Sezione II del Capo VI del regolamento, il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera v), del Regolamento medesimo, anche di propria iniziativa e avvalendosi dell'Ufficio, in conformita' alla disciplina vigente e nei confronti di uno o piu' titolari del trattamento, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico;

b) trattare i reclami presentati ai sensi del regolamento, e delle disposizioni del presente codice, anche individuando con proprio regolamento modalita' specifiche per la trattazione, nonche' fissando annualmente le priorita' delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di riferimento;

c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2-quater;

d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa

delle funzioni;

e) trasmettere la relazione, predisposta annualmente ai sensi dell'articolo 59 del Regolamento, al Parlamento e al Governo entro il 31 maggio dell'anno successivo a quello cui si riferisce;

f) assicurare la tutela dei diritti e delle liberta' fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice;

g) provvedere altresi' all'espletamento dei compiti ad esso attribuiti dal diritto dell'Unione europea o dello Stato e svolgere le ulteriori funzioni previste dall'ordinamento.

2. Il Garante svolge altresi', ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da atti comunitari o dell'Unione europea e, in particolare:

a) dal Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) e Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II);

b) dal Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attivita' di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI;

c) dal Regolamento (UE) 2015/1525 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che modifica il Regolamento (CE) n. 515/97 del Consiglio relativo alla mutua assistenza tra le autorita' amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola e decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale;

d) dal Regolamento (CE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'Eurodac per il confronto delle impronte digitali per l'efficace applicazione del Regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorita' di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il Regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di liberta', sicurezza e giustizia;

e) dal Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (Regolamento VIS) e decisione n. 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte

delle autorita' designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi;

f) dal Regolamento (CE) n. 1024/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, relativo alla cooperazione amministrativa attraverso il sistema di informazione del mercato interno e che abroga la decisione 2008/49/CE della Commissione (Regolamento IMI) Testo rilevante ai fini del SEE;

g) dalle disposizioni di cui al capitolo IV della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorita' designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

3. Per quanto non previsto dal Regolamento e dal presente codice, il Garante disciplina con proprio Regolamento, ai sensi dell'articolo 156, comma 3, le modalita' specifiche dei procedimenti relativi all'esercizio dei compiti e dei poteri ad esso attribuiti dal Regolamento e dal presente codice.

4. Il Garante collabora con altre autorita' amministrative indipendenti nazionali nello svolgimento dei rispettivi compiti.

5. Fatti salvi i termini piu' brevi previsti per legge, il parere del Garante, anche nei casi di cui agli articoli 36, paragrafo 4, del Regolamento, e' reso nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione puo' procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non puo' essere rispettato il termine di cui al presente comma, tale termine puo' essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

6. Copia dei provvedimenti emessi dall'autorita' giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalita' informatica e' trasmessa, a cura della cancelleria, al Garante.

7. Il Garante non e' competente per il controllo dei trattamenti effettuati dalle autorita' giudiziarie nell'esercizio delle loro funzioni.»;

d) dopo l'articolo 154 sono inseriti i seguenti:

«Art. 154-bis (Poteri). - 1. Oltre a quanto previsto da specifiche disposizioni, dalla Sezione II del Capo VI del Regolamento e dal presente codice, ai sensi dell'articolo 58, paragrafo 6, del Regolamento medesimo, il Garante ha il potere di:

a) adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento;

b) approvare le regole deontologiche di cui all'articolo 2-quater.

2. Il Garante puo' invitare rappresentanti di un'altra autorita' amministrativa indipendente nazionale a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorita' amministrativa indipendente nazionale, prendendo parte alla discussione di argomenti di comune interesse; puo' richiedere, altresi', la collaborazione di personale specializzato addetto ad altra autorita' amministrativa indipendente nazionale.

3. Il Garante pubblica i propri provvedimenti sulla base di quanto previsto con atto di natura generale che disciplina anche la durata di tale pubblicazione, la pubblicita' nella Gazzetta Ufficiale della Repubblica italiana e sul proprio sito internet istituzionale nonche' i casi di oscuramento.

4. In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla raccomandazione 2003/361/CE, il Garante per la protezione dei dati personali, nel rispetto delle disposizioni del Regolamento e del presente Codice, promuove, nelle linee guida adottate a norma del comma 1, lettera a), modalita' semplificate di adempimento degli obblighi del titolare del trattamento.

Articolo 154-ter (Potere di agire e rappresentanza in giudizio). - 1. Il Garante e' legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali.

2. Il Garante e' rappresentato in giudizio dall'Avvocatura dello Stato, ai sensi dell'articolo 1 del regio decreto 30 ottobre 1933, n. 1611.

3. Nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, puo' stare in giudizio tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero avvocati del libero foro.»;

e) all'articolo 155, la rubrica e' sostituita dalla seguente: «(Ufficio del Garante)»;

f) l'articolo 156 e' sostituito dal seguente:

«Art. 156 (Ruolo organico e personale). - 1. All'Ufficio del Garante e' preposto un segretario generale, nominato tra persone di elevata e comprovata qualificazione professionale rispetto al ruolo e agli obiettivi da conseguire, scelto anche tra i magistrati ordinari, amministrativi e contabili, gli avvocati dello Stato, i professori universitari di ruolo in materie giuridiche ed economiche, nonche' i dirigenti di prima fascia dello Stato.

2. Il ruolo organico del personale dipendente e' stabilito nel limite di centosessantadue unita'. Al ruolo organico del Garante si accede esclusivamente mediante concorso pubblico. Nei casi in cui sia ritenuto utile al fine di garantire l'economicita' e l'efficienza dell'azione amministrativa, nonche' di favorire il reclutamento di personale con maggiore esperienza nell'ambito delle procedure concorsuali di cui al secondo periodo, il Garante puo' riservare una quota non superiore al cinquanta per cento dei posti banditi al personale di ruolo delle amministrazioni pubbliche che sia stato assunto per concorso pubblico e abbia maturato un'esperienza almeno triennale nel rispettivo ruolo organico. La disposizione di cui

La “privacy” negli studi professionali

all'articolo 30 del decreto legislativo 30 marzo 2001, n. 165, si applica esclusivamente nell'ambito del personale di ruolo delle autorita' amministrative indipendenti di cui all'articolo 22, comma 1, del decreto-legge 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n.114.

3. Con propri regolamenti pubblicati nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce:

a) l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti e dell'esercizio dei poteri di cui agli articoli 154, 154-bis, 160, nonche' all'articolo 57, paragrafo 1, del Regolamento;

b) l'ordinamento delle carriere e le modalita' di reclutamento del personale secondo i principi e le procedure di cui agli articoli 1, 35 e 36 del decreto legislativo n. 165 del 2001;

c) la ripartizione dell'organico tra le diverse aree e qualifiche;

d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla legge 31 luglio 1997, n. 249, e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23-bis del decreto legislativo 30 marzo 2001, n. 165, tenuto conto delle specifiche esigenze funzionali e organizzative. Nelle more della piu' generale razionalizzazione del trattamento economico delle autorita' amministrative indipendenti, al personale e' attribuito l'80 per cento del trattamento economico del personale dell'Autorita' per le garanzie nelle comunicazioni;

e) la gestione amministrativa e la contabilita', anche in deroga alle norme sulla contabilita' generale dello Stato.

4. L'Ufficio puo' avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, in numero non superiore, complessivamente, a venti unita' e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo.

5. In aggiunta al personale di ruolo, l'Ufficio puo' assumere dipendenti con contratto a tempo determinato o avvalersi di consulenti incaricati ai sensi dell'articolo 7, comma 6, del decreto legislativo n. 165 del 2001, in misura comunque non superiore a venti unita' complessive. Resta in ogni caso fermo, per i contratti a tempo determinato, il rispetto dell'articolo 36 del decreto legislativo n. 165 del 2001.

6. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti, sia durante che dopo il mandato, al segreto su cio' di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

7. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 e agli articoli 57, paragrafo 1, lettera h), 58, paragrafo 1, lettera b), e 62, del Regolamento riveste, nei

limiti del servizio cui e' destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

8. Le spese di funzionamento del Garante, in adempimento all'articolo 52, paragrafo 4, del Regolamento, ivi comprese quelle necessarie ad assicurare la sua partecipazione alle procedure di cooperazione e al meccanismo di coerenza introdotti dal Regolamento, nonche' quelle connesse alle risorse umane, tecniche e finanziarie, ai locali e alle infrastrutture necessarie per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposita missione e programma di spesa del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria e' soggetto al controllo della Corte dei conti. Il Garante puo' esigere dal titolare del trattamento il versamento di diritti di segreteria in relazione a particolari procedimenti.»;

g) l'articolo 157 e' sostituito dal seguente:

«Art. 157 (Richiesta di informazioni e di esibizione di documenti). - 1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante puo' richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.»;

h) l'articolo 158 e' sostituito dal seguente:

«Art. 158 (Accertamenti). - 1. Il Garante puo' disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1, nonche' quelli effettuati ai sensi dell'articolo 62 del Regolamento, sono eseguiti da personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorita' di controllo di altri Stati membri dell'Unione europea.

3. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali.

4. Gli accertamenti di cui ai commi 1 e 2, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al piu' tardi entro tre giorni dal ricevimento della richiesta del Garante quando e' documentata l'indifferibilita' dell'accertamento.

5. Con le garanzie di cui al comma 4, gli accertamenti svolti nei luoghi di cui al medesimo comma possono altresi' riguardare reti di comunicazione accessibili al pubblico, potendosi procedere

all'acquisizione di dati e informazioni on-line. A tal fine, viene redatto apposito verbale in contradditorio con le parti ove l'accertamento venga effettuato presso il titolare del trattamento.»;

i) all'articolo 159:

1) al comma 1, le parole «ai sensi dell'articolo 156, comma 8» sono sostituite dalle seguenti: «su cio' di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete»;

2) al comma 3, dopo le parole «o il responsabile» sono inserite le seguenti: «o il rappresentante del titolare o del responsabile» e le parole «agli incaricati» sono sostituite dalle seguenti: «alle persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies»;

3) al comma 5, le parole «e telefax» sono soppresse;

l) l'articolo 160 e' sostituito dal seguente:

«Art. 160 (Particolari accertamenti). - 1. Per i trattamenti di dati personali di cui all'articolo 58, gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

2. Se il trattamento non risulta conforme alle norme del Regolamento ovvero alle disposizioni di legge o di Regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento e' stato richiesto dall'interessato, a quest'ultimo e' fornito in ogni caso un riscontro circa il relativo esito, se cio' non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.

3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificita' della verifica, il componente designato puo' farsi assistere da personale specializzato tenuto al segreto su cio' di cui sono venuti a conoscenza in ordine a notizie che devono rimanere segrete. Gli atti e i documenti acquisiti sono custoditi secondo modalita' tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal Regolamento di cui all'articolo 156, comma 3, lettera a).

4. Per gli accertamenti di cui al comma 3 relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.».

m) dopo l'articolo 160 e' inserito il seguente:

«Art. 160-bis (Validita', efficacia e utilizzabilita' nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento). - 1. La validita', l'efficacia e l'utilizzabilita' nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a

disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali.».

Art. 15

Modifiche alla parte III, titolo III,
del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte III, titolo III, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) l'articolo 166 e' sostituito dal seguente:

«Art. 166 (Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori). - 1. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-quinquies, comma 2, 2-quinquiesdecies, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132-ter. Alla medesima sanzione amministrativa e' soggetto colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma.

2. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-ter, 2-quinquies, comma 1, 2-sexies, 2-septies, comma 7, 2-octies, 2-terdecies, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110-bis, commi 2 e 3, 111, 111-bis, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132-bis, comma 2, 132-quater, 157, nonche' delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.

3. Il Garante e' l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, paragrafo 2, del Regolamento, nonche' ad irrogare le sanzioni di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1 e 2.

4. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 4 puo' essere avviato, nei confronti sia di soggetti privati, sia di autorita' pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 del Regolamento o di attivita' istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58, paragrafo 1, del Regolamento, nonche' in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.

5. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attivita' di cui al comma 5 configurino una o piu' violazioni indicate nel presente titolo e nell'articolo 83, paragrafi

4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 4 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 10, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalita' del provvedimento da adottare.

6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 6, il contravventore puo' inviare al Garante scritti difensivi o documenti e puo' chiedere di essere sentito dalla medesima autorita'.

7. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 4 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi puo' essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 8, per essere destinati alle specifiche attivita' di sensibilizzazione e di ispezione nonche' di attuazione del Regolamento svolte dal Garante.

8. Entro il termine di cui all'articolo 10, comma 3, del decreto legislativo n. 150 del 2011 previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla meta' della sanzione irrogata.

9. Nel rispetto dell'articolo 58, paragrafo 4, del Regolamento, con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalita' del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 4 ed i relativi termini, in conformita' ai principi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonche' della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione.

10. Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'articolo 83 del Regolamento non si applicano in relazione ai trattamenti svolti in ambito giudiziario.».

b) l'articolo 167 e' sostituito dal seguente:

«Art. 167 (Trattamento illecito di dati). - 1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, e' punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni

di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, e' punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca piu' grave reato, la pena di cui al comma 2 si applica altresi' a chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attivita' di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al piu' tardi al termine dell'attivita' di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto e' stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa e' stata riscossa, la pena e' diminuita.»;

c) dopo l'articolo 167, sono inseriti i seguenti:

«Art. 167-bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala). - 1. Salvo che il fatto costituisca piu' grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, e' punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, e' punito con la reclusione da uno a sei anni, quando il consenso dell'interessato e' richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.».

«Art. 167-ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala). - 1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala e' punito con la reclusione da uno a quattro anni.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.»;

d) l'articolo 168 e' sostituito dal seguente:

«Art. 168 (Falsita' nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante). - 1. Salvo che il fatto costituisca piu' grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, e' punito con la reclusione da sei mesi a tre anni.

2. Fuori dei casi di cui al comma 1, e' punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarita' di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.»;

e) l'articolo 170 e' sostituito dal seguente:

«Art. 170 (Inosservanza di provvedimenti del Garante). - 1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonche' i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 e' punito con la reclusione da tre mesi a due anni.»;

f) l'articolo 171 e' sostituito dal seguente:

«Art. 171 (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori). - 1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, e' punita con le sanzioni di cui all'articolo 38 della medesima legge.»;

g) all'articolo 172, comma 1, dopo le parole «pubblicazione della sentenza» sono aggiunte le seguenti: «, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale».

Art. 16

Modifiche all'allegato A
del decreto legislativo 30 giugno 2003, n. 196

1. L'allegato A e' ridenominato: «Regole deontologiche».

Capo V
Disposizioni processuali

Art. 17

Modifiche al decreto legislativo
1° settembre 2011, n. 150

1. L'articolo 10 del decreto legislativo 1° settembre 2011, n. 150,

e' sostituito dal seguente:

«Art. 10 (Delle controversie in materia di applicazione delle disposizioni in materia di protezione dei dati personali). - 1. Le controversie previste dall'articolo 152 del decreto legislativo 30 giugno 2003, n. 196, sono regolate dal rito del lavoro, ove non diversamente disposto dal presente articolo.

2. Sono competenti, in via alternativa, il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato.

3. Il ricorso avverso i provvedimenti del Garante per la protezione dei dati personali, ivi compresi quelli emessi a seguito di un reclamo dell'interessato, e' proposto, a pena di inammissibilita', entro trenta giorni dalla data di comunicazione del provvedimento ovvero entro sessanta giorni se il ricorrente risiede all'estero.

4. Decorso il termine previsto per la decisione del reclamo dall'articolo 143, comma 3, del decreto legislativo n. 196 del 2003, chi vi ha interesse puo', entro trenta giorni dalla scadenza del predetto termine, ricorrere al Tribunale competente ai sensi del presente articolo. La disposizione di cui al primo periodo si applica anche qualora sia scaduto il termine trimestrale di cui all'articolo 143, comma 3, del decreto legislativo n. 196 del 2003 senza che l'interessato sia stato informato dello stato del procedimento.

5. L'interessato puo' dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle liberta' degli interessati con riguardo alla protezione dei dati personali, di esercitare per suo conto l'azione, ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile.

6. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

7. L'efficacia esecutiva del provvedimento impugnato puo' essere sospesa secondo quanto previsto dall'articolo 5.

8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

9. Nei casi in cui non sia parte in giudizio, il Garante puo' presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali. Il giudice dispone che sia data comunicazione al Garante circa la pendenza della controversia, trasmettendo copia degli atti introduttivi, al fine di consentire l'eventuale presentazione delle osservazioni.

10. La sentenza che definisce il giudizio non e' appellabile e puo' prescrivere le misure necessarie anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), anche

in relazione all'eventuale atto del soggetto pubblico titolare o responsabile dei dati, nonche' il risarcimento del danno.».

Capo VI
Disposizioni transitorie, finali e finanziarie

Art. 18

Definizione agevolata delle violazioni in materia di protezione dei dati personali

1. In deroga all'articolo 16 della legge 24 novembre 1981, n. 689, per i procedimenti sanzionatori riguardanti le violazioni di cui agli articoli 161, 162, 162-bis, 162-ter, 163, 164, 164-bis, comma 2, del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, e le violazioni delle misure di cui all'articolo 33 e 162, comma 2-bis, del medesimo Codice, che, alla data di applicazione del Regolamento, risultino non ancora definiti con l'adozione dell'ordinanza-ingiunzione, e' ammesso il pagamento in misura ridotta di un somma pari a due quinti del minimo edittale. Fatti salvi i restanti atti del procedimento eventualmente gia' adottati, il pagamento potra' essere effettuato entro novanta giorni dalla data di entrata in vigore del presente decreto.

2. Decorsi i termini previsti dal comma 1, l'atto con il quale sono stati notificati gli estremi della violazione o l'atto di contestazione immediata di cui all'articolo 14 della legge 24 novembre 1981, n. 689, assumono il valore dell'ordinanza-ingiunzione di cui all'articolo 18 della predetta legge, senza obbligo di ulteriore notificazione, sempre che il contravventore non produca memorie difensive ai sensi del comma 4.

3. Nei casi di cui al comma 2, il contravventore e' tenuto a corrispondere gli importi indicati negli atti di cui al primo periodo del predetto comma entro sessanta giorni dalla scadenza del termine previsto dal comma 1.

4. Entro il termine di cui al comma 3, il contravventore che non abbia provveduto al pagamento puo' produrre nuove memorie difensive. Il Garante, esaminate tali memorie, dispone l'archiviazione degli atti comunicandola all'organo che ha redatto il rapporto o, in alternativa, adotta specifica ordinanza-ingiunzione con la quale determina la somma dovuta per la violazione e ne ingiunge il pagamento, insieme con le spese, all'autore della violazione ed alle persone che vi sono obbligate solidalmente.

5. L'entrata in vigore del presente decreto determina l'interruzione del termine di prescrizione del diritto a riscuotere le somme dovute a norma del presente articolo, di cui all'art. 28 della legge 24 novembre 1981, n. 689.

Art. 19

Trattazione di affari pregressi

1. Entro il termine di sessanta giorni dalla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana dell'avviso di cui al comma 3, i soggetti che dichiarano il loro attuale interesse possono presentare al Garante per la protezione dei dati personali motivata richiesta di trattazione dei reclami, delle segnalazioni e delle richieste di verifica preliminare pervenuti entro la predetta data.

2. La richiesta di cui al comma 1 non riguarda i reclami e le segnalazioni di cui si e' gia' esaurito l'esame o di cui il Garante per la protezione dei dati personali ha gia' esaminato nel corso del 2018 un motivato sollecito o una richiesta di trattazione, o per i quali il Garante medesimo e' a conoscenza, anche a seguito di propria denuncia, che sui fatti oggetto di istanza e' in corso un procedimento penale.

3. Entro quindici giorni dalla data di entrata in vigore del presente decreto il Garante per la protezione dei dati personali provvede a dare notizia di quanto previsto dai commi 1 e 2 mediante avviso pubblicato nel proprio sito istituzionale e trasmesso, altresi', all'Ufficio pubblicazioni leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

4. In caso di mancata presentazione di una richiesta di trattazione ai sensi del comma 1, e salvo quanto previsto dal comma 2, i relativi procedimenti di cui al comma 1 sono improcedibili.

5. I ricorsi pervenuti al Garante per la protezione dei dati personali e non definiti, neppure nelle forme del rigetto tacito, alla data di applicazione del Regolamento (UE) 2016/679 sono trattati come reclami ai sensi dell'articolo 77 del medesimo Regolamento.

Art. 20

Codici di deontologia e di buona condotta vigenti alla data di entrata in vigore del presente decreto

1. Le disposizioni del codice di deontologia e di buona condotta di cui agli allegati A.5 e A.7 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, continuano a produrre effetti, sino alla definizione della procedura di approvazione cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni:

a) entro sei mesi dalla data di entrata in vigore del presente decreto le associazioni e gli altri organismi rappresentanti le categorie interessate sottopongano all'approvazione del Garante per la protezione dei dati personali, a norma dell'articolo 40 del Regolamento (UE) 2016/679, i codici di condotta elaborati a norma del

paragrafo 2 del predetto articolo;

b) la procedura di approvazione si concluda entro sei mesi dalla sottoposizione del codice di condotta all'esame del Garante per la protezione dei dati personali.

2. Il mancato rispetto di uno dei termini di cui al comma 1, lettere a) e b) comporta la cessazione di efficacia delle disposizioni del codice di deontologia di cui al primo periodo a decorrere dalla scadenza del termine violato.

3. Le disposizioni contenute nei codici riportati negli allegati A.1, A.2, A.3, A.4 e A.6 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, continuano a produrre effetti fino alla pubblicazione delle disposizioni ai sensi del comma 4.

4. Entro novanta giorni dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali verifica la conformita' al Regolamento (UE) 2016/679 delle disposizioni di cui al comma 3. Le disposizioni ritenute compatibili, ridenominate regole deontologiche, sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono successivamente riportate nell'allegato A del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003.

5. Il Garante per la protezione dei dati personali promuove la revisione delle disposizioni dei codici di cui al comma 3 con le modalita' di cui all'articolo 2-quater del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003.

Art. 21

Autorizzazioni generali del Garante
per la protezione dei dati personali

1. Il Garante per la protezione dei dati personali, con provvedimento di carattere generale da porre in consultazione pubblica entro novanta giorni dalla data di entrata in vigore del presente decreto, individua le prescrizioni contenute nelle autorizzazioni generali gia' adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonche' al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento di cui al presente comma e' adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica.

2. Le autorizzazioni generali sottoposte a verifica a norma del comma 1 che sono state ritenute incompatibili con le disposizioni del Regolamento (UE) 2016/679 cessano di produrre effetti dal momento della pubblicazione nella Gazzetta Ufficiale della Repubblica

italiana del provvedimento di cui al comma 1.

3. Le autorizzazioni generali del Garante per la protezione dei dati personali adottate prima della data di entrata in vigore del presente decreto e relative a trattamenti diversi da quelli indicati al comma 1 cessano di produrre effetti alla predetta data.

4. Sino all'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-quater e 2-septies del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 producono effetti, per la corrispondente categoria di dati e di trattamenti, le autorizzazioni generali di cui al comma 2 e le pertinenti prescrizioni individuate con il provvedimento di cui al comma 1.

5. Salvo che il fatto costituisca reato, le violazioni delle prescrizioni contenute nelle autorizzazioni generali di cui al presente articolo e nel provvedimento generale di cui al comma 1 sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento (UE) 2016/679.

Art. 22

Altre disposizioni transitorie e finali

1. Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'articolo 1, paragrafo 3, del Regolamento (UE) 2016/679.

2. A decorrere dal 25 maggio 2018 le espressioni «dati sensibili» e «dati giudiziari» utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo regolamento.

3. Sino all'adozione dei corrispondenti provvedimenti generali di cui all'articolo 2-quinquiesdecies del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, i trattamenti di cui al medesimo articolo, gia' in corso alla data di entrata in vigore del presente decreto, possono proseguire qualora avvengano in base a espresse disposizioni di legge o regolamento o atti amministrativi generali, ovvero nel caso in cui siano stati sottoposti a verifica preliminare o autorizzazione del Garante per la protezione dei dati personali, che abbiano individuato misure e accorgimenti adeguati a garanzia dell'interessato.

4. A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto.

5. A decorrere dal 25 maggio 2018, le disposizioni di cui ai commi

1022 e 1023 dell'articolo 1 della legge 27 dicembre 2017, n. 205 si applicano esclusivamente ai trattamenti dei dati personali funzionali all'autorizzazione del cambiamento del nome o del cognome dei minorenni. Con riferimento a tali trattamenti, il Garante per la protezione dei dati personali puo', nei limiti e con le modalita' di cui all'articolo 36 del Regolamento (UE) 2016/679, adottare provvedimenti di carattere generale ai sensi dell'articolo 2-quinquiesdecies. Al fine di semplificare gli oneri amministrativi, i soggetti che rispettano le misure di sicurezza e gli accorgimenti prescritti con i provvedimenti di cui al secondo periodo sono esonerati dall'invio al Garante dell'informativa di cui al citato comma 1022. In sede di prima applicazione, le suddette informative, se dovute a norma del terzo periodo, sono inviate entro sessanta giorni dalla pubblicazione del provvedimento del Garante nella Gazzetta Ufficiale della Repubblica italiana.

6. Dalla data di entrata in vigore del presente decreto, i rinvii alle disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, abrogate dal presente decreto, contenuti in norme di legge e di regolamento, si intendono riferiti alle corrispondenti disposizioni del Regolamento (UE) 2016/679 e a quelle introdotte o modificate dal presente decreto, in quanto compatibili.

7. All'articolo 1, comma 233, della legge 27 dicembre 2017, n. 205, dopo le parole «le modalita' di restituzione» sono inserite le seguenti: «in forma aggregata».

8. Il registro dei trattamenti di cui all'articolo 37, comma 4, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, cessa di essere alimentato a far data dal 25 maggio 2018. Da tale data e fino al 31 dicembre 2019, il registro resta accessibile a chiunque secondo le modalita' stabilite nel suddetto articolo 37, comma 4, del decreto legislativo n. 196 del 2003.

9. Le disposizioni di legge o di regolamento che individuano il tipo di dati trattabili e le operazioni eseguibili al fine di autorizzare i trattamenti delle pubbliche amministrazioni per motivi di interesse pubblico rilevante trovano applicazione anche per i soggetti privati che trattano i dati per i medesimi motivi.

10. La disposizione di cui all'articolo 160, comma 4, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, nella parte in cui ha riguardo ai dati coperti da segreto di Stato, si applica fino alla data di entrata in vigore della disciplina relativa alle modalita' di opposizione al Garante per la protezione dei dati personali del segreto di Stato.

11. Le disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, relative al trattamento di dati genetici, biometrici o relativi alla salute continuano a trovare applicazione, in quanto compatibili con il Regolamento (UE) 2016/679, sino all'adozione delle corrispondenti misure di garanzia di cui all'articolo 2-septies del citato codice, introdotto dall'articolo 2, comma 1, lett. e) del presente decreto.

12. Sino alla data di entrata in vigore del decreto del Ministro della giustizia di cui all'articolo 2-octies, commi 2 e 6, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, da adottarsi entro diciotto mesi dalla data di entrata in vigore del presente decreto, il trattamento dei dati di cui all'articolo 10 del Regolamento (UE) 2016/679 e' consentito quando e' effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalita' organizzata stipulati con il Ministero dell'interno o con le Prefetture - UTG, previo parere del Garante per la protezione dei dati personali, che specificano la tipologia dei dati trattati e delle operazioni eseguibili.

13. Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie.

14. All'articolo 1 della legge 11 gennaio 2018, n. 5 sono apportate le seguenti modificazioni:

a) al comma 9, le parole «di cui all'articolo 162, comma 2-bis» sono sostituite dalle seguenti: «di cui all'articolo 166, comma 2»;

b) al comma 10, le parole «di cui all'articolo 162, comma 2-quater» sono sostituite dalle seguenti: «di cui all'articolo 166, comma 2».

15. All'articolo 5-ter, comma 1, lettera c), del decreto legislativo 14 marzo 2013, n. 33 le parole «di cui all'articolo 162, comma 2-bis» sono sostituite dalle seguenti: «di cui all'articolo 166, comma 2».

Art. 23

Disposizioni di coordinamento

1. A decorrere dalla data di entrata in vigore del presente decreto:

a) all'articolo 37, comma 2, alinea, del decreto legislativo 18 maggio 2018, n. 51, il riferimento all'articolo 154 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, si intende effettuato agli articoli 154 e 154-bis del medesimo codice;

b) all'articolo 39, comma 1, del decreto legislativo 18 maggio 2018, n. 51, il riferimento agli articoli 142 e 143 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003 si intende effettuato agli articoli 141, 142 e 143 del medesimo codice;

c) all'articolo 42 del decreto legislativo 18 maggio 2018, n. 51, il riferimento all'articolo 165 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, si

intende effettuato all'articolo 166, comma 7, del medesimo codice;

d) all'articolo 45 del decreto legislativo 18 maggio 2018, n. 51, il riferimento all'articolo 143, comma 1, lettera c), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, si intende effettuato all'articolo 58, paragrafo 2, lettera f), del Regolamento (UE) 2016/679.

Art. 24

Applicabilita' delle sanzioni amministrative alle violazioni anteriormente commesse

1. Le disposizioni del presente decreto che, mediante abrogazione, sostituiscono sanzioni penali con le sanzioni amministrative previste dal Regolamento (UE) 2016/679 si applicano anche alle violazioni commesse anteriormente alla data di entrata in vigore del decreto stesso, sempre che il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili.

2. Se i procedimenti penali per i reati depenalizzati dal presente decreto sono stati definiti, prima della sua entrata in vigore, con sentenza di condanna o decreto irrevocabili, il giudice dell'esecuzione revoca la sentenza o il decreto, dichiarando che il fatto non e' previsto dalla legge come reato e adotta i provvedimenti conseguenti. Il giudice dell'esecuzione provvede con l'osservanza delle disposizioni dell'articolo 667, comma 4, del codice di procedura penale.

3. Ai fatti commessi prima della data di entrata in vigore del presente decreto non puo' essere applicata una sanzione amministrativa pecuniaria per un importo superiore al massimo della pena originariamente prevista o inflitta per il reato, tenuto conto del criterio di ragguaglio di cui all'articolo 135 del codice penale. A tali fatti non si applicano le sanzioni amministrative accessorie introdotte dal presente decreto, salvo che le stesse sostituiscano corrispondenti pene accessorie.

Art. 25

Trasmissione degli atti all'autorita' amministrativa

1. Nei casi previsti dall'articolo 24, comma 1, l'autorita' giudiziaria, entro novanta giorni dalla data di entrata in vigore del presente decreto, dispone la trasmissione all'autorita' amministrativa competente degli atti dei procedimenti penali relativi ai reati trasformati in illeciti amministrativi, salvo che il reato risulti prescritto o estinto per altra causa alla medesima data.

2. Se l'azione penale non e' stata ancora esercitata, la trasmissione degli atti e' disposta direttamente dal pubblico ministero che, in caso di procedimento gia' iscritto, annota la

trasmissione nel registro delle notizie di reato. Se il reato risulta estinto per qualsiasi causa, il pubblico ministero richiede l'archiviazione a norma del codice di procedura penale; la richiesta ed il decreto del giudice che la accoglie possono avere ad oggetto anche elenchi cumulativi di procedimenti.

3. Se l'azione penale e' stata esercitata, il giudice pronuncia, ai sensi dell'articolo 129 del codice di procedura penale, sentenza inappellabile perche' il fatto non e' previsto dalla legge come reato, disponendo la trasmissione degli atti a norma del comma 1. Quando e' stata pronunciata sentenza di condanna, il giudice dell'impugnazione, nel dichiarare che il fatto non e' previsto dalla legge come reato, decide sull'impugnazione ai soli effetti delle disposizioni e dei capi della sentenza che concernono gli interessi civili.

4. L'autorita' amministrativa notifica gli estremi della violazione agli interessati residenti nel territorio della Repubblica entro il termine di novanta giorni e a quelli residenti all'estero entro il termine di trecentosettanta giorni dalla ricezione degli atti.

5. Entro sessanta giorni dalla notificazione degli estremi della violazione l'interessato e' ammesso al pagamento in misura ridotta, pari alla meta' della sanzione irrogata, oltre alle spese del procedimento. Si applicano, in quanto compatibili, le disposizioni di cui all'articolo 16 della legge 24 novembre 1981, n. 689.

6. Il pagamento determina l'estinzione del procedimento.

Art. 26

Disposizioni finanziarie

1. Agli oneri derivanti dall'articolo 18 del presente decreto, pari ad € 600.000 per ciascuno degli anni dal 2019 al 2021, si provvede mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 1025, della legge 27 dicembre 2017, n. 205.

2. Dall'attuazione del presente decreto, ad esclusione dell'articolo 18, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni interessate provvedono agli adempimenti previsti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

3. Il Ministro dell'economia e delle finanze e' autorizzato ad apportare le occorrenti variazioni di bilancio.

Art. 27

Abrogazioni

1. Sono abrogati i titoli, capi, sezioni, articoli e allegati del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, di seguito elencati:

a) alla parte I:
1) gli articoli 3, 4, 5 e 6;
2) il titolo II, il titolo III, il titolo IV, il titolo V, il titolo VI e il titolo VII;
b) alla parte II:
1) il capo I del titolo I;
2) i capi III, IV e V del titolo IV;
3) gli articoli 76, 81, 83 e 84;
4) il capo III del titolo V;
5) gli articoli 87, 88 e 89;
6) il capo V del titolo V;
7) gli articoli 91, 94, 95, 98, 112, 117, 118 e 119;
8) i capi II e III del titolo X, il titolo XI e il titolo XIII;
c) alla parte III:
1) la sezione III del capo I del titolo I;
2) gli articoli 161, 162, 162-bis, 162-ter, 163, 164, 164-bis,165 e 169;
3) gli articoli 173, 174, 175, commi 1 e 2, 176, 177, 178 e 179;
4) il capo II del titolo IV;
5) gli articoli 184 e 185;
d) gli allegati B e C.

Il presente decreto, munito del sigillo dello Stato, sara' inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addi' 10 agosto 2018

MATTARELLA

Conte, Presidente del Consiglio dei ministri

Savona, Ministro per gli affari europei

Bonafede, Ministro della giustizia

Bongiorno, Ministro per la pubblica amministrazione

Moavero Milanesi, Ministro degli affari esteri e della cooperazione internazionale

Tria, Ministro dell'economia e delle finanze

Di Maio, Ministro dello sviluppo

economico

Visto, il Guardasigilli: Bonafede

PRIVACY E NOTAIO

N°1-marzo 2018

Di cosa parliamo quando parliamo di...

di Gea Arcella, Notaio

La parola inglese privacy (resa in italiano con **riservatezza**) in abbinata al notaio può sembrare un **ossimoro**, poiché quando si va dal notaio lo si fa per rendere volontariamente pubblico qualcosa: una vendita, una donazione, una convenzione matrimoniale; vi sono anche nell’attività notarile alcune ipotesi di attività coperte da riservatezza (redazione di testamenti) o anche da segreto (segnalazione di operazioni sospette a fini di contrasto del riciclaggio o del terrorismo internazionale) ma sono limitate e specifiche. Naturale destinatario degli atti notarili, infatti, non sono solo le parti, ma è lo **Stato** inteso sia come Pubblica Amministrazione (gli atti notarili sono per legge soggetti alla registrazione fiscale e quindi destinati ad essere conosciuti dall’amministrazione finanziaria nelle sue varie articolazioni tributarie e catastali) che come comunità dei cittadini (l’atto notarile alimenta tutti i principali registri pubblici che regolano i rapporti tra i privati e fondano la certezza dei nostri diritti: registri immobiliari, registri delle imprese, anagrafe, stato civile, registro delle successioni, registro generale testamenti, solo per citarne alcuni tra i più conosciuti e diffusi).

La stessa **Corte di Giustizia Europea** ha riaffermato il principio che la **conoscibilità legale** connessa al pubblico registro è **prevalente** rispetto all’esigenza del singolo di non veder riconnesso il proprio nome a determinate vicende per lui pregiudizievoli, quando è in gioco la completezza stessa del registro e l’affidamento che i terzi vi ripongono.

Il notaio garante

La pubblicità legale è una **garanzia insostituibile di conoscibilità e tracciabilità delle convenzioni tra privati** e dunque rispetto ad essa non può essere invocata alcuna riservatezza, così come saremmo portati ad immaginarla rispetto alle nostre vicende più personali; ciò non toglie che ogni singolo registro abbia delle ben precise **regole di accesso e consultazione** coe-

renti con le sue finalità: una informazione destinata ad un determinato registro deve pertanto essere comunicata solo ad esso e non essere utilizzata, o peggio fraudolentemente carpita, a meri fini di sfruttamento commerciale. **Il notaio è garante** nei confronti del cittadino proprio del rispetto di tali regole e da sempre ha assicurato trasparenza ma anche certezza nella conservazione del dato, coerentemente al moderno principio della “protezione” dei dati personali.

I limiti alla trasparenza

Sul fronte della trasparenza il **Regolamento Ue 2016/679**, noto come **GDPR** (General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali, pone a carico del titolare - nel nostro caso il notaio - un **obbligo di informazione sulle finalità del trattamento, sulle sue modalità ma anche sui diritti** che l’interessato ha. Proprio questi ultimi sono stati in parte rimodulati dal legislatore comunitario, seppure anch’essi vanno contemperati con l’interesse pubblico a cui presidio è stabilito l’intervento notarile, per cui se ciascun interessato avrà sicuramente il diritto di accedere in ogni momento ai dati personali che lo riguardano, altre prerogative - come la rettifica o la cancellazione degli stessi, la limitazione del trattamento e lo stesso diritto all’oblio, rilevante novità portata dal GDPR - incontrano i **limiti** connessi a qualsiasi altro documento pubblico destinato a pubblici archivi, che deve essere conservato inalterato nel tempo nel suo tenore originario, salvo la sua possibilità di rettifica nei modi di legge; pertanto i dati personali conferiti per l’incarico professionale e confluiti nell’atto notarile, non potranno essere oggetto di cancellazione o di limitazione del trattamento quando siano stati riportati in registri o atti tenuti secondo la Legge Notarile (L. 89/1913).

Il trattamento dei dati

Dal punto di vista della **certezza** della conservazione e dell’assoluto rispetto delle libertà personali dei singoli, nonostante la grande mole di dati personali trattati, il notaio **non riutilizza i dati personali** per fini commerciali cedendoli a terzi, né nella sua attività istituzionale effettua alcuna forma di monitoraggio degli interessati, non adotta alcun processo decisionale automatizzato, tanto meno procede a forme di **profilazione** automatizzata degli stessi, tratta solo sporadicamente e non su larga scala categorie particolari di dati (gli ex *dati sensibili*) o dati personali

relativi a condanne penali e reati, di norma non conserva tali dati in modo strutturato, poiché essi sono presenti esclusivamente negli atti notarili, ovvero nei documenti utilizzati per la loro preparazione, e sempre e solo in quanto tale trattamento è previsto da disposizioni di legge o essi gli sono volontariamente affidati.

La protezione dei dati

Se, però, un tempo per la corretta conservazione, o meglio “protezione”, bastavano carta pregiata ed inchiostri indelebili, **l’evoluzione tecnologica** ci consegna l’esigenza di attualizzare questi strumenti adattandoli al mutato contesto storico: le procedure di backup e di ripristino dei dati, così come i dispositivi anti intrusione ed i programmi antivirus non fanno che continuare a garantire che i dati personali contenuti negli atti notarli - ora non più solo cartacei - siano preservati e custoditi nel rispetto delle finalità per le quali sono stati volontariamente affidati al notaio. Altrettanto importante a questi fini è un’attenta **valutazione della propria organizzazione e la distribuzione dei compiti** al suo interno: la sicurezza, come ormai da anni siamo abituati ad intenderla, non costituisce un prodotto da acquistare, ma un **processo complesso** fatto di uomini e mezzi, continuamente in evoluzione in relazione alle nuove esigenze, ma anche alle nuove minacce che possano minare la corretta conservazione dei dati personali.

Rispetto a tali sfide, quindi, il notaio si farà trovare pronto, sia nell’informare correttamente i propri clienti come giustamente richiesto in modo puntuale dal GDPR, sia nell’organizzare il proprio studio in modo da preservare i dati personali, utilizzando gli strumenti tecnici opportuni e coinvolgendo il proprio personale.

Identità, privacy ed antiriciclaggio: linee guida per notai e professionisti

“La protezione dei dati personali nello studio notarile alla luce del Regolamento Europeo (GDPR)”

“GDPR e notaio”

Gea Arcella - **Notaio in Tavagnacco**

Bergamo
16 novembre 2018

La protezione dei dati personali – Le figure coinvolte nel trattamento dati

I principali obblighi del titolare

- Informativa
- Accountability
- Privacy by design e Privacy by default
- Registro delle attività di trattamento
- nomina DPO nei casi previsti
- Valutazione di impatto sulla protezione dei dati nei casi previsti;
- Data Breach;
- Riscontro alle richieste degli interessati.

La protezione dei dati personali - Generalità

“i diritti dell'interessato nel GDPR”

- L’informazione **concisa, trasparente, intelligibile e facilmente accessibile** sui sui diritti
- La conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni di cui all’art.15
- La rettifica (art. 16) e la cancellazione (diritto all’oblio) del dato (art.17)
- La limitazione al trattamento (art. 18) e la notifica (art. 19)
- La portabilità in formato strutturato del dato (art.20)
- L'opposizione trattamento dei propri dati, in qualsiasi momento e senza motivazione in caso di trattamento a fini di marketing (art.22)
- Di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona (art. 22)

La protezione dei dati personali - Generalità

“Le informazioni da fornire nel GDPR”

a)l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo

Art. 13 GDPR

La protezione dei dati personali - Generalità

“informativa nel GDPR”

Assolve ad una funzione di trasparenza, consiste nel rendere edotte le parti dell'uso che si farà dei dati personali comunicati, è obbligatoria per qualsiasi soggetto, invi inclusi quelli pubblici.

Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Art. 12 GDPR

La protezione dei dati personali - Generalità

“Le informazioni da fornire nel GDPR”

a)il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Art. 13 GDPR

L’informativa

L’informativa aggiornata, resa per iscritto o con strumenti elettronici, può essere:

- Generale (v. modello CNN)
- Per i dati grafometrici (v. modello CNN)

Il trattamento lecito per il GDPR

per i dati “comuni”

a)l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b)il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c)il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d)il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e)**il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;**

f)il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Art.6 GDPR

Il trattamento lecito per il GDPR

per i dati “particolari”

Il trattamento è consentito se:

a) l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche

b) il trattamento è necessario per assolvere **gli obblighi ed esercitare i diritti in materia di diritto del lavoro e della sicurezza sociale e protezione sociale**,

c)il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d)il trattamento è effettuato, nell'ambito delle sue legittime attività da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, e che riguardi i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo per le sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e)il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g)il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri,

Art.9 GDPR

Il consenso

Il consenso è necessario:

- Per i dati personali “comuni” solo per le finalità di trattamento **non** connesse all’incarico professionale o all’esercizio di pubblica funzione
- Per i dati particolari o giudiziari, solo se **non** siano già resi pubblici dall’interessato o non rientrino in trattamenti per motivi di interesse pubblico o a fini di archiviazione nel pubblico interesse

Il trattamento lecito senza consenso dei dati particolari

Le materie di rilevate interesse pubblico

Il trattamento dei dati particolari è consentito, in quanto rilevante per l'interesse pubblico, per i soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie indicate dall’art. 2 sexies Codice Privacy.

Nell’elencazione rientrano la maggior parte dei registri pubblici di competenza del notaio

Il trattamento lecito senza consenso dei dati “giudiziari”

Il principio

Il trattamento dei dati relativi a condanne penali e a reati o a connesse misure di sicurezza che non avviene sotto il controllo dell'autorita' pubblica, e' consentito, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le liberta' degli interessati

Il trattamento dei dati “giudiziari” e il contrasto al riciclaggio

La liceità del trattamento

Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza e' consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare gli adempimenti antiriciclaggio:

m)l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo.

Art. 2 -octies, comma 3, lett. m) D.Lgs. 196/2003

Il trattamento dei dati “giudiziari” e il contrasto al riciclaggio

L’obbligo

I soggetti obbligati assicurano che il trattamento dei dati acquisiti nell'adempimento degli obblighi di cui al presente decreto avvenga, per i soli scopi e per le attivita' da esso previsti e nel rispetto delle prescrizioni e delle garanzie stabilite dal Codice in materia di protezione dei dati personali.

Art. 3, comma 9, D.Lgs. 231/2007

Il trattamento dei dati “giudiziari” e il contrasto al riciclaggio

L’obbligo

I soggetti obbligati adottano misure proporzionate ai propri rischi, alla propria natura e alle proprie dimensioni, idonee a rendere note al proprio personale gli obblighi cui sono tenuti ai sensi del presente decreto, ivi compresi quelli in materia di protezione dei dati personali. (omissis)

I sistemi e le procedure adottati ai sensi del presente articolo rispettano le prescrizioni e garanzie stabilite dal presente decreto e dalla normativa vigente in materia di protezione dei dati personali.

Art. 16, comma 3 e 4 , D.Lgs. 231/2007

Il trattamento dei dati “giudiziari” ed il contrasto al riciclaggio

L’obbligo

I soggetti obbligati adottano sistemi di conservazione dei

documenti, dei dati e delle informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali nonche' il trattamento dei medesimi esclusivamente per

le finalita' di cui al presente decreto.

Art. 32, comma 1, D.Lgs. 231/2007

Il trattamento lecito senza consenso dei dati “giudiziari”

I diritti dell'interessato e gli obblighi antiriciclaggio

Il diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia

di riciclaggio;

Art. 2 -undecies, comma 1, lett. a), Codice Privacy

La Responsabilizzazione del titolare del trattamento

La c.d. “accountability”

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Art. 24 GDPR

Le misure di accountability organizzative

Il manuale della sicurezza

descrive la natura dei dati trattati nello studio, l’organizzazione delle persone preposte al loro trattamento, le modalità di assegnazione dei compiti a ciascuna di esse, i processi del trattamento, la soluzione manuale e/o informatica adottata a supporto, è utile riferimento per l’eventuale redazione della DPIA e l’individuazione dei meccanismi di sicurezza, sia fisica degli ambienti che informatica degli strumenti sw ed hw, adottati e da adottare, nonchè dei processi di formazione previsti per il personale ed i collaboratori e contiene gli elementi utili e necessari alla formulazione del Registro delle attività di trattamento .

Le misure di accountability organizzative

Il manuale della sicurezza

Il documento è composto dalle seguenti parti:

1. Informazioni generali sullo studio
2. Dati trattati nello studio
3. Organizzazione delle persone preposte al trattamento e responsabilità assegnate a ciascuna di esse
4. Analisi dei rischi: valutazione di impatto sulla protezione dati (o DPIA)
5. Meccanismi di sicurezza fisica, informatica e telematica adottati negli ambienti di lavoro
6. Criteri e modalità di ripristino della disponibilità dei dati, comunicazione data bridge
7. Processi di formazione del personale adottati e previsti ai fini della sicurezza
8. Categorie di destinatari a cui i dati personali siano stati o saranno comunicati
9. Registro delle attività di trattamento

Le misure di accountability organizzative

Le istruzioni e l’individuazione dei responsabili del trattamento

- Istruire il personale di studio (c.d. incaricati/ designati: v. lettere di incarico)
- Aggiornare i contratti con i responsabili del trattamento con apposite clausole (v. gli esempi di clausole fornite dal CNN)
- Laddove sia dubbio il ruolo del soggetto (titolare/ responsabile del trattamento o si abbia contitolarità nel trattamento ex art. 26 GDPR) scambiarsi la dichiarazione di impegno (v. es. CNN)

La sicurezza del trattamento

Le misure di accountability

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure **tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, **tra le altre, se del caso**:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 32 GDPR

Le misure di accountability tecniche

Revisionare le “misure minime di sicurezza”:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) [soppressa] (1);

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

La protezione dei dati personali – Il registro delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Art. 30 GDPR

Le misure di accountability specifiche

Il registro dei trattamenti

- tenuto in forma scritta, anche in formato elettronico (v. es. forniti dal CNN)
- obbligatorio per le imprese o organizzazioni con 250 o più dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10

Le misure di accountability specifiche

la FAQ del Garante dell’ 8 ottobre 2018 sul registro dei trattamenti:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all’articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all’articolo 10 RGPD.

Le misure di accountability specifiche

Il DPO

Obbligatorio solo quando:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

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 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Le misure di accountability specifiche

La DPIA

Obbligatoria solo quando vengono utilizzate le nuove tecnologie ed il trattamento può presentare un “rischio elevato” per i diritti e libertà delle persone fisiche,oppure quando si esegue

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 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;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

HACIA UN NUEVO DERECHO EUROPEO DE PROTECCIÓN DE DATOS

TOWARDS A NEW EUROPEAN DATA PROTECTION REGIME

Artemi Rallo Lombarte
Rosario García Mahamut
Editores

tirant lo blanch
Valencia, 2015

"Diritto alla protezione dei dati di carattere personale": appunti di un viaggio non ancora concluso[*]

Roberto Lattanzi

Direttore del Servizio studi e documentazione
Garante per la protezione dei dati personali

1. DA NIZZA A LISBONA

All'interno del capo II della Carta dei diritti fondamentali dell'Unione europea, dedicato alle "*Libertà*", il "tradizionale" diritto alla tutela della vita privata è seguito da un "nuovo" diritto fondamentale, il "diritto alla protezione dei dati di carattere personale": questa la locuzione presente nell'articolo 8.

Con la Carta siglata a Nizza il 7 dicembre 2000, specie a seguito del Trattato di Lisbona che alla medesima ha espressamente riconosciuto pieno valore giuridico[1], ha così trovato formale compimento a livello europeo[2] non solo il processo di *costituzionalizzazione* del diritto alla protezione dei dati personali, nel solco di quanto già accaduto in alcune Carte fondamentali nazionali, non di rado con l'ispirazione di interventi autorevoli da parte di alcune corti costituzionali[3], ma anche il percorso di sua *autonomizzazione* rispetto ad altre situazioni giuridiche soggettive[4], in particolare al diritto alla tutela della vita privata[5].

Considerazione, quest'ultima, che dovrebbe spingere l'interprete a non confondere più i tratti del nuovo "diritto" –grazie al quale, invero, si individuano, con formulazione ellittica, una se-

[*] Il contributo riprende, con riferimento ai paragrafi da 1 a 6 (in parte modificati), i contenuti del saggio intitolato *"Diritto alla protezione dei dati di carattere personale": appunti di viaggio*, pubblicato nel volume curato da Mario Napoli, *La libertà*, Milano, 2013, 63 ss. Le considerazioni svolte, proprie dell'autore, non sono riferibili all'Istituzione presso la quale opera.

1 L'art. 6, par. 1 del Trattato sull'Unione europea (in *G.U.* C 83, 30.3.2010, p. 13) dispone infatti che "L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati". Si è così superato il dibattito sul valore (prevalentemente politico piuttosto che) giuridico della Carta, rispetto al quale v., tra i primi contributi, quello di S. Rodotà, *The Charter of Fundamental Rights*, in *Zeitschr. Schweiz. Recht*, 2001, 7.

2 E più precisamente, in base all'art. 16, par. 2 del Trattato sul funzionamento dell'Unione europea (TFUE), nelle materie che rientrano nel campo di applicazione del diritto dell'Unione europea (per le quali cfr., in particolare, gli artt. 2-4 TFUE).

3 Su tale aspetto si tornerà nel par. 3. Quanto alle previsioni inserite nelle carte fondamentali, basti considerare l'art. 35° *Constituição da República Portuguesa*, del 2 aprile 1976 (più volte rimaneggiato), l'art. 18, comma 4, *Constitución española* del 27 dicembre 1978 e l'art. 10 della costituzione olandese del 17 febbraio 1983, come pure, in tempi meno remoti, quelle contenute nei testi costituzionali dei "nuovi" *Länder* tedeschi (come, del resto, di molti Paesi dell'est-Europa). Evidentemente influenzato dalla Carta di Nizza, l'art. 9A della Costituzione greca è stato introdotto nella revisione cui la medesima è stata sottoposta nel 2001.

4 In merito a tale profilo cfr. par. 2.

5 Con riferimento all'ordinamento italiano, v. già S. Rodotà, *Libertà personale. Vecchi e nuovi nemici*, in M. Bovero (a cura di), *Quale libertà. Dizionario minimo contro i falsi liberali*, Roma – Bari, 2004, 33, 52; Id., *Il progetto della Carta europea e l'art. 42 Cost.*, in M. Comporti (a cura di), *La proprietà nella Carta europea dei diritti fondamentali*. Atti del Convegno di studi organizzato presso l'Università degli Studi di Siena, 18-19 ottobre 2002, Milano, 2005, 155, 167; anche U. De Siervo, *La privacy*, in S.P. Panunzio (a cura di), *I diritti fondamentali e le Corti in Europa*, Napoli, 2005, 345, nell'*incipit* del saggio – che, in questo (prezioso ed esplicito) avvertimento, si differenzia dall'articolo pubblicato dall'Autore con il titolo *Tutela dei dati personali e riservatezza*, in *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in onore di Paolo Barile*, Padova, 2003, 297 – chiarisce che la tutela dei dati personali è concetto "ormai largamente autonomo dalla riservatezza personale [e] qualcosa di radicalmente diverso da quello a cui ci si riferiva nel passato anche recente [parlando di *privacy*]"; incertezza, invece, manifestano sul punto ancora R. Leenes – B.-J. Koops – P. De Hert, *Conclusions and Recommendations*, all'esito dello studio comparatistico dagli stessi curato e pubblicato con il titolo *Constitutional Rights and New Technologies. A Comparative Study*, The Hague, 2008, 265, 271.

La "privacy" negli studi professionali

rie di “tecniche di tutela che si offrono all’interessato ove esso intenda reagire ad un trattamento dei dati non conforme a legge”[6]– con altre situazioni giuridiche soggettive; ove si voglia più puntualmente far riferimento alla situazione giuridica soggettiva di cui si tratta, dovranno quindi essere utilizzate con grande parsimonia (o, meglio, tutt’affatto) le locuzioni “vita privata” o riservatezza (familiari alla tradizione italiana) e, a maggior ragione (per quanto divenute di uso comune)[7], “*privacy*” o “diritto alla *privacy*”, ancorché da queste si sia formato, per gemmazione, il diritto alla protezione dei dati[8]. Ciò per la ragione che quest’ultimo ha trovato ormai adeguata caratterizzazione in più corpi normativi, dapprima a livello internazionale e comunitario[9] e, quindi, nazionale[10]; né il richiamo ad un maggiore rigore terminologico riposa sul solo tradizionale brocardo “*entia non sunt multiplicanda sine necessitate*”, ma sull’esigenza di “alleggerire” la clausola generale della “*privacy*”, espressione che, tanto più spazio è venuta guadagnando in estensione, tanto più è venuta mostrando incerti confini (con un accentuarsi del pericolo di un suo uso meno “controllato”)[11].

Diritto, quello in esame, che, mediante l’introduzione di forme di tutela che si appuntano sui dati personali –tasselli del mosaico che va a comporre (e ricomporre) la “persona elettronica”, quale risulta dal trattamento dei dati di volta in volta effettuato[12]–, intende invero proteggere la persona (“in carne e ossa”, verrebbe da aggiungere) da usi impropri o illegittimi delle informazioni

6 A. di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in *Studi in onore di Pietro Rescigno*, II Diritto privato, 1. Persone, famiglia, successioni e proprietà, Milano, 1998, 263, 271.

7 Nel contesto italiano un contributo in questa direzione è stato forse offerto dall’utilizzo colloquiale della dizione “Garante della privacy” attribuito al Garante per la protezione dei dati personali che, con più precisa, ma purtroppo lunga dizione, era stato originariamente denominato “Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali” dall’art. 30, l. 31 dicembre 1996, n. 675.

8 V. già, con riguardo al trattamento di dati personali riferiti alle condizioni di salute, la sentenza della Corte europea dei diritti dell’uomo, 25 febbraio 1997, *Z c. Finlandia*, App. 22009/93; 27 agosto 1997, *M.S. c. Svezia*, App. 20837/92.

9 V. infra parr. 2 e 3. Non deve trarre in inganno la più sobria individuazione dei caratteri del diritto alla protezione dei dati personali contenuta nell’art. 8 della Carta di Nizza (della quale è peraltro criticabile il peso che, diversamente da quanto emerge dall’esperienza, sembra essere attribuito al consenso individuale, i cui limiti quale strumento effettivo di tutela dell’interessato sono stati già da tempo rilevati: cfr. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 45) rispetto al più ricco armamentario del quale il diritto risulta dotato nella direttiva 95/46/CE, posto che l’art. 53 della Carta medesima prevede che “Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell’uomo e delle libertà fondamentali riconosciuti, nel rispettivo ambito di applicazione, dal diritto dell’Unione, dal diritto internazionale, dalle convenzioni internazionali delle quali l’Unione o tutti gli Stati membri sono parti, in particolare dalla Convenzione europea per la salvaguardia dei Diritti dell’Uomo e delle Libertà fondamentali, e dalle costituzioni degli Stati membri”.

10 Per quanto riguarda, in particolare, l’ordinamento italiano, dapprima con la l. 31 dicembre 1996, n. 675 (sulla quale v. G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella società dell’informazione. Commento analitico alle leggi 31 dicembre 1996, núms. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Milano, 1997, *passim*) e, quindi, con il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), con il quale si è riordinata la materia che nel volgere di pochi anni – anche in ragione del parziale esercizio della delega contenuta nella legge 31 dicembre 1996, n. 676 – era divenuta caotica, completando con lo stesso il recepimento delle direttive 95/46/CE e 2002/58/CE.

11 Come è noto, non sono mancate critiche autorevoli rispetto all’espressione “*privacy*” proprio in ragione dell’indeterminatezza che la connota: celebre quella con la quale si apre il saggio di R.A. Posner, *The Right of Privacy*, 12 *Ga. L. Rev.* 393 (1978): “[t]he concept of “privacy” is elusive and ill defined”; Id., *Privacy, Secrecy and Reputation*, 28 *Buff. L. Rev.* 1, 3 (1979); pure R. Wacks, *The Poverty of Privacy*, 96 *L. Quart. Rev.* 73, 86 ss. (1980) ha (criticamente) rilevato l’attitudine del termine “*privacy*” a colonizzare altre (più tradizionali) situazioni giuridiche soggettive e, a trent’anni di distanza, ancora stima che “an acceptable definition of privacy remains elusive” (cfr. Wacks, *Privacy. A Very Short Introduction*, Oxford, 2010, 40).

12 Ciò è reso evidente da F. Hondius, *A Decade of International Data Protection*, 30 *Netherlands Int. L. Rev.* 103, 109 (1983), per il quale “in the information age people should be protected by protecting the information relating to them”; nello stesso senso P. Ancel, *La protection des données personnelles. Aspect de droit privé français*, in *Rev. int. dr. comp.*, 1987, 609, 611 ss., 624.

La “privacy” negli studi professionali

che ad essa si riferiscono o specifiche situazioni giuridiche soggettive alla stessa riconducibili, prime fra tutte la vita privata o l'identità personale[13], assicurando forme di partecipazione della stessa al processo decisionale basato sul trattamento dei dati personali che la riguardano[14] e –come di recente riconosciuto con formulazione felice dalla Corte di Cassazione– concorrendo "a delineare l'assetto di una società rispettosa dell'altro e della sua dignità in condizioni di eguaglianza"[15]. E diritto che, per un verso, ha una portata più ristretta rispetto al diritto alla tutela della vita privata, specie ove si intenda quest'ultimo alla luce della giurisprudenza della Corte europea dei diritti dell'uomo[16], avendo come punto

13 Circostanza che ha indotto autorevole dottrina a ricondurre il diritto alla protezione dei dati personali alla figura del "diritto su diritti": C. Castronovo, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Europa dir. priv.*, 1998, 653, 656. Più in generale, sulla valenza strumentale del rispetto della stessa *privacy* ad altri valori, primo fra tutti la dignità della persona (come in caso di utilizzo delle informazioni personali in chiave discriminatoria), v. il classico saggio di C. Fried, *Privacy*, 77 *Yale L.J.* 475 (1968), ove si mette in luce che "privacy in its dimension of control over information is an aspect of personal liberty" (p. 483).

14 Per il tramite della previa informativa e, in talune ipotesi, del consenso dell'interessato al trattamento dei dati che lo riguarda nonché mediante l'esercizio del diritto d'accesso ai medesimi.

15 Cass. (ord.), 4 gennaio 2011, n. 186, (sintetizzata) in *Giur. it.*, 2011, 256, 257, ordinanza che – peraltro aderendo contenutisticamente a quanto già affermato dal Garante nel provvedimento generale relativo al trattamento dei dati personali nell'amministrazione dei condomini del 18 maggio 2006, punto 3.2, in *www.garanteprivacy.it*, doc. *web* n. 1297626 (oltre che nei Provv.ti 12 dicembre 2001, doc. *web* n. 31007, 20 novembre 2008, doc. *web* n. 1576139 e 8 luglio 2010, doc. *web* n. 1741950) – ha ritenuto illecita (e fonte di responsabilità) l'affissione nella bacheca dell'androne condominiale dell'informazione concernente le posizioni di debito del singolo partecipante al condominio.

16 Per una sintetica analisi della portata applicativa attribuita all'art. 8 della Convenzione cfr. [F.G. Jacobs] – R.C.A. White – C. Ovey, *The European Convention on Human Rights*, V ed., Oxford, 2010, 357 ss.; R.J. Schweizer, *Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz*, in *DuD*, 2009, 462; v. altresì, più diffusamente, gli scritti raccolti in F. Sudre (a cura di), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, 2005.

di riferimento immediato "soltanto" la protezione dei dati relativi a un soggetto individuato o individuabile[17]; ma, per altro verso, diritto che ha portata più ampia rispetto al tradizionale diritto alla riservatezza –la cui eco risuona ancora nella "tutela rinforzata" apprestata nei confronti dei c.d. dati sensibili (art. 8 direttiva 95/46/CE)[18]– trovando applicazione rispetto al trattamento di qualunque dato personale, finanche pubblico[19], e non solo di quelli che interessano la sfera intima dell'individuo[20].

2. DA PARIGI E STRASBURGO …

Il processo di autonomizzazione sopra segnalato, sviluppatosi lungo un ampio arco temporale, ha avuto inizio non appena percepiti –a partire dalla metà degli anni sessanta del secolo scorso,

17 Nozione, quella di "dato personale", assai lata, giunta a ricomprendere anche i campioni biologici [cfr. Corte europea dei diritti dell'uomo (Grande Camera), *S. e Marper c. Regno Unito*, 4 dicembre 2008 (Ricorsi no 30562/04 e 30566/04)], sulla quale v. Gruppo di lavoro per la protezione dei dati personali Articolo 29 (Gruppo articolo 29), *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno 2007, WP 136.

18 Cfr. S. Simitis, *"Sensitive Daten" – Zur Geschichte und Wirkung einer Fiktion*, in *Festschrift für Mario M. Pedrazzini*, Bern, 1990, 469; sia consentito rinviare altresì, anche per ulteriori riferimenti, a Lattanzi, *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in *Europa dir. priv.*, 1998, 713, 742, ove si mette in luce, tra le ragioni addotte per una tutela "rafforzata" di tali informazioni, il loro "tradizionale" prestarsi ad utilizzi di tipo discriminatorio [e in questo senso, in *obiter*, v. ora Cass. (ord.), 4 gennaio 2011, n. 186, cit.].

19 Così Corte europea dei diritti dell'uomo, 4 maggio 2000 (*Rotaru c. Romania*) (Application no. 28341/95); v. pure Cass., 25 giugno 2004, n. 11864, in *Foro it.*, 2004, I, 3380.

20 Cfr. pure Corte di giustizia, 20 maggio 2003, *Rechnungshof/*Österreichischer Rundfunk e al.; *Christa Neukomm* e *Joseph Lauermann/*Österreichischer Rundfunk (casi riuniti C-465/00, C-138/01 e; Cass. (ord.), 4 gennaio 2011, n. 186, cit.

anzitutto negli Stati Uniti d’America[21] e, quindi, in Europa[22] – i rischi connessi all’elaborazione elettronica delle informazioni personali, in particolare la multifunzionalità dei dati personali (con il conseguente possibile impiego degli stessi in contesti e per finalità diversi da quelli che ne avevano giustificato l’originaria raccolta)[23]. È stata questa, infatti, l’occasione (ma non l’unica causa

[21] Cfr., in particolare, A.R. Miller, *Technology, Social Change, and the Constitution*, 33 *Geo. Wash. L. Rev.* 17 (1964); Id., *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 *Mich. L. Rev.* 1089 (1968); A.F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970’s*, 66 *Colum. L. Rev.* 1003 (1966); Id., *Science, Privacy, and Freedom: Issues and Proposals for the 1970’s. Part II: Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance*, 66 *Colum. L. Rev.* 1205 (1966); A.F. Westin – M.A. Baker, *Databanks in a Free Society. Computers, Record-Keeping and Privacy*, New York, 1972; cfr. altresì P. Baran, *Communications, Computers and People*, in *Proceedings of the Fall Joint Computer Conference*, 1965, 45; K.L. Karst, *“The Files”: Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 *L. Contemp. Problems* 354 (1966). Ma si vedano altresì le risultanze delle audizioni svoltesi presso la House of Representatives – Subcommittee of the Committee on Government Operations, “*The Computer and Invasion of Privacy*”, Hearings before a Subcomm. of the Comm. on Government Operations – House of Representatives, 89th Congress, July 26, 27, and 28, 1966, pubblicate in *The Computer and Invasion of Privacy. The Controversial U.S. Government Hearings on the Proposed National Data Center*, New York, 1967, *passim*.

[22] R. Kamlah, *Right of privacy: das allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen*, Köln, 1969, *passim*; U. Seidel, *Datenbanken und Persönlichkeitsrecht. Unter besondere Berücksichtigung der amerikanischen Computer Privacy,* Köln, 1972, 56 ss. e 130 ss.; Simitis, *Datenschutz – Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung*, in *DVR*, 1973, 138; G. Braibant, *La protection des droits individuels au regard du développement de l’informatique*, in *Rev. int. dr. comp.*, 1971, 793. Per una ricognizione sul tema da parte della letteratura italiana v., tra i primi contributi, Rodotà, *Elaboratori elettronici, strutture amministrative e garanzie della collettività*, in *Riv. trim. dir. pubbl.*, 1971, 1841; Id., *Elaboratori elettronici e controllo sociale*, Bologna, 1973, *passim*; R. Pardolesi, *Riservatezza: problemi e prospettive*, in M. Spinelli (a cura di), *Responsabilità civile*, vol. II, Bari, s.d. (ma 1974), 310, 316 ss. e 378 ss.; Baldassarre, *Privacy e Costituzione. L’esperienza statunitense*, Roma, 1974, *passim*.

[23] Cfr. Simitis, *Gesetzliche Regelungen für Personalinformationssysteme – Chancen und Grenzen*, *Informationsgesellschaft oder Überwachungsstaat. Strategien zur Wahrung der Freiheitsrechte im Computerzeitalter*, Wiesbaden, 1986, 43.

efficiente) per elaborare principi e modalità di protezione della persona che di gran lunga sopravanzavano le tradizionali tecniche di tutela dei diritti della personalità (prevalentemente incentrate sul risarcimento del danno e l’inibitoria), inidonee ad offrire una tutela (più tempestiva e, al tempo almeno, più) soddisfacente a fronte del mutato panorama tecno-sociale[24].

Principi e modalità di protezione originali la cui attualità è in larga misura rimasta inalterata nel tempo[25]– destinati a consolidarsi, a livello internazionale, nelle *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* del 23 settembre 1980, aggiornate nel luglio 2013[26], e nella Convenzione n. 108 sulla tutela dell’individuo rispetto al trattamento dei dati a carattere personale adottata dal Comitato dei Ministri del Consiglio d’Europa il 28 gennaio 1981[27]. Testi sostanzialmente coevi e contenutisticamente prossimi, aventi

[24] Cfr. (tra i tanti) A. Proto Pisani, *Le procedure cautelari d’urgenza in relazione ai dati raccolti con elaboratori elettronici*, in V. Zeno Zencovich (a cura di), *Le banche dati in Italia*, Napoli, 1985, 155, 163.

[25] Cfr. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, Brussels, 4.11.2010, COM(2010) 609 final, che pur nella prospettiva di un aggiornamento della direttiva 95/46/CE (sul punto si tornerà nei parr. 6 ss.), riconosce che “the core principles of the Directive are still valid and that its technologically neutral character should be preserved”.

[26] Il processo di revisione ha portato all’introduzione nelle *Guidelines* (consultabili in http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf), ora caratterizzate dal c.d. *risk-based approach*, di nuovi concetti e definizioni (in parte prossimi a quelli sottesi alla riforma del quadro giuridico dell’Unione europea), quali quello di *data security breach notification*, *accountability*, *privacy by design* e *by default*, e dalla previsione di autorità di *enforcement* che possano cooperare tra loro.

[27] Convenzione essa stessa integrata dall’*Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows* nonché da una pluralità di Raccomandazioni settoriali, ed allo stato in corso di revisione (cfr. http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp): per una compilazione dei materiali del Consiglio d’Europa cfr. http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf.

però diverso valore giuridico: non vincolanti le *Guidelines* redatte a Parigi (in particolare grazie alle pressioni esercitate da gruppi d'interesse di marca nordamericana); vincolante, invece, per le Parti contraenti del Consiglio d'Europa, la Convenzione di Strasburgo che, muovendo dalle rilevate carenze dell'art. 8 della Convenzione europea dei diritti umani e delle libertà fondamentali del 1950 (CEDU) nei confronti delle (allora) nuove tecnologie dell'informazione, viene ad integrarne l'armamentario giuridico "*with regard to automatic processing of personal data*" (art. 1, par. 1 Convenzione n. 108/1981)[28]. Già in questo diverso tratto –ma è solo un inciso, dato che la questione richiederebbe una più diffusa analisi– risiede il germe del diverso approccio di fondo che, nella materia della c.d. *informational privacy*, tuttora connota l'ordinamento statunitense rispetto a quelli europei (con riflessi sulla valutazione di adeguatezza del livello di protezione offerto dagli Stati Uniti d'America ai sensi dell'art. 25 direttiva 95/46/CE in relazione al flusso transfrontaliero di dati personali): impostato su interventi normativi di settore il primo (e, va aggiunto, con una spiccata propensione a favore della *self-regulation* nel settore privato, nonostante i limiti dalla stessa manifestati)[29]; i secondi, in-

[28] Il nucleo dei principi poi trasfusi nella Convenzione si rinviene già nell'*Annex* alla Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector del Council of Europe - Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies e nell'*Annex* alla Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).

[29] Si tratta di constatazione ricorrente nell'esperienza statunitense: v., per tutti, J.R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 *Fed. Comm. L. J.* 195, 208 ss. (1992); Id., *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 *Fordham L. Rev.* 137, 148 (1992), che contrappone l' "*ad hoc approach*" americano all' "*omnibus approach*" europeo (p. 153); M.S. Dorney, *Privacy and the Internet*, 19 *Hastings Comm. & Ent. L.J.* 635, 642 ss. (1997). Tralasciando il settore delle telecomunicazioni, tra le principali discipline afferenti alla *informational privacy* (in più occasioni adottate sull'onda di scandali che hanno colpito l'opinione pubblica), sono essenzialmente riconducibili al *Freedom of Information Act*, al *Privacy Act*, al *Fair Credit Reporting Act* (FCRA) nonché al *Video Privacy Protection Act*.

vece, caratterizzati da discipline normative a vocazione generalista[30], integrate dall'operato di autorità di controllo che si vogliono indipendenti[31] e (in modo più marcato nel disegno della Convenzione di Strasburgo) da discipline settoriali[32].

3. (SEGUE) VIA KARLSRUHE …

Anticipando gli esiti della Carta di Nizza, non solo l'enucleazione, ma il processo di *costituzionalizzazione* del diritto alla protezione dei dati personali (cui si è fatto cenno al par. 1) ha conosciuto un sicuro punto di svolta con l'enunciazione del *Recht auf informationelle Selbstbestimmung*[33] da parte del *Bundesverfassungsgericht* (che lo

[30] Ma v. al par. 5 il *patchwork* di regole nei settori del trattamento di dati personali per finalità di polizia e giustizia.

[31] Cfr. Corte di giustizia (Grande Sezione), 9 marzo 2010, Repubblica Federale Tedesca c. Commissione europea (causa C-518/07); 16 ottobre 2012, Commissione c. Austria (C-614/10); 8 aprile 2014, Commissione c. Ungheria (causa C-288/12).

[32] Strategia questa che, con la (pur) significativa eccezione del settore delle telecomunicazioni e, quindi, delle comunicazioni elettroniche, purtroppo non è stata sufficientemente coltivata a livello comunitario (cfr. nota 58). Né (salvo rare eccezioni) l'autoregolazione (regolata) è stata in grado di produrre "regole" sufficientemente strutturate in grado, se non di sostituire, quanto meno di preparare il terreno per futuri interventi normativi: a questo proposito una nota positiva può però ritrarsi dall'ordinamento italiano, nel quale hanno dato buona prova (trovando ampia applicazione nella prassi), in particolare, il "Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica" e, per quanto perfezionabile, il "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".

[33] BVerfG, 15 dicembre 1983, in *BVerfGE*, 65, 1; v. anche in *NJW*, 1984, 419 con il commento di Simitis, *Die informationelle Selbstbestimmung – Grundbedingungen einer verfassungskonformen Informationsordnung*, in *NJW*, 1984, 398. In realtà la dottrina tedesca aveva già preconizzato l'elaborazione del diritto all'autodeterminazione informativa (riecheggiato poi in altri ordinamenti: cfr. in Spagna lo studio di P. Lucas Murillo de la Cueva, *El derecho a la autode-*

àncora ai §§ 1 e 2 del *Grundgesetz*) –e, quindi, esplicitamente, del *Recht auf Datenschutz*[34]– quale concretizzazione della figura (dogmaticamente) sovraordinata dell'*allgemeines Persönlichkeitsrecht*[35]: diritto che, nella prospettiva di questo insegnamento, filtrato al di là del sistema giuridico nel quale è stato formulato[36], consiste, in prima approssimazione, nella libertà accordata all'individuo –salva diversa *chiara* e *dettagliata* previsione normativa[37]– di decidere se e in che misura rendere disponibili informazioni sul proprio conto[38] nonché nel potere di controllarne la successiva circola-

terminación informativa, Madrid, 1990, *passim*): v. lo sguardo retrospettivo di uno dei protagonisti del dibattito in materia offerto da W. Steinmüller, *Das informationelle Selbstbestimmungsrecht: wie es entstand und was man daraus lernen kann*, in *RDV*, 2007, 158.

34 Espressamente enunciato in BVerfG, 27 giugno 1991, in *NJW*, 1991, 2129, 2132.

35 Processo analogo a quello che ha generato l'*informationelle Selbstbestimmungsrecht* è stato di recente reiterato dal *Bundesverfassungsgericht* con l'elaborazione di una figura allo stesso prossima, quella del *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*: cfr. BVerfG, 1 BvR 370/07 del 27 febbraio 2008, in particolare parr. 201 ss., in http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

36 Si tratta di decisione che ha avuto eco assai ampia: sulle orme della giurisprudenza costituzionale tedesca v., ad esempio, nell'ordinamento spagnolo, la fondamentale sentenza del *Tribunal Constitucional*, 30 novembre 2000, n. 292, in *BOE* n. 4, 4 gennaio 2001 (e già in precedenza STC 254/93 del 20 luglio 1993, in *BOE*, n. 197, 18 agosto 1993). Ma pure la *Supreme Court of Canada* ha descritto la *informational privacy* come "the right of the individual to determine for himself when, how and to what extent he will release personal information about himself" (*R. v. Duarte*, [1990] 1 S.C.R. 30, 46).

37 Oltre alla sentenza della Corte costituzionale tedesca, v. altresì Corte europea dei diritti dell'uomo, *Copland v. The United Kingdom*, 3 aprile 2007, 62617/00, punto 46: "the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures".

38 In tal senso si esprimevano già O.M. Ruebhausen – O.G. Brim, *Privacy and Behavioral Research*, 65 *Colum. L. Rev.* 1184, 1189 (1965): "[t]he essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behaviour and opinion are to be shared with or withheld from others".

zione[39] (per far valere, se del caso, ulteriori pretese individuali ed eventualmente attivare il controllo pubblico sui trattamenti effettuati), senza però, come di recente ribadito con forza dalla Corte di giustizia[40], che ciò si traduca in una sorta di signoria dello stesso sui dati personali a sé riferiti[41], sì da orientarne (arbitrariamente o capricciosamente) la circolazione[42].

39 Peculiarità che, per marcare la diversità rispetto al "tradizionale" diritto alla riservatezza, è stata sintetizzata nello slogan "dal segreto al controllo" da Rodotà, *Tecnologie e diritti*, Bologna, 1995, 102. Anche Corte cost., 7 luglio 2005, n. 271, in *Giur. cost.*, 2005, 4, giunge ad affermare che la disciplina sulla protezione dei dati personali attribuisce all'interessato il "potere di controllare le informazioni che lo riguardano e le modalità con cui viene effettuato il loro trattamento".

40 Cfr. Corte di giustizia, 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke* e *Eifert*, punto 48 (con ulteriori riferimenti) e Corte di giustizia (III Sez.), 5 maggio 2011, C-543/09, avente ad oggetto una domanda di pronuncia pregiudiziale proposta dal *Bundesverwaltungsgericht*, secondo la quale il "diritto alla protezione dei dati personali non appare […] come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale" (punto 50).

41 Chiarissimo a questo proposito il passo della sentenza secondo cui il diritto alla protezione dei dati "würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist" (BVerfG, 15 dicembre 1983, *BVerfGE* 65, 43). Nel senso che debba essere esclusa con riguardo alle discipline di protezione dei dati la prospettazione di una sorta di diritto reale dell'interessato sulle "proprie" informazioni mi sono espresso in Lattanzi, *Dati sensibili*, cit., 717 ss. (cui sia consentito rinviare per una più ampia trattazione); ribadisce chiaramente il rifiuto di contaminazione con modelli proprietari di tutela (già argomentato in *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 339) D. Messinetti, *Per un'ecologia della modernità: il destino dei concetti giuridici. L'apertura di R. Nicolò a situazioni complesse*, in *Riv. crit. dir. priv.*, 2010, 23, 32: "si può dire che oggi la riservatezza è incommensurabilmente più esposta di ieri. Tuttavia il rimedio a questa maggiore esposizione non si trova certo riconducendo dati e vicende personali ad un problema appropriativo".

42 Risalente, infatti, è la critica all'approccio quasi proprietario sulle informazioni personali che implicherebbe un illimitato potere di esclusione dell'accesso ad esse in assenza dell'autorizzazione dell'interessato medesimo: cfr. Baldassarre, *Privacy e Costituzione*, cit., 432, secondo il quale "[…] è stato giu-

La natura di diritto fondamentale (*Grundrecht*) attribuito all'*informationelles Selbstbestimmungsrecht* non lascia tuttavia spazio a concezioni grettamente individualistiche o a radicalizzazioni: vale infatti anche in questo ambito l'insegnamento di Luigi Mengoni secondo cui, "in quanto valori costituzionalmente riconosciuti e garantiti, i diritti fondamentali sono sempre intrinsecamente limitati, anche quelli enunciati nella Carta costituzionale senza richiamo, nemmeno generico, di limiti […]. Nel caso di collisione tra due diritti o tra un diritto individuale e un interesse collettivo costituzionalmente protetto occorre procedere a una valutazione ponderata (c.d. bilanciamento) per determinare, in rapporto alle circostanze concrete, la prevalenza dell'uno o dell'altro oppure la misura del contemperamento dell'uno con l'altro"[43]. Operazione (talvolta assai difficoltosa in termini di politica del diritto) rimessa, anzitutto, alla discrezionalità del legislatore: a quest'ultimo spetta la concreta articolazione tra varie opzioni di

stamente detto che una disciplina che si fondasse unicamente sul consenso dell'interessato, onde permettere o meno la lecita intrusione nella propria vita privata, sarebbe una disciplina anacronistica, demagogica e fuorviante, poiché finirebbe per dimenticare sia i più complessi problemi sollevati dall'uso delle più moderne tecnologie, sia, soprattutto, i vari condizionamenti economici e sociali che normalmente incidono sulle manifestazioni di consenso dei singoli. Al contrario, il maggior onere relativo alla tutela della *privacy* non può non gravare sul legislatore, su cui ricade il dovere di stabilire una disciplina rigida e tassativa, laddove siano in questione interessi fondamentali dell'individuo". Non diversa posizione è sostenuta nella comparazione: cfr., tra i tanti, Blume, *New Technologies and Human Rights*, cit., 3.

[43] Mengoni, *Fondata sul lavoro: la Repubblica tra diritti inviolabili e doveri inderogabili di solidarietà*, in *Jus*, 1998, 45, 48. Sulla stessa linea, proprio in materia di protezione dei dati personali, la recente sentenza della Corte di giustizia (Grande Sezione), 9 novembre 2010, *Schecke e Eifert c. Land Hessen* (cause riunite C-92/09 e C-93/09), in part. punti 76 e 77 (con riguardo alla pubblicazione di dati personali in internet da parte di un soggetto pubblico per soddisfare esigenze di trasparenza); v. altresì, a seguito di una domanda di pronuncia pregiudiziale nelle cause riunite C-465/00, C-138/01 e C-139/01, la pronuncia della Corte di giustizia, 20 Maggio 2003, *Rechnungshof c. Österreichischer Rundfunk e a.* e tra *Neukomm e Lauermann c. Österreichischer Rundfunk*, punti 88-90. Ciò, peraltro, risulta chiaramente dall'art. 8, par. 2 CEDU.

politica del diritto (e dunque la definizione dei termini del c.d. bilanciamento), salvo l'assoggettamento delle decisioni frutto del processo legislativo al vaglio di legittimità costituzionale (nonché al controllo di compatibilità con il diritto convenzionale europeo ed eurounitario); solo in seconda battuta, in via interpretativa, l'attività di bilanciamento compete al giudice[44] e, per quanto qui interessa, in materia di protezione dei dati personali, anche alle autorità di controllo.

4. (SEGUES) A BRUXELLES

Quanto finora descritto –unitamente alle esperienze nazionali nel frattempo maturate a partire dalla prima disciplina europea del 1970 nel *Land* dell'Assia– ha, da un lato, rappresentato il retroterra della direttiva 95/46/CE[45], matrice delle vigenti discipli-

[44] Si tratta di profilo già acutamente rilevato, proprio in relazione ai diritti della personalità, da A. Belvedere, *Riservatezza e strumenti d'informazione*, in N. Irti (a cura di), *Dizionari di diritto privato*, vol. 1, Diritto civile, Milano, 1980, 727, 752 ss., del quale è opportuno riferire il passo: "[l]a tutela giuridica della riservatezza nasce quindi dalla valutazione comparativa di interessi, costituzionalmente garantiti e tendenzialmente contrastanti, il cui "peso specifico" andrà, però, valutato caso per caso. Questo difficile bilanciamento di interessi spetta in primo luogo al legislatore ordinario […], ma può essere compiuto anche dal giudice (e in genere dall'interprete) quando si tratti di interpretare le norme già esistenti, di regolarne l'estensione analogica, o di esprimere i principi generali applicabili, quando a questi debba farsi ricorso. Questo apprezzamento comparativo degli interessi in gioco, raggiungerà le punte della massima difficoltà quando a favore sia della circolazione che del "blocco" delle notizie militino ragioni di tutela della libertà del cittadino e della sua possibilità di partecipare alla vita politico-sociale del Paese […]. Più facile invece potrebbe essere la valutazione quando di fronte ad interessi di questo tipo ci fossero – a favore sia del riserbo […], sia della comunicazione […] – interessi di natura principalmente economica, tutelati sì dalla Costituzione (art. 41 e 42), ma subordinatamente alla difesa della libertà e dignità umane […]".

[45] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali,

ne di protezione dei dati personali nell'Unione europea –(pur con i dovuti adattamenti, in larga parte) indifferentemente applicabili a soggetti pubblici e privati– con la correlativa creazione di un ampio spazio geo-economico nel quale la materia è regolata secondo principi armonizzati e, dall'altro, ha favorito il (parziale) superamento della precedente situazione di (più o meno accentuata) frammentazione[46]. Esito divenuto improrogabile a livello comunitario atteso che, volendosi realizzare la libera circolazione di beni, servizi e persone, anche le informazioni personali avrebbero dovuto fluire liberamente all'interno dei confini europei[47], ovviandosi così anche alla situazione di disparità concorrenziale nella quale venivano ad operare le imprese all'interno del mercato unico (quelle obbligate a conformarsi alle regole di protezione dei dati e quelle "autorizzate", dall'inerzia dei legislatori nazionali, a farne a meno).

Questi i fattori che hanno quindi condotto –attraverso un processo ostacolato da forti resistenze[48]– all'adozione della direttiva 95/46/CE, preordinata a rendere possibile, secondo il dettato del

nonché alla libera circolazione di tali dati, in G.U. L 281, 23.11.1995, p. 31.

46 Per una ricognizione dei contenuti delle principali normative europee alle soglie dell'emanazione della direttiva 95/46/CE, cfr. C.O. Dressel, *Die gemeinschaftsrechtliche Harmonisierung des Europäischen Datenschutzrechts*, München, 1995, *passim*; sulle fasi che hanno condotto alla redazione della direttiva e sui diversi modelli che ne hanno influenzato il contenuto v. Simitis, *From the Market to the Polis: The EU Data Protection Directive on the Protection of Personal Data*, 80 *Iowa L. Rev.* 447 (1995) che, correttamente, in altro studio (Simitis, *Datenschutz und Europäische Gemeinschaft*, in *RDV*, 1990, 2, 3) evidenzia l'improprietà del ricorso ai termini "armonizzazione" o "ravvicinamento" delle legislazioni in materia di protezione dei dati (obiettivo proprio delle direttive) posto che, in taluni casi (come quello italiano o greco), la direttiva ha rappresentato l'ennesima spinta a colmare (più o meno ampie) lacune negli ordinamenti nazionali.

47 Cfr. Simitis, *Datenschutz und Europäische Gemeinschaft*, cit., 6.

48 Cfr. Bennett, *Regulating Privacy*, cit., *passim*, seppur con prevalente attenzione agli ordinamenti francese e tedesco.

suo art. 1, la coesistenza di due valori[49]: da un lato, il raggiungimento di un livello di protezione dei diritti fondamentali della persona (come pure si legge nei considerando da 1 a 3 e 10) che il legislatore comunitario ha voluto di grado "elevato"; dall'altro, la realizzazione della libera circolazione dei dati personali (come esplicitato anche nei considerando 3 e 9) all'interno della Comunità europea, dando vita così a un "*informationeller Großraum*"[50] regolato da principi generali, già consolidatisi nelle normative di protezione dei dati personali all'epoca vigenti[51]. In particolare –e senza poter procedere, in questa sede, ad un esame di dettaglio– i principi "cardine" di liceità e correttezza del trattamento, al centro dei quali sta il principio di trasparenza (imperniato sul diritto dell'interessato ad essere informato circa le caratteristiche essenziali del trattamento) e di pubblicità (con la costituzione di registri dei trattamenti liberamente consultabili presso le autorità di controllo), ai quali sono affiancati il principio di qualità dei dati[52], comprensivo dei principi di pertinenza e non eccedenza nell'uso delle informazioni (ulteriormente esplicitato, in taluni ordinamenti, dal principio di "minimizzazione" nella configura-

49 Cfr. Maxeiner, *Freedom of Information and EU Data Protection Directive*, 48 *Fed. Comm. L.J.* 93 (1995).

50 Cfr. A. Einwag, *Grenzüberschreitender Datenverkehr aus Sicht des Bundesbeauftragten für den Datenschutz*, in *RDV*, 1990, 1; non diversamente G. Pearce, *Regulating Personal Data Transfers from the European Union to Third Countries*, 1999, in <www.abs.aston.ac.uk>, p. 4, parla di un "common data protection space enabling the unrestricted transfer of personal data across the UE".

51 Simitis, *From the Market to the Polis*, cit., 451, ha messo in luce, criticandola, la tendenza degli stati membri (che ha contribuito a frenare il processo di adozione della direttiva) nel far filtrare nella disciplina comunitaria per quanto possibile i (propri) modelli nazionali piuttosto che forgiarne uno nuovo (con più ambiziose mete).

52 Cfr. Simitis, *Datenschutz – eine notwendige Utopie*, in R.M. Kiesow – R. Ogorek – S. Simitis (a cura di), *Summa. Dieter Simon zum 70. Geburtstag*, Frankfurt a. M., 2005, 511, 526.

zione dei sistemi informativi)[53], il principio di finalità[54] e quello di sicurezza del trattamento[55]; si devono ricordare, infine, i “diritti” attribuiti all’interessato, primo fra tutti quello di accesso (ten-

[53] *Sparsamkeitsprinzip*, letteralmente “principio di economicità”, inizialmente introdotto nell’ordinamento tedesco (ma già molto tempo addietro Simitis, *Computer, Sozialtechnologie und Jurisprudenz*, cit., 468, ebbe modo di affermare che “nur die Ökonomie der Daten garantiert die individuelle Freiheit”) e, quindi, in quello italiano, con l’introduzione del precetto contenuto nell’art. 3 d.lgs. n. 196/2003, applicazione del più generale principio di necessità previsto all’art. 11, secondo cui “i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l’utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l’interessato solo in caso di necessità”: principio, quello della “minimizzazione” dei dati personali, destinato ad assumere crescente rilevanza nella realtà attuale, specie in caso di interconnessione di diversi archivi [in merito, cfr. le conclusioni di Simitis, *Datenschutz – eine notwendige Utopie*, in R.M. Kiesow – R. Ogorek – S. Simitis (a cura di), *Summa. Dieter Simon zum 70. Geburtstag*, Frankfurt a. M., 2005, 511] e in corrispondenza dei c.d. trattamenti invisibili, rispetto ai quali, oltre ad una ridotta consapevolezza delle operazioni effettuate da parte degli interessati, vi è anche una compressione del potere attribuito agli stessi di influenzare il trattamento (cfr. Institut für Technikfolgen-Abschätzung der österreichischen Akademie der Wissenschaften, *Datenvermeidung in der Praxis. Individuelle und gesellschaftliche Verantwortung. Endbericht*, Wien, 2002, 45 ss.).

[54] Con ragione, insiste sulla sua centralità P. Blume, *New Technologies and Human Rights: Data Protection, Privacy and the Information Society*, Paper no. 67, Institute of Legal Science, Section B, University of Copenhagen, 1998, 8: “[i]t should generally be made clear that the *finalité* principle must be conceived as a human rights principle which must be upheld and taken seriously by supervisory authorities, courts, etc. In this respect it must be maintained that the purpose of data processing should be stated precisely by controllers and also be formulate in a way that is comprehensible for the average individual. In particular it should be seen as unacceptable that a multitude of purposes are stated as the reason for the collection of data because this in reality means that the individual cannot grasp the situation”. Merita aggiungere che la finalità del trattamento deve essere attuale, e non futura e ipotetica.

[55] Così li sintetizza Rodotà, *Protezione dei dati e circolazione delle informazioni*, (già in *Riv. crit. dir. priv.*, 1984, 757 e) in Id., *Tecnologie e diritti*, Bologna, 1995, 41, 62 ss.

denzialmente gratuito) ai dati che lo riguardano[56], che prelude ad ulteriori facoltà attribuite all’interessato medesimo, quali –ricorrendone i presupposti– la richiesta di rettifica o cancellazione dei dati ovvero di opposizione ad un loro ulteriore trattamento o, ancora, quella volta a conoscere l’origine delle informazioni nonché le categorie di soggetti o i soggetti cui le stesse sono state comunicate[57].

5. SCHENGEN – L’ AJA - PRÜM

Per quanto la direttiva 95/46/CE (e le rispettive discipline nazionali cui è stato affidato il suo recepimento)[58] abbia occupato (e tuttora occupi) larga parte della scena, essendo la sede dei

[56] Si tratta di una delle prerogative fondamentali riconosciute all’interessato il quale “di regola non [sa] cosa sta succedendo e non lo [può] scoprire, perché un abuso di questo tipo viene normalmente nascosto alla fonte, anche se potrebbe avere conseguenze reali sulla vita delle persone”: così A. Belsey, *Privacy, pubblicità e politica*, in A. Belsey – R. Chadwick, *Etica e giornalismo* (orig., *Ethical Issues in Journalism and the Media*, 1992, trad. it. di C. Montani), Torino, 1996, 109, 112. Uno strumento, non altrimenti ricavabile dall’ordinamento (come ebbi modo di rilevare in Lattanzi, *La tutela dei dati personali dopo la ratifica della Convenzione europea sulle banche-dati*, in *Dir. inf.*, 1990, 220, 227) – oggi disciplinato in tutte le normative di protezione dei dati – che si affianca (rimanendo tuttavia da esse distinto) ad altre ipotesi (ciascuna delle quali ha un proprio autonomo fondamento) di accesso (anziché a *dati*) a *documenti*: in merito, v. da ultimo la sentenza della Corte di giustizia (Terza Sezione) del 17 luglio 2014 (cause riunite C 141/12 e C 372/12), Y.S. (C-141/12), Minister voor Immigratie, Integratie en Asiel (C-372/12) c. Minister voor Immigratie, Integratie en Asiel (C-141/12), M S (C-372/12).

[57] Profilo, quest’ultimo, assai delicato (e sul quale opportunamente, in sede di revisione della direttiva 95/46/CE, si dovrebbe intervenire), che ha determinato la pronuncia della Corte di Giustizia, 7 maggio 2009, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer* (C-553/07), in particolare ai punti 57, 63 e 64.

[58] Merita qui ricordare che, coerentemente con quanto riportato nel considerando 68 della direttiva 95/46/CE, solo nel settore delle telecomunicazioni e, quindi, delle comunicazioni elettroniche, si sono introdotte discipline armonizzate a livello europeo in materia di riservatezza e protezione dei

principi di portata generale appena indicati, essa trova però applicazione alle sole materie (in passato denominate) di c.d. primo pilastro, restando invece estranea alle materie di c.d. secondo e terzo pilastro[59]. Ciò risulta a chiare lettere, peraltro, dall'art. 3, par. 2 direttiva 95/46/CE che espressamente esclude dal proprio ambito di applicazione, tra l'altro, i trattamenti "effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale"[60].

Per quanto in più di una circostanza sia risultato difficoltoso distinguere chiaramente i confini tra i vari "pilastri"[61], nel (preesi-

dati personali, rispettivamente con le direttive 97/66/CE (poi abrogata) e 2002/58/CE.

59 Come è noto, a far data dall'entrata in vigore del Trattato di Maastricht (1° novembre 1993) e sino al 1° dicembre 2009, con il Trattato di Lisbona, la struttura istituzionale dell'Unione europea si è articolata su tre "pilastri".

60 V. altresì i considerando 13 e 16. Cfr. P. De Hert, *Trends in European police and judicial cooperation with regard to data exchange*, in *Panopticon*, Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk, 2004, vol. 25, no 1, (26-56), 38 in http://www.panopticon-net.org.

61 Cfr. Corte di Giustizia (Grande Sezione), 30 maggio 2006, *Parlamento europeo c. Consiglio dell'Unione europea* (cause riunite C-317/04 e C-318/04), con la quale si sono annullate la decisione del Consiglio 2004/496/CE del 17 maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (*Passenger Name Record*, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti, e la decisione 2004/535/CE della Commissione 14 maggio 2004 relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti *United States' Bureau of Customs and Border Protection*; Corte di Giustizia (Grande Sezione), 10 febbraio 2009, *Irlanda/Parlamento europeo, Consiglio dell'Unione europea* (causa C-301/06) con la quale si è, invece, respinto il ricorso per

stente) terzo pilastro, relativo alle materie di cooperazione di polizia e giudiziaria in materia penale, hanno continuato a trovare applicazione le discipline nazionali, dettate avendo principalmente a mente i principi della menzionata Convenzione di Strasburgo n. 108/1981[62], oltre ad una serie di altri strumenti i quali pure, sommatisi nel tempo in assenza di un disegno unitario a livello comunitario (prima ancora che di un quadro regolamentare unitario), hanno fatto riferimento alla Convenzione di Strasburgo quale standard minimo[63]: ciò risulta chiaramente dalle regole che presiedevano al funzionamento del Sistema d'informazioni

l'annullamento della direttiva 2006/24/CE del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

62 Normative arricchite, in taluni ordinamenti, dalle regolamentazioni che hanno tenuto conto della Recommendation R (87) 15 regulating the use of personal data in the police sector, 17.9.1987 e della Recommendation R (92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system. Talvolta normative lacunose: si pensi, rimanendo all'ordinamento italiano, alla (persistente) inerzia nell'adozione dell'allegato C al Codice in materia di protezione dei dati personali, contenente i trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia, da adottarsi con decreto del Ministro della giustizia ai sensi dell'art. 46 d.lgs. n. 196/2003 e con decreto del Ministro dell'interno ai sensi dell'art. 53 d.lgs. n. 196/2003. In materia cfr. il parere del Garante del 10 settembre 2009, in http://www.garanteprivacy.it doc. *web* n. 1658464 che in passato ebbe a segnalare al Presidente del Consiglio dei ministri e al Ministro della difesa la necessità di un intervento, a livello legislativo e regolamentare, per integrare la normativa che regola attualmente le varie attività di raccolta e utilizzo dei dati da parte dell'Arma dei Carabinieri: cfr. Segnalazione 11 gennaio 2001, in *Bollettino* n. 16/gennaio 2001, p. 27 e doc. *web* n. 1074795.

63 Cfr. P. de Hert – V. Papakonstantinou – C. Riehle, *Data protection in the third pillar: cautious pessimism*, in M. Mike (a cura di), *Crime, rights and the EU: the future of police and judicial cooperation*, Justice, London, 2008, 121, 162.

Schengen (SIS)[64] –ora integrato nel quadro dell’Unione[65]– e del sistema di informazione visti (VIS)[66] o con le quali si sono regolati i flussi informativi necessari al perseguimento delle finalità istituzionali di Europol[67] ed Eurojust[68] o, ancora, inserite nella

64 Il SIS è stato istituito a norma del titolo IV della Convenzione del 1990 di applicazione dell’accordo di Schengen del 14 giugno 1985 relativo all’eliminazione graduale dei controlli alle frontiere comuni. Cfr. il Capitolo 3 della Convenzione di applicazione dell’Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell’Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all’eliminazione graduale dei controlli alle frontiere comuni dedicato alla “Protezione dei dati personali e sicurezza dei dati nel quadro del sistema d’informazione Schengen”, con particolare riferimento agli artt. 115 e 117 per i richiami ai principi della Convenzione di Strasburgo.

65 Cfr. Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio del 20 dicembre 2006 sull’istituzione, l’esercizio e l’uso del sistema d’informazione Schengen di seconda generazione (SIS II) e la Decisione 2007/533/GAI del Consiglio del 12 giugno 2007 sull’istituzione, l’esercizio e l’uso del sistema d’informazione Schengen di seconda generazione (SIS II), che costituisce la base giuridica necessaria per disciplinare il SIS II nelle materie rientranti nell’ambito di applicazione del trattato sull’Unione europea.

66 Cfr. (il testo consolidato del) Regolamento (CE) n. 767/2008 del Parlamento Europeo e del Consiglio del 9 luglio 2008 concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (Regolamento VIS).

67 V. la Decisione del Consiglio del 6 aprile 2009 che istituisce l’Ufficio europeo di polizia (Europol) (2009/371/GAI), in *G.U.* L 121, 15.5.2009, p. 37, con particolare riferimento al capo II dedicato ai “Sistemi di trattamento delle informazioni” (e all’art. 27 per il rinvio ai principi della Convenzione di Strasburgo). Cfr., ora, nell’ambito del progetto di riforma avviato, la Proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce l’Agenzia dell’Unione europea per la cooperazione e la formazione delle autorità di contrasto (Europol) e abroga le decisioni 2009/371/GAI del Consiglio e 2005/681/GAI del Consiglio, considerando 32.

68 Cfr. la versione consolidata della decisione 2002/187/GAI del Consiglio, del 28 febbraio 2002, che istituisce Eurojust per rafforzare la lotta contro le forme gravi di criminalità, modificata dalla decisione 2003/659/GAI del Consiglio e dalla decisione 2009/426/JHA del Consiglio, del 16 dicembre 2008, relativa al rafforzamento di Eurojust, con particolare riferimento all’art. 14 per il richiamo dei principi della Convenzione di Strasburgo cui si sono

disciplina convenzionale del trattato di Prüm (sottoscritto il 27 maggio 2005)[69].

In tale ambito, solo tardivamente, e dopo una lunga trattativa, è stata adottata la Decisione quadro 2008/977/GAI[70], invero per controbilanciare l’introduzione a livello comunitario del (tuttora non chiaramente precisato) c.d. principio di disponibilità, secondo il quale le informazioni (anche personali) necessarie per contrastare la criminalità dovrebbero attraversare le frontiere interne dell’Unione europea senza ostacoli[71]. La decisione tuttavia è stata

ispirate le Disposizioni del regolamento interno dell’Eurojust relative al trattamento e alla protezione dei dati personali (Testo adottato all’unanimità dal collegio dell’Eurojust nella riunione del 21 ottobre 2004 e approvato dal Consiglio il 24 febbraio 2005), in *G.U.* C 68, 19.3.2005, p. 1. Il processo di revisione che caratterizza questo momento, e di cui si dirà meglio in seguito, tocca anche questo settore; nell’agosto 2013 la Commissione europea ha infatti presentato due nuove proposte di regolamento che sono attualmente in discussione: Proposta di regolamento del Consiglio che istituisce la Procura europea (n. COM (2013) 534 definitivo); Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce l’Agenzia dell’Unione europea per la cooperazione giudiziaria penale (Eurojust) (n. COM (2013) 535 definitivo).

69 V. la Decisione 2008/615/GAI del Consiglio del 23 giugno 2008 sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera**,** in *G.U.* L 210, 6.8.2008, p. 1, con particolare riferimento al capo 6 contenente “Disposizioni generali relative alla protezione dei dati” (e all’art. 25 il richiamo alla Convenzione di Strasburgo).

70 Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell’ambito della cooperazione giudiziaria e di polizia in materia penale, pubblicata in *G.U.* L 350 del 30.12.2008, p. 60.

71 Principio originariamente introdotto nel Programma dell’Aja, accantonato con la Decisione quadro 2006/960/GAI del Consiglio del 18 dicembre 2006 relativa alla semplificazione dello scambio di informazioni e *intelligence* tra le autorità degli Stati membri dell’Unione europea incaricate dell’applicazione della legge (in *G.U.* L 386, 29.12.2006, p. 89), ma nuovamente menzionato nel Programma di Stoccolma (punto 4.2.2., p. 18: “Il principio di disponibilità continuerà ad imprimere un notevole slancio a questi lavori”). V. in merito le considerazioni critiche svolte nel Parere del Garante europeo della protezione dei dati (GEPD) sulla proposta di Decisione quadro del

oggetto di numerose critiche già solo in relazione al limitato ambito di applicazione che la connota[72], confinato ai soli dati trattati all'esito della cooperazione tra autorità degli Stati membri e non esteso ai c.d. trattamenti domestici" (quelli, cioè effettuati a livello nazionale), né (come risulta espressamente dal considerando 39) a tutti i trattamenti di dati personali effettuati nell'ambito della cooperazione giudiziaria in materia penale e di polizia disciplinati dagli specifici strumenti sopra menzionati, alla cui regolamentazione (comprensiva di meccanismi di controllo) la stessa è venuta quindi ad affiancarsi.

6. DOPO LISBONA

Se, come si è accennato, il diritto alla protezione dei dati personali ha trovato il proprio culmine nella Carta dei diritti fondamentali (e nei Trattati dell'Unione europea) e, come si è visto, a macchia di leopardo, ha interessato settori specifici, radicandosi nel panorama europeo[73], deve tuttavia aggiungersi che la situa-

Consiglio sullo scambio di informazioni in virtù del principio di disponibilità (COM (2005)490 def.), in *G.U.* C 116, 17.5.2006, p. 8, in particolare ai punti 27 ss.

72 Per ulteriori rilievi, v. le considerazioni svolte dal Garante europeo della protezione dei dati in tre distinti pareri resi nel corso del processo di approvazione della Decisione quadro (Parere 19 dicembre 2005, in *G.U.* C 47, 25.02.2006, p. 27; 29 novembre 2006, in *G.U.* C 91, 26.04.2007, p. 9; 27 aprile 2007, in *G.U.* C 139, 23.06.2007, p. 1), ribadite nel parere del 5 ottobre 2010 sull'ordine di protezione europeo e sull'ordine europeo di indagine penale (in *G.U.* C 355, 29.12.2010, p. 1, punti 51 ss.). Analoghi rilievi sono stati sollevati dal Gruppo di lavoro dell'articolo 29 per la protezione dei dati e dal Gruppo di lavoro "polizia e giustizia", *Il futuro della privacy. Contributo congiunto alla consultazione della Commissione europea sul quadro giuridico relativo al diritto fondamentale alla protezione dei dati personali*, WP 168, adottato il 1° dicembre 2009, pp. 4, 7 e ss. e 24 e ss.

73 Cfr. Report from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions, *2010 Report on the Application of the EU Charter of Fundamental Rights*,

zione, lungi dall'essere pervenuta ad un assestamento, è in pieno movimento.

Il consolidamento dello Spazio europeo di libertà, sicurezza e giustizia[74] e le modifiche introdotte con il trattato di Lisbona[75] hanno mutato la cornice istituzionale entro la quale il diritto alla protezione dei dati personali è oggi chiamato ad operare all'interno dell'Unione europea, estendendola ben al di là degli angusti confini (del mercato interno) entro i quali la direttiva 95/46/CE è stata costretta[76]. Ciò risulta chiaramente dall'art. 16 TFEU, disposizione che (abbandonata la collocazione più "periferica" nella quale la materia della protezione dei dati era confinata con il previgente articolo 286 TCE) trova applicazione generale nelle materie di competenza dell'Unione[77].

Brussels, 30.3.2011, COM(2011) 160 final, p. 6. Sulla pressante necessità percepita dalle istituzioni europee di aggiornare il quadro normativo in materia, v. ora Report from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions, *2013 Report on the Application of the EU Charter of Fundamental Rights*, Brussels, 14.4.2014, COM(2014) 224 final, p. 6.

74 Cfr., per primi riferimenti, D. Rinoldi, *Lo spazio di libertà, sicurezza e giustizia*, Napoli, 2010, *passim*; con particolare riferimento alle interrelazioni con le discipline di protezione dei dati personali, v. le critiche sollevate da F. Dumortier – C. Gayrel – Y. Poullet – J. Jouret – D. Moreau, *La protection des données dans l'espace européen de liberté, de sécurité e de justice*, in *J. dr. eur.*, 2010, 33 ss.

75 In particolare l'art. 87, par. 2, lett. *a*), TFEU, disposizione che, in materia di cooperazione di polizia, rimette al Parlamento europeo e al Consiglio (chiamati a deliberare secondo la procedura legislativa ordinaria) il compito di stabilire misure riguardanti "la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni", da svolgersi in conformità ai principi di protezione dei dati personali, pur tenendo conto delle necessarie peculiarità che tali trattamenti richiedono.

76 E non diversamente la direttiva 2002/58/CE, con le forzature che si sono poste in essere con la direttiva 2006/24/CE per la conservazione dei dati di traffico (cui si è fatto cenno in nota 59).

77 La menzionata disposizione prevede che "Parlamento europeo e Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli

Il venir meno del c.d. “terzo pilastro” e l’attribuzione della competenza in materia di cooperazione giudiziaria e di polizia all’Unione europea[78] hanno reso ormai superata la formulazione dell’art. 3, par. 2 della direttiva 95/46/CE, non più coerente, almeno in parte, con la prospettiva schiusa dal trattato di Lisbona. Alla luce di ciò, pur tenendo a mente la peculiarità degli ambiti appena richiamati[79], ma considerando altresì l’intenso utilizzo di dati personali, spesso di natura sensibile, che in essi si realizza –con trattamenti che viepiù erodono il principio di finalità[80], an-

organismi dell’Unione, *nonché da parte degli Stati membri nell’esercizio di attività che rientrano nel campo di applicazione del diritto dell’Unione*, e le norme relative alla libera circolazione di tali dati”, ribadendo che il “rispetto di tali norme è soggetto al controllo di autorità indipendenti” (mio il corsivo). Peraltro grande cautela traspare dalla 20ª Dichiarazione relativa all’art. 16 TFUE secondo cui “La conferenza dichiara che, ogniqualvolta le norme in materia di protezione dei dati personali da adottare in base all’articolo 16 possano avere implicazioni dirette per la sicurezza nazionale, si dovrà tenere debito conto delle caratteristiche specifiche della questione. Rammenta che la legislazione attualmente applicabile (vedasi in particolare la direttiva 95/46/CE) prevede deroghe specifiche al riguardo”.

78 Ancorché, proprio in tale ambito, lo *status quo* sia destinato (nei fatti) a sopravvivere per i cinque anni successivi all’entrata in vigore del trattato di Lisbona (arg. ex art. 10 del Protocollo n. 36 sulle disposizioni transitorie allegato ai trattati dell’Unione europea).

79 Peraltro ribadita nella 21ª Dichiarazione relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia secondo cui “La conferenza riconosce che potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all’articolo 16 del trattato sul funzionamento dell’Unione europea”.

80 Non solo considerato il crescente accesso ad archivi formati da soggetti privatie nello svolgimento della propria attività d’impresa da parte di *law enforcement agencies* (volendo usare l’ampia terminologia in uso nel contesto sovranazionale), ma anche per il “via libera” contenuto nell’art. 11, par. 1, lett. *d*), Decisione quadro 2008/977/GAI secondo cui “i dati personali trasmessi o resi disponibili dall’autorità competente di un altro Stato membro possono essere successivamente trattati” per “qualsiasi altra finalità, soltanto previa autorizzazione dello Stato membro che trasmette i dati o con il consenso

che in ragione della crescente “interoperabilità” degli archivi[81]–, si è reso più che opportuno un complessivo ripensamento sulla materia –peraltro chiaramente anticipato nella Comunicazione della Commissione europea intitolata *Un approccio globale alla protezione dei dati personali nell’Unione europea*[82]– per quanto non sia affatto scontato che, nell’ambito delle modifiche attese, si riuscirà a porre rimedio al *patchwork* di discipline cui si è fatto cenno nel paragrafo che precede[83]. *Patchwork* che sembra altresì caratterizzare, peraltro, la strategia europea in materia di antiterrorismo[84]:

della persona interessata espresso conformemente alla legislazione nazionale”. Cfr. I. Andoulsi, *Personal Data Protection and the First Implementation Semester of the Lisbon Treaty: Achievements and Prospects*, in *New J. Europ. Criminal L.*, 2010, 362.

81 Cfr. S. Preuss-Laussinotte, *L’élargissement problématique de l’accès aux bases de données européennes en matière de sécurité*, in *Cultures & Conflits*, Numéro 74, 2009, 81; P. De Hert – S. Gutwirth, *Interoperability of police databases within the European Union: an accountable political choice?*, TILT Law & Technology Working Paper Series, n° 001/2006, April 2006, in http://ssrn.com/abstract=971855.

82 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell’Unione europea*, Bruxelles, 4.11.2010, COM(2010) 609 definitivo, punto 2.3.

83 Invero anche tra i *privacy advocates* si riscontrano posizioni diverse: a chi (operando all’interno del Garante europeo per la protezione dei dati) si pronunciava a favore di un *framework* normativo unitario [cfr. H. Hijmans – A. Scirocco, *Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?*, 46 *Common Market L. Rev.* 1485, 1496 ss. (2009)] si oppone chi (dall’osservatorio di Eurojust) ritiene preferibile mantenere il sistema vigente, ormai collaudato [cfr. D. Alonso Blas, *Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom*, in *ERA Forum*, 2010, 233: Ead., *First Pillar and Third Pillar: Need for a common approach?*, in S. Gutwirth – Y. Poullet – P. de Hert – C. de Terwangne – S. Nouwt (a cura di), *Reinventing Data Protection*, Bruxelles, 2009, 225].

84 Strategia che, peraltro, si muove nel solco già segnato dal Consiglio dell’Unione europea del 30 novembre 2005 (cfr. Council of the European Union, Presidency and the Counterterrorism Coordinator, The European Union Counter-Terrorism Strategy, Document 14469/4/05 REV 4, November 30, 2005) relativo alla strategia antiterrorismo dell’Unione europea, che si articola in quattro linee d’azione principali incentrate sulla “prevenzione” (della radicalizzazione del terrorismo e del reclutamento), sulla “protezione”

ricompresa anch’essa nel Programma di Stoccolma[85], essa ha trovato svolgimento in più testi (non sempre coordinati) elaborati dalla Commissione[86], sì che una più ordinata regolazione delle forme di cooperazione che riguardano i flussi informativi all’interno dell’Unione europea –ma che pure possono coinvolgere Paesi terzi[87]–, previa valutazione del loro impatto sui diritti fondamentali e nel rispetto dei principi di protezione dei dati personali, deve essere attentamente considerata[88].

(dei cittadini europei), sull’azione di investigazione e contrasto al terrorismo e sulla capacità di “risposta” ad eventuali attacchi terroristici (per minimizzarne le conseguenze).

85 Cfr. Consiglio Europeo, *Programma di Stoccolma – Un’Europa aperta e sicura al servizio e a tutela dei cittadini*, in *G.U.* C 115, 4.5.2010, p. 1, *passim* e, in particolare, punto 4.5.; v. pure Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Creare uno spazio di libertà, sicurezza e giustizia per i cittadini europei. Piano d’azione per l’attuazione del programma di Stoccolma*, Bruxelles, 20.4.2010, COM(2010) 171 definitivo, 5 ss. e 41 ss.

86 Comunicazione della Commissione al Parlamento europeo e al Consiglio, *La politica antiterrorismo dell’UE: principali risultati e sfide future*, Bruxelles, 20.7.2010, COM(2010) 386 definitivo; Communication on *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, Brussels, 22.11.2010, COM(2010) 673 final; in materia cfr. altresì EU Counter-Terrorism Coordinator (CTC), *EU Action Plan on combating terrorism*, 15893/1/10, Brussels, 17 January 2011 (del quale v. il recente Report on the implementation of the EU Counter-Terrorism Strategy del 10 ottobre 2014, doc. 13971/14). Ma v. pure le numerose perplessità al tempo sollevate dalla *Rapporteur* Rita Borsellino nel *Working document on the European Union’s internal security strategy*, Committee on Civil Liberties, Justice and Home Affairs, 14.2.2011 e i rilievi sollevati nel Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio “La strategia di sicurezza interna dell’UE in azione: cinque tappe verso un’Europa più sicura”, in G.U. C 101, 1.4.2011, p. 6, in particolare (salvo gli aspetti di dettaglio, pur trattati nel parere) ai punti 20, 29 e 40. Un rendiconto dell’attività nel frattempo svolta (ed un aggiornamento rispetto ad essa) può rinvenirsi nella Communication from the Commission to the European Parliament and the Council, *The final implementation report of the EU Internal Security Strategy 2010-2014*, Brussels, 20.6.2014, COM(2014) 365 final.

87 Merita qui segnalare la formale apertura, avvenuta nel 2011, delle negoziazioni tra Unione europea e Stati Uniti d’America per il raggiungimento di un “agreement to protect personal information exchanged in the context of fighting crime and terrorism”, iniziativa che fa seguito ai *Reports* presentati dall’*High Level Contact Group (HLCG) on information sharing and privacy and personal data protection*, Brussels, 23 November 2009 (in *http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf*). Le negoziazioni (il cui fondamento risiede nell’art. 218 TFUE), come noto, non si sono ancora concluse e continuano ad essere all’attenzione della Commissione che, nonostante le rivelazioni di Edward Snowden sull’esistenza e la rilevanza di programmi di sorveglianza di massa (cfr. in merito M. Nico, *Il caso* Datagate*: I problemi di compatibilità del programma di sorveglianza PRISM con la normative europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e dir. int.*, 2013, 727), ha sostenuto che l’adozione di tale accordo dovrebbe portare a un elevato livello di protezione per i cittadini di entrambe le sponde dell’Atlantico e rafforzare la fiducia degli europei negli scambi di dati fra l’UE e gli USA, fornendo una base per sviluppare ulteriormente la cooperazione e il partenariato in materia di sicurezza tra l’Unione europea e gli Stati Uniti (cfr. Comunicazione della Commissione, *Rebuilding Trust in EU-U.S. Data Flows*, 27 novembre 2013, COM(2013) 846, p. 8). Molto critico sul punto, invece, il Parlamento europeo che, con la Risoluzione del 12 marzo 2014 sul programma di sorveglianza dell’Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell’UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni (2013/2188(INI)), ha chiesto (tra l’altro) di riavviare i negoziati per la definizione di tale accordo, sottolineando che lo stesso deve “porre i diritti dei cittadini dell’UE sullo stesso piano dei diritti dei cittadini statunitensi” e “prevedere mezzi di ricorso amministrativo e giudiziario efficaci e applicabili per tutti i cittadini dell’UE negli Stati Uniti, senza alcuna discriminazione”; v. inoltre il parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio «Ripristinare un clima di fiducia negli scambi di dati fra l’UE e gli USA» e sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «Approdo sicuro» dal punto di vista dei cittadini dell’UE e delle aziende ivi stabilite del 20 febbraio 2014.

88 Utile premessa è stata la ricognizione dei trattamenti in essere che, effettuata per la prima volta, è rinvenibile nella Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia*, Bruxelles, 20.7.2010, COM(2010)385 definitivo (ed ivi, al punto 4, v. ampi riferimenti ai principi di protezione dei dati personali).

Nel “dopo Lisbona”, il diritto alla protezione dei dati personali dovrebbe poi trovare adeguata articolazione –e con diversa procedura legislativa, questa volta radicata nell’art. 39 TUE[89]– anche nei settori della politica estera e della sicurezza comune.

7. TRA LUSSEMBURGO E, ANCORA UNA VOLTA, BRUXELLES …

I numerosi richiami alle sentenze della Corte di Lussemburgo che hanno fatto da contrappunto alla presente trattazione[90] evidenziano il ruolo determinante da questa ormai assunto (anche) nella materia della protezione dei dati personali. Avanti alla Corte sono state infatti portate le criticità e i nodi principali (non sempre sciolti) della direttiva 95/45/CE[91], (auspicabilmente) destinati a trovare una più appagante soluzione nell’ambito della riforma della complessiva cornice giuridica della protezione dei dati avviata nel 2012 dalla Commissione europea[92]: il riferimento va principalmente al tema dell’ambito di applicazione territoriale della normativa europea di protezione dei dati personali, specie in relazione ai soggetti che a vario titolo operano in internet e all’aggiornamento delle prerogative che competono all’interessato (con particolare riferimento alle crescenti lesioni connesse alla diffusione e alla permanenza in internet di informazioni personali)[93].

---

89 “Conformemente all’articolo 16 del Trattato sul funzionamento dell’Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell’esercizio di attività che rientrano nel campo di applicazione del presente capo [i.e. in materia di politica estera e di sicurezza comune], e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti”.

90 Cfr. in particolare le sentenze sopra richiamate alle note 20, 31, 40, 43, 56, 57 e 61.

91 Si pensi al caso affrontato da Corte di Giustizia, 6 novembre 2003, Lindqvist c. Svezia (C-101/01), nel quale la Corte, chiamata a valutare se l’inserimento su una pagina Internet di dati personali, per il solo fatto di rendere tali dati accessibili alle persone che si trovano in un paese terzo, costituisse un trasferimento di dati verso un paese terzo ai sensi dell’art. 25 della direttiva 95/46/CE, lascia chiaramente trasparire che le (varie) problematiche connesse ad Internet non fossero state tenute in considerazione al tempo della redazione della direttiva (cfr. punto 68).

92 Come noto, essa si articola in due distinti strumenti: la Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati, COM(2012) 11 final, Bruxelles, 25.1.2012) e la Proposta di Direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (COM/2012/010 final, Bruxelles, 25.1.2012). Per una prima (ampia) presentazione della proposta di regolamento v. lo studio di A. Rallo Lombarte, *Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma*, in *Rev. derecho político*, 2012, 13, 29 ss.; v. pure R. Knyrim, *Entwurf der neuen EU-Datenschutzrecht-Grundverordnung*, in Scholz/Funk, *DGRI Jahrbuch 2012*, Köln, 2013, 25 ss.

93 In questa cornice si inseriscono i profili della disciplina applicabile ai sensi dell’art. 4 della direttiva 95/46/CE e del c.d. “diritto all’oblio” dei dati personali oggetto di reperimento tramite i motori di ricerca di recente affrontati dalla Corte di giustizia con la sentenza del 13 maggio 2014, *Google Spain SL e Google Inc.*, causa C-131/12 (che, alla luce di un’amplia interpretazione formita alla nozione di “stabilimento”, ha affermato l’applicabilità della disciplina spagnola di protezione dei dati nei confronti di Google Inc.): per primi rilievi critici nei confronti della decisione (rispetto alla quale più che di diritto all’oblio dovrebbe parlarsi piuttosto di “diritto alla deindicizzazione dei dati” dai motori di ricerca), cfr. A. Palmieri – R. Pardolesi, *Diritto all’oblio: il futuro dietro le spalle* (Nota a Corte giust., 13 maggio 2014, causa C-131/12), in *Foro it.*, 2014, IV, 317; v. altresì P. Koutrakos, *To Strive, to Seek, to Google, to Forget*, in *Europ. L. Rev.*, 2014, 293. Tra i soggetti istituzionali, fortemente critico nei confronti della sentenza (come pure in relazione alla proposta della Commissione europea volta ad introdurre il c.d. diritto all’oblio) è House of Lords - European Union Committee, 2nd Report of Session 2014–15, *EU Data Protection law: a ‘right to be forgotten’?*, 30 July 2014, *passim*; il documento fa anche espresso riferimento alle discussioni ancora aperte in relazione alla previsione di un tale “diritto” nella proposta generale di regolamento (art. 17), previsione accolta in prima lettura – seppur con qualche modifica – dal Parlamento europeo con il voto del 12 marzo 2014 ma ancora oggetto di discussione in seno al Consiglio.

Ma la Corte è stata anche (ripetutamente) chiamata a declinare il requisito della “piena indipendenza” delle autorità di controllo (già contenuto nell’art. 28, par. 1 della direttiva 95/46/CE e quindi oggetto di esplicita previsione nel Trattato e nella Carta dei diritti fondamentali)[94], istituzioni che rappresentano una delle chiavi di volta dell’intero edificio europeo in materia di protezione dei dati personali[95]. Anche questo tema è destinato a rifluire nella riformulazione del futuro quadro normativo, con l’obiettivo di consolidare ed uniformare i poteri delle autorità di controllo (superando le attuali differenze, specie con riguardo a quelli sanzionatori), nonché di precisarne le modalità di rafforzata cooperazione (nel rispetto della reciproca indipendenza)[96].

Di tutto rilievo, poi, le sentenze nelle quali la Corte si è soffermata sulla necessità e, in parte, sui criteri che presiedono al “bilanciamento” in caso di conflitto tra il diritto alla protezione dei dati personali e altri diritti fondamentali o interessi generali. La vicenda più eclatante è quella concernente tempi e modalità di conservazione dei dati di traffico: è proprio in relazione alla (criticata) direttiva 2006/24/CE che si è avuta infatti la prima pronuncia fondata sul diritto alla protezione dei dati riconosciuto dall’art. 8 della Carta; con una severa censura, la Corte di giustizia, nel ritenere che i tempi di conservazione dei dati stabiliti nella direttiva determinavano un’ingerenza di vasta portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, non limitata allo stretto necessario, ha dichiarato l’invalidità della direttiva[97]. Non sono di minor rilevanza con riguardo all’enunciazione del principio di proporzionalità (*id est*, nel valutare il rispetto dei principi di pertinenza e non eccedenza), infine, le decisioni concernenti il regime di pubblicità (anche mediante la diffusione in internet), in ossequio al principio di trasparenza, di compensi e indennità provenienti dalle casse pubbliche[98] o dall’Unione europea[99].

Al di là però delle questioni portate all’attenzione della Corte di giustizia e dell’impatto che la sua giurisprudenza potrà avere

94 Cfr. *supra* nota 31.

95 V. pure European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, 2010, *passim*.

96 Questo profilo si intreccia con il tema, assai controverso, del c.d. *one stop shop* (cfr. art. 51.2 della Proposta di regolamento presentata dalla Commissione) oggetto ancora di acceso dibattito: cfr., in proposito, Council of the European Union, Brussels, 26 May 2014, Interinstitutional File: 2012/0011 (COD), 10139/14, *Orientation debate on one-stop-shop mechanism*. In merito v. pure Gruppo Art. 29, Statement of the WP29 on current discussions in the Council regarding the EU General Data Protection Regulation - Main points for a one-stop-shop and consistency mechanism for businesses and individuals, Ref. Ares(2014)1206666 - 16/04/2014.

97 Corte di Giustizia, 8 aprile 2014, *Digital Rights Ireland e Seitlinger and Others* (Cause riunite C-293/12, C-594/12): come è noto, nel valutare la proporzionalità delle misure adottate, la Corte ha rilevato non solo che la direttiva toccava “in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l’insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell’obiettivo di lotta contro i reati gravi” (punto 57), rimettendo peraltro l’individuazione di questi ultimi al diritto interno (punto 60), ma pure che essa non conteneva “le condizioni sostanziali e procedurali” per accedere ai dati memorizzati (punto 61), né garanzie sufficienti “riguardanti la sicurezza e la protezione dei dati conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione” (punto 66); infine, nella valutazione della Corte, elemento ulteriore preso in considerazione è stata la circostanza che la direttiva “non impone che i dati di cui trattasi siano conservati sul territorio dell’Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un’autorità indipendente, esplicitamente richiesto dall’articolo 8, paragrafo 3, della Carta”.

98 Cfr. Corte di giustizia, 20 maggio 2003, *Rechnungshof*, cit., in particolare punti 86 ss.

99 Cfr. Corte di giustizia, 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke e Eifert*, cit., nel quale si ribadisce che “le istituzioni, prima di divulgare informazioni riguardanti una persona fisica, devono soppesare l’interesse dell’Unione a garantire la trasparenza delle proprie azioni con la lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta [senza che possa] riconoscersi alcuna automatica prevalenza dell’obiettivo di trasparenza sul diritto alla protezione dei dati personali (v., in tal senso, sentenza Commissione/Bavarian Lager, cit., punti 75-79), anche qualora siano coinvolti rilevanti interessi economici” (punto 85).

La “privacy” negli studi professionali

sul processo di revisione della direttiva 95/46/CE, tale processo ha radici lontane. Pur ritenendosi, da parte dei più, validi i principi generali di protezione dei dati personali in essa contenuti, nel corso degli anni sono stati tuttavia messi in luce sia la parziale armonizzazione dalla stessa conseguita –di tal che non sarebbe peregrino interrogarsi circa il ruolo effettivamente svolto dalla Commissione europea nel corso di questi anni nell'attivare i necessari procedimenti di infrazione per inosservanza o errata applicazione della direttiva[100]–, sia gli effetti profondi sui trattamenti di dati

[100] Troppo spesso, specie nel formulare critiche alla direttiva 95/46/CE rispetto alla parziale armonizzazione suo tramite conseguita, si dimentica peró che le diverse "risposte" a livello nazionale derivano dall'applicazione del principio di liceità del trattamento, che esige una valutazione effettuata alla luce dell'ordinamento giuridico nazionale, non necessariamente armonizzato a livello europeo, sì che eventuali discrasie non possono non ripercuotersi, in seconda battuta, sui profili connessi (alla liceità del) trattamento dei dati personali. Per altro verso le critiche sono ingenerose (e, in fondo, poco lungimiranti) rispetto alla tecnica normativa, per norme e cla(Troppo spesso, specie nel formulare critiche alla direttiva 95/46/CE rispetto alla parziale armonizzazione suo tramite conseguita, si dimentica che le diverse "risposte" a livello nazionale derivano dall'applicazione del principio di liceità del trattamento, che esige una valutazione effettuata alla luce dell'ordinamento giuridico nazionale, non necessariamente armonizzato a livello europeo, sì che eventuali discrasie non possono non ripercuotersi, in seconda battuta, sui profili connessi (alla liceità del) trattamento dei dati personali. Per altro verso le critiche sono ingenerose (e, in fondo, poco lungimiranti) rispetto alla tecnica normativa, per norme e clausole generali, seguita dalla direttiva 95/46/CE, fattore che ne ha assicurato la longevità (nonostante i profondi mutamenti tecnologici), come peraltro riconosciuto anche dalla Corte di giustizia: cfr. Corte di Giustizia, 6 novembre 2003, *Lindqvist c. Svezia* (C-101/01), punto 83, che riferendosi alla direttiva 95/46/CE, evidenzia che "le sue disposizioni sono per forza di cose relativamente generiche, visto che essa deve applicarsi a un gran numero di situazioni molto diverse". A quest'ultimo riguardo, vero è, semmai, che in alcuni contesti sarebbe stato necessario (e tuttora sarebbe più che auspicabile) introdurre discipline armonizzate di settore a livello europeo (come si è sopra segnalato in nota 30): un macro settore (tra i tanti) è certo quello del trattamento dei dati riferiti ai lavoratori, specie in relazione all'utilizzo delle tecnologie dell'informazione e della comunicazione (profilo peraltro sollevato in passato dall'Article 29 Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context*, 13 September 2001, WP 48): sia consentito in merito rinviare

personali determinati dallo sviluppo delle tecnologie della comunicazione, anzitutto internet. La dimensione accentuatamente globalizzata dell'economia, inoltre, ha inciso –in particolare sotto la pressione esercitata dalle multinazionali– sulla disciplina relativa al diritto nazionale applicabile[101] e su quella relativa al flusso transfrontaliero dei dati personali, entrambe destinate a subire (più o meno significativi) ritocchi[102].

Sono queste le punte dell'*iceberg* che, in assenza di una più larga convergenza su scala globale sui principi ispiratori della materia (convergenza che, specie in relazione all'ordinamento statunitense, tarda a venire), oggi minacciano il bene più prezioso che il diritto alla protezione dei dati personali, nel suo lungo (e mai agevole) cammino, ha inteso assicurare: quello dell'*effettività*, al di là del pur necessario riconoscimento nelle *black letters of law*, della protezione dei diritti fondamentali direttamente e indirettamente tutelati dal diritto alla protezione dei dati personali. In questa prospettiva (e per perseguire questo obiettivo) si sono progressivamente fatte strada alcune *buzzwords*, destinate a trovare spazio nel programma di riforma del quadro normativo comunitario: il principio di *accountability*[103], la necessità che i sistemi informativi incorporino sin dalla fase di progettazione i principi di protezione dei dati personali e siano rispettosi della *privacy* degli interessati

a Lattanzi, *Dallo statuto dei lavoratori alla disciplina di protezione dei dati personali*, in *Riv. it. dir. lav.*, 2011, I, 147, 154 ss.

[101] Cfr. Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, 16 December 2010, WP 179.

[102] In particolare, quanto accaduto a livello nazionale in taluni Stati membri (tra cui l'Italia, dando seguito alla segnalazione del Garante al Parlamento e al Governo in materia di trasferimento di dati personali in paesi terzi e norme vincolanti d'impresa dell'8 novembre 2007, doc. *web* n. 1467485) – dando autonoma rilevanza alle c.d. *binding corporate rules* – potrebbe ripetersi anche a livello europeo.

[103] Cfr. Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010, WP 173; v. pure P. Hustinx, *Accountability in the Proposed Regulation*, Brussels, 3 December 2012, in https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-12-03_KnowledgeNet_EN.pdf.

(c.d. *privacy by design* e *by default*)[104], l'opportunità che ad un sistema di controllo centralizzato (prevalentemente incentrato sulle autorità di protezione dei dati) si possano affiancare strumenti decentrati in grado di contribuire ad una corretta implementazione delle discipline di protezione dei dati personali (mediante, in particolare, la figura, già sperimentata nelle linee essenziali in alcuni stati membri, del *data protection officer*).

Nell'economia del presente contributo, non è possibile qui soffermarsi su questi istituti, ciascuno dei quali meriterebbe un approfondimento (ed un esame di dettaglio del dato normativo che più precisamente ne dovrebbe connotare i contenuti).

[104] Principio soggetto ad ampia elaborazione, in particolare ad opera dell'Ontario Commissioner Ann Cavoukian (v. per più ampi riferimenti http://www.privacybydesign.ca), ormai già filtrato (prima ancora che nelle proposte in discussione in materia di protezione dei dati), in alcuni atti normativi dell'Unione europea: cfr., ad esempio, l'art. 3 della direttiva 2014/53/UE del Parlamento europeo e del Consiglio del 16 aprile 2014 concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (secondo il quale le apparecchiature radio di determinate categorie o classi sono fabbricate in modo tale da contenere elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata dell'utente e dell'abbonato; alla Commissione è conferito il potere di adottare atti delegati al riguardo); anche l'art. 3 della direttiva 2014/55/UE del Parlamento europeo e del Consiglio del 16 aprile 2014, relativa alla fatturazione elettronica negli appalti pubblici, dà attuazione al c.d. principio della privacy by design (pbd) prevedendo che "la norma europea sulla fatturazione elettronica […] tenga conto dell'esigenza di tutela dei dati personali conformemente alla direttiva 95/46/CE, di un approccio basato sulla tutela dei dati fin dalla progettazione e dei principi di proporzionalità, minimizzazione dei dati e limitazione delle finalità". Cfr. pure il considerando n. 77 della direttiva 2014/24/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014 sugli appalti pubblici e che abroga la direttiva 2004/18/CE (e analogamente il considerando n. 86 della direttiva 2014/25/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014 sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE).

In chiave sintetica, si può invece affermare che la risposta istituzionale finora posta in essere a livello europeo non è stata pienamente soddisfacente; nel Programma di Stoccolma si leggeva che "l'Unione deve garantire una strategia globale in materia di protezione dei dati all'interno dell'Unione e nell'ambito delle relazioni con i paesi terzi"[105].

A distanza di oltre tre anni, il processo legislativo europeo che avrebbe dovuto condurre ad un "rinnovato" e rinsaldato quadro di tutele per la protezione dei dati personali è ancora in mezzo al guado, vittima dei gorghi delle rivelazioni di Edward Snowden (la cui portata, ancorché le molte zone d'ombra non siano state dissipate dalle inchieste svolte da soggetti istituzionali, è comunque inquietante e rischia, al fondo, di banalizzare, se non vanificare o ridicolizzare, l'affermazione progressiva, mai agevole, del diritto alla protezione dei dati personali), invischiato dalle resistenze delle *lobbies* (interne ed esterne), imbrigliato nelle divergenti visioni degli Stati membri.

Tutto ciò –prima ancora dei limiti tecnici delle proposte presentate, peraltro oggetto di critiche numerose e, talune delle quali, di non poco momento[106]– rende oltremodo difficile la definizione di un quadro giuridico unitario a livello regionale che possa autenticamente aspirare ad una protezione effettiva dei diritti delle persone nella società digitale.

[105] Consiglio Europeo, *Programma di Stoccolma*, cit. punto 2.5.

[106] Tra i primi rilievi critici merita segnalare quelli provenienti dall'Article 29 Data Protection Working Party, WP 191, *Opinion 01/2012 on the data protection reform proposals, adopted on 23 March 2012*, in e le riserve espresse nell'Opinion of the European Data Protection Supervisor on the data protection reform package, 7 marzo 2012. V. inoltre l'*Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, 1st October 2012.

8. (SEGUE) GUARDANDO AL DI LÀ DELLE COLONNE D´ERCOLE

Ma non ci si può, in questa rapida ricognizione, solo soffermare sugli ostacoli che il processo in corso incontra, atteso che, allargando lo sguardo verso un orizzonte più ampio, si intravedono, sullo scenario globale, anche segnali favorevoli all'introduzione di garanzie effettive per la protezione dei dati personali –persino negli Stati Uniti[107]– nonché ferme prese di distanza rispetto alle forme di controllo indiscriminato che le rivelazioni recenti hanno (in parte) portato alla luce[108]. Il segnale più chiaro proviene dall'ordinamento brasiliano che si è dotato della della *Lei* n. 12.965, del 23 aprile 2014, *Marco Civil da Internet*; ma i semi gettati al vento dalle discipline di marca europea sembrano altresì germogliare nella recente Convenzione dell'Unione africana sulla sicurezza informatica e protezione dei dati personali (*African Union convention on cyber security and personal data protection*) del 27 giugno 2014[109].

[107] Nel recente *report* predisposto dalla Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability*, May 2014, ad esempio, si evidenzia che nei quasi due decenni da quando la Commissione ha iniziato ad esaminare i *data broker* (operatori economici che raccolgono dati riferiti ai consumatori e li rivendono o li condividono con terzi), pochi progressi sono stati fatti nell'ordinamento statunitense per migliorare la trasparenza e il potere di scelta degli interessati (peraltro già oggetto di puntuali raccomandazioni formulate nel rapporto del 2012 *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*). Nelle proposte legislative meno risalenti – si pensi al *"Commercial Privacy Bill of Rights Act of 2011*", proposta rimasta senza seguito, benché *bipartisan,* presentata dagli (influenti) senatori Kerry e McCain – facevano capolino non pochi dei principi tradizionali di protezione dei dati personali, (e trasparivano i contenuti del dibattito europeo in materia, come, ad esempio, il richiamo ai *minimization* e *accountability principles*).

[108] Si vedano, anzitutto, le preoccupazioni espresse nella Risoluzione n. 68/167 adottata dall'Assemblea Generale delle Nazioni Unite del 18 dicembre 2013 e quindi nel rapporto "*The right to privacy in the digital age*" del 30 giugno 2014, curato dall'Alto commissario per i diritti umari delle Nazioni Unite, Navi Pillay.

[109] Vedila in http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf.

Solo il tempo, che ora sembra farsi breve stando alle intenzioni di recente enunciate dal neo-presidente della Commissione europea[110], dirà se l'ambizioso obiettivo fissato dal Programma di Lisbona potrà essere conseguito –o se "la montagna partorirà il (proverbiale) topolino". Ciò non toglie che l'irreversibile affermarsi della dimensione digitale, nelle multiformi modalità di sua

[110] Negli Orientamenti politici per la prossima Commissione europea formulati il 15 luglio 2014 (contenuti nel documento "*Un nuovo inizio per l'Europa Il mio programma per l'occupazione, la crescita, l'equità e il cambiamento democratico*"), Jean-Claude Juncker ha attribuito (non secondaria) rilevanza alla materia della protezione dei dati personali. In particolare, per realizzare un mercato unico del digitale connesso ha dichiarato che "dovremo avere il coraggio di superare i compartimenti stagni delle regolamentazioni nazionali […] sulla protezione dei dati […]. Se agiamo in tal senso [… potremo] inoltre creare condizioni eque affinché tutte le imprese che offrono prodotti o servizi nell'Unione europea siano soggette alle medesime norme sulla protezione dei dati […], indipendentemente dal luogo in cui si trovano i loro server" (p. 5 s.). "Per realizzare questo proposito, nei primi sei mesi del mio mandato intendo prendere decisioni legislative ambiziose per realizzare un mercato unico del digitale connesso, in particolare concludendo rapidamente i negoziati sulla normativa comune europea in materia di protezione dei dati […]" (p. 6). Con riguardo alle negoziazioni relative all'accordo (definito "realistico e equilibrato") di libero scambio con gli Stati Uniti ha dichiarato che "da Presidente della Commissione sarò […] inequivocabile nell'indisponibilità a immolare sull'altare del libero scambio le norme europee in materia di sicurezza, salute, protezione sociale e protezione dei dati […]. Da Presidente della Commissione, saranno per me non negoziabili, in particolare, la sicurezza degli alimenti di cui ci nutriamo e la protezione dei dati personali degli europei" (p. 9). "La protezione dei dati è un diritto fondamentale di particolare rilevanza nell'era digitale. Oltre a perfezionare rapidamente i lavori legislativi sulle norme comuni di protezione dei dati all'interno dell'Unione europea, dobbiamo affermare questo diritto anche nelle relazioni esterne. Alla luce delle recenti rivelazioni sulle pratiche di sorveglianza di massa, partner a noi vicini, come gli Stati Uniti d'America, devono convincerci che l'attuale regime dell'approdo sicuro garantisce effettivamente la sicurezza: solo così potrà essere mantenuto. Gli USA devono dare inoltre la garanzia che tutti i cittadini dell'UE, che risiedano o no sul suolo statunitense, siano in grado di far valere i propri diritti alla protezione dei dati dinanzi ai giudici americani: si tratta di un elemento essenziale per ristabilire la fiducia nelle relazioni transatlantiche" (p. 10).

concreta manifestazione e che con internet ha travalicato i confini nazionali (vanificando così inevitabilmente i meccanismi di tutela apprestati, non solo a livello nazionale, ma pure regionale, ed indipendentemente dalla loro efficacia) renda sempre più urgente – ove, ovviamente, i valori personalistici in gioco intendano continuare ad essere riconosciuti e protetti – che trovi ampio riconoscimento il nucleo duro dei principi fondamentali di protezione dei dati riconosciuti nel contesto dell'Unione europea e del Consiglio d'Europa[111], con un suo svecchiamento e con la contestuale individuazione (allo stato non agevole) di forme originali di protezione, atteso che il modello di tutela vigente (che pure rappresenta ancora l'ossatura della Proposta di regolamento), tecnologicamente orientato a forme più tradizionali di trattamento dei dati, sotto più aspetti mostra la corda.

Ciò che oggi può continuarsi ad affermare è che la traiettoria del diritto alla protezione dei dati personali – che nell'economia del presente intervento si è qui potuta solo per sommi capi trat-

[111] In questa direzione muove da ultimo la bozza di "Dichiarazione dei diritti in internet", elaborata, in un contesto istituzionale, dalla Commissione per i diritti e i doveri relativi ad Internet, presieduta da Stefano Rodotà ed istituita dalla Presidente della Camera dei deputati, Laura Boldrini, sottoposta a consultazione pubblica il 13 ottobre 2014 (in http://www.camera.it/application/xmanager/projects/leg17/attachments/upload_file/upload_files/000/000/187/dichiarazione_dei_diritti_internet_pubblicata.pdf). Merita sottolineare che, anticipando alcuni dei contenuti del tradizionale "Discorso sullo stato dell'Unione" (che si terrà il prossimo 20 gennaio 2015), Barak Obama, durante un intervento tenuto presso la Federal *Trade Commission* (cfr. http://www.whitehouse.gov/live/president-obama-speaks-tackling-identity-theft-and-improving-consumer-and-student-privacy), ha anticipato la volontà di introdurre discipline federali miranti a promuovere un intervento legislativo di natura generale a tutela dei consumatori contenente (nella sostanza) alcuni dei principi fondamentali di protezione dei dati personali (mediante un *Consumer Privacy Bill of Rights*) oltre ad interventi più mirati per contrastare il furto di identità (mediante *The Personal Data Notification & Protection Act*) e a proteggere la *privacy* degli studenti (mediante *The Student Digital Privacy Act*).

teggiare – è tutt'altro che esaurita e il dibattito intorno ad esso è vivissimo.

Nell'attesa, c'è da augurarsi che la discussione non segni ancora il passo e che il diritto alla protezione dei dati personali trovi nuove ed originali forme di riconoscimento che, lungi dal ridurlo ad un simulacro (nei fatti svuotato dalla vague technologique e dalle forze che la sospingono), ne possano assicurare invece l'efficace l'applicazione[112].

[112] Conviene qui tenere a mente il monito di RODOTÀ, *Diritti e libertà nella storia d'Italia. Conquiste e conflitti. 1861-2011*, Roma, 2011, 141 s.: «la cultura della *privacy* è fragile, le norme alle quali si affida sono sempre esposte a strumentalizzazioni e restrizioni, provenienti soprattutto da imperativi di sicurezza e pressioni di mercato. Le speranze in essa riposte rischiano d'essere deluse senza una convinta e continua attenzione istituzionale, indispensabile per mantenere e rafforzare la fiducia dei cittadini».

00062/10/IT
WP 173

Parere 3/2010 sul principio di responsabilità

adottato il 13 luglio 2010

Il Gruppo di lavoro è stato istituito in virtù dell’articolo 29 della direttiva 95/46/CE. È l’organo consultivo indipendente dell’UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all’articolo 30 della direttiva 95/46/CE e all’articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione
europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio LX-46 01/190.

Sito Internet: http://ec.europa.eu/justice/policies/privacy/index_en.htm

[NdT] Ai fini del presente parere, con “responsabile del trattamento” e con “incaricato del trattamento” si intendono rispettivamente il “titolare” e il “responsabile” di cui all’articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

SINTESI

I principi e gli obblighi dell’Unione europea in materia di protezione dei dati sono spesso applicati in modo insufficiente a livello di misure e pratiche interne sostanziali. Se la protezione dei dati non diventa parte integrante delle pratiche e dei valori condivisi di un’organizzazione e se le relative responsabilità non sono espressamente ripartite, il rispetto effettivo delle norme in materia di protezione dei dati sarà messo notevolmente a rischio e gli incidenti in questo settore saranno destinati a continuare.

Per favorire l’attuazione della protezione dei dati nella pratica, il quadro normativo dell’Unione europea necessita di strumenti aggiuntivi. Il presente parere intende consigliare la Commissione su come modificare in tal senso la direttiva sulla protezione dei dati. In particolare, questo parere avanza una proposta concreta per l’introduzione di un principio di responsabilità che richieda ai responsabili del trattamento di mettere in atto misure adeguate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati e per dimostrare tale osservanza, su richiesta, alle autorità di controllo. Ciò dovrebbe contribuire a passare “dalla teoria alla pratica” e ad aiutare le autorità di protezione dei dati nello svolgimento dei loro compiti di controllo e di verifica dell'applicazione.

Il parere contiene suggerimenti volti ad assicurare che il principio di responsabilità garantisca la certezza del diritto, lasciando spazio al tempo stesso ad una certa adattabilità (che consenta di determinare le misure concrete da applicare in funzione dei rischi connessi al trattamento e dei tipi di dati trattati). Si analizza quindi in che modo tale principio potrebbe ripercuotersi in altri settori, tra i quali i trasferimenti internazionali di dati, gli obblighi di notificazione, le sanzioni e, infine, anche lo sviluppo di programmi o sigilli di certificazione.

Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti l’articolo 29, l’articolo 30, paragrafo 1, lettera a), e l’articolo 30, paragrafo 3, della suddetta direttiva e l’articolo 15, paragrafo 3, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 giugno 2002,

visto il proprio regolamento interno,

ha adottato il seguente parere:

1. INTRODUZIONE

1. La protezione dei dati deve passare “dalla teoria alla pratica”. Gli obblighi giuridici devono essere tradotti in misure concrete di protezione dei dati. Per favorire la protezione dei dati nella pratica, il quadro giuridico dell’UE in materia necessita di meccanismi aggiuntivi. Nei dibattiti sul futuro del quadro europeo e globale sulla protezione dei dati, sono stati proposti meccanismi basati sulla responsabilità come mezzo per incoraggiare i responsabili del trattamento ad attuare strumenti pratici per una protezione dei dati efficace.

2. Nel suo documento sul futuro della privacy (WP168) del dicembre 2009, il Gruppo di lavoro articolo 29 ha ritenuto che l’attuale quadro giuridico non sia riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si traducano in meccanismi efficaci atti a fornire una protezione reale. Per migliorare la situazione, il Gruppo di lavoro ha proposto che la Commissione esamini l’opportunità di introdurre meccanismi basati sulla responsabilità, con un particolare accento sulla possibilità di includere un principio di “responsabilità” nella versione riveduta della direttiva sulla protezione dei dati[1]. Tale principio rafforzerebbe il ruolo del responsabile del trattamento e ne aumenterebbe la responsabilità.

3. In breve, un principio di responsabilità vincolante imporrebbe esplicitamente ai responsabili del trattamento di attuare misure appropriate ed efficaci per dare

[1] “Per risolvere questo problema, sarebbe opportuno introdurre nel quadro globale un principio di responsabilità in base al quale i responsabili del trattamento dei dati siano tenuti ad adottare le misure necessarie per garantire il rispetto degli obblighi e dei principi fondamentali dell’attuale direttiva al momento del trattamento dei dati personali. Una disposizione di questo tipo rafforzerebbe la necessità di mettere in atto politiche e meccanismi per l’attuazione efficace dei principi e degli obblighi fondamentali della direttiva attuale. Avrebbe inoltre l’obiettivo di confermare l’esigenza di adottare misure adeguate che determinino un’efficace applicazione interna degli obblighi e dei principi fondamentali attualmente stabiliti dalla direttiva. Inoltre, il principio della responsabilità imporrebbe ai responsabili del trattamento dei dati di disporre dei meccanismi interni necessari per dimostrarne la conformità agli interessati esterni, comprese le autorità nazionali di protezione dei dati. Infine, il fatto di dover dimostrare che sono state adottate misure adeguate per garantire la conformità favorirà notevolmente l’applicazione delle norme vigenti” (WP168, punto 79. Per maggiori informazioni, v. anche punti 74-78).

applicazione ai principi e agli obblighi della direttiva, e per dimostrarne su richiesta l’osservanza. In pratica, ciò dovrebbe concretarsi in programmi improntati all'adattabilità mirati ad attuare i principi esistenti di protezione dei dati (talvolta denominati “programmi di conformità”). Quale complemento a tale principio, potrebbero essere istituiti obblighi aggiuntivi diretti ad attuare garanzie di protezione dei dati o ad assicurarne l’efficacia. Potrebbe trattarsi, per esempio, di una disposizione che obbliga a effettuare una valutazione d’impatto sulla privacy per le operazioni di trattamento di dati a più alto rischio.

4. Il presente parere intende sviluppare il precedente contributo fornito sull’argomento dal Gruppo di lavoro articolo 29 con il parere sul futuro della privacy, allo scopo di assistere la Commissione nella revisione della direttiva 95/46, attualmente in corso. A tal fine, il presente parere è suddiviso in quattro sezioni: la prima esamina la necessità che i responsabili del trattamento rafforzino le prassi interne (politiche e procedure) per garantire che la totalità del trattamento avvenga in base alle norme vigenti, e spiega in che modo i sistemi basati sulla responsabilità possono contribuire a questo obiettivo. Prospetta quindi la forma che l’architettura giuridica di un sistema basato sulla responsabilità potrebbe assumere e i precedenti nel settore della protezione dei dati e in altri settori. La seconda sezione presenta una proposta concreta per un principio di responsabilità e descrive la logica alla base dei diversi aspetti della proposta. La terza sezione illustra vari elementi collegati ad un sistema giuridico che integri un sistema generale di responsabilità. Comprende un’analisi della necessità che tale proposta fornisca certezza giuridica e che sia al tempo stesso formulata in termini sufficientemente ampi da consentire una certa adattabilità (in modo da permettere di determinare le misure concrete e i metodi di verifica da applicare in funzione del rischio del trattamento e del tipo di dati trattati). Affronta quindi taluni elementi correlati, come ad esempio il rapporto con i trasferimenti all’estero, descrive i vantaggi che un meccanismo basato sulla responsabilità offrirebbe alle autorità di protezione dei dati e delinea il ruolo che potrebbe svolgere la certificazione.

II. RESPONSABILITÀ: OBIETTIVI, ARCHITETTURA GIURIDICA, PRECEDENTI E TERMINOLOGIA

II.1 Responsabilità come motore per l’attuazione efficace dei principi di protezione dei dati

5. Oggi si rivela sempre più necessario e importante che i responsabili del trattamento adottino misure efficaci per una reale protezione dei dati. Le ragioni sono molteplici e vengono analizzate nel prosieguo.

6. Anzitutto, rispetto ai dati stiamo assistendo ad un cosiddetto “effetto diluvio” , con un continuo aumento della quantità di dati personali esistenti, elaborati e ulteriormente trasferiti. Questo fenomeno è favorito sia dai progressi tecnologici, vale a dire lo sviluppo dei sistemi di informazione e di comunicazione, sia dalla crescente capacità degli utenti di impiegare le tecnologie e interagire con esse. Con l’aumento della quantità di dati trasferiti in tutto il mondo, aumentano anche i rischi di abuso. Ciò evidenzia ulteriormente la necessità che i responsabili del

trattamento, sia nel settore pubblico che in quello privato, attuino meccanismi interni reali ed efficaci per salvaguardare la tutela delle informazioni personali.

7. In secondo luogo, la quantità sempre crescente di dati personali è accompagnata da un aumento del loro valore in termini sociali, politici ed economici. In alcuni settori, soprattutto in ambiente online, i dati personali sono diventati *de facto* la valuta di scambio per i contenuti online. Nel contempo, da un punto di vista sociale, vi è un crescente riconoscimento della protezione dei dati come valore sociale. In sintesi, via via che i dati personali diventano sempre più preziosi per i responsabili del trattamento in tutti i settori, anche i cittadini, i consumatori e la società in generale sono sempre più consapevoli della loro rilevanza. Questo fatto rafforza a sua volta la necessità di applicare misure rigorose per salvaguardarli.

8. Infine, da quanto precede consegue che la violazione della privacy può avere notevoli ripercussioni negative per i responsabili del trattamento nei settori pubblico e privato. Potenziali anomalie nelle applicazioni di governo elettronico e di sanità elettronica avranno conseguenze devastanti sia in termini economici sia, soprattutto, in termini di reputazione. Pertanto, ridurre al minimo i rischi, costruire e mantenere una buona reputazione e garantire la fiducia dei cittadini e dei consumatori stanno diventando compiti fondamentali dei responsabili del trattamento in tutti i settori.

9. In sintesi, da quanto precede emerge l’assoluta necessità per i responsabili del trattamento di applicare misure reali ed efficaci di protezione dei dati dirette alla corretta gestione della loro protezione, riducendo inoltre al minimo i rischi giuridici, economici e di reputazione che possono derivare da pratiche inadeguate in materia. Come ulteriormente illustrato nel prosieguo, i meccanismi basati sulla responsabilità mirano a realizzare tali obiettivi.

II.2 Possibile architettura giuridica generale dei meccanismi basati sulla responsabilità

10. In questo contesto, una questione pertinente da chiarire riguarda il modo in cui il quadro giuridico potrebbe incoraggiare i responsabili del trattamento ad adottare misure che offrano una protezione reale nella pratica. In altri termini, la forma che dovrebbe assumere l’architettura giuridica dei sistemi basati sulla responsabilità.

11. In via preliminare, prima di analizzare tale architettura, occorre sottolineare che tali sistemi non modificano né influiscono in alcun modo sui principi sostanziali di protezione dei dati, bensì sono intesi a farli funzionare meglio.

12. Un modo per indurre i responsabili del trattamento a predisporre tali misure sarebbe inserire un principio di responsabilità nella versione riveduta della direttiva. Si prevede che una disposizione di questo tipo possa condurre all’attuazione di misure e procedure interne volte a rendere effettivi i principi di protezione dei dati esistenti assicurandone l’efficacia, e ad introdurre l’obbligo di dimostrarne il rispetto qualora le autorità di protezione dei dati ne facciano richiesta. Come ulteriormente descritto di seguito, il tipo di procedure e di meccanismi varierebbe in funzione dei rischi intrinseci al trattamento e alla natura dei dati.

13. In aggiunta a quanto precede, si potrebbe svolgere una riflessione su disposizioni specifiche quali l’obbligo di effettuare valutazioni d’impatto sulla privacy in determinati casi o la nomina di responsabili della protezione dei dati. Tali disposizioni specifiche potrebbero completare il principio generale di responsabilità.

14. Il Gruppo di lavoro articolo 29 riconosce che i responsabili del trattamento potrebbero avere la volontà di attuare politiche e procedure non strettamente previste dalla legislazione sulla protezione dei dati. Ad esempio, un responsabile del trattamento potrebbe volersi impegnare a rispondere alle richieste di accesso entro un periodo di tempo molto breve, anche se la legge prevede una certa flessibilità. Potrebbe anche volersi impegnare a rispondere contemporaneamente alle richieste di accesso sia on-line che off-line, per assicurare la ricezione tempestivo ed efficace di tali informazioni. Si potrebbero anche immaginare situazioni in cui il responsabile del trattamento desideri offrire una tutela più ampia di quella garantita dalle disposizioni minime previste dal quadro giuridico generale. Ad esempio, il responsabile del trattamento potrebbe decidere di nominare un responsabile della protezione dei dati anche se la legge vigente non dispone un obbligo in tal senso. Ancora, il responsabile del trattamento potrebbe voler affidare a terzi l’incarico di eseguire un audit relativo a *tutte* le sue operazioni di trattamento dei dati, al fine di valutarne la conformità con il quadro giuridico in materia di protezione dei dati. Il Gruppo di lavoro apprezza queste iniziative e incoraggia il nuovo quadro giuridico di protezione dei dati a fornire incentivi affinché i responsabili del trattamento si orientino in tale direzione.

15. Conformemente a quanto precede, l’architettura giuridica dei meccanismi di responsabilità prevedrebbe due livelli: il primo livello sarebbe costituito da un obbligo di base vincolante per *tutti* i responsabili del trattamento. Tale obbligo comprenderebbe due elementi: l’attuazione di misure e/o procedure, e la conservazione delle relative prove. Questo primo livello potrebbe essere integrato da disposizioni specifiche. Il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell’efficacia delle misure (norme di attuazione eccedenti il livello minimo). Pur riconoscendo l’importanza e i benefici di tali sistemi, il presente parere si occupa per lo più dell’obbligo di primo livello, in particolare del principio generale di responsabilità.

II.3 Principio della responsabilità nel settore della protezione dei dati e in altri settori e terminologia

Precedenti

16. Il Gruppo di lavoro articolo 29 osserva che il principio di responsabilità non è una novità in sé. Il suo espresso riconoscimento è ravvisabile nelle linee guida per la protezione della vita privata dell’Organizzazione per la cooperazione e lo sviluppo economico (OCSE) adottati nel 1980. Il principio di responsabilità ivi contenuto

enuncia: “Il responsabile del trattamento dei dati dovrebbe essere responsabile del rispetto delle misure che rendono effettivi i principi indicati sopra”.

17. Di recente tale principio è stato inserito esplicitamente tra gli standard internazionali di Madrid, elaborati dalla Conferenza internazionale sulla protezione dei dati e la privacy[2]. È inoltre accolto nel più recente progetto di norma ISO 29100 che stabilisce un quadro per la privacy, ed è uno dei principali concetti del quadro giuridico sulla privacy sviluppato dall’APEC e delle sue norme sulla privacy transfrontaliera[3].

18. Da un punto di vista “statutario”, il Gruppo di lavoro articolo 29 rileva che i principi canadesi di informazione equa contenuti nella legge "Personal Information Protection And Electronic Documents Act" fanno riferimento alla responsabilità. Tra gli altri, il primo principio richiede lo sviluppo e l’attuazione di politiche e pratiche atte a garantire il rispetto dei dieci principi di informazione equa tra cui procedure per la protezione dei dati personali e per ricevere e rispondere a reclami e richieste di informazioni.

19. In aggiunta a quanto sopra, il Gruppo di lavoro articolo 29 rileva che le regole d’impresa vincolanti, utilizzate nel contesto dei trasferimenti internazionali di dati, riflettono il principio di responsabilità. Tra le regole d’impresa vincolanti si annoverano i codici di condotta elaborati e seguiti da organizzazioni multinazionali, contenenti misure interne intese a dare applicazione ai principi di protezione dei dati (ad esempio audit, programmi di formazione, reti di incaricati della privacy, sistemi di gestione dei reclami). Una volta esaminate dalle autorità nazionali di protezione dei dati, le regole d’impresa vincolanti sono considerate idonee a garantire un livello di protezione adeguato in relazione a un trasferimento o a una categoria di trasferimenti di dati personali tra le imprese che fanno parte dello stesso gruppo e che sono vincolate da tali regole ai sensi dell'articolo 25 e dell'articolo 26, paragrafo 2, della direttiva 95/46.

20. Al di fuori dell'ambito della protezione dei dati, vi sono alcuni esempi di responsabilità: tra questi, un programma che specifica le politiche e le procedure che un responsabile del trattamento deve seguire per garantire la conformità con leggi e regolamenti. Per esempio, i programmi di conformità sono obbligatori ai sensi dei regolamenti in materia di servizi finanziari. In altri casi, i programmi di conformità non sono obbligatori, ma vengono incoraggiati, come ad esempio nel settore delle regole in materia di concorrenza. In Canada per esempio, il commissario per la concorrenza ha sviluppato politiche elaborate relative ai programmi di conformità aziendale. La decisione delle aziende di applicare o meno un programma è facoltativa. Tuttavia, il commissario canadese per la concorrenza sottolinea l’importanza della conformità come strumento di

[2] La persona responsabile deve: “a. adottare tutte le misure necessarie per rispettare i principi e gli obblighi istituiti dal presente documento e dalla normativa nazionale vigente e b. predisporre i meccanismi interni necessari per dimostrare tale conformità sia agli interessati sia alle autorità di controllo nell’esercizio dei loro poteri, come stabilito alla sezione 23”.

[3] Oltre a quanto sopra esposto, il Centre for Information Policy Leadership è impegnato in un’iniziativa tesa a esplorare gli effetti del principio di responsabilità per quanto riguarda la protezione dei dati e la privacy. Cfr il sito www.informationpolicycentre.com

mitigazione del rischio ed evidenziai benefici giuridici, economici e in termini di reputazione[4].

Terminologia

21. Il termine inglese “accountability” (responsabilità) proviene dal mondo anglosassone, dove è di uso comune e dove il suo significato è ampiamente compreso e condiviso. Ciononostante, risulta complesso definire che cosa esattamente significhi “accountability” in pratica. In generale, comunque, l’accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e 'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente.

22. Nella maggior parte delle altre lingue europee, principalmente a causa delle differenze tra i sistemi giuridici, il termine “accountability” non è facilmente traducibile. Di conseguenza, il rischio di un’interpretazione variabile del termine, e quindi di una mancanza di armonizzazione, è sostanziale. Altri termini che sono stati suggeriti per rendere il senso di “accountability” sono: “reinforced responsibility” (responsabilità rafforzata), “assurance” (assicurazione), “reliability” (affidabilità), “trustworthiness” (attendibilità) e, in francese, “obligation de rendre des comptes” (obbligo di rendere conto) ecc. Si potrebbe altresì inferire che “accountability” si riferisce alla “attuazione dei principi relativi alla protezione dei dati”.

23. Il presente documento si occupa quindi delle misure che dovrebbero essere adottate o previste per garantire la conformità nel settore della protezione dei dati. I riferimenti alla responsabilità devono pertanto essere intesi nel senso utilizzato nel presente parere, fatta salva la possibilità di trovare un’altra formulazione che meglio rispecchi il concetto qui esposto. È per questo che il documento non è incentrato sui termini, ma si concentra pragmaticamente sulle misure da adottare, piuttosto che sul concetto in sé.

III. VERSO UNA PROPOSTA PER UNA DISPOSIZIONE GENERALE SULLA RESPONSABILITÀ

III.1 Una disposizione generale per riaffermare e rafforzare la responsabilità dei responsabili del trattamento

24. Il Gruppo di lavoro articolo 29 ha esaminato ulteriormente la possibilità di introdurre soluzioni basate sulla responsabilità nel nuovo quadro giuridico globale sulla protezione dei dati alla luce delle considerazioni esposte nella sezione I.

25. Di conseguenza, ha confermato il punto di vista già espresso nel parere sul futuro della privacy, secondo cui nel nuovo quadro legislativo globale dovrebbe essere inserito un principio generale di responsabilità. Lo scopo di tale disposizione

[4] www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

sarebbe quello di riaffermare e rafforzare l'"accountability" dei responsabili del trattamento dei dati personali. Ciò non pregiudica le misure di responsabilità concrete che potrebbero integrare questo principio.

26. Questa nuova disposizione sarebbe in linea con le disposizioni specifiche già esistenti nel quadro legislativo attuale. Si può citare in particolare l’articolo 6 della direttiva 95/46/CE, che al paragrafo 1 fa riferimento ai principi relativi alla qualità dei dati e al paragrafo 2 stabilisce che “[i]l responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1”. la nuova disposizione sarebbe conforme anche all’articolo 17, paragrafo 1, in cui si stabilisce che il responsabile del trattamento deve attuare misure tecniche ed organizzative. In effetti, una norma generale sulla responsabilità rafforzerebbe la necessità che i responsabili del trattamento applichino le norme sulla sicurezza di cui all’articolo 17, in aggiunta a quanto previsto nelle rimanenti disposizioni.

III.2 Verso una proposta concreta per un principio generale di responsabilità

27. La nuova disposizione avrebbe lo scopo di promuovere l’adozione di misure concrete e pratiche, in quanto trasformerebbe i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del responsabile del trattamento, nel rispetto delle leggi e dei regolamenti applicabili. Il responsabile del trattamento dovrebbe anche garantire l’efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni.

28. In modo schematico, una disposizione generale di questo tipo si incentrerebbe su due elementi principali:

    (i) la necessità che il responsabile del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati;
    (ii) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile del trattamento deve fornire la prova di quanto esposto al punto (i).

29. L’obbligo dovrebbe applicarsi a tutti i responsabili del trattamento e a tutte le situazioni.

30. Il primo elemento dell’obbligo imporrebbe ai responsabili del trattamento di attuare misure appropriate. I tipi di misure non sarebbero specificati nel testo della norma generale sulla responsabilità. Orientamenti successivi forniti dalle autorità nazionali di protezione dei dati, dal Gruppo di lavoro articolo 29 o dalla Commissione (attraverso procedure di comitatologia) potrebbero indicare, in determinati casi, un insieme minimo di misure specifiche costituenti misure appropriate. Un esempio di tali misure sarebbe l’adozione in alcuni casi di politiche e processi interni necessari per l’attuazione dei principi di protezione dei dati, che rispecchino le leggi e i regolamenti vigenti.

31. L’attuazione di tali misure e processi può anche avvenire in maniera efficace attraverso l’attribuzione di responsabilità e la formazione del personale impegnato nelle operazioni di trattamento. In particolare, conformemente all’articolo 18 della direttiva, i responsabili del trattamento devono essere incoraggiati a designare

incaricati della protezione dei dati personali. Si dovrebbe caldeggiare in ogni caso l’attribuzione di responsabilità a diversi livelli dell’organizzazione, in modo da renderle effettive.

32. Per quanto riguarda i trasferimenti di dati personali al di fuori dell’Unione europea, i responsabili del trattamento dovrebbero adottare ed attuare misure appropriate per ottemperare all'obbligo della presentazione di “garanzie sufficienti” di cui all’articolo 26 della direttiva, quali le regole d’impresa vincolanti.

33. I responsabili del trattamento dovrebbero altresì garantire che le misure pratiche attuate per conformarsi ai principi di protezione dei dati siano efficaci. Nel caso di trattamenti di dati di maggiori dimensioni, più complessi o ad alto rischio, l’efficacia delle misure adottate dovrebbe essere verificata periodicamente. Esistono diversi modi per valutare l’efficacia (o inefficacia) delle misure: monitoraggio, audit interni ed esterni, ecc.

34. In considerazione delle osservazioni svolte finora, il Gruppo di lavoro articolo 29 ha formulato una disposizione sostanziale che potrebbe essere introdotta in un quadro legislativo globale, il cui testo recita::

“*Articolo X - Applicazione dei principi di protezione dei dati*

1. Il responsabile del trattamento attua misure appropriate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati.
2 Su richiesta dell'autorità di vigilanza, il responsabile del trattamento dimostra la conformità con il paragrafo 1.

IV. ANALISI DI VARI ELEMENTI COLLEGATI AL PRINCIPIO GENERALE DI RESPONSABILITÀ

IV.1 Rafforzamento degli obblighi esistenti

35. Il Gruppo di lavoro articolo 29 rileva che alcuni responsabili del trattamento potrebbero percepire il principio generale di responsabilità come un’onerosa imposizione di nuovi obblighi giuridici in capo ai responsabili del trattamento, in particolare vista l’attuale difficile situazione economica dell’UE. Quest'interpretazione non sarebbe corretta.

36. Il Gruppo di lavoro articolo 29 desidera sottolineare che, per la maggior parte, gli obblighi contemplati nella nuova disposizione sono in realtà già previsti, anche se meno esplicitamente, dalla normativa vigente. Infatti, in forza dell’attuale quadro giuridico, i responsabili del trattamento sono tenuti a rispettare i principi e gli obblighi stabiliti dalla direttiva. A tal fine, è intrinsecamente necessario creare, ed eventualmente verificare, le procedure relative alla protezione dei dati. In quest'ottica, una disposizione sulla responsabilità non rappresenta una grande novità, e per la maggior parte non impone obblighi che non fossero già impliciti nella normativa vigente. In sintesi, la nuova disposizione non mira ad assoggettare

i responsabili del trattamento a nuovi principi, ma piuttosto a garantire di fatto l’effettiva osservanza di quelli esistenti.

37. In effetti, uno sviluppo legislativo in qualche modo simile è avvenuto nel 2009 in occasione della modifica della direttiva 2002/58[5], che ha imposto l’obbligo di attuare una politica di sicurezza, in particolare di “*garanti[re] l’attuazione di una politica di sicurezza in ordine al trattamento dei dati personali”*. Così, per quanto riguarda le disposizioni di sicurezza di tale direttiva, il legislatore ha deciso che era necessario introdurre l'obbligo esplicito di predisporre e attuare una politica di sicurezza. Inoltre, l’articolo 18 della direttiva 95/46, che fa riferimento alla designazione di incaricati della protezione dei dati, accanto al sistema di regole d’impresa vincolanti di cui sopra, offrono già esempi di misure pratiche che possono essere adottate dai responsabili del trattamento.

38. Una questione collegata alla precedente riguarda le conseguenze connesse al rispetto (o al mancato rispetto) del principio di responsabilità. Il Gruppo di lavoro articolo 29 evidenzia che osservare il principio di responsabilità non significa necessariamente che il responsabile del trattamento agisca in conformità ai principi sostanziali enunciati nella direttiva, cioè esso non fornisce una presunzione legale di conformità né sostituisce tali principi. Il responsabile del trattamento può avere attuato e verificato le misure che ha posto in essere, e tuttavia può trovarsi coinvolto in irregolarità. Di conseguenza, l’adozione di misure volte al rispetto dei principi non deve in nessun caso esonerare i responsabili del trattamento dalle azioni di verifica dell'applicazione delle autorità di protezione dei dati. In pratica, i responsabili del trattamento del settore pubblico e privato che abbiano adottato misure nell’ambito di robusti programmi di conformità hanno maggiori probabilità di essere in regola con la legge. In effetti, poiché hanno predisposto misure efficaci dirette al rispetto dei principi sostanziali di protezione dei dati, dovrebbe essere meno probabile per loro incorrere in violazioni. Pertanto, nel valutare sanzioni relative a violazioni della privacy, le autorità di protezione dei dati potrebbero considerare rilevanti l’attuazione (o la mancata attuazione) delle misure e la loro verifica.

IV.2 Misure appropriate per l’attuazione delle disposizioni della direttiva

39. Una disposizione sulla responsabilità imporrebbe ai responsabili del trattamento di definire e attuare le misure necessarie per garantire il rispetto dei principi e degli obblighi della direttiva e di verificarne periodicamente l’efficacia.

40. Il principio generale di responsabilità proposto evita volutamente di precisare nei dettagli il tipo di misure da attuare. Ciò solleva le seguenti due questioni fondamentali interconnesse: *(i)* quali misure comuni soddisferebbero il principio di responsabilità? *(ii)* in che modo graduare e adattare le misure a circostanze specifiche?

[5] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio (del 25 novembre 2009) recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell’esecuzione della normativa a tutela dei consumatori.

Le misure: descrizione

41. Il Gruppo di lavoro articolo 29 ritiene che le misure comuni concernenti la responsabilità potrebbero includere il seguente elenco non esaustivo:

- istituzione di procedure interne *prima* della creazione di nuove operazioni di trattamento dei dati personali (revisione interna, valutazione, ecc.)[6];
- formulazione per iscritto di politiche di protezione dei dati vincolanti da prendere in considerazione e applicare alle nuove operazioni di trattamento dei dati (ad esempio, qualità dei dati, comunicazione, principi di sicurezza, accesso, ecc.), che dovrebbero essere a disposizione degli interessati;
- mappatura delle procedure per garantire la corretta identificazione di tutte le operazioni di trattamento dei dati e gestione di un inventario di dette operazioni;
- nomina di un incaricato della protezione dei dati e di altri soggetti responsabili della protezione dei dati;
- adeguata formazione e istruzione del personale in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (o responsabili) del trattamento dei dati personali (come i direttori delle risorse umane), ma anche dirigenti e sviluppatori in campo informatico, e direttori di unità commerciali. Dovrebbero essere stanziate risorse sufficienti per la gestione della privacy, ecc.;
- creazione di procedure trasparenti per gli interessati finalizzate alla gestione delle richieste di accesso, rettifica e cancellazione;
- istituzione di un meccanismo interno di gestione dei reclami;
- definizione di procedure interne per la gestione e la comunicazione efficace di violazioni della sicurezza;
- effettuazione di valutazioni d’impatto sulla privacy, in circostanze specifiche;
- attuazione e controllo delle procedure di verifica per assicurare che tutte le misure esistano non solo sulla carta, ma siano applicate e funzionino nella pratica (audit interni o esterni ecc.).

42. Si potrebbe anche prevedere un approccio complementare al principio generale di responsabilità, secondo cui il quadro normativo includerebbe non solo un principio generale di responsabilità, ma anche un elenco illustrativo di misure che potrebbero essere incoraggiate a livello nazionale[7]. Questa disposizione potrebbe fornire un elenco esemplificativo e non esaustivo di misure che potrebbero costituire uno "strumentario" per i responsabili del trattamento, offrendo loro orientamenti su quali potrebbero essere, a seconda dei casi, le misure appropriate da adottare. Tale elenco esemplificativo sarebbe ovviamente soltanto un complemento all’obbligo giuridico generale di adottare le misure appropriate.

[6] Occorrerebbe un periodo di transizione per rendere le operazioni di trattamento dei dati in essere conformi alla normativa.

[7] Per esempio, gli standard internazionali adottati a Madrid dalle autorità di protezione dei dati contengono all’articolo 22 una disposizione che prevede misure proattive, così formulata: “*Gli Stati devono incoraggiare, tramite la legislazione nazionale, l’attuazione, da parte di coloro che partecipano a qualsiasi fase del trattamento, di misure dirette a promuovere una migliore conformità alle leggi applicabili sulla protezione della privacy in relazione al trattamento dei dati personali. Tali misure potrebbero includere, tra l’altro:*

a) l’attuazione di procedure di prevenzione e di individuazione delle violazioni, che potrebbero basarsi sui modelli standardizzati di governance e/o di gestione della sicurezza dell’informazione;

b) la nomina di uno o più incaricati per la protezione dei dati o della privacy dotati di qualifiche, risorse e competenze adeguate a esercitare la loro funzione di sorveglianza in modo appropriato;

Graduare le misure

43. Quello che precede costituisce un elenco esemplificativo di misure che i responsabili del trattamento potrebbero realizzare per ottemperare alla prima parte del principio di responsabilità (*Il responsabile del trattamento attua misure appropriate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati)*.

44. Alcune delle misure sono “elementi base” che dovranno essere attuati nella maggior parte delle operazioni di trattamento. L’elaborazione di politiche e procedure interne di attuazione dei principi (procedure per gestire le richieste di accesso e i reclami) potrebbe costituire un esempio di misure appropriate per alcuni trattamenti di dati. L’idoneità delle misure dovrà essere decisa caso per caso. Spetta ai responsabili del trattamento prendere tali decisioni, seguendo gli orientamenti emessi dalle autorità nazionali di protezione dei dati e dal Gruppo di lavoro articolo 29, se disponibili (v. sotto).

45. Da quanto precede risulta che nel determinare i tipi di azioni da attuare, non esistono alternative valide alle soluzioni “su misura”. Infatti, le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati. Un approccio uguale per tutti avrebbe il solo effetto di costringere i responsabili del trattamento all’interno di strutture inadatte e si rivelerebbe quindi fallimentare.

46. Secondo questo approccio, i responsabili del trattamento devono essere in grado di adattare le misure alle specificità concrete delle loro situazioni particolari e delle operazioni di trattamento dei dati in questione. In questo contesto, il Gruppo di

c) la regolare attuazione di programmi di formazione, istruzione e sensibilizzazione rivolti ai membri delle organizzazioni per una migliore comprensione delle leggi applicabili in materia di tutela della privacy in relazione al trattamento dei dati personali, nonché procedure stabilite a tal fine dalle organizzazioni;

d) l’effettuazione periodica di audit trasparenti, realizzati da soggetti qualificati e preferibilmente indipendenti per verificare la conformità con le leggi vigenti in materia di protezione della privacy in relazione al trattamento dei dati personali, e con le procedure stabilite a tal fine dalle organizzazioni;

e) l’adeguamento delle tecnologie e/o dei sistemi informatici per il trattamento dei dati personali alle leggi vigenti sulla tutela della privacy in relazione al trattamento dei dati personali, in particolare al momento di decidere le specifiche tecniche, lo sviluppo e l’attuazione;

f) la realizzazione di valutazioni d’impatto sulla privacy prima dell’attuazione di nuove tecnologie e/o nuovi sistemi informatici per il trattamento dei dati personali, e prima dell’applicazione di nuovi metodi di trattamento dei dati personali o di qualunque modifica sostanziale nel trattamento esistente;

g) l’adozione di codici di autoregolamentazione vincolanti, che includano elementi per misurarne l’efficacia in termini di conformità e di livello di protezione dei dati personali, e che prevedano misure efficaci in caso di non conformità;

h) l’attuazione di un piano d’azione che stabilisca orientamenti per l’azione da intraprendere in caso di violazione delle leggi sulla tutela della privacy in relazione al trattamento dei dati personali, compreso quanto meno l’obbligo di determinare la causa e l’entità della violazione, di descriverne gli effetti negativi e di adottare le misure appropriate per evitare che si ripeta in futuro.”

lavoro articolo 29 rammenta i criteri di cui all’articolo 17 dell’attuale direttiva[8] per determinare il tipo di misure di sicurezza da applicare, ossia i rischi rappresentati dal trattamento dei dati e dalla loro natura. Questi due fattori potrebbero essere utilizzati per analogia per determinare i tipi generali di misure da applicare. Più concretamente, taluni aspetti come le dimensioni delle operazioni di trattamento, gli obiettivi dello stesso e il numero di trasferimenti di dati previsti possono contribuire a definire il livello di rischio. Occorre altresì tenere conto del tipo di dati, in particolare se si tratta o meno di dati sensibili. Si potrebbe inoltre riflettere sulla necessità di imporre determinati obblighi all’incaricato del trattamento o ai progettisti e/o produttori di tecnologie dell’informazione e della comunicazione alla luce di questo principio di responsabilità.

47. In base a tali criteri, in linea di principio, i grandi responsabili del trattamento dovrebbero attuare misure rigorose. In alcuni casi, può essere necessario anche per i piccoli e medi responsabili del trattamento presentare garanzie rigorose, per esempio se sono impegnati in operazioni rischiose di trattamento dei dati, come alcune operazioni nel quadro dei servizi sanitari online. Ad esempio, un ente locale (municipio), una multinazionale, una piccola impresa (Internet), un’organizzazione la cui attività principale sia il trattamento dei dati o un organizzazione che abbia commesso violazioni in passato richiederebbero tutti misure specifiche, al fine di garantire una governance credibile ed efficace delle informazioni. Come risultato, nei casi più semplici e basilari, come per il trattamento dei dati personali relativi a risorse umane per la creazione di una directory, l’“obbligo di dimostrare”, cui si fa riferimento nel paragrafo 2 della disposizione sulla responsabilità, potrebbe essere rispettato facilmente (attraverso, ad esempio, le note informative utilizzate, la descrizione delle misure di sicurezza di base, ecc.). Al contrario, in altri casi più complessi, come ad esempio l’utilizzo di dispositivi biometrici innovativi, l’adempimento dell’“obbligo di dimostrare” potrebbe richiedere altre misure. Il responsabile del trattamento potrebbe ad esempio dover dimostrare di aver effettuato una valutazione d’impatto sulla privacy, che il personale che si occupa del trattamento ha ricevuto formazioni e informazioni su base regolare, ecc.

48. La trasparenza è parte integrante di molte misure concernenti responsabilità. La trasparenza nei confronti degli interessati e del pubblico in generale contribuisce alla responsabilità dei responsabili del trattamento. Per esempio, un maggiore livello di responsabilità si consegue pubblicando su Internet le politiche in materia di privacy, fornendo trasparenza riguardo alle procedure interne di gestione dei reclami, e attraverso la pubblicazione di relazioni annuali.

Orientamento e certezza del diritto

49. Mentre l'esigenza di adattabilità e quindi di una certa flessibilità richiede l’uso di un linguaggio aperto, il Gruppo di lavoro articolo 29 è consapevole del fatto che una disposizione di massima che lasci spazio a flessibilità e adattabilità potrebbe anche causare incertezza. I responsabili del trattamento potrebbero ritenere che la

[8] “*Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere*”.

disposizione non sia sufficientemente precisa per garantire la certezza del diritto. Per esempio, potrebbero nutrire dubbi circa il livello di dettaglio richiesto per le politiche e le procedure sulla privacy, per i tempi e i modi per designare l'incaricato della protezione dei dati, per l'organizzazione di sessioni di formazione, ecc. L’incertezza potrebbe riguardare anche il tipo di verifica necessario, da parte di terzi ovvero interno. Inoltre, i responsabili del trattamento potrebbero anche temere di essere oggetto di interpretazioni divergenti e arbitrarie a livello nazionale per quanto riguarda la portata e la natura dei loro obblighi.

50. Il Gruppo di lavoro articolo 29 comprende questa preoccupazione. Tuttavia, per le ragioni esposte in precedenza circa l'esigenza di flessibilità e di adattabilità, la soluzione per conseguire la certezza del diritto non può essere fornita nella direttiva stessa. A tal fine, il Gruppo di lavoro articolo 29 ritiene che gli orientamenti per l’armonizzazione emanati dalla Commissione (per esempio, tramite misure tecniche di attuazione) e/o dallo stesso Gruppo di lavoro possano diventare uno strumento utile per fornire maggiore certezza ed eliminare potenziali differenze a livello di attuazione[9]. Il Gruppo di lavoro potrebbe anche preparare orientamenti generali che forniscano una base di elementi necessari per un responsabile del trattamento standard. Questa base potrebbe essere adattata alle esigenze specifiche di ciascun responsabile del trattamento di dati.

51. Potrebbe anche essere utile sviluppare un *programma modello per la conformità dei dati*, che potrebbe essere utilizzato da responsabili del trattamento di medie e grandi dimensioni come base su cui elaborare i loro programmi particolari, come è avvenuto per le regole d’impresa vincolanti elaborate sulla base degli orientamenti del Gruppo di lavoro articolo 29[10]. Tali modelli dovrebbero essere creati in seguito a un attento riesame delle prassi correnti e dei modelli disponibili, e previa consultazione di tutte le parti interessate. Si tratta di un settore che richiederà investimenti ingenti da parte di tutti i soggetti coinvolti.

Efficacia delle misure

52. Le stesse questioni trattate in precedenza riguardanti le misure applicabili emergono nel contesto della necessità di garantirne l’efficacia. Il modo in cui questa può essere assicurata sarà diverso a seconda del tipo di trattamento dei dati.

53. Esistono vari metodi a disposizione dei responsabili del trattamento per valutare l’efficacia (o l’inefficacia) delle misure. Per il trattamento di dati di maggiori dimensioni, più complesso e ad alto rischio, gli audit interni ed esterni sono metodi comuni di verifica. Anche il modo in cui vengono condotti gli audit può variare, da audit completi ad audit negativi (che possono a loro volta assumere forme diverse). Nel decidere come garantire l’efficacia delle misure, il Gruppo di lavoro articolo 29 suggerisce di utilizzare gli stessi criteri applicati per decidere le

[9] Un esempio di questo tipo di orientamento è lo strumento di autovalutazione PIPEDA, pubblicato dall’Ufficio del commissario canadese per la privacy per aiutare i responsabili del trattamento di medie e grandi dimensioni a sviluppare ed attuare una buona governance e gestione della privacy. Lo strumento di autovalutazione è disponibile all’indirizzo: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf .

[10] Documento di lavoro 153 del Gruppo di lavoro articolo 29 che stabilisce una tabella comprendente gli elementi e i principi delle regole d’impresa vincolanti e documento di lavoro 154 che stabilisce un quadro per la struttura delle regole d’impresa vincolanti.

misure mutuati dall’articolo 17 della direttiva 95/46/CE, vale a dire, i rischi presentati dal trattamento e la natura dei dati. Pertanto, il modo in cui un responsabile del trattamento deve assicurare l’efficacia delle misure dipende dalla sensibilità dei dati, dalla quantità dei dati trattati e dai particolari rischi che il trattamento comporta . Gli orientamenti del Gruppo di lavoro relativi alle misure potrebbero comprendere anche indicazioni su questo aspetto.

IV.3 Collegamento con altri obblighi

Notificazioni preliminari

54. Si potrebbe intraprendere una riflessione sul possibile impatto sulle notificazioni preliminari quando adeguate garanzie siano definite a livello del responsabile del trattamento. Si potrebbe prevedere la possibilità che determinati meccanismi di responsabilità sostituiscano o riducano gli obblighi amministrativi dell’attuale legislazione sulla protezione dei dati, come già suggerito dal Gruppo di lavoro articolo 29 nel suo parere sul futuro della privacy.

Trasferimenti internazionali di dati

55. Le regole d’impresa vincolanti rappresentano un esempio di attuazione dei principi di protezione dei dati sulla base del principio di responsabilità. Si tratta di una modalità individuata e accettata dal Gruppo di lavoro articolo 29 per fornire adeguate garanzie per i trasferimenti al di fuori dell’Unione europea.

56. Questo è un settore che trarrebbe beneficio da un’ulteriore analisi alla luce della revisione della direttiva 95/46. In particolare, sarebbe importante esaminare se nell'ambito di applicazione dell’articolo 26, paragrafo 2, della direttiva (*uno Stato membro può autorizzare un trasferimento [...] qualora il responsabile del trattamento presenti garanzie sufficienti […]; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate”)* rientrino a pieno titolo le regole d’impresa vincolanti e altri meccanismi analoghi di responsabilità vincolanti quali strumenti atti a fornire garanzie sufficienti.

57. In questo contesto, è molto importante valutare, tra l'altro, i meccanismi usati per dare attuazione ai principi e agli obblighi di protezione dei dati all’interno degli stessi responsabili del trattamento e dei sistemi di verifica. È inoltre importante analizzare i meccanismi per ottimizzare l’attuale sistema basato sull’autorizzazione dei trasferimenti di dati da parte delle autorità nazionali di protezione dei dati.

IV.4 Il ruolo delle autorità di protezione dei dati

58. Una questione da affrontare è se il principio di responsabilità proposto nel presente parere influirà sui poteri delle autorità di protezione dati, in particolare in sede di verifica dell'applicazione. Come ulteriormente descritto di seguito, il principio non sottrae alcun potere alle autorità di protezione dei dati, bensì apporterà loro vantaggi.

59. Per quanto riguarda la verifica dell'applicazione, il principio proposto riconosce la competenza delle autorità di protezione dei dati a chiedere al titolare del trattamento la prova della conformità con il principio di responsabilità, rafforzandone così i poteri. Questo garantisce che le autorità mantengano, in qualsiasi momento, la competenza a svolgere azioni di verifica. . Occorre chiarire che, in ogni caso, le autorità di protezione dei dati resterebbero competenti a controllare non solo le misure adottate dai responsabili del trattamento, ma anche e soprattutto il rispetto dei principi e degli obblighi di fondo.

60. Inoltre, l’attuazione del principio di responsabilità fornirà alle autorità di protezione dei dati informazioni utili per monitorare i livelli di conformità. Infatti, poiché i responsabili del trattamento dovranno essere in grado di dimostrare alle autorità se e come hanno attuato le misure, le autorità in discorso disporranno di informazioni altamente rilevanti in materia di conformità e potranno in seguito utilizzare tali informazioni nel contesto delle loro azioni di verifica dell'applicazione. Inoltre, se tali informazioni non sono fornite su richiesta, le autorità di protezione dei dati avranno un motivo per agire immediatamente contro i responsabili del trattamento, indipendentemente dalla presunta violazione di altri principi basilari di protezione dei dati.

61. Il principio dovrebbe anche essere utile alle autorità di protezione dei dati in quanto le aiuterebbe ad essere più selettive e strategiche, consentendo loro di investire le proprie risorse in modo da generare il maggior livello possibile di conformità.

62. Il Gruppo di lavoro articolo 29 osserva che il principio di responsabilità potrebbe contribuire allo sviluppo di competenze giuridiche e tecniche nel campo dell’attuazione delle disposizioni sulla protezione dei dati. Saranno indispensabili in questo settore persone altamente competenti, dotate di approfondite conoscenze tecniche e giuridiche in materia di protezione dei dati, nonché di capacità di comunicare, formare il personale, elaborare e attuare politiche e svolgere audit. Tali competenze saranno necessarie sia internamente sia nella forma di servizi esterni che le imprese potranno richiedere. Questa evoluzione sarà fondamentale per garantire che i responsabili del trattamento possano svolgere i propri compiti, compreso, se necessario, lo svolgimento di audit interni ed esterni/interni. Al tempo stesso, questo sviluppo sarà positivo per le autorità di protezione dei dati, poiché il sistema contribuirà alla conformità in generale, le autorità avranno a loro disposizione informazioni più affidabili riguardo alle pratiche interne delle società, e la formazione di professionisti qualificati con conoscenze approfondite in materia di protezione dei dati sarà certamente di aiuto nella loro interazione con i responsabili del trattamento.

63. Si può concludere che il ruolo delle autorità di protezione dei dati si traduce prevalentemente in attività “ex post” piuttosto che “ex ante”. Poiché la responsabilità pone l’accento su determinati risultati da raggiungere in termini di buona governance della protezione dei dati, si dice che è orientata ai risultati ed incentrata sull’aspetto “ex post” (cioè, successivo all’inizio del trattamento dei dati).

IV. 5 Sanzioni

64. Il sistema proposto può funzionare solo se le autorità di protezione dei dati sono dotate di poteri sanzionatori di una certa entità. In particolare, quando e se i responsabili del trattamento non riescono a soddisfare il principio di responsabilità, sorge la necessità di sanzioni appropriate. Per esempio, deve essere punibile il mancato rispetto da parte di un responsabile del trattamento degli impegni formulati nel quadro di politiche interne vincolanti. Ovviamente, ciò si aggiunge all'effettiva violazione dei principi sostanziali di protezione dei dati.

65. Inoltre, il Gruppo di lavoro articolo 29 ritiene che i poteri delle autorità nazionali di protezione dei dati debbano comprendere la possibilità di imporre ai responsabili del trattamento istruzioni precise riguardo al loro sistema di conformità.

IV.6 Lo sviluppo di sistemi di certificazione

66. Nel lungo periodo, la disposizione sulla responsabilità potrebbe favorire lo sviluppo di programmi o sigilli di certificazione. Tali programmi contribuirebbero a dimostrare che un responsabile del trattamento ha rispettato la disposizione e che, quindi, ha definito e attuato misure appropriate che sono state periodicamente sottoposte a revisione. Vari fattori, illustrati di seguito, potrebbero favorire tale sviluppo.

67. In generale, si può prevedere che, per differenziarsi, i servizi di protezione dei dati/auditing/valutazione d’impatto sulla privacy offriranno probabilmente sempre più spesso certificati o sigilli per distinguersi all’interno del mercato e anche per acquisire un vantaggio competitivo. I responsabili del trattamento potrebbero decidere di avvalersi di servizi affidabili che rilasciano certificati. Mano a mano che acquisteranno notorietà in virtù delle verifiche rigorose, i sigilli di certificazione potranno riscuotere il favore dei responsabili del trattamento in quanto più "comodi" in termini di sicurezza oltre che più vantaggiosi sul piano competitivo.

68. L’uso di regole d’impresa vincolanti come base giuridica per i trasferimenti internazionali di dati implica che i responsabili del trattamento dimostrino di aver messo in atto adeguate garanzie, nel cui caso le autorità di protezione dei dati possono autorizzare i trasferimenti. Questo è un ambito in cui i servizi di certificazione potrebbero essere utili. Tali servizi analizzerebbero le assicurazioni fornite dal responsabile del trattamento e, se del caso, emetterebbero il relativo sigillo di certificazione. Un’autorità di protezione dei dati potrebbe utilizzare la certificazione fornita da un dato programma di certificazione nella sua analisi delle regole d’impresa vincolanti tesa a verificare se un responsabile del trattamento abbia fornito garanzie sufficienti ai fini dei trasferimenti internazionali di dati, contribuendo così all’ottimizzazione del processo di autorizzazione di tali trasferimenti.

IV.7 La regolamentazione dei sistemi di certificazione

69. Le stesse ragioni che favoriscono lo sviluppo di servizi di certificazione avvalorano la necessità che tali servizi siano regolamentati. Infatti, se tali servizi sono intesi a fornire prove affidabili di conformità in termini di protezione dei dati (alle autorità di protezione dei dati, ai responsabili del trattamento e ai consumatori in generale) e a funzionare correttamente nel mercato interno, risultano necessarie norme disciplinanti la fornitura di tali servizi. Le autorità di protezione dei dati dovrebbero svolgere un ruolo chiave nello sviluppo di tali norme (ad esempio modelli, ecc.) e dovrebbero essere in grado di farne rispettare l’attuazione. Ciò impone altresì che siano dotate di risorse sufficienti. Inoltre, le autorità di protezione dei dati dovrebbero svolgere un ruolo nella certificazione dei certificatori. Questo potrebbe essere particolarmente importante nell’ambito dei trasferimenti internazionali di dati. Poiché la qualità dei servizi e il loro funzionamento nel mercato interno sono un criterio fondamentale, la legge dovrà stabilire le condizioni atte a conseguire tale qualità. Non sembra un’opzione possibile lasciare questo aspetto al mercato. L’esperienza in altri settori, ad esempio la certificazione delle merci, ha mostrato una tendenza al ribasso. La concorrenza tra i prestatori di servizi può condurre ad una riduzione dei prezzi e anche a una certa flessibilità o rilassamento delle procedure. In sintesi, in ambito transfrontaliero o meno, le risultano necessarie norme dirette a garantire la buona qualità dei servizi e una base di parità.

70. Il Gruppo di lavoro articolo 29 osserva che la legislazione vigente in materia di accreditamento[11] potrebbe essere applicabile nel settore dei servizi di certificazione nel campo della protezione dei dati. Tale normativa fornisce già la struttura necessaria, stabilendo norme sull’organizzazione e il funzionamento degli organismi di accreditamento. Queste regole valgono per l’accreditamento facoltativo e anche nei casi specifici in cui l’accreditamento è obbligatorio.

71. Ovviamente, questo tipo di servizio darebbe altresì un impulso all’armonizzazione delle norme di base rispetto alle quali i soggetti sarebbero sottoposti a verifica. Gli orientamenti menzionati (elaborati dal gruppo articolo 29 o dalla Commissione), indicando programmi modello di conformità dei dati, sarebbero di grande utilità.

V. CONCLUSIONI

72. Lo sviluppo di nuove tecnologie e la costante globalizzazione dell’economia e della società hanno condotto ad una proliferazione di dati personali raccolti, selezionati, trasferiti o altrimenti conservati. I rischi connessi a tali dati, pertanto, si moltiplicano.

73. Il Gruppo di lavoro articolo 29 è convinto che l’aumento sia dei rischi sia del valore dei dati personali in sé renda necessario rafforzare il ruolo e la responsabilità dei responsabili del trattamento. Un quadro normativo che provveda a questa nuova realtà deve contenere gli strumenti necessari per incoraggiare i

[11] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93.

responsabili del trattamento ad applicare in pratica misure appropriate ed efficaci in grado di realizzare i risultati derivanti dai principi di protezione dei dati. Esempi di tali misure sono le procedure per garantire l’identificazione di tutte le operazioni di trattamento dei dati e per rispondere alle richieste di accesso, lo stanziamento di risorse e la designazione di persone responsabili per l’organizzazione della conformità della protezione dei dati.

74. Per incoraggiare la protezione dei dati nella pratica, il Gruppo di lavoro articolo 29 propone in primo luogo di includere nelle proposte di modifica della direttiva sulla protezione dei dati una nuova disposizione che obblighi i responsabili del trattamento ad attuare misure appropriate ed efficaci per garantire che i principi e gli obblighi della direttiva sulla protezione dei dati siano rispettati e di dimostrarlo, su richiesta, alle autorità. Tali misure dovrebbero favorire il rispetto dei principi e degli obblighi di protezione dei dati, riducendo al minimo i rischi di accesso non autorizzato, uso improprio, perdita, ecc. L’obbligo di dimostrare, su richiesta, la predisposizione delle misure necessarie dovrebbe diventare uno strumento utile alle autorità di protezione dei dati nello svolgimento dei loro compiti di verifica dell'applicazione.

75. L’obbligo di attuare tali misure dovrebbe applicarsi ai responsabili del trattamento di tutti i settori (pubblico e privato) ed essere adattabile, di modo che il tipo di misure sia adeguato ai rischi presentati dal trattamento e alla natura dei dati.

Fatto a Bruxelles, 13 luglio 2010

Per il Gruppo di lavoro,
Il presidente
Jacob KOHNSTAMM

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 [1571514]

[doc. web n. 1571514]

Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008
G.U. n. 287 del 9 dicembre 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

VISTI gli atti d´ufficio relativi alla problematica del rinvenimento di dati personali all´interno di apparecchiature elettriche ed elettroniche cedute a un rivenditore per la dismissione o la vendita o a seguito di riparazioni e sostituzioni; viste, altresì, le recenti notizie di stampa in ordine al rinvenimento da parte dell´acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;

VISTO il d.lg. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*), con particolare riferimento agli artt. 31 e ss. e 154, comma 1, lett. *h)*, nonché alle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza allegato "B" al Codice;

VISTO il d.lg. 25 luglio 2005, n. 151 (*Attuazione delle direttive 2002/95/Ce, 2002/96/Ce e 2003/108/Ce, relative alla riduzione dell´uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti*), che prevede misure e procedure finalizzate a prevenire la produzione di rifiuti di apparecchiature elettriche e elettroniche, nonché a promuovere il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurne la quantità da avviare allo smaltimento (cfr. art. 1, comma 1, lett. *a)* e *b)*);

CONSIDERATO che l´applicazione della disciplina contenuta nel menzionato d.lg. n. 151/2005, mirando (tra l´altro) a privilegiare il recupero di componenti provenienti da rifiuti di apparecchiature elettriche ed elettroniche (Raee), anche nella forma del loro reimpiego o del riciclaggio in beni oggetto di (nuova) commercializzazione (cfr. in particolare artt. 1 e 3, comma 1, lett. *e)* ed *f)*, d.lg. n. 151/2005), comporta un rischio elevato di "circolazione" di componenti elettroniche "usate" contenenti dati personali, anche sensibili, che non siano stati cancellati in modo idoneo, e di conseguente accesso ad essi da parte di terzi non autorizzati (quali, ad esempio, coloro che provvedono alle predette operazioni propedeutiche al riutilizzo o che acquistano le apparecchiature sopra indicate);

CONSIDERATO che il "reimpiego" consiste nelle operazioni che consentono l´utilizzo dei rifiuti

elettrici ed elettronici o di loro componenti *"allo stesso scopo per il quale le apparecchiature erano state originariamente concepite, compresa l´utilizzazione di dette apparecchiature o di loro componenti successivamente alla loro consegna presso i centri di raccolta, ai distributori, ai riciclatori o ai fabbricanti"* (art. 3, comma 1, lett. e), d.lg. n. 151/2005) e il "riciclaggio" consiste nel *"ritrattamento in un processo produttivo dei materiali di rifiuto per la loro funzione originaria o per altri fini"* (art. 3, comma 1, lett. e), d.lg. n. 151/2005);

CONSIDERATO che rischi di accessi non autorizzati ai dati memorizzati sussistono anche in relazione a rifiuti di apparecchiature elettriche ed elettroniche avviati allo smaltimento (art. 3, comma 1, lett. i), d.lg. n. 151/2005);

RILEVATA la necessità di richiamare l´attenzione su tali rischi di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali (di seguito sinteticamente individuati con la locuzione "titolari del trattamento": art. 4, comma 1, lett. *f)* del Codice), dismettono sistemi informatici o, più in generale, apparecchiature elettriche ed elettroniche contenenti dati personali (come pure dei soggetti che, su base individuale o collettiva, provvedono al reimpiego, al riciclaggio o allo smaltimento dei rifiuti di dette apparecchiature);

RILEVATO che la disciplina di cui al citato d.lg. n. 151/2005 e alla normativa secondaria che ne è derivata (allo stato contenuta nel d.m. 25 settembre 2007, n. 185, recante *"Istituzione e modalità di funzionamento del registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei rifiuti di apparecchiature elettriche ed elettroniche (Raee)"*, nell´ulteriore d.m. del 25 settembre 2007, recante *"Istituzione del Comitato di vigilanza e di controllo sulla gestione dei Raee"*, nonché nel d.m. 8 aprile 2008, recante *"Disciplina dei centri di raccolta dei rifiuti urbani raccolti in modo differenziato come previsto dall´art. 183, comma 1, lettera cc) del decreto legislativo 3 aprile 2006, n. 152 e successive modifiche"*) lascia impregiudicati gli obblighi che gravano sui titolari del trattamento relativamente alle misure di sicurezza nel trattamento dei dati personali (e la conseguente responsabilità);

RILEVATO che ogni titolare del trattamento deve quindi adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della dismissione dei menzionati apparati elettrici ed elettronici (artt. 31 ss. del Codice); ciò, considerato anche che, impregiudicati eventuali accordi che prevedano diversamente, produttori, distributori e centri di assistenza di apparecchiature elettriche ed elettroniche non risultano essere soggetti, in base alla particolare disciplina di settore, a specifici obblighi di distruzione dei dati personali eventualmente memorizzati nelle apparecchiature elettriche ed elettroniche a essi consegnate;

RILEVATO che dall´inosservanza delle misure di sicurezza può derivare in capo al titolare del trattamento una responsabilità penale (art. 169 del Codice) e, in caso di danni cagionati a terzi, civile (artt. 15 del Codice e 2050 cod. civ.);

RILEVATO che analoghi obblighi relativi alla destinazione dei dati gravano sul titolare del trattamento nel caso in cui la dismissione delle apparecchiature coincida con la cessazione del trattamento (art. 16 del Codice);

RILEVATO che le misure da adottare in occasione della dismissione di componenti elettrici ed elettronici suscettibili di memorizzare dati personali devono consistere nell´effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, sì da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venirne a conoscenza non avendone diritto (si pensi, ad esempio, ai dati personali memorizzati sul disco rigido dei *personal computer* o nelle cartelle di posta elettronica, oppure custoditi nelle rubriche dei terminali di comunicazione elettronica);

CONSIDERATO che tali misure risultano allo stato già previste quali misure minime di sicurezza per i trattamenti di dati sensibili o giudiziari, sulla base delle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza che disciplinano la custodia e l´uso dei supporti rimovibili sui quali sono memorizzati i dati, che vincolano il riutilizzo dei supporti alla cancellazione effettiva dei dati o alla loro trasformazione in forma non intelligibile;

RITENUTO che i titolari del trattamento, in occasione della dismissione delle menzionate apparecchiature elettriche ed elettroniche, qualora siano sprovvisti delle necessarie competenze e strumentazioni tecniche per la cancellazione dei dati personali, possono ricorrere all´ausilio o conferendo incarico a soggetti tecnicamente qualificati in grado di porre in essere le misure idonee a cancellare effettivamente o rendere non intelligibili i dati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l´esecuzione di tali operazioni o si impegnino ad effettuarle;

RITENUTO che chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti debba comunque assicurarsi dell´inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l´autorizzazione a cancellarli o a renderli non intelligibili;

CONSIDERATO che, ferma restando l´adozione di ulteriori opportune cautele volte a prevenire l´indebita acquisizione di informazioni personali, anche fortuita, da parte di terzi, le predette misure, suscettibili di aggiornamento alla luce dell´evoluzione tecnologica, possono in particolare consistere, a seconda dei casi, anche nelle procedure di cui agli allegati documenti, che costituiscono parte integrante del presente provvedimento;

RITENUTA la necessità di curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati (art. 154, comma 1, lett. *h)*, del Codice), con riferimento alla dismissione di apparecchiature elettriche ed elettroniche, anche attraverso la pubblicazione del presente provvedimento sulla *Gazzetta Ufficiale* della Repubblica Italiana;

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

RELATORE il dott. Giuseppe Fortunato;

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell´art. 154, comma 1, lett. *h)* del Codice, richiama l´attenzione di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, non distruggono, ma dismettono supporti che contengono dati personali, sulla necessità di adottare idonei accorgimenti e misure, anche con l´ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:

   a. reimpiegate o riciclate, anche seguendo le procedure di cui all´allegato A);

   b. smaltite, anche seguendo le procedure di cui all´allegato B).

Tali misure e accorgimenti possono essere attuate anche con l´ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di

apparecchiature che attestino l´esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell´inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l´autorizzazione a cancellarli o a renderli non intelligibili;

2. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 13 ottobre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

Allegato A) al provvedimento del Garante del 13 ottobre 2008

Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche
In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l´effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l´altro, in:

Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:
1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l´applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file), e comporta la necessità per l´utente di tenere traccia separatamente delle parole-chiave utilizzate.

2. Memorizzazione dei dati sui dischi rigidi (*hard-disk*) dei *personal computer* o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l´uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, *drive* logici, *file-system*) realizzando le funzionalità di un c.d. *file-system crittografico* (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo *personal computer*, e dispositivi elettronici) in grado di proteggere, con un´unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L´unica parola-chiave di volume verrà automaticamente utilizzata per le operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l´uso dei programmi *software* con cui i dati vengono trattati.

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:
3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l´utente abbia eliminato dei file da un´unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.
Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all´importanza delle informazioni di cui si vuole impedire l´indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.

4. Formattazione "a basso livello" dei dispositivi di tipo *hard disk* (*low-level formatting–LLF*), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;

5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, *floppy-disk*, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione *software* (che richiedono l´accessibilità del dispositivo da parte del sistema a cui è interconnesso).

Allegato B) al provvedimento del Garante del 13 ottobre 2008

Smaltimento di rifiuti elettrici ed elettronici
In caso di smaltimento di rifiuti elettrici ed elettronici, l´effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l’acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

sistemi di punzonatura o deformazione meccanica;
distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
demagnetizzazione ad alta intensità.

Parere del Garante europeo della protezione dei dati in merito alla proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

(2010/C 280/02)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in particolare l'articolo 17,

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in particolare l'articolo 41,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

1. Il 3 dicembre 2008 la Commissione ha adottato una proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) (in prosieguo «la proposta») [1]. La proposta è finalizzata a rifondere la direttiva 2002/96/CE sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) adottata il 27 gennaio 2003 (in prosieguo «la direttiva») [2] senza modificare le cause o le motivazioni alla base della raccolta e del riciclaggio di RAEE.

2. Diversamente da quanto prescritto dall'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 [3], il GEPD non è stato consultato. Agendo di propria iniziativa, il GEPD ha quindi adottato l'attuale parere in base all'articolo 41, paragrafo 2, del medesimo regolamento. Il GEPD raccomanda di includere nel preambolo della proposta un riferimento al presente parere.

3. Il GEPD, pur consapevole del fatto che questo documento giunge in una fase tardiva del processo legislativo, ritiene utile e appropriato emettere il presente parere visto che la proposta solleva questioni importanti in materia di protezione dei dati che nel testo non sono state affrontate. Il parere non intende modificare lo scopo e i contenuti principali e preponderanti della proposta, il cui «centro di gravità» [4] rimane la protezione dell'ambiente, bensì solo aggiungere un'ulteriore dimensione che sta divenendo sempre più rilevante per la nostra società dell'informazione [5].

4. Il GEPD, consapevole altresì della portata limitata della procedura di rifusione, invita nondimeno il legislatore a tener conto di tali raccomandazioni in conformità con il punto 8 dell'accordo interistituzionale sulla procedura di rifusione (che prevede la possibilità di modificare le disposizioni immutate) [6].

II. CONTESTO E ANTEFATTI DELLA PROPOSTA E SUA RILEVANZA PER LA PROTEZIONE DEI DATI

5. Lo scopo della proposta è aggiornare la direttiva esistente in materia di smaltimento, reimpiego e riciclo dei RAEE. Problemi di carattere tecnico, giuridico e amministrativo emersi nei primi anni di attuazione della direttiva hanno portato alla presentazione della proposta, come previsto dall'articolo 17, paragrafo 5, della direttiva.

6. Per apparecchiature elettriche ed elettroniche (AEE) si intende un'ampia gamma di prodotti che comprende una disparata serie di supporti in grado di contenere dati personali — quali le apparecchiature informatiche e di telecomunicazione (per esempio, personal computer, laptop, terminali per i servizi di comunicazione elettronica) — caratterizzati nell'attuale contesto tecno-economico da sempre più rapidi cicli d'innovazione e, data la convergenza tecnologica, dalla disponibilità di dispositivi multifunzionali. L'evoluzione dei supporti elettronici di memorizzazione è sempre più veloce, in particolare per quanto concerne la capacità di memorizzazione e le dimensioni. Di conseguenza, le forze di mercato fanno crescere in misura analoga il ricambio delle apparecchiature elettriche ed elettroniche (contenenti una grande quantità di dati personali,

[1] COM(2008) 810 definitivo.
[2] GU L 37 del 13.2.2003, pag. 24.
[3] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, GU L 8 del 12.1.2001, pag. 1.
[4] Cfr. la sentenza della Corte del 23 febbraio 1999, causa C-42/97, *Parlamento europeo/Consiglio dell'Unione europea*, Racc. 1999, pag. I-869, punto 43.
[5] Cfr. anche, tra l'altro, la sentenza della Corte del 30 gennaio 2001, causa C-36/98 *Spagna/Consiglio*, Racc. 2001, pag. I-779, punto 59: «Se l'esame di un atto comunitario dimostra che esso persegue una duplice finalità o che esso ha una doppia componente e se una di queste è identificabile come principale o preponderante, mentre l'altra è solo accessoria, l'atto deve fondarsi su una sola base giuridica, ossia quella richiesta dalla finalità o componente principale o preponderante».
[6] Accordo interistituzionale, del 28 novembre 2001, ai fini di un ricorso più strutturato alla tecnica della rifusione degli atti normativi, GU C 77 del 28.3.2002, pag. 1.

spesso sensibili). Da ciò deriva non solo che i RAEE «sono considerati il flusso di rifiuti in più rapida crescita nell'UE» ([7]), bensì anche, nel caso di smaltimento inadeguato, che è prevedibile un aumento del rischio di perdita e dispersione di dati personali contenuti in questo tipo di AEE.

7. Per molto tempo le politiche dell'Unione europea sull'ambiente e sullo sviluppo sostenibile si sono concentrate sulla riduzione dello spreco di risorse naturali e sull'introduzione di misure volte a prevenire l'inquinamento.

8. In questo quadro normativo rientrano lo smaltimento, il reimpiego e il riciclo dei RAEE. Le misure introdotte mirano a evitare lo smaltimento di apparecchiature elettriche ed elettroniche insieme ai rifiuti indifferenziati, imponendo ai produttori l'obbligo di provvedere allo smaltimento secondo le modalitá previste dalla direttiva.

9. In particolare, tra le varie misure previste dalla direttiva, vale la pena mettere in luce quelle destinate al *reimpiego* (ossia le operazioni in virtù delle quali i RAEE o loro componenti sono utilizzati allo stesso scopo per cui erano stati originariamente concepiti, incluso l'uso continuativo delle apparecchiature o loro componenti riportati a punti di raccolta, a distributori, riciclatori o fabbricanti), al *riciclaggio* (ossia il ritrattamento in un processo di produzione dei materiali di rifiuto per la loro funzione originaria o per altri fini) e alla ricerca di altre forme di recupero dei RAEE in maniera tale da ridurre lo smaltimento dei rifiuti [cfr. l'articolo 1 e l'articolo 3, lettere d) ed e), della direttiva].

10. Queste operazioni, in particolare il reimpiego e il riciclaggio dei RAEE, soprattutto di apparecchiature informatiche e di telecomunicazione, possono implicare il rischio, superiore rispetto al passato, che chi raccoglie i RAEE o vende e acquista i dispositivi usati o riciclati possa avere accesso a eventuali dati personali in essi contenuti. Tali dati spesso possono essere sensibili o riferirsi a un ampio numero di soggetti.

11. Per tutti questi motivi, il GEPD ritiene urgente che tutte le parti interessate (utilizzatori e fabbricanti di AEE) siano rese edotte in merito ai rischi concernenti i dati personali, specialmente nella fase conclusiva del ciclo di vita delle AEE. In tale stadio è probabile che le AEE contengano una grande quantità di dati personali e pertanto, pur avendo un minor valore dal punto di vista economico, presumibilmente possiedono un elevato valore «intrinseco» per la persona interessata e/o per altri soggetti.

([7]) Documento di lavoro dei servizi della Commissione che accompagna la proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) (rifusione). Valutazione dell'impatto, 3.12.2008 [COM(2008) 810 definitivo] SEC(2008) 2933, pag. 17.

III. ANALISI DELLA PROPOSTA

III.1. Applicabilità della direttiva 95/46/CE

12. Il GEPD non muove osservazioni sull'obiettivo generale della proposta e sostiene appieno l'iniziativa adottata, volta a migliorare le politiche ecocompatibili correlate ai RAEE.

13. Ciò nondimeno, la proposta, così come la direttiva, si concentra unicamente sui rischi ambientali legati allo smaltimento dei RAEE, senza tener conto di ulteriori rischi di diversa natura per i singoli individui e/o le organizzazioni che possono insorgere a seguito delle operazioni di smaltimento, reimpiego o riciclo dei RAEE, in particolare quelli legati alla possibilità di un'acquisizione, comunicazione o diffusione improprie dei dati personali contenuti nei RAEE.

14. È importante notare che la direttiva 95/46/CE ([8]) si applica a «qualsiasi operazione o insieme di operazioni […] applicate a dati personali», compresa la loro «cancellazione o distruzione» [articolo 2, lettera b)]. Lo smaltimento delle AEE può includere operazioni di trattamento dei dati. Per questo motivo esiste una sovrapposizione tra la proposta e la testé citata direttiva, per cui le norme sulla protezione dei dati sono applicabili alle attività interessate dalla proposta.

III.2. Smaltimento dei RAEE e misure di sicurezza

15. Il GEPD intende evidenziare i rischi elevati a carico dei singoli individui e/o delle organizzazioni nella loro funzione di «responsabili del trattamento dei dati» ([9]) nel caso in cui i RAEE, in particolar modo le apparecchiature informatiche e di telecomunicazione, contengano dati personali relativi agli utenti di tali dispositivi e/o a parti terze al momento dello smaltimento. L'accesso non autorizzato o la comunicazione di tali informazioni personali, a volte consistenti in particolari categorie di dati, che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati relativi alla salute e alla vita sessuale (i cosiddetti «dati sensibili») ([10]), sono infatti in grado di influire sulla vita privata e sulla dignità della persona a cui si riferiscono, nonché su altri interessi legittimi di tali singoli individui/organizzazioni (per esempio, quelli economici).

([8]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, pag. 31.

([9]) Per la definizione di «responsabile del trattamento» cfr. l'articolo 2, lettera d), della direttiva 95/46/CE.

([10]) Cfr. l'articolo 8 della direttiva 95/46/CE.

16. In generale, il GEPD ritiene necessario sottolineare l'importanza dell'adozione di misure di sicurezza appropriate in ogni fase (da quella iniziale a quella finale) del trattamento dei dati personali, come più volte affermato in altri pareri ([11]). Ciò si applica a maggior ragione nella delicata fase in cui il responsabile del trattamento dei dati intende smaltire i dispositivi contenenti dati personali.

17. Di fatto, il rispetto delle misure di sicurezza è spesso un prerequisito per garantire efficacemente il diritto alla protezione dei dati personali.

18. Sarebbe pertanto incoerente introdurre l'obbligo di mettere in atto misure di sicurezza (talvolta costose) nel corso delle normali operazioni di trattamento dei dati personali [come previsto dall'articolo 17 della direttiva 95/46/CE, ove applicabile ([12])] e poi semplicemente omettere di prendere in considerazione l'adozione di adeguate misure di sicurezza per quanto concerne lo smaltimento dei RAEE.

19. Parimenti non sarebbe coerente, da un lato, riconoscere importanza alla questione della sicurezza del trattamento dei dati al punto da dover introdurre l'obbligo di comunicazioni delle violazioni dei dati attraverso l'articolo 2 della direttiva 2009/136/CE ([13]) e, dall'altro lato, non fornire alcuna garanzia o protezione nel corso dello smaltimento dei RAEE nonché nel caso di loro reimpiego o riciclaggio.

20. Il GEPD si rammarica del fatto che la proposta non tenga conto dei potenziali effetti dannosi dello smaltimento dei RAEE sulla protezione dei dati personali contenuti nell'apparecchiatura «usata».

21. Questo aspetto non è stato nemmeno considerato nella valutazione dell'impatto effettuata dalla Commissione ([14]), sebbene l'esperienza abbia dimostrato che la mancata adozione di misure di sicurezza appropriate nel caso dello smaltimento dei RAEE possa pregiudicare la protezione dei dati personali ([15]). Vista la complessità delle questioni (per esempio, la grande quantità di metodi legittimi, tecnologie e parti interessate nel ciclo di smaltimento dei RAEE), il GEPD è del parere che sarebbe stato opportuno effettuare una «valutazione di impatto sulla tutela della vita privata e sulla protezione dei dati» in relazione ai processi correlati allo smaltimento dei RAEE.

22. Nondimeno, il GEPD raccomanda vivamente che vengano elaborate «migliori tecniche disponibili» per la tutela della vita privata, la protezione dei dati e la sicurezza in questo settore.

23. Inoltre, nel corso della consultazione pubblica che ha preceduto la rifusione della direttiva, alcune parti interessate, in particolare le società informatiche e di comunicazione elettronica, hanno talvolta sollevato questioni concernenti la sicurezza e la protezione dei dati personali ([16]).

24. Infine, è bene evidenziare che alcune autorità nazionali preposte alla protezione dei dati hanno pubblicato linee guida per ridurre al minimo i rischi derivanti dalla mancata adozione delle necessarie misure di sicurezza, nello specifico all'atto dello smaltimento di materiali soggetti all'applicazione della direttiva ([17]).

([11]) Cfr. il parere del Garante europeo della protezione dei dati sull'agenzia per la gestione operativa dei sistemi di tecnologia dell'informazione su larga scala (GU C 70 del 19.3.2010, pag. 13), punti 46 e 47; il parere sulla proposta di direttiva concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU C 128 del 6.6.2009, pag. 20), punti 27-31.

([12]) Cfr. l'articolo 3 della direttiva.

([13]) Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, GU L 337 del 18.12.2009, pag. 11.

([14]) Documento di lavoro dei servizi della Commissione che accompagna la proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) (rifusione), SEC(2008) 2933, 3.12.2008; cfr. anche Università delle Nazioni Unite, 2008 *Review of Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE)*, Commissione europea, Belgio, 2007, pag. 273 (http://ec.europa.eu/environment/waste/weee/pdf/final_rep_unu.pdf); *Data security is also an issue — removing personal data from a hard-drive.*

([15]) Cfr. per esempio l'articolo della BBC disponibile online *Children's files on eBay computer*, del 4 maggio 2007, che riporta l'episodio di un computer contenente dati personali concernenti l'affidamento e l'adozione di bambini venduto su eBay (http://news.bbc.co.uk/2/hi/uk_news/england/6627265.stm); cfr. anche l'articolo della BBC disponibile online *Bank customer data sold on eBay*, del 26 agosto 2008, nel quale si segnala che il disco rigido contenente dati personali relativi a un milione di clienti bancari era stato venduto su eBay (http://news.bbc.co.uk/2/hi/uk_news/7581540.stm).

([16]) Cfr. HP, *Stakeholder Consultation on the Review of Directive 2002/96/EC of the European Parliament and of the Council on Waste Electrical and Electronic Equipment (WEEE)*, pagg. 7-8; DELL (bozza di osservazioni), *WEEE Review Policy Options of the stakeholder consultation on the review of directive 2002/96/EC of the European Parliament and of the Council on Waste Electrical And Electronic Equipment (WEEE)*, pag. 2, punti 1.1 e 4, punto 1.3 (3.6.2008); Posizione e proposta di Royal Philips Electronics, *Stakeholder consultation on the Revision of the WEEE Directive*, pag. 12 (5.6.2008) (http://circa.europa.eu/Public/irc/env/weee_2008_review/library). Cfr. anche WEEE Consultation Response, *Summary of responses and Government response to fourth consultation on implementation of Directives 2002/96/EC and 2003/108/EC on Waste Electrical and Electronic Equipment*, dicembre 2006, pag. 30: «Data protection and security. Some waste management companies would like there to be some guidance issued on data protection and security, particularly in light of the fact they will be handling sensitive data» (http://www.berr.gov.uk/files/file35961.pdf).

([17]) Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen, *Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen*, 16. Mai 2007 (http://www.datenschutz-bremen.de/rtf/datenloeschung.rtf); Garante per la protezione dei dati personali, *Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali*, 13 ottobre 2008 (http://www.garanteprivacy.it/garante/doc.jsp?ID=1571514), menzionato anche nella *Twelfth Annual Report of the Article 29 Working Party on Data Protection*, 16 giugno 2009, pag. 57; cfr. anche Gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni, *Recommendation on Data Protection and E-Waste*, Sofia, 12-13.3.2009 (http://www.datenschutz-berlin.de/attachments/650/675.38.14.pdf?1264671551).

25. Il GEPD ribadisce che la direttiva 95/46/CE è applicabile nella fase di smaltimento dei RAEE contenenti dati personali. I responsabili del trattamento dei dati, in particolare quelli che utilizzano dispositivi informatici e di comunicazione, devono pertanto soddisfare gli obblighi di sicurezza al fine di evitare la comunicazione o la diffusione improprie di dati personali. A tal fine e per non essere ritenuti responsabili della violazione delle norme di sicurezza, i responsabili del trattamento dei dati del settore pubblico o privato devono adottare, con la collaborazione degli incaricati aziendali della protezione dei dati (ove presenti), politiche adeguate per lo smaltimento dei RAEE contenenti dati personali.

26. Nel caso in cui i responsabili del trattamento dei dati incaricati dello smaltimento di AEE non siano in possesso delle competenze e/o del *know-how* tecnico necessari per la cancellazione dei dati personali in questione, possono affidare tale compito a incaricati del trattamento qualificati (per esempio, centri di assistenza, fabbricanti e distributori di apparecchiature) in base a quanto stabilito dall'articolo 17, paragrafi 2, 3 e 4, della direttiva 95/46/CE. Tali incaricati del trattamento dovranno a loro volta certificare lo svolgimento delle operazioni in questione e/o effettuarle.

27. Alla luce di tali considerazioni, il GEPD giunge alla conclusione che la rifusione della direttiva dovrebbe aggiungere i principi di protezione dei dati alle disposizioni dedicate alla tutela dell'ambiente.

28. Il GEPD raccomanda pertanto al Consiglio e al Parlamento europeo di includere nell'attuale proposta una disposizione specifica che affermi l'applicabilità della direttiva allo smaltimento dei RAEE, fermo restando quanto disposto dalla direttiva 95/46/CE.

III.3. **Reimpiego o riciclaggio dei RAEE e misure di sicurezza**

29. Ove si trovino nella posizione di decidere in maniera autonoma in merito ai dati contenuti nelle AEE, i soggetti incaricati delle operazioni di smaltimento potrebbero essere considerati quali «responsabili del trattamento dei dati» ([18]). Essi devono pertanto adottare procedure interne al fine di evitare inutili operazioni di trattamento di qualsiasi dato personale contenuto nei RAEE, ossia operazioni diverse da quelle strettamente necessarie per verificare l'effettiva eliminazione dei dati in essi contenuti.

30. Inoltre, non devono consentire a soggetti non autorizzati di venire a conoscenza o di trattare i dati contenuti nei RAEE. In particolare, in caso di riciclaggio o reimpiego di supporti di memorizzazione, e quindi di una loro reimmissione in commercio, sussiste un rischio accresciuto di comunicazione o diffusione impropria di dati personali, nonché la necessità di impedire l'accesso non autorizzato a questo genere di dati.

31. Il GEPD pertanto raccomanda che il Consiglio e il Parlamento europeo includano nella proposta attuale una disposizione specifica che vieti l'immissione in commercio di dispositivi usati non precedentemente sottoposti a misure di sicurezza adeguate, in conformità con gli standard tecnici più avanzati (per esempio, sovrascrittura ripetuta con metodo «multi-pass»), per cancellare eventuali dati personali in essi contenuti.

III.4. **Sicurezza e tutela della vita privata garantite fin dalla fase di progettazione**

32. Il nuovo quadro giuridico sui rifiuti elettrici ed elettronici dovrebbe contenere non soltanto una disposizione specifica relativa al più ampio «principio della progettazione ecocompatibile» delle apparecchiature (cfr. l'articolo 4 della proposta in merito alla «Progettazione dei prodotti»), bensì anche, come è già stato precisato in altri pareri del GEPD ([19]), una disposizione riguardante il principio della «Tutela della vita privata fin dalla fase di progettazione» ([20]) o, più esattamente in questo contesto, della «Sicurezza sin dalla progettazione» ([21]). Nei limiti del possibile, la tutela della vita privata e la protezione dei dati dovrebbero essere integrate «di norma» sin dalla fase della progettazione delle apparecchiature elettriche ed elettroniche, al fine di consentire agli utenti di cancellare, usando un mezzo semplice e gratuito, i dati personali che potrebbero essere contenuti nei dispositivi in caso di loro smaltimento ([22]).

([18]) «Il concetto di responsabile del trattamento è […] basato sui fatti, nel senso che è inteso a ripartire le responsabilità nel caso di influenza reale, e quindi basata su un'analisi *effettiva* piuttosto che formale»: cfr. Gruppo di lavoro articolo 29 per la protezione dei dati, WP 169, parere 1/2010 sui concetti di «responsabile del trattamento» e «incaricato del trattamento», adottato il 16 febbraio 2010.

([19]) Cfr., per esempio, *The EDPS and EU Research and Technological Development*, documento orientativo, 28 aprile 2008, pag. 2; parere del GEPD sui sistemi di trasporto intelligenti (GU C 47 del 25.2.2010, pag. 6); parere del GEPD per quanto riguarda la farmacovigilanza (GU C 229 del 23.9.2009, pag. 19).

([20]) A favore di un'ampia applicazione di tale principio, cfr. il Gruppo di lavoro articolo 29 sulla protezione dei dati — Gruppo di lavoro «Polizia e giustizia», *The Future of Privacy*. Contributo congiunto alla consultazione della Commissione europea sul quadro giuridico per il diritto fondamentale alla protezione dei dati personali, WP 168, adottato il 1º dicembre 2009, pagg. 3 e 12; cfr. anche la raccomandazione della Commissione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza, C(2009) 3200 definitivo, pag. 8.

([21]) Cfr. comunicazione della Commissione, Programma europeo di ricerca e innovazione in materia di sicurezza — Posizione iniziale della Commissione sulle principali constatazioni e raccomandazioni dell'ESRIF, COM(2009) 691 definitivo, pagg. 6 e 14.

([22]) Cfr. anche GEPD, *Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy*.

33. Questo approccio è chiaramente sostenuto dall'articolo 3, paragrafo 3, lettera c), della direttiva 1999/5/CE ([23]) riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione nonché dall'articolo 14, paragrafo 3, della direttiva 2002/58/CE ([24]).

34. Pertanto, i produttori dovrebbero «integrare» elementi di salvaguardia per la sicurezza e la tutela della vita privata tramite soluzioni tecnologiche ([25]). In questo contesto sarebbe bene promuovere e sostenere iniziative mirate a fornire consulenza ai soggetti interessati a cancellare eventuali dati personali contenuti nei RAEE prima del loro smaltimento (compresi i produttori affinché mettano a disposizione software gratuiti adatti allo scopo) ([26]).

IV. **CONCLUSIONI**

35. Alla luce di quanto precede, il GEPD raccomanda che le autorità preposte alla protezione dei dati, in particolare attraverso il Gruppo di lavoro articolo 29, e il GEPD stesso partecipino in stretta collaborazione a iniziative vertenti sullo smaltimento dei RAEE, mediante una consultazione in una fase sufficientemente precoce prima dell'elaborazione di misure pertinenti.

36. Considerando il contesto in cui i dati personali vengono sottoposti a trattamento, il GEPD raccomanda l'inserimento nella proposta di disposizioni specifiche che:

— affermino che la direttiva sui RAEE trova applicazione fermo restando il disposto della direttiva 95/46/CE,

— vietino l'immissione in commercio dei dispositivi usati che non siano stati precedentemente sottoposti a misure di sicurezza adeguate, in conformità con gli standard tecnici più avanzati, al fine di cancellare eventuali dati personali in essi contenuti,

— in merito al principio della «Tutela della vita privata fin dalla fase della progettazione» o della «Sicurezza sin dalla progettazione»: nei limiti del possibile, la tutela della vita privata e la protezione dei dati dovrebbero essere integrate «di norma» sin dalla fase della progettazione delle apparecchiature elettriche ed elettroniche, al fine di consentire agli utenti di cancellare, usando modalità semplici e gratuitamente, i dati personali che potrebbero essere contenuti in dispositivi in caso di smaltimento.

37. Pertanto, il GEPD raccomanda vivamente che, in conformità con la direttiva 95/46/CE, la proposta venga così modificata:

— considerando 11: «Inoltre, la presente direttiva dovrebbe applicarsi fatta salva la normativa in materia di protezione dei dati, in particolare la direttiva 95/46/CE. Poiché per apparecchiature elettriche ed elettroniche (AEE) si intende un'ampia gamma di prodotti che comprende una disparata serie di supporti in grado di contenere dati personali — quali le apparecchiature informatiche e di telecomunicazione (per esempio, personal computer, laptop, terminali per i servizi di comunicazione elettronica) — le operazioni di smaltimento collegate a tali apparecchiature, in particolare il reimpiego e il riciclaggio, possono presentare rischi di accesso non autorizzato ai dati personali contenuti nei RAEE. Pertanto, nei limiti del possibile, sarebbe opportuno includere di norma elementi di salvaguardia per la tutela della vita privata e la protezione dei dati nella progettazione di apparecchiature elettriche ed elettroniche capaci di contenere dati personali per consentire agli utenti di cancellare, agevolmente e senza costi aggiuntivi, eventuali informazioni di questo genere al momento dello smaltimento»,

— articolo 2, paragrafo 3: «La presente direttiva si applica fatta salva la normativa in materia di protezione dei dati, in particolare la direttiva 95/46/CE.»

38. In aggiunta, il GEPD ritiene opportuno che si considerino le seguenti modifiche:

— articolo 4, paragrafo 2: «Gli Stati membri incoraggiano misure volte a favorire la progettazione e la produzione di apparecchiature elettriche ed elettroniche che agevolino la cancellazione di eventuali dati personali contenuti nelle AEE al momento del loro smaltimento»,

— articolo 8, paragrafo 7: «Gli Stati membri assicurano che ogni RAEE raccolto contenente dati personali che sia sottoposto a trattamento ai fini del riciclaggio o del reimpiego non sia reimmesso in commercio a meno che tali dati non siano stati cancellati utilizzando le migliori tecniche disponibili»,

([23]) Articolo 3, paragrafo 3, della direttiva 1999/5/CE del Parlamento europeo e del Consiglio, del 9 marzo 1999, riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità (GU L 91 del 7.4.1999, pag. 10): «[…] la Commissione può stabilire che gli apparecchi all'interno di determinate categorie o determinati tipi di apparecchi siano costruiti in modo da […] contenere elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata dell'utente o dell'abbonato».

([24]) «All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni». Cfr. anche il considerando 46 della medesima direttiva, menzionato alla nota 13.

([25]) A sostegno di questa prospettiva politica, cfr. anche V. Reding, discorso programmatico in occasione della Giornata della protezione dei dati, 28 gennaio 2010, Parlamento europeo, Bruxelles, SPEECH/10/16: «Le imprese devono sfruttare il proprio potenziale innovativo per migliorare la tutela della vita privata e la protezione dei dati personali fin dall'inizio del ciclo di produzione. Il principio della “tutela della vita privata fin dalla fase di progettazione” è un principio che risponde agli interessi dei cittadini e delle imprese. La tutela della vita privata fin dalla fase di progettazione comporterà un aumento della protezione dei singoli individui, nonché un incremento della fiducia nei nuovi prodotti e servizi, che a sua volta avrà un impatto positivo per l'economia. Ho potuto vedere di persona alcuni esempi incoraggianti, ma c'è ancora molto da fare in tal senso».

([26]) Cfr., per esempio, Royal Canadian Mounted Police, *B2-002 — IT Media Overwrite and Secure Erase Products* (05/2009), in http://www.rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/index-eng.htm

— articolo 14, paragrafo 6: «Gli Stati membri possono esigere che gli utenti delle AEE contenenti dati personali siano informati da produttori e/o distributori, per esempio nelle istruzioni d'uso o presso i punti vendita, in merito alla necessità di cancellare dati personali che potrebbero essere contenuti nelle AEE prima del loro smaltimento».

Fatto a Bruxelles, il 14 aprile 2010.

Peter HUSTINX

Garante europeo della protezione dei dati

Consiglio Nazionale del Notariato

Regole tecniche in materia di Antiriciclaggio[1] (D.Lgs. 25 maggio 2017, n. 90)

CAPO I

Ambito di applicazione:

REGOLA TECNICA N. 1

Non rientrano tra le operazioni di cui all’art. 3, comma 4, lettera c) del D.Lgs. 231 del 2007 novellato tutti i negozi di natura non patrimoniale.

Alla luce di ciò, fermo restando l’approccio *risk based* e l’accertamento della concreta natura non patrimoniale dell’operazione, è possibile enucleare un elenco, indicativo e non esaustivo, riferito all’attività notarile di prestazioni professionali escluse dal novero di quelle che fanno sorgere gli obblighi di adeguata verifica:

- gli atti notori;
- gli atti *mortis causa*;
- la pubblicazione di testamento;
- il passaggio nel fascicolo degli atti tra vivi del testamento pubblico;
- la costituzione di fondo patrimoniale senza trasferimento di beni;
- le convenzioni matrimoniali, in quanto atti meramente programmatici;
- le rinunce meramente abdicative;
- il verbale di apertura di una cassetta di sicurezza;
- gli inventari in generale;
- la levata del protesto (in quanto atto di accertamento che non implica alcuna movimentazione di denaro), restando invece soggetto agli obblighi antiriciclaggio il servizio di “cassa cambiali”, salvo la possibilità di ricevere pagamenti superiori alle soglie limite di utilizzo del denaro contante, come precisato nella nota MEF dell’8 aprile 2009, prot. 28107.

Per le procure ed i mandati, è da ritenere che esse diano luogo al sorgere degli obblighi di adeguata verifica se generali, ovvero se contengono un’espressa autorizzazione a contrarre con se stessi, se sono irrevocabili o a termine, ovvero se sono conferite per il compimento di un atto giuridico avente ad oggetto mezzi di pagamento, beni o utilità di valore pari o superiore a 15.000 euro ovvero di valore non determinato o determinabile.

[1] Le presenti Regole tecniche sono state adottate con Delibere del CNN nn. 3-40/27 luglio 2017 e 2-4627 ottobre 2017, su Parere del Comitato di Sicurezza Finanziaria del 18 settembre 2018.

Capo II

Disciplina transitoria - Artt. 11, comma 2, e art. 23, comma 2, del D.Lgs. n. 90/2017:

REGOLA TECNICA N. 2

Le linee guida in materia di adeguata verifica della clientela, approvate dal Consiglio Nazionale del Notariato nella seduta del 4 aprile 2014, trovano applicazione per le parti non in contrasto con il D. Lgs. 25 maggio 2017, n. 90 e con le regole tecniche che seguono; precisamente sono vigenti, quali regole tecniche: relativamente alla Parte II, le linee guida dettate nella sezione I, nella sezione II, nella sezione III e nella sezione IV, con la precisazione che i riferimenti alle modalità di registrazione e conservazione dei dati e delle informazioni non sono più attuali in quanto modificati e semplificati dai novellati artt. 32 e seguenti del D. Lgs. 231/2007, ai quali, quindi, unitamente alle regole tecniche che seguono, va fatto riferimento. Per quanto riguarda la sezione V relativa agli obblighi derivanti dalle norme di contrasto al finanziamento del terrorismo restano vigenti le relative linee guida sul tema, con la precisazione che l'art. 7 del D.Lgs. n. 109/2017 è stato integrato - relativamente ai soggetti nei cui confronti devono essere applicate le misure di congelamento dei fondi e delle risorse economiche - dalle decisioni degli organismi internazionali e dell'Unione europea di cui all'articolo 4-ter e dai decreti di cui gli articoli 4 e 4-bis e con l'ulteriore precisazione - limitatamente alle misure aventi ad oggetto risorse economiche - che la comunicazione di cui al citato art. 7 va effettuata oltre che all'UIF anche al Nucleo speciale di polizia valutaria della Guardia di Finanza. Anche per la sezione V, il riferimento all'archivio informatico ed al registro della clientela istituito presso il singolo professionista va sostituito con "fascicolo del cliente". In ordine alla Parte III restano vigenti le linee guida dettate nella sezione I, nella sezione IV, da integrare, per le parti che interessano, dalle regole tecniche che seguono e le linee guida in tema di deroga all'obbligo di astensione contenute nella sezione V.

In allegato, la tabella di concordanza tra la normativa in vigore e quella previgente.

CAPO III

Procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo cui i professionisti sono esposti nell'esercizio della propria attività:

REGOLA TECNICA N. 3

In tema di adeguata verifica semplificata, tenuto conto:
- che il notaio potrà applicare misure semplificate di adeguata verifica della clientela nelle ipotesi in cui, alla stregua di un processo valutativo ricostruibile e dimostrabile, emerga in concreto un basso rischio di riciclaggio e di finanziamento del terrorismo, in quanto

l'estensione dell'adeguata verifica va commisurata al rischio in concreto rilevato, sulla base degli indici di cui all'articolo 23, commi 1 e 2, del D.Lgs. n. 90/2017;
- che in tali ipotesi, quali indici di basso rischio relativi a tipologie di clienti, possono individuarsi, a titolo esemplificativo, le seguenti tipologie di soggetti:
1) società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva;
2) pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea;
3) clienti che sono residenti in aree geografiche a basso rischio, ai sensi della lettera c) dell'art. 23 del decreto stesso;
i soggetti sottoposti a vigilanza ai sensi del D.Lgs. 1° settembre 1993 n. 385, del D.Lgs. 24 febbraio 1998, n. 58, e del D.Lgs. 7 settembre 2005 n. 209 si considerano a basso rischio di riciclaggio.
Pertanto è possibile, qualora ricorrano in concreto i presupposti, applicare misure semplificate di adeguata verifica della clientela che consistono nella identificazione del rappresentante del soggetto, inclusa la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente. In tal caso, l'obbligo di identificazione del titolare effettivo è da ritenersi assolto con l'acquisizione dei dati identificativi forniti dal cliente, con le modalità e nei termini di cui alla regola tecnica n. 5.
Gli obblighi di adeguata verifica sono attenuati ogniqualvolta i soggetti summenzionati intervengano in un atto per porre in essere un'operazione che la legge riserva espressamente ad essi in via esclusiva nonché con riferimento a tutti gli atti consequenziali o collegati a tali operazioni. A titolo di mera esemplificazione, è possibile far riferimento a contratti di mutuo, finanziamenti, aperture di credito, ivi compresi i patti aggiuntivi e modificativi degli stessi, gli atti di quietanza totale e parziale, di ristrutturazione e rinegoziazione, di erogazione, di surrogazione, di accollo, di delegazione e relativi atti connessi od accessori, ad atti e contratti che comportino la costituzione, la conferma, l'estensione, la rinnovazione, il frazionamento, la postergazione, la surroga, la riduzione, la cancellazione o lo svincolo di ipoteche, pegni o privilegi, fidejussioni e altre garanzie stabilite a favore dell'istituto, ad atti e contratti di cessione, a qualsiasi titolo, dei contratti di cui sopra e/o dei crediti nascenti dagli stessi, ai leasing mobiliari ed immobiliari.
Gli obblighi semplificati di adeguata verifica della clientela non si applicano qualora si abbia motivo di ritenere che l'identificazione effettuata non sia attendibile e qualora vi sia sospetto di riciclaggio o di finanziamento del terrorismo. I soggetti obbligati potranno dunque applicare misure semplificate di adeguata verifica solo qualora dalla valutazione emerga in concreto un basso rischio di riciclaggio.

CAPO IV

Adeguata verifica della clientela:

REGOLA TECNICA N. 4

Sono considerate idonee misure semplificate di adeguata verifica della clientela l'acquisizione delle informazioni sullo scopo e sulla natura della prestazione effettuata in contestualità della stipula, mediante la richiesta delle medesime, fermo restando l'obbligo della loro valutazione da parte del notaio. Allo scopo di definire l'idoneità delle misure semplificate di adeguata verifica della clientela nell'ambito dell'attività notarile, si precisa che lo scopo e la natura della prestazione professionale dei notai coincidono, per la quasi totalità dei casi, con il negozio giuridico oggetto dell'incarico, e che, a differenza delle operazioni finanziarie, negli atti notarili, scopo e natura delle prestazioni risultano manifesti nell'atto stesso, pertanto, salva diversa valutazione da parte del notaio, non è necessario formalizzare in autonomo documento l'acquisizione di tali informazioni dal cliente. Occorre comunque considerare le ipotesi di più atti, anche della stessa specie, che possono risultare collegati e rispetto alle quali va fatta salva la valutazione del complesso di operazioni compiute.

REGOLA TECNICA N. 5

Ai fini dell'identificazione del titolare effettivo, rileva il disposto di cui all'articolo 19 comma 1 lettera a) ai sensi del quale il cliente, all'atto dell'identificazione, fornisce "le informazioni necessarie a consentire l'identificazione del titolare effettivo".
La verifica dell'identità del titolare effettivo, necessaria qualora sussistano dubbi, incertezze o incongruenze in relazione ai dati acquisiti in sede di identificazione, può essere effettuata, ai sensi dell'articolo 19, comma 1, lettera b) anche attraverso il riscontro di tali dati con quelli riportati da fonti attendibili e indipendenti. Con riferimento alla titolarità effettiva di imprese dotate di personalità giuridica, tenute all'iscrizione nel registro delle imprese, il riscontro dei dati acquisiti in sede di identificazione può avvenire anche attraverso l'accesso alla sezione del registro delle imprese, ad hoc istituita, ai sensi dell'articolo 21, d.lgs. n. 231/07. Resta fermo quanto stabilito dal comma 7 del medesimo articolo 20 in ordine alla circostanza che la consultazione dei registri di cui al presente articolo non esonera i soggetti obbligati dal valutare il rischio di riciclaggio e finanziamento del terrorismo cui sono esposti nell'esercizio della loro attività e dall'adottare misure adeguate al rischio medesimo.
Fermo quanto sopra, e fermo restando che ai sensi dell'art. 19 del medesimo decreto, non si è tenuti all'acquisizione del documento di identità del titolare effettivo, qualora il titolare effettivo sia individuato attraverso la consultazione di pubblici registri, salva la valutazione del rischio e la conseguente applicazione di misure ad esso proporzionate, l'identificazione può essere ritenuta correttamente eseguita mediante la sola acquisizione dei dati e delle informazioni risultanti dai pubblici registri stessi, confermati nella loro validità dal cliente. Ai fini dell'individuazione del titolare effettivo, nelle ipotesi in cui sia possibile la consultazione di un pubblico registro, tale consultazione è da ritenersi idonea ai fini dell'espletamento

dell'obbligo di identificazione dello stesso titolare effettivo, salvo che ci si trovi in presenza di elementi oggettivi che mettano in dubbio o rendano palesemente incerti o incongrui i dati e le informazioni pubblicate. Detti dati e informazioni sono, infatti, da ritenere affidabili a fronte dell'obbligo giuridico a carico dei responsabili delle imprese, persone giuridiche e trust, di comunicare notizie vere, aggiornate e complete, ferma restando la possibilità di acquisire, in funzione del rischio, ulteriori informazioni.
Ai sensi dell'articolo 18, comma 1, lettera b, l'identificazione del titolare effettivo deve essere attuata nel contesto dell'adozione di regole comportamentali proporzionate al rischio.
L'obbligo di identificazione del titolare effettivo può ritenersi assolto attraverso l'acquisizione delle informazioni fornite dal cliente (direttamente o tramite conferma, ove già acquisite o in possesso del notaio nel contesto del rapporto con il cliente) in ordine al nome, cognome, luogo e data di nascita del titolare effettivo; laddove, in relazione ai dati forniti dal cliente, sussistano dubbi, incertezze o incongruenze il notaio provvederà a riscontrare la veridicità dei dati forniti ai sensi dell'art. 19 lett.b) del D.Lgs. 231/2007.

REGOLA TECNICA N. 6

Fermo restando quanto previsto dall'articolo 20 d.lgs. n. 231/07 e successive modificazioni per l'individuazione del titolare effettivo di clienti diversi dalle persone fisiche, nelle società di persone e consorzi e negli enti privati non riconosciuti, può assumere rilievo, ai fini dell'individuazione del titolare effettivo, la figura della persona fisica che agisce, quale tramite di essi, in qualità di legale rappresentante. Nell'individuazione del titolare effettivo delle società di persone e consorzi, è consentita l'utilizzazione dei dati dei soci, risultanti dal Registro delle Imprese, salvo che sussistano dubbi, incertezze o incongruenze sull'identità dello stesso e salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni.
Nell'individuazione del titolare effettivo degli enti privati non riconosciuti, in assenza di indici che rivelino l'esistenza di associati che ne detengano di fatto il controllo, ovvero di beneficiari determinati, si farà riferimento ai soggetti titolari di funzioni di direzione e/o amministrazione.

REGOLA TECNICA N. 7

Nelle ipotesi in cui ricorra un basso rischio di riciclaggio e di finanziamento del terrorismo, ed esista, ai sensi dell'ordinamento vigente, l'obbligo per il notaio di ricevere l'atto ed egli sia certo, ai sensi della legge 16 febbraio 1913, n. 89 dell'identità personale del cliente o dell'esecutore, la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo, fermo l'obbligo di acquisizione dei dati identificativi, può essere posticipata ad un momento successivo al conferimento dell'incarico per lo svolgimento della prestazione professionale, secondo quanto prescritto dall'articolo 18, comma 3, d.lgs. n. 231/07. In dette ipotesi, l'indisponibilità di un documento di riconoscimento in corso di validità costituisce presupposto per l'effettuazione, da parte del notaio, dell'aggiornamento dei dati e delle

informazioni necessarie all'adeguata verifica della clientela, senza rappresentare, di per sé elemento idoneo e sufficiente a fondare un sospetto meritevole di segnalazione, in assenza di concomitanti ulteriori evidenze relative al profilo soggettivo del cliente o a quello oggettivo della prestazione. In caso di prestazioni professionali non occasionali, il notaio provvederà ad aggiornare i documenti di identità in base al rischio: ogni 2 anni se a basso rischio, ogni anno se a rischio ordinario, con frequenza inferiore e comunque calibrata al rischio, per le ipotesi di elevato rischio di riciclaggio e di finanziamento del terrorismo.

Ai sensi dell'articolo 19, comma 1, lettera a) l'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, per i clienti i cui dati identificativi risultino da atti pubblici o da scritture private autenticate.

Nel caso in cui sia materialmente impossibile, per il notaio, effettuare l'adeguata verifica e fuori dalle ipotesi in cui sussista l'obbligo giuridico di ricevere l'atto, egli deve astenersi dall'esecuzione della prestazione e valutare se sussistano gli estremi per l'effettuazione di una segnalazione di operazioni sospette alla UIF, senza che possa ravvisarsi alcun automatismo tra astensione e segnalazione.

Ai sensi del combinato disposto dell'art. 18, comma 1, lett. a), e dell'art. 19, comma1, lettera a) n. 1 del D.Lgs. n. 231/2007 gli atti notarili da cui risultano i dati identificativi dei soggetti persone fisiche o non fisiche sono sempre considerati una fonte affidabile e indipendente ai fini dell'espletamento degli obblighi di adeguata verifica e ciò anche nel caso di intervento in atto di un esecutore dotato di procura notarile.

Ai sensi degli articoli 18, comma 1, lettera a) e 19, comma 1, lettera a) n. 1, il solo obbligo di identificazione del cliente può ritenersi assolto, senza la presenza fisica del medesimo, per i clienti i cui dati identificativi risultino, tra gli altri, da atti pubblici o scritture private autenticate e che, ai sensi del citato articolo 18, comma 1, lettera a), l'identificazione dell'esecutore non si esaurisce nel riscontro dei rispettivi dati identificativi ma abbraccia la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome del cliente.

REGOLA TECNICA N. 8

Il termine ultimo per la conclusione delle operazioni di adeguata verifica coincide, nel caso di atto notarile, con la stipula del medesimo, che costituisce il momento ultimo per l'esecuzione degli adempimenti prescritti in funzione di adeguata verifica della clientela, fermo restando che il complesso dei presidi antiriciclaggio si attiva al momento del conferimento dell'incarico per lo svolgimento della prestazione professionale, secondo il combinato disposto delle definizioni di cui all'articolo 1, comma 2, lettere h) e gg) del D.Lgs. n. 231/2007, come modificato dal D.Lgs. n. 90/2017. L'incarico per la stipula non sempre viene conferito da tutte le parti dell'atto, congiuntamente e nello stesso momento, al notaio, che pertanto potrà effettuare gli adempimenti di adeguata verifica della clientela anche in momenti diversi, purché si concludano alla stipula, in quanto è in quel momento che lo stesso notaio può concludere la valutazione della prestazione professionale per cui l'incarico è stato conferito.

Ai sensi dell'art. 32, comma 2, lettera b), è comunque considerata tempestiva l'acquisizione dei dati e delle informazioni relativi all'adeguata verifica del cliente conclusa entro trenta giorni dall'instaurazione del rapporto continuativo o dal conferimento dell'incarico per lo svolgimento della prestazione professionale, dall'esecuzione dell'operazione o della prestazione professionale, dalla variazione e dalla chiusura del rapporto continuativo o della prestazione professionale.

CAPO V

Conservazione:

REGOLA TECNICA N. 9

La conservazione, può essere sia cartacea che informatica. Il fascicolo cartaceo del cliente può rimandare ad alcuni documenti conservati elettronicamente come, a titolo esemplificativo, visure tratte dai pubblici registri conservate in formato statico e non modificabile così come fornite dal registro pubblico consultato, nel sistema informatico dello studio. Non vi è alcun limite, dunque, alla possibilità di avvalersi di modalità di conservazione dei documenti, dei dati e delle informazioni informatici piuttosto che cartacei, purché i soggetti obbligati adottino sistemi di conservazione idonei a garantire il rispetto dei principi di cui agli articoli 31 e 32 d.lgs. n. 231/07, delle norme dettate dal codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità di cui al citato decreto.

Le modalità di conservazione, in concreto, devono essere adottate in modo da prevenire qualsiasi perdita di dati e di informazioni ed essere idonee a garantire la ricostruzione dell'operatività o attività del cliente ai sensi di quanto disposto all'articolo 32, comma 2, del novellato D.Lgs. n. 231/2007.

REGOLA TECNICA N. 10

I sistemi di protezione contro la perdita dei dati e delle informazioni, quelli di autenticazione ed autorizzazione adottati per l'accesso al sistema informatico dello studio ed al relativo archivio cartaceo costituiscono idonea modalità di conservazione ai sensi dell'art. 32 del D.Lgs. n. 231/2007, come modificato dal D.Lgs. n. 90/2017. L'integrità dei dati e delle informazioni e la non alterabilità dei medesimi successivamente alla loro acquisizione si considera garantita qualora gli stessi si ricavino da un documento informatico conservato in formato statico e non modificabile o siano desumibili da un documento analogico correttamente conservato ai sensi della Legge notarile o ai sensi del D.P.R. n. 445/2000.

CONSIGLIO NAZIONALE DEL NOTARIATO

LA NOVELLA ANTIRICICLAGGIO - D.Lgs. 25.05.2017 n. 90

La Novella alla luce delle Regole Tecniche approvate dal CNN e del relativo parere del Comitato di Sicurezza Finanziaria

(Sara Carioni - Vincenzo Gunnella)

Il decreto legislativo 25 maggio 2017 n. 90[1], di recepimento della Quarta Direttiva Comunitaria (Direttiva UE 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo) sostituisce integralmente il D.Lgs. 231/2007.

Differentemente dal passato, in questa occasione l'intervento di recepimento della cd. IV Direttiva[2] è stato attuato lasciando in essere il D.Lgs. 231/2007, come contenitore formale, nel cui testo sono stati svolti gli interventi modificativi, e abrogando i relativi Allegati Tecnici, che in passato erano stati in alcuni casi di estrema utilità per l'operatore giuridico: si pensi ad esempio all'art. 2, comma 1, lettera a), punto 2, dell'Allegato Tecnico,- il quale dettava criteri residuali per l'identificazione del titolare effettivo, individuandolo nella persona fisica o nelle persone fisiche che esercitassero in altro modo il controllo sulla direzione di un'entità giuridica.[3]

L'impianto normativo è stato mantenuto unitario, sia con riguardo agli obblighi antiriciclaggio che con riferimento alle relative sanzioni, con ciò non recependo la tanto ripetuta richiesta di opportuni distinguo tra le due categorie di soggetti destinatari degli obblighi (operatori del settore finanziario e professionisti), richiesta più volte avanzata dai professionisti in sede di recepimento della normativa comunitaria.

Pertanto anche l'attuale testo normativo risente di quel "peccato originale" più volte lamentato dai commentatori della normativa antiriciclaggio e tradisce ancora oggi l'origine della norma come destinata in prima battuta, agli operatori del settore finanziario e poi adattata al mondo delle professioni.

Vi è peraltro da osservare che il decreto delegato 25 maggio 2017 n. 90 ha avuto il merito di introdurre un parziale rimedio sul punto, che in parte dà la possibilità di meglio calibrare gli obblighi antiriciclaggio alle specificità dei singoli destinatari. Si è deciso infatti di delegare alle autorità di vigilanza (per i soggetti di area bancaria e finanziaria) e agli organismi di autoregolamentazione (per i professionisti), il compito di integrare la norma primaria e

[1] Pubblicato sulla Gazzetta Ufficiale n. 140 del 19 giugno 2017.

[2] Si ricordi la recentissima emanazione della cd. Quinta Direttiva comunitaria 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018, pubblicata sulla Gazzetta Ufficiale UE del 19 giugno 2018, la quale dovrà essere recepita dagli ordinamenti nazionali entro il 10 gennaio 2020 e che introdurrà ulteriori significative novità in materia di identificazione del titolare effettivo e di accesso pubblico alle informazioni sulla titolarità effettiva nei trust e istituti affini, come anticipato dalla nota comparsa, a firma di Maria Concetta Cignarella, su CNN Notizie del 27 giugno 2018.

3 Vedasi a commento il "Quesito Antiriciclaggio n. 11-2017/B. Antiriciclaggio – identificazione titolare effettivo – fattispecie", a cura di Maria Concetta Cignarella, pubblicato su CNN Notizie del 4 dicembre 2017.

adeguarla alle specificità dei destinatari degli obblighi, mediante l'elaborazione delle cd. "**Regole Tecniche**".

Le Regole Tecniche e/o le indicazioni vincolanti, previste dagli articoli 11 comma 2 e 16 comma 2 del D.Lgs. 231/2017, hanno il compito di disciplinare, con maggior grado di dettaglio e più pregnante riferimento ai soggetti specifici per cui vengono emanate, procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo, di controlli interni, di adeguata verifica, anche semplificata della clientela e di conservazione; parimenti vengono individuati i requisiti dimensionali e organizzativi in base ai quali i soggetti obbligati adottano specifici presidi, controlli e procedure per la valutazione e gestione del rischio di riciclaggio e di finanziamento del terrorismo.

Nel caso dei notai, la normativa regolamentare (cd. "Regole Tecniche") è stata approvata dal CNN con le Delibere nn. 3-40/27 luglio 2017 e 2-46/27 ottobre 2017, su Parere del Comitato di Sicurezza Finanziaria.

Il prescritto parere del Comitato di Sicurezza Finanziaria è datato 18 settembre 2018 ed è stato trasmesso al CNN in data 1^ ottobre 2018.

Tali Regole tecniche vanno a comporre il quadro attuale della normativa di riferimento in materia di obblighi antiriciclaggio, che potremmo dire articolato sulle seguenti fonti:

- **a)** Direttiva Comunitaria, relativi Considerando e Principi Generali (di immediata portata precettiva);
- **b)** Legge Delega e Decreto Delegato;
- **c)** Circolari Ministeriali;
- **d)** Regole Tecniche ed indicazioni vincolanti del CNN;
- **e)** Studi del CNN
- **f)** Linee Guida e Direttive Interne adottate da ciascun professionista.

Dal quadro or ora delineato e dall'esame della normativa di riferimento, emerge un sistema di fonti stratificato, che richiede un notevole sforzo interpretativo all'operatore oltre che la necessità da parte di quest'ultimo di completare la norma di rango superiore con le proprie Linee Guida e i protocolli interni di studio.

A livello applicativo, quindi, si capisce come, oggi più di prima, la corretta applicazione dei presidi antiriciclaggio non possa prescindere da una adeguata valutazione delle dimensioni, della tipologia di clientela, dell'area geografica di operatività del professionista.

L'adozione di Linee Guida e protocolli interni è quindi il primo passo da compiere, e ciò, unitamente al corretto assolvimento dell'obbligo di formazione del personale, riveste notevole importanza anche per la conseguente valutazione dell'elemento soggettivo in caso di infrazione della normativa (v. art. 56 comma 2[4]).

La valutazione da compiersi è di aver dotato (tramite Protocolli e Linee Guida interni, nonché con adeguata formazione del personale) lo studio di presidi che lo rendano un "avamposto antiriciclaggio".

Scopo del presente studio è quello di delineare l'odierno perimetro degli obblighi di adeguata verifica, riempiendoli di contenuto alla luce delle Regole Tecniche approvate dal CNN, su

[4] L'art. 56 comma 2, dedicato alle sanzioni amministrative per inosservanza degli obblighi di adeguata verifica e di astensione, prevede, tra l'altro, che la gravità della violazione sia determinata anche tenuto conto "dell'intensità e del grado dell'elemento soggettivo, anche avuto riguardo all'ascrivibilità, in tutto o in parte, della violazione alla carenza, incompletezza o alla non adeguata diffusione di prassi operative e procedure di controllo interno".

parere del Comitato di Sicurezza Finanziaria, e calibrandoli differentemente a seconda che ricorra un'ipotesi di adeguata verifica semplificata, ordinaria o rafforzata.

È proprio con riguardo agli obblighi di adeguata verifica della clientela che la normativa, salvo alcune conferme, introduce significative novità.

Le conferme

A. I PRINCIPI GENERALI (art. 2)

Sotto il profilo dei principi generali, la normativa non presenta innovazioni.
Vengono pertanto confermati, all'art. 2, i principi generali ispiratori della materia, che hanno, come del resto in passato, immediata portata precettiva:

a) Proporzionalità

Le misure da adottare per adempiere agli obblighi devono essere proporzionate sia in rapporto all'attività, dimensioni e complessità dell'obbligato che in rapporto al rischio in relazione al tipo di cliente, al rapporto continuativo, alla prestazione professionale, al prodotto o alla transazione (art. 8 della Direttiva).

(Art. 16, comma 1) I soggetti obbligati adottano i presidi e attuano i controlli e le procedure, adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi di riciclaggio.

Già dal principio di proporzionalità emerge con tutta evidenza la necessità di calibrare le proprie misure antiriciclaggio a elementi non solo riconducibili al tipo di cliente (come del resto è ovvio), ma anche riconducibili al tipo di professionista obbligato (in termini anzitutto dimensionali).

A ben vedere, allora, il principio di proporzionalità potrebbe essere considerato il primo corollario dell'approccio basato sul rischio, in un rapporto tra i due elementi tale per cui l'uno può considerarsi logica conseguenza dell'altro.

Si potrebbe da ciò ricavare il primo assunto per cui una adeguata *compliance* presuppone, anzitutto, un'autovalutazione del proprio studio in termini di presidio antiriciclaggio (prima ancora della valutazione delle casistiche ricorrenti), quali un'adeguata formazione del personale, l'adozione di linee guida interne o, ancora, la predisposizione e adozione di idonea modulistica.

b) Circoscrizione dell'attenzione alle circostanze conosciute in ragione delle funzioni esercitate

Il soggetto obbligato deve tener conto dei dati e delle informazioni acquisiti o posseduti nell'esercizio della propria attività istituzionale o professionale (art. 18 comma 1, lett. d).

c) Approccio basato sul rischio

Il rinvio è contenuto all'Art. 22 dei Considerando, all'art. 8 della Direttiva, nonché in numerosi articoli del D.Lvo: è il cd. "*risk based approach*", "che non rappresenta una scelta metodologica rimessa esclusivamente alla volontà dei soggetti obbligati, bensì lo strumento

ritenuto fondamentale per consentire, attraverso il processo di valutazione, l'adozione di procedure e strumenti in grado di riconoscere e mitigare il rischio stesso"[5].

Necessario corollario operativo dell'approccio basato sul rischio è, come sopra anticipato, la necessità di dare compiuta formalizzazione, con linee guida interne, all'operatività del professionista in merito alla valutazione del rischio, al fine di poter dimostrare, ad esempio, con riguardo alla valutazione del rischio, il procedimento in base al quale per un'operazione è stata optata un'adeguata verifica semplificata, ordinaria o rafforzata (dando un proprio giudizio alla classe di rischio rilevata – ad esempio rischio basso, medio o alto).

B. L' AMBITO DI APPLICAZIONE. (art. 3)

Per quanto attiene ai notai, l'ambito di applicazione della normativa, definito dall'art. 3, di fatto include tutta l'attività tipica con la sola eccezione degli atti (negoziali e non) di natura non patrimoniale, in quanto investe i notai degli obblighi antiriciclaggio quando "in nome o per conto dei propri clienti compiono qualsiasi operazione di natura finanziaria o immobiliare o quando assistono i propri clienti nella predisposizione o nella realizzazione di operazioni riguardanti:

1) il trasferimento a qualsiasi titolo di diritti reali su beni immobili o attività economiche;
2) la gestione di denaro, strumenti finanziari o altri beni;
3) l'apertura o la gestione di conti bancari, libretti di deposito e conti di titoli;
4) l'organizzazione degli apporti necessari alla costituzione, alla gestione o all'amministrazione della società;
5) la costituzione, la gestione o l'amministrazione di società, enti, trust o soggetti giuridici analoghi".

Il nuovo testo ricalca pedissequamente il precedente, sotto il profilo dell'ambito di applicazione, mentre perimetra in modo diverso l'obbligo di adeguata verifica della clientela, come si vedrà.

Una lettura coordinata del nuovo testo con le definizioni assunte dalla nuova normativa consente di ritenere **escluse** le prestazioni professionali relative ad **atti (negoziali e non) di natura non patrimoniale.**

Tale conclusione emerge in particolare dal raffronto tra la definizione di "**operazione**" nel previgente e nel nuovo testo.

Nuova definizione	Vecchia definizione
l'attività consistente nella movimentazione, nel trasferimento o nella trasmissione di mezzi di pagamento o nel compimento di atti negoziali a contenuto patrimoniale; costituisce operazione anche la stipulazione di un atto negoziale, a contenuto patrimoniale, rientrante nell'esercizio dell'attività professionale o commerciale	la trasmissione o la movimentazione di mezzi di pagamento; per i soggetti di cui all' articolo 12 , un'attività determinata o determinabile, finalizzata a un obiettivo di natura finanziaria patrimoniale modificativo della situazione giuridica esistente, da realizzare tramite una prestazione professionale.

[5] Così in Allegato n. 1 alla Circolare della Guardia di Finanza n. 210557 del 7 luglio 2017, ove si ribadisce la rilevanza del cd. "approccio basato sul rischio".

Si può quindi ritenere che non rientrino tra le operazioni di cui all'art. 3, comma 4, lettera c) del D.Lgs. 231 del 2007 novellato, tutti i meri atti giuridici e i negozi di natura non patrimoniale.

Pertanto dovrebbero rimanere esclusi gli atti negoziali a contenuto non patrimoniale, di norma gli atti compiuti su delega dell'autorità giudiziaria (almeno quelli privi di effetti patrimoniali), le certificazioni in genere, gli atti *mortis causa*.

Conclusione, questa, confermata dalla **Regola Tecnica n. 1**, rubricata "ambito di applicazione", di seguito riportata:

REGOLA TECNICA N. 1[6]

Non rientrano tra le operazioni di cui all'art. 3, comma 4, lettera c) del D.Lgs. 231 del 2007 novellato tutti i negozi di natura non patrimoniale.

Alla luce di ciò, fermo restando l'approccio *risk based* e l'accertamento della concreta natura non patrimoniale dell'operazione, è possibile enucleare un elenco, indicativo e non esaustivo, riferito all'attività notarile di prestazioni professionali escluse dal novero di quelle che fanno sorgere gli obblighi di adeguata verifica:

- gli atti notori;
- gli atti *mortis causa*;
- la pubblicazione di testamento;
- il passaggio nel fascicolo degli atti tra vivi del testamento pubblico;
- la costituzione di fondo patrimoniale senza trasferimento di beni;
- le convenzioni matrimoniali, in quanto atti meramente programmatici;
- le rinunce meramente abdicative;
- il verbale di apertura di una cassetta di sicurezza;
- gli inventari in generale;
- la levata del protesto (in quanto atto di accertamento che non implica alcuna movimentazione di denaro), restando invece soggetto agli obblighi antiriciclaggio il servizio di "cassa cambiali", salvo la possibilità di ricevere pagamenti superiori alle soglie limite di utilizzo del denaro contante, come precisato nella nota MEF dell'8 aprile 2009, prot. 28107.

Per le procure ed i mandati, è da ritenere che esse diano luogo al sorgere degli obblighi di adeguata verifica se generali, ovvero se contengono un'espressa autorizzazione a contrarre con se stessi, se sono irrevocabili o a termine, ovvero se sono conferite per il compimento di un atto giuridico avente ad oggetto mezzi di pagamento, beni o utilità di valore pari o superiore a 15.000 euro ovvero di valore non determinato o determinabile.

[6] Nota bene: il parere del CSF ricorda che circa l'enucleazione dell'elenco contenuto nella medesima regola e al fine di graduare l'estensione e la frequenza degli adempimenti di adeguata verifica alla luce del rischio in concreto rilevato, si ritiene opportuno rimettere all'organismo di autoregolamentazione la definizione di procedure e metodologie utili a classificare le attività notarili secondo l'approccio risk based, procedendo al vaglio in ordine alla sussumibilità delle prestazioni professionali "riferite all'attività notarile" nell'ambito di applicazione della normativa di prevenzione del riciclaggio e di finanziamento del terrorismo, tenuto conto della definizione di operazione e operazione occasionale declinata dall'articolo 1, comma 2, rispettivamente alle lettere t) e z), del medesimo decreto. Tale attività è in corso di esecuzione.

Le novità

A. IL PERIMETRO DEGLI OBBLIGHI DI ADEGUATA VERIFICA

Notiamo una diversa formulazione del **perimetro degli obblighi di adeguata verifica**, previsti dall'art. 17, in quanto rispetto al precedente testo, non si prevede più la necessità che la prestazione abbia per oggetto "mezzi di pagamento, beni od utilità di valore pari o superiore a 15.000 euro".
Salvo il caso di esecuzione di operazione occasionale, scompare, pertanto, il riferimento al limite dei 15.000 Euro, con conseguente estensione degli obblighi posti a carico del professionista.
Viene espressamente confermato (all'art. 17 comma 7) che non vi è obbligo di adeguata verifica con riferimento alle attività di mera redazione e trasmissione ovvero di sola trasmissione delle dichiarazioni derivanti da obblighi fiscali.

Ne ricaviamo pertanto, come prima istruzione operativa, che il preliminare accertamento da effettuare è la verifica del perimetro di applicazione degli obblighi di adeguata verifica antiriciclaggio.

A tal fine, di fronte all'interrogativo "quali sono gli atti compresi nell'AV e quali sono esclusi?", potremmo ritenere soggetti ad obbligo di adeguata verifica tutti gli atti a contenuto patrimoniale, senza limiti di importo.

Particolari categorie di atti
- <u>la redazione di moduli e denunce fiscali e la loro trasmissione (es. denunzie di successione):</u> è esclusa dall'obbligo di adeguata verifica (art. 17.7), tuttavia è opportuno verificare se la denuncia fiscale venga utilizzata in maniera strumentale ed abusiva per perseguire uno scopo illecito;
- <u>il ricevimento di una procura (speciale o generale):</u> impone, alla luce della sopra richiamata Regola Tecnica n.1, l'esecuzione degli obblighi di AV da parte del notaio che riceve la procura, che dovrà profilare sia il mandante che il procuratore e verificare lo scopo e la natura della prestazione, tenendo conto che il rilascio di una procura può essere strumentale a fini non dichiarati e non leciti;
- <u>l'atto nel quale intervenga un procuratore (esecutore nelle definizioni del 231):</u> oltre alla identificazione e profilatura del procuratore, occorre profilare il mandante e verificare la congruità dell'utilizzo dello strumento della procura; non occorre acquisire il documento di identità del mandante in quanto l'identificazione la si ricava dall'autentica della procura (art. 19.a.1);
- <u>atti di ultima volontà, accettazioni di eredità e legati, pubblicazione di testamenti:</u> sono normalmente esclusi da AV, salvo ipotesi di scuola, come confermato dalla sopra riportata Regola Tecnica n. 1;
- <u>apertura di cassette di sicurezza:</u> l'AV non va eseguita nei confronti dei soggetti defunti (intestatari della cassetta); occorre invece eseguire l'AV nei confronti dei cointestatari viventi, anche in rapporto all'eventuale contenuto della cassetta che viene inventariato; occorre infine prestare attenzione all'eventuale ipotesi di intestazione fittizia di cassetta di sicurezza a prestanome;

- <u>atti a contenuto non patrimoniale:</u> sono esclusi da AV, tutti gli atti a contenuto non patrimoniale come ad es. dichiarazioni di scienza, atti notori, consensi e autorizzazioni, ecc.;
- <u>rilascio di copie, certificati, estratti, ricorsi di volontaria giurisdizione, vidimazioni:</u> sono esclusi da AV; tuttavia nel caso di ricorsi di volontaria giurisdizione, occorre considerare che quando sono attività prodromiche al ricevimento di atti notarili, soggetti ad AV, è per questi ultimi che va eseguita l'AV, dovendosi ritenere già conferito l'incarico relativo.

Incidentalmente si ricorda che **se l'atto richiesto è un atto privato, non notarile**, gli obblighi di adeguata verifica e di segnalazione delle operazioni sospette sono identici; tuttavia, quando la prestazione richiesta è l'assistenza al perfezionamento di una **scrittura privata**, non si applicano le deroghe previste dagli art. 35.2 e 42.4 e pertanto:

- in presenza di elementi di sospetto, il soggetto obbligato non può compiere l'operazione fino al momento in cui non ha provveduto alla SOS;
- nel caso in cui il soggetto obbligato non riesca a completare l'adeguata verifica deve astenersi dal compiere l'operazione (mentre nel caso trattasi di atto notarile, vi sarà comunque l'obbligo di ricevere l'atto, salvo poi provvedere ad informare "immediatamente" l'UIF, posto che l'incompleta adeguata verifica della clientela, per effetto dell'art. 42 comma 4, determina automaticamente l'obbligo di SOS);
- nel caso in cui l'operazione coinvolga fiduciarie, società anonime, trust e simili, aventi sede in Paesi ad alto rischio, il soggetto obbligato deve astenersi.

B. L'ESECUTORE

Compare la figura dell'**esecutore**: trattasi del *"soggetto delegato ad operare in nome e per conto del cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del cliente"* (vedasi art. 1 comma 2 lettera p).
L'esecutore **è soggetto alle medesime verifiche del cliente**, a cui va aggiunta la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente (art.18).

C. L'IDENTIFICAZIONE DEL TITOLARE EFFETTIVO

I riferimenti normativi principali sono i seguenti:

Art.1 - titolare effettivo: la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza .... la prestazione professionale è resa o l'operazione è eseguita

Art.20, comma 1: **Il titolare effettivo di clienti diversi dalle persone fisiche** coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'ente ovvero il relativo controllo.

Sotto il vigore della precedente normativa era di fatto ammessa l'eventualità che non fosse identificabile alcun titolare effettivo (in mancanza di partecipazioni qualificate nella società, come indicate dall'Allegato Tecnico); oggi tale eventualità non è più contemplata: per i soggetti

non persone fisiche **è sempre quindi necessario pervenire all'individuazione del titolare effettivo**.
Il legislatore, da un lato, ha infatti espressamente riconosciuto il ruolo strategico che può avere il titolare effettivo (o "beneficial owner") come effettivo controllore di strutture societarie; dall'altro, ha preso atto delle difficoltà, riscontrate nel passato, in ordine all'esatta individuazione del titolare effettivo, generate dal previgente quadro normativo non sufficientemente esaustivo.

Cambiano i **criteri per l'identificazione del titolare effettivo**, prima contenuti all'art. 2 dell'allegato Tecnico e ora, almeno parzialmente, nell'art. 20 del D.Lgs.

Nuova disciplina (art. 20 d.lgs. 90/2017)	**Vecchia disciplina (art. 2 Allegato Tecnico)**
2. Nel caso in cui il cliente sia una **società di capitali**: a) costituisce indicazione di **proprietà diretta** la titolarità di una partecipazione superiore al 25 per cento del capitale del cliente, detenuta da una persona fisica; b) costituisce indicazione di **proprietà indiretta** la titolarità di una percentuale di partecipazioni superiore al 25 per cento del capitale del cliente, posseduto per il tramite di società controllate, società fiduciarie o per interposta persona. 3. Nelle ipotesi in cui l'esame dell'assetto proprietario non consenta di individuare in maniera univoca la persona fisica o le persone fisiche cui è attribuibile la proprietà diretta o indiretta dell'ente, il titolare effettivo coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile il **controllo** del medesimo in forza: a) del controllo della maggioranza dei voti esercitabili in assemblea ordinaria; b) del controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria; c) dell'esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante. 4. Qualora l'applicazione dei criteri di cui ai precedenti commi non consenta di individuare univocamente uno o più titolari effettivi, il titolare effettivo coincide con la persona fisica o le persone fisiche titolari di poteri di amministrazione o direzione della società.	a) in caso di società: 1) la persona fisica o le persone fisiche che, in ultima istanza, possiedano o controllino un'entità giuridica, attraverso il possesso o il controllo diretto o indiretto di una percentuale sufficiente delle partecipazioni al capitale sociale o dei diritti di voto in seno a tale entità giuridica, anche tramite azioni al portatore, purché non si tratti di una società ammessa alla quotazione su un mercato regolamentato e sottoposta a obblighi di comunicazione conformi alla normativa comunitaria o a standard internazionali equivalenti; tale criterio si ritiene soddisfatto ove la percentuale corrisponda al 25 per cento più uno di partecipazione al capitale sociale; 2) la persona fisica o le persone fisiche che esercitano in altro modo il controllo sulla direzione di un'entità giuridica; b) in caso di entità giuridiche quali le fondazioni e di istituti giuridici quali i trust, che amministrano e distribuiscono fondi: 1) se i futuri beneficiari sono già stati determinati, la persona fisica o le persone fisiche beneficiarie del 25 per cento o più del patrimonio di un'entità giuridica; 2) se le persone che beneficiano dell'entità giuridica non sono ancora state determinate, la categoria di persone nel cui interesse principale è istituita o agisce l'entità giuridica; 3) la persona fisica o le persone fisiche che esercitano un controllo sul 25 per cento o più del patrimonio di un'entità giuridica.

5. Nel caso in cui il cliente sia una **persona giuridica privata**, di cui al decreto del Presidente della Repubblica 10 febbraio 2000, n. 361, sono **cumulativamente** individuati, come titolari effettivi: a) i fondatori, ove in vita; b) i beneficiari, quando individuati o facilmente individuabili; c) i titolari di funzioni di direzione e amministrazione.	

Osserviamo che sono stati introdotti nel nostro ordinamento:

a) **<u>Dei criteri residuali per l'identificazione dei titolari effettivi delle società di capitali</u>:** qualora non sia possibile individuare univocamente uno o più titolari effettivi, il titolare effettivo coincide in via residuale, con la persona che è investita dei poteri di amministrazione o di direzione della società.[7]

b) **<u>Dei criteri per l'identificazione cumulativa dei titolari effettivi delle persone giuridiche private</u>**

c) **<u>L'istituzione di un registro pubblico</u>**, in apposita sezione ad accesso riservato (a pagamento) del Registro Imprese, che conserverà le informazioni sui titolari effettivi delle imprese dotate di personalità giuridica, delle persone giuridiche private e di trust produttivi di effetti giuridici rilevanti ai fini fiscali.

Con apposito decreto del Ministro dell'Economia, da adottarsi di concerto con il Ministro dello sviluppo economico saranno individuati i dati e le informazioni oggetto di comunicazione al Registro delle imprese; lo stesso provvedimento provvederà a disciplinare i termini e le modalità di accesso alle informazioni da parte dei soggetti autorizzati, nonché le modalità di consultazione e di accreditamento da parte dei soggetti obbligati.

Il registro è una novità della IV Direttiva e in ogni caso la sua consultazione non esonera dalle altre valutazioni o dall'adozione di misure idonee; si può comunque richiedere all'amministratore o al soggetto che rappresenta l'entità giuridica ai sensi dell'art. 22, comma 2 di fornire, in occasione degli adempimenti strumentali all'adeguata verifica della clientela, le informazioni adeguate, accurate e aggiornate sulla propria titolarità effettiva, quindi, sostanzialmente, le stesse che vengono pubblicate nel registro; le informazioni, ai sensi del comma 1 dell'art.22, devono essere fornite per iscritto.

[7] Particolare attenzione andrà prestata ai casi in cui la società sia controllata da altra società. Sorge spontaneo chiedersi se gli amministratori da identificare siano quelli della società cliente del Notaio o quelli della società a monte della catena di controllo. All'interrogativo risponde la Risposta a Quesito pubblicata su CNN Notizie del 4 dicembre 2017, a cura di Maria Concetta Cignarella, che sul punto testualmente si riporta: "Con riferimento al primo quesito, occorre far presente che, indipendentemente dalla identificazione del titolare effettivo, è necessario anzitutto procedere all'identificazione degli amministratori della società cliente, in quanto esecutori, anche attraverso l'acquisizione del documento d'identità degli stessi nonché alla verifica dei loro poteri di rappresentanza. Atteso ciò, si precisa che, nel caso di specie, si può preliminarmente verificare la catena di controllo e, conseguentemente, procedere all'individuazione del titolare effettivo applicando i criteri dianzi illustrati - che, come detto, seguono un ordine "a cascata" - in relazione alla società a monte della catena di controllo stessa. Pertanto, ove non vi siano proprietari o controllanti, secondo il disposto delle norme sopra richiamate, il titolare effettivo coinciderà con la persona fisica o le persone fisiche titolari di poteri di amministrazione o direzione della società controllante."

Si rammenta, peraltro, l'obbligo di collaborazione attiva espressamente posto dalla nuova normativa a carico degli amministratori delle società, alla luce dell'art. 22 comma 3, in virtù del quale "le informazioni di cui al comma 2, inerenti le imprese dotate di personalità giuridica tenute all'iscrizione nel Registro delle imprese di cui all'articolo 2188 del codice civile, sono acquisite, a cura degli amministratori, sulla base di quanto risultante dalle scritture contabili e dai bilanci, dal libro dei soci, dalle comunicazioni relative all'assetto proprietario o al controllo dell'ente, cui l'impresa è tenuta secondo le disposizioni vigenti nonché dalle comunicazioni ricevute dai soci e da ogni altro dato a loro disposizione. Qualora permangano dubbi in ordine alla titolarità effettiva, le informazioni sono acquisite, a cura degli amministratori, a seguito di espressa richiesta rivolta ai soci rispetto a cui si renda necessario approfondire l'entità dell'interesse nell'ente. L'inerzia o il rifiuto ingiustificati del socio nel fornire agli amministratori le informazioni da questi ritenute necessarie per l'individuazione del titolare effettivo ovvero l'indicazione di informazioni palesemente fraudolente rendono inesercitabile il relativo diritto di voto e comportano l'impugnabilità, a norma dell'articolo 2377 del codice civile, delle deliberazioni eventualmente assunte con il suo voto determinante."

Ne consegue che, mentre per il cliente-persona fisica (o per l'esecutore in sua rappresentanza) non vi sono cambiamenti di rilievo, per il cliente non personificato (limitatamente alle persone giuridiche ed alle società di capitale) l'art. 22 prevede che le informazioni sui titolari, necessarie per compiere l'adeguata verifica, siano preventivamente già acquisite dagli amministratori (o simili) e rese disponibili al soggetto obbligato a compiere l'AV; questo dovrebbe evitare, nei casi ordinari, la necessità di consultare il registro di cui sopra.

Se il legislatore ha dettato specifici criteri per l'individuazione del titolare effettivo delle società di capitale e delle persone giuridiche private, non ha dato altro che un criterio generale ("la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'ente ovvero il relativo controllo") per l'individuazione del titolare effettivo degli altri enti non personificati.

Sul punto il Ministero dell'Economia e delle Finanze, in occasione delle FAQ pubblicate il 3 ottobre 2017, interpellato circa la possibilità di utilizzare, anche per i soggetti non richiamati dal citato art. 20 i criteri nello stesso previsti per l'identificazione del titolare effettivo, ha avuto modo di fornire la sua interpretazione sulla portata della norma, riconoscendo alla stessa la valenza di "una norma specifica introdotta dal legislatore per dare soluzione ai dubbi sollevati nella pratica in merito alla identificazione del titolare effettivo di un soggetto di diritto giuridicamente e patrimonialmente distinto dalle persone fisiche che agiscono tramite esso" e aggiungendo che tale problema non si pone, ad esempio, per le società di persone, "laddove vi è una sovrapposizione sostanziale e giuridica della proprietà legale ed effettiva, attesa l'imputabilità degli effetti degli atti, posti in essere attraverso il veicolo societario, in capo al legale rappresentante."

Tenuto conto di tutto quanto sopra, possiamo quindi osservare che:

- manca una definizione dei criteri per la determinazione del titolare effettivo nel caso di **trust**; occorrerà ricorrere a quanto disciplinato dal comma 5 dell'art. 22, che individua quali sono le informazioni rilevanti ai fini dell'individuazione del titolare effettivo come: l'identità del fondatore, del fiduciario o dei fiduciari, del guardiano ovvero di altra persona per conto del fiduciario, ove esistenti, dei beneficiari o classe di beneficiari e delle altre persone fisiche che esercitano il controllo sul trust e di qualunque altra persona fisica che esercita, in ultima istanza, il controllo sui beni conferiti nel trust attraverso la proprietà diretta o indiretta o attraverso altri mezzi;
- l'articolato non è coerente riguardo alla differenziazione tra persone fisiche e soggetti diversi dalle persone fisiche, in quanto ricomprende tra i soggetti diversi dalle persone fisiche solo

alcuni dei possibili: le persone giuridiche private (non comprendendo tutte le organizzazioni senza scopo di lucro che non sono dotate di personalità giuridica) e le società di capitali (non comprendendo le società di persone);

- l'art. 2 dell'allegato tecnico è stato abrogato, quindi occorre riferirsi (peraltro per le sole società di capitali e persone giuridiche private, non essendo state oggetto di disciplina le altre "entità giuridiche" – espressione usata dal legislatore sotto il vigore della precedente norma) solamente all'art. 20, che fa coincidere la titolarità effettiva con la **proprietà diretta o indiretta o con il controllo, ma solo in via sussidiaria**; si amplia e si chiarisce il concetto di controllo estendendolo anche alle ipotesi in cui consenta di esercitare una "influenza dominante in assemblea ordinaria" o sia realizzato mediante vincoli contrattuali;
- nel caso di persone giuridiche private, cambia il criterio di determinazione del titolare effettivo: è determinato **"cumulativamente"** nel fondatore, nei beneficiari e nei titolari di funzioni di direzione e amministrazione;
- con specifico riferimento alle **società di persone**, in adesione all'interpretazione fornita dal Ministero dell'Economia e delle Finanze, già sopra richiamata, come anche in caso di consorzi e enti privati non riconosciuti, si può ritenere che assuma particolare rilievo, ai fini dell'individuazione del titolare effettivo, la figura della persona fisica che agisce come tramite di essi in qualità di legale rappresentante, cui vengono imputati gli effetti degli atti compiuti;
- nell'individuazione del titolare effettivo delle società di persone e consorzi, dovrebbe ritenersi consentita l'utilizzazione dei dati dei soci, risultanti dal Registro delle Imprese, salvo che sussistano dubbi, incertezze o incongruenze sull'identità dello stesso e salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni;
- nell'individuazione del titolare effettivo degli enti privati non riconosciuti, in assenza di indici che rivelino l'esistenza di associati che ne detengano di fatto il controllo, ovvero di beneficiari determinati, dovrebbe farsi riferimento ai soggetti titolari di funzioni di direzione e/o amministrazione;
- dovrebbe infine ritenersi confermata la possibilità per il notaio di accedere alle informazioni sugli assetti proprietari, autonomamente, mediante consultazione di un registro pubblico; in ogni caso, ai sensi dell'art. 20 comma 6 occorre conservare traccia delle verifiche effettuate ai fini dell'individuazione del titolare effettivo; la visura camerale degli assetti proprietari (se confermata dal cliente) dovrebbe essere ancora sufficiente a questi fini. Si ricorda che la normativa richiede l'identificazione del titolare effettivo, non l'acquisizione del suo documento (vedasi art. 19 D.Lgs. 231/2017), qualora il titolare effettivo sia individuato attraverso la consultazione dei Pubblici Registri.

Recepiscono le indicazioni di cui sopra circa l'identificazione del titolare effettivo le Regole tecniche n. 5 e n. 6, poste entrambe nel Capo IV delle Regole Tecniche, dedicato all'assolvimento degli obblighi di adeguata verifica.

REGOLA TECNICA N. 5

Ai fini dell'identificazione del titolare effettivo, rileva il disposto di cui all'articolo 19 comma 1 lettera a) ai sensi del quale il cliente, all'atto dell'identificazione, fornisce "le informazioni necessarie a consentire l'identificazione del titolare effettivo".
La verifica dell'identità del titolare effettivo, necessaria qualora sussistano dubbi, incertezze o incongruenze in relazione ai dati acquisiti in sede di identificazione, può essere effettuata,

ai sensi dell'articolo 19, comma 1, lettera b) anche attraverso il riscontro di tali dati con quelli riportati da fonti attendibili e indipendenti. Con riferimento alla titolarità effettiva di imprese dotate di personalità giuridica, tenute all'iscrizione nel registro delle imprese, il riscontro dei dati acquisiti in sede di identificazione può avvenire anche attraverso l'accesso alla sezione del registro delle imprese, ad hoc istituita, ai sensi dell'articolo 21, d.lgs. n. 231/07. Resta fermo quanto stabilito dal comma 7 del medesimo articolo 20 in ordine alla circostanza che la consultazione dei registri di cui al presente articolo non esonera i soggetti obbligati dal valutare il rischio di riciclaggio e finanziamento del terrorismo cui sono esposti nell'esercizio della loro attività e dall'adottare misure adeguate al rischio medesimo.
Fermo quanto sopra, e fermo restando che ai sensi dell'art. 19 del medesimo decreto, non si è tenuti all'acquisizione del documento di identità del titolare effettivo, qualora il titolare effettivo sia individuato attraverso la consultazione di pubblici registri, salva la valutazione del rischio e la conseguente applicazione di misure ad esso proporzionate, l'identificazione può essere ritenuta correttamente eseguita mediante la sola acquisizione dei dati e delle informazioni risultanti dai pubblici registri stessi, confermati nella loro validità dal cliente.
Ai fini dell'individuazione del titolare effettivo, nelle ipotesi in cui sia possibile la consultazione di un pubblico registro, tale consultazione è da ritenersi idonea ai fini dell'espletamento dell'obbligo di identificazione dello stesso titolare effettivo, salvo che ci si trovi in presenza di elementi oggettivi che mettano in dubbio o rendano palesemente incerti o incongrui i dati e le informazioni pubblicate. Detti dati e informazioni sono, infatti, da ritenere affidabili a fronte dell'obbligo giuridico a carico dei responsabili delle imprese, persone giuridiche e trust, di comunicare notizie vere, aggiornate e complete, ferma restando la possibilità di acquisire, in funzione del rischio, ulteriori informazioni.
Ai sensi dell'articolo 18, comma 1, lettera b, l'identificazione del titolare effettivo deve essere attuata nel contesto dell'adozione di regole comportamentali proporzionate al rischio. L'obbligo di identificazione del titolare effettivo può ritenersi assolto attraverso l'acquisizione delle informazioni fornite dal cliente (direttamente o tramite conferma, ove già acquisite o in possesso del notaio nel contesto del rapporto con il cliente) in ordine al nome, cognome, luogo e data di nascita del titolare effettivo; laddove, in relazione ai dati forniti dal cliente, sussistano dubbi, incertezze o incongruenze il notaio provvederà a riscontrare la veridicità dei dati forniti ai sensi dell'art. 19 lett.b) del D.Lgs. 231/2007.

REGOLA TECNICA N. 6

Fermo restando quanto previsto dall'articolo 20 d.lgs. n. 231/07 e successive modificazioni per l'individuazione del titolare effettivo di clienti diversi dalle persone fisiche, nelle società di persone e consorzi e negli enti privati non riconosciuti, può assumere rilievo, ai fini dell'individuazione del titolare effettivo, la figura della persona fisica che agisce quale tramite di essi, in qualità di legale rappresentante. Nell'individuazione del titolare effettivo delle società di persone e consorzi, è consentita l'utilizzazione dei dati dei soci, risultanti dal Registro delle Imprese, salvo che sussistano dubbi, incertezze o incongruenze sull'identità dello stesso e salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni.
Nell'individuazione del titolare effettivo degli enti privati non riconosciuti, in assenza di indici che rivelino l'esistenza di associati che ne detengano di fatto il controllo, ovvero di beneficiari determinati, si farà riferimento ai soggetti titolari di funzioni di direzione e/o amministrazione.

D. LE PERSONE POLITICAMENTE ESPOSTE (PEP)

Viene ampliato il concetto di **persona politicamente esposta:** adeguandosi alle Raccomandazioni GAFI, si assiste ad un ampliamento significativo del concetto di persona politicamente esposta, che non è più solo identificata nei "foreign PEP" ma estesa ai cd. PEP domestici.

Si ricordi, peraltro, che sono persone politicamente esposte non solo le persone fisiche che occupano o che hanno cessato di occupare da meno di un anno importanti cariche pubbliche, bensì anche "i loro familiari e coloro che con i predetti intrattengono stretti legami", laddove per:

- "Familiari" si intendono "i genitori, il coniuge o la persona legata in unione civile o convivenza di fatto o istituti assimilabili alla persona politicamente esposta, i figli e i loro coniugi nonché le persone legate ai figli in unione civile o convivenza di fatto o istituti assimilabili";
- "coloro che intrattengono stretti rapporti" si intendono anche coloro che intrattengono stretti rapporti coi familiari di PEP.

Si ricorda che per "coloro che intrattengono stretti legami" si intendono:

- le persone fisiche legate alla persona politicamente esposta per via della titolarità effettiva congiunta di enti giuridici o di altro stretto rapporto di affari;
- le persone fisiche che detengono solo formalmente il controllo totalitario di un'entità notoriamente costituita, di fatto, nell'interesse e a beneficio di una persona politicamente esposta.

Si capisce pertanto come con il nuovo testo diviene indispensabile l'istituzione di un registro consultabile delle PEP; è d'altro canto evidente che una banca dati di persone politicamente esposte, quanto meno nell'accezione lata accolta dall'ordinamento, non esiste.

Ne consegue che sarà sempre cura del Notaio acquisire la dichiarazione scritta del cliente – resa ai sensi dell'art. 22 primo comma - circa l'insussistenza della qualifica di PEP / di rapporti con PEP, per conservarla nel fascicolo.

E. LA TEMPISTICA DEGLI OBBLIGHI DI ADEGUATA VERIFICA

La norma sembra anticipare il momento in cui vanno adempiuti gli obblighi, prevedendo che "le attività di identificazione e verifica delle identità del cliente, dell'esecutore e del titolare effettivo debbano essere compiute *prima* dell'instaurazione del rapporto continuativo o del conferimento dell'incarico" (art. 18 comma 2).
Peraltro i professionisti, ai sensi del comma 4 del medesimo articolo, fermo l'obbligo di identificazione, sono esonerati dall'obbligo di verifica dell'identità del cliente o del titolare effettivo sino al momento del conferimento dell'incarico.
Per i notai, in particolare, dovrebbe ritenersi che il termine ultimo per la conclusione delle operazioni di adeguata verifica coincida con la stipula dell'atto notarile, che costituisce il momento ultimo per l'esecuzione degli adempimenti prescritti in funzione di adeguata verifica della clientela, fermo restando che il complesso dei presidi antiriciclaggio si attiva al momento del conferimento dell'incarico per lo svolgimento della prestazione professionale.
Tra l'altro, l'incarico per la stipula non sempre viene conferito da tutte le parti dell'atto, congiuntamente e nello stesso momento, al notaio, che pertanto dovrebbe poter effettuare gli adempimenti di adeguata verifica della clientela anche in momenti diversi, purché si

concludano alla stipula, in quanto è in quel momento che lo stesso notaio può concludere la valutazione della prestazione professionale per cui l'incarico è stato conferito.

Recepisce espressamente la tempistica indicata la Regola Tecnica n. 8, da coordinarsi con la precedente Regola Tecnica n. 7, che indica, tra l'altro, la scansione temporale degli obblighi di verifica dell'identità e di aggiornamento dei documenti, Regole Tecniche entrambe di seguito riportate.

REGOLA TECNICA N. 7

Nelle ipotesi in cui ricorra un basso rischio di riciclaggio e di finanziamento del terrorismo, ed esista, ai sensi dell'ordinamento vigente, l'obbligo per il notaio di ricevere l'atto ed egli sia certo, ai sensi della legge 16 febbraio 1913, n. 89 dell'identità personale del cliente o dell'esecutore, la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo, fermo l'obbligo di acquisizione dei dati identificativi, può essere posticipata ad un momento successivo al conferimento dell'incarico per lo svolgimento della prestazione professionale, secondo quanto prescritto dall'articolo 18, comma 3, d.lgs. n. 231/07. In dette ipotesi, l'indisponibilità di un documento di riconoscimento in corso di validità costituisce presupposto per l'effettuazione, da parte del notaio, dell'aggiornamento dei dati e delle informazioni necessarie all'adeguata verifica della clientela, senza rappresentare, di per sé elemento idoneo e sufficiente a fondare un sospetto meritevole di segnalazione, in assenza di concomitanti ulteriori evidenze relative al profilo soggettivo del cliente o a quello oggettivo della prestazione. In caso di prestazioni professionali non occasionali, il notaio provvederà ad aggiornare i documenti di identità in base al rischio: ogni 2 anni se a basso rischio, ogni anno se a rischio ordinario, con frequenza inferiore e comunque calibrata al rischio, per le ipotesi di elevato rischio di riciclaggio e di finanziamento del terrorismo.
Ai sensi dell'articolo 19, comma 1, lettera a) l'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, per i clienti i cui dati identificativi risultino da atti pubblici o da scritture private autenticate.
Nel caso in cui sia materialmente impossibile, per il notaio, effettuare l'adeguata verifica e fuori dalle ipotesi in cui sussista l'obbligo giuridico di ricevere l'atto, egli deve astenersi dall'esecuzione della prestazione e valutare se sussistano gli estremi per l'effettuazione di una segnalazione di operazioni sospette alla UIF, senza che possa ravvisarsi alcun automatismo tra astensione e segnalazione.
Ai sensi del combinato disposto dell'art. 18, comma 1, lett. a), e dell'art. 19, comma1, lettera a) n. 1 del D.Lgs. n. 231/2007 gli atti notarili da cui risultano i dati identificativi dei soggetti persone fisiche o non fisiche sono sempre considerati una fonte affidabile e indipendente ai fini dell'espletamento degli obblighi di adeguata verifica e ciò anche nel caso di intervento in atto di un esecutore dotato di procura notarile.
Ai sensi degli articoli 18, comma 1, lettera a) e 19, comma 1, lettera a) n. 1, il solo obbligo di identificazione del cliente può ritenersi assolto, senza la presenza fisica del medesimo, per i clienti i cui dati identificativi risultino, tra gli altri, da atti pubblici o scritture private autenticate e che, ai sensi del citato articolo 18, comma 1, lettera a), l'identificazione dell'esecutore non si esaurisce nel riscontro dei rispettivi dati identificativi ma abbraccia la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome del cliente.

REGOLA TECNICA N. 8

Il termine ultimo per la conclusione delle operazioni di adeguata verifica coincide, nel caso di atto notarile, con la stipula del medesimo, che costituisce il momento ultimo per l'esecuzione degli adempimenti prescritti in funzione di adeguata verifica della clientela, fermo restando che il complesso dei presidi antiriciclaggio si attiva al momento del conferimento dell'incarico per lo svolgimento della prestazione professionale, secondo il combinato disposto delle definizioni di cui all'articolo 1, comma 2, lettere h) e gg) del D.Lgs. n. 231/2007, come modificato dal D.Lgs. n. 90/2017. L'incarico per la stipula non sempre viene conferito da tutte le parti dell'atto, congiuntamente e nello stesso momento, al notaio, che pertanto potrà effettuare gli adempimenti di adeguata verifica della clientela anche in momenti diversi, purché si concludano alla stipula, in quanto è in quel momento che lo stesso notaio può concludere la valutazione della prestazione professionale per cui l'incarico è stato conferito.
Ai sensi dell'art. 32, comma 2, lettera b), è comunque considerata tempestiva l'acquisizione dei dati e delle informazioni relativi all'adeguata verifica del cliente conclusa entro trenta giorni dall'instaurazione del rapporto continuativo o dal conferimento dell'incarico per lo svolgimento della prestazione professionale, dall'esecuzione dell'operazione o della prestazione professionale, dalla variazione e dalla chiusura del rapporto continuativo o della prestazione professionale.

F. I CONTENUTI DEGLI OBBLIGHI DI ADEGUATA VERIFICA

Sotto il profilo dei **contenuti** degli obblighi di adeguata verifica, fermo restando che la stessa continua a declinarsi negli obblighi di:

a. identificazione del cliente e del titolare effettivo e di verifica delle loro identità;
b. acquisizione e valutazione di informazioni sullo scopo e la natura della prestazione;
c. controllo costante del rapporto;

la novella non prevede più, a differenza che in passato, la possibilità che l'identificazione sia effettuata da un pubblico ufficiale a ciò abilitato e ciò appare come una regressione, con un ritorno alla situazione vigente sotto il vigore del d.lgs. 56/2004, quando la normativa antiriciclaggio non teneva conto della normativa di settore dettata per i notai.
Sul punto è ragionevole ritenere, nonostante la lacuna normativa, che il notaio, se è certo dell'identità personale del cliente o dell'esecutore, secondo la Legge 16 febbraio 1913 n. 89, avrà comunque l'obbligo di ricevere l'atto; in tale caso, l'assenza di un valido documento d'identificazione ovvero il caso di un documento d'identità o di riconoscimento scaduti dovrebbero unicamente indurre il notaio a richiedere un aggiornamento ai fini dell'adeguata verifica della clientela (come sopra precisato alla Regola Tecnica n. 7), ma non dovrebbero rappresentare, di per sé, elementi idonei e sufficienti a fondare un sospetto, con conseguente obbligo di segnalazione, se non in concomitanza con eventuali ulteriori elementi relativi al profilo soggettivo del cliente o a quello oggettivo della prestazione.

Ai sensi del combinato disposto dell'art. 18, comma 1, lett. a), e dell'art. 19, comma1, lettera a) n. 1 del D.Lgs. n. 231/2007 gli atti notarili da cui risultano i dati identificativi dei soggetti persone fisiche o non fisiche dovrebbero poter essere sempre considerati una fonte affidabile e indipendente ai fini dell'espletamento degli obblighi di adeguata verifica e ciò anche nel caso di intervento in atto di un esecutore dotato di procura notarile.

L'art. 19, dedicato alle modalità con cui deve essere compiuta l'adeguata verifica, chiarisce:

- che il notaio può essere coadiuvato negli adempimenti di obblighi di AV anche dai propri collaboratori;
- il riscontro di veridicità delle informazioni fornite va effettuato **solo quando sorgono dubbi, incertezze o incongruenze;**
- in ogni caso le misure di adeguata verifica vanno proporzionate in funzione del rischio: v. art.17 comma 3.

Volendo richiamare i contenuti degli obblighi di adeguata verifica, è opportuno ricordare la tripartizione tra le diverse tipologie di adeguata verifica (semplificata, ordinaria e rafforzata).

L'ADEGUATA VERIFICA SEMPLIFICATA

Viene ridefinita la nozione di **"adeguata verifica semplificata"**; in particolare scompare la "rassicurante" elencazione dei soggetti di cui al precedente art. 25: non esiste più, pertanto un'elencazione tassativa espressa delle categorie di soggetti destinatari dell'adeguata verifica semplificata. Sul punto la norma innova rispetto al passato.

Adeguata verifica semplificata nella nuova disciplina (art. 23)	**Adeguata verifica semplificata nella precedente disciplina (art. 25)**
1. In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, i soggetti obbligati possono applicare misure di adeguata verifica della clientela semplificate sotto il profilo dell'estensione e della frequenza degli adempimenti prescritti dall'articolo 18. 2. Ai fini dell'applicazione di misure semplificate di adeguata verifica della clientela e fermo l'obbligo di commisurarne l'estensione al rischio in concreto rilevato, i soggetti obbligati tengono conto, tra l'altro, dei seguenti **indici di basso rischio**: a) indici di rischio relativi a tipologie di clienti quali: 1) società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva; 2) pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea; 3) clienti che sono residenti in aree geografiche a basso rischio, ai sensi della lettera c); b) indici di rischio relativi a tipologie di prodotti, servizi, operazioni o canali di distribuzione quali: ..... c) indici di rischio relativi ad aree geografiche quali: 1) Stati membri;	**1.** I destinatari del presente decreto non sono soggetti agli obblighi di cui agli articoli della Sezione I, ad eccezione di quelli di cui alla lettera c) dell'articolo 15, alla lettera d) dell'articolo 16 ed alla lettera c) dell'articolo 17 se il cliente è: **a)** uno dei soggetti indicati all' articolo 11, commi 1 e 2, lettere b) e c); **b)** un ente creditizio o finanziario comunitario soggetto alla direttiva; **c)** un ente creditizio o finanziario situato in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalla direttiva e preveda il controllo del rispetto di tali obblighi. c-bis) una società o un altro organismo quotato i cui strumenti finanziari sono ammessi alla negoziazione su un mercato regolamentato ai sensi della direttiva 2004/39/CE in uno o più Stati membri, ovvero una società o un altro organismo quotato di Stato estero soggetto ad obblighi di comunicazione conformi alla normativa comunitaria. **2.** Il Ministro dell'economia e delle finanze, con proprio decreto, sentito il Comitato di sicurezza finanziaria, individua gli Stati extracomunitari il cui regime è ritenuto equivalente.

2) Paesi terzi dotati di efficaci sistemi di prevenzione del riciclaggio e del finanziamento del terrorismo; 3) Paesi terzi che fonti autorevoli e indipendenti valutano essere caratterizzati da un basso livello di corruzione o di permeabilità ad altre attività criminose; 4) Paesi terzi che, sulla base di fonti attendibili e indipendenti, quali valutazioni reciproche ovvero rapporti di valutazione dettagliata pubblicati, prevedano e diano effettiva applicazione a presidi di prevenzione del riciclaggio e di finanziamento del terrorismo, coerenti con le raccomandazioni del GAFI. 3. ..gli organismi di autoregolamentazione, in conformità delle regole tecniche di cui all'articolo 11, comma 2, possono individuare **ulteriori fattori di rischio** da prendere in considerazione al fine di integrare o modificare l'elenco di cui al precedente comma e **stabiliscono misure semplificate di adeguata verifica della clientela da adottare in situazioni di basso rischio.** 4. L'applicazione di obblighi semplificati di adeguata verifica della clientela è comunque esclusa quando vi è sospetto di riciclaggio o di finanziamento del terrorismo.	**3.** L'identificazione e la verifica non sono richieste se il cliente è un ufficio della pubblica amministrazione ovvero una istituzione o un organismo che svolge funzioni pubbliche conformemente al trattato sull'Unione europea, ai trattati sulle Comunità europee o al diritto comunitario derivato. **4.** Nei casi di cui ai commi 1 e 3, gli enti e le persone soggetti al presente decreto raccolgono comunque informazioni sufficienti per stabilire se il cliente possa beneficiare di una delle esenzioni previste in tali commi. **5.** Gli obblighi semplificati di adeguata verifica della clientela non si applicano qualora si abbia motivo di ritenere che l'identificazione effettuata ai sensi del presente articolo non sia attendibile ovvero qualora essa non consenta l'acquisizione delle informazioni necessarie. **6.** Gli enti e le persone soggetti al presente decreto sono autorizzati a non applicare gli obblighi di adeguata verifica della clientela, in relazione a: **a)** contratti di assicurazione-vita, il cui premio annuale non ecceda i 1.000 euro o il cui premio unico sia di importo non superiore a 2.500 euro; **b)** forme pensionistiche complementari disciplinate dal decreto legislativo 5 dicembre 2005, n. 252, a condizione che esse non prevedano clausole di riscatto diverse da quelle di cui all' articolo 14 del medesimo decreto e che non possano servire da garanzia per un prestito al di fuori delle ipotesi previste dalla normativa vigente; **c)** regimi di pensione obbligatoria e complementare o sistemi simili che versino prestazioni di pensione, per i quali i contributi siano versati tramite deduzione dal reddito e le cui regole non

	permettano ai beneficiari, se non dopo il decesso del titolare, di trasferire i propri diritti; **d)** moneta elettronica quale definita nell' articolo 1, comma 2, lettera h-ter), del TUB, nel caso in cui, se il dispositivo non è ricaricabile, l'importo massimo memorizzato sul dispositivo non ecceda 150 euro, oppure nel caso in cui, se il dispositivo è ricaricabile, sia imposto un limite di 2.500 euro sull'importo totale trattato in un anno civile, fatta eccezione per i casi in cui un importo pari o superiore a 1.000 euro sia rimborsato al detentore nello stesso anno civile ai sensi dell'articolo 3 della direttiva 2000/46/CE ovvero sia effettuata una transazione superiore a 1.000 euro, ai sensi dell'articolo 3, paragrafo 3, del regolamento (CE) n. 1781/2006; **e)** qualunque altro prodotto o transazione caratterizzato da uno basso rischio di riciclaggio o di finanziamento del terrorismo che soddisfi i criteri tecnici stabiliti dalla Commissione europea a norma dell' articolo 40, paragrafo 1, lettera b), della direttiva, se autorizzato dal Ministro dell'economia e delle finanze con le modalità di cui all' articolo 26.

La nuova norma:

a) indica quali siano **le condizioni concorrenti** per procedere ad adeguata verifica semplificata e precisamente:

1. presenza di almeno un **indice di basso rischio** (quale usualmente sarà la presenza di soli clienti residenti in UE o in Paesi a basso rischio);
2. **non emersione di fattori di rischio:** nella rilevazione del rischio, oltre che i fattori indicati dal Decreto (v. art. 24), andranno tenuti presenti, come detto, anche gli Indicatori di anomalia, in quanto, benché emanati in vigenza del precedente testo di legge, come anche risulta da comunicazione dell'UIF pubblicata su CNN Notizie del 6 luglio 2017, sono da considerare ancora efficaci e/o applicabili in via transitoria, e gli Schemi di Comportamento emanati dall'UIF.

A queste due pre-condizioni, dal complessivo tenore del D.Lgs, e da una prudente applicazione della norma che preveda l'adozione di linee guida interne che ne integrino il suo contenuto, individuando aree e situazioni di alto e basso rischio nella concreta realtà dello studio professionale, si aggiungeranno:

3. **l'inesistenza di fattori di dubbio**, incongruenza o incertezze nell'acquisizione di informazioni in sede di adeguata verifica;

4. **la persistenza**, in base alle linee guida interne, **delle condizioni** per cui si possa effettuare l'adeguata verifica semplificata; in sostanza nelle linee guida interne si saranno individuate preventivamente le operazioni che, oggettivamente o per il loro importo, richiedono una adeguata verifica che va oltre la modalità semplificata.

b) non specifica in quali comportamenti materialmente si concretizzino gli obblighi di adeguata verifica semplificata, limitandosi ad aggettivare tali obblighi come misure semplificate sotto il profilo della **minore estensione e frequenza**.

Circa il contenuto degli obblighi di adeguata verifica semplificata, pare ragionevole ritenere che siano idonee misure semplificate di adeguata verifica della clientela l'acquisizione delle informazioni sullo scopo e sulla natura della prestazione effettuata in contestualità della stipula, mediante la richiesta delle medesime, fermo restando l'obbligo della loro valutazione da parte del notaio.
Nell'ambito dell'attività notarile, infatti, lo scopo e la natura della prestazione professionale coincidono, per la quasi totalità dei casi, con il negozio giuridico oggetto dell'incarico; a differenza delle operazioni finanziarie, negli atti notarili, scopo e natura delle prestazioni risultano manifesti nell'atto stesso e, salva diversa valutazione da parte del notaio, non pare necessario formalizzare in autonomo documento l'acquisizione di tali informazioni dal cliente.

Soccorre al riguardo la Regola Tecnica n. 4, di seguito riportata.

REGOLA TECNICA N. 4

Sono considerate idonee misure semplificate di adeguata verifica della clientela l'acquisizione delle informazioni sullo scopo e sulla natura della prestazione effettuata in contestualità della stipula, mediante la richiesta delle medesime, fermo restando l'obbligo della loro valutazione da parte del notaio. Allo scopo di definire l'idoneità delle misure semplificate di adeguata verifica della clientela nell'ambito dell'attività notarile, si precisa che lo scopo e la natura della prestazione professionale dei notai coincidono, per la quasi totalità dei casi, con il negozio giuridico oggetto dell'incarico, e che, a differenza delle operazioni finanziarie, negli atti notarili, scopo e natura delle prestazioni risultano manifesti nell'atto stesso , pertanto, salva diversa valutazione da parte del notaio, non è necessario formalizzare in autonomo documento l'acquisizione di tali informazioni dal cliente. Occorre comunque considerare le ipotesi di più atti, anche della stessa specie, che possono risultare collegati e rispetto alle quali va fatta salva la valutazione del complesso di operazioni compiute.

c) non individua più categorie di soggetti sempre astrattamente considerati destinatari di possibile adeguata verifica semplificata.

Sul punto, una ragionevole interpretazione della norma consente di individuare, quali **indici di basso rischio** relativi a tipologie di clienti, oltre ai seguenti soggetti, già individuati dall'art.23 comma 2, lettera a):

- società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva;

- pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea;
- clienti che sono residenti in aree geografiche a basso rischio, ai sensi della lettera c) dell'art. 23 del decreto stesso;

anche, per analogia, i soggetti sottoposti a vigilanza ai sensi del D.Lgs. 1° settembre 1993 n. 385, del D.Lgs. 24 febbraio 1998, n. 58, e del D.Lgs. 7 settembre 2005 n. 209

Per tutti tali soggetti, qualora non emergano fattori di rischio in concreto, è ragionevole applicare misure semplificate di adeguata verifica della clientela che consistono nella identificazione del rappresentante del soggetto, inclusa la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente; in tal caso, l'obbligo di identificazione del titolare effettivo è da ritenersi assolto con l'acquisizione dei dati identificativi forniti dal cliente, con le modalità e nei termini di cui alla regola tecnica n. 5.

Gli obblighi semplificati di adeguata verifica della clientela non si applicano qualora si abbia motivo di ritenere che l'identificazione effettuata non sia attendibile e qualora vi sia sospetto di riciclaggio o di finanziamento del terrorismo: i soggetti obbligati potranno dunque applicare misure semplificate di adeguata verifica solo qualora dalla valutazione emerga in concreto un basso rischio di riciclaggio.

Il caso delle società fiduciarie

Con riferimento alle **società fiduciarie**, si invita alla massima prudenza:

- vero è che l'art. 3 comma 2 ascrive al novero degli "intermediari bancari e finanziari" anche "le società fiduciarie iscritte nell'albo previsto ai sensi dell'art. 106 TUB", con ciò sembrando recepire la distinzione (già in vigore per effetto del d.lgs. 141/2010) tra le fiduciarie "di primo livello" e quelle di cui alla Legge 23 novembre 1966 (cd. "fiduciarie di secondo livello");
- è altresì vero, tuttavia, che l'inasprimento degli obblighi di adeguata verifica semplificata e, soprattutto, il venir meno dell'art. 25 del precedente d.lgs. 231/2007, rende la posizione delle fiduciarie di primo livello esposta alle medesime incertezze interpretative di cui sopra circa l'applicabilità dell'adeguata verifica semplificata, soprattutto con riferimento all'obbligo di identificazione del titolare effettivo.

Pertanto sembrerebbe doversi trarre, quale conseguenza, la necessità di prestare la massima attenzione alle fiduciarie, tanto di primo quanto di secondo livello.

Ciò sarebbe peraltro confermato dal disposto dell'art. 24 comma 2 numero 4), che nell'ambito dell'"adeguata verifica rafforzata" ravvisa un fattore di rischio relativo al cliente ogni qual volta nella struttura societaria risulti la partecipazione di "fiduciari".

Il generico riferimento all'espressione "fiduciari" non pare consentire purtroppo alcun margine di interpretazione in merito ad un distinto trattamento tra società fiduciarie vigilate da Banca d'Italia e piccole società fiduciarie. Inoltre, la stessa espressione utilizzata ("società partecipate da fiduciari") sembrerebbe far sì che ogni qual volta risalendo la catena delle partecipazioni societarie, si ravvisi la presenza di una fiduciaria, indipendentemente dal fatto che trattasi di partecipazione qualificata o meno, debba aversi luogo a tale "adeguata verifica rafforzata".

Soccorre in merito la Regola Tecnica n. 3, dedicata proprio all'adeguata verifica semplificata e di seguito riportata:

REGOLA TECNICA N. 3

In tema di adeguata verifica semplificata, tenuto conto:
- che il notaio potrà applicare misure semplificate di adeguata verifica della clientela nelle ipotesi in cui, alla stregua di un processo valutativo ricostruibile e dimostrabile, emerga in concreto un basso rischio di riciclaggio e di finanziamento del terrorismo, in quanto l'estensione dell'adeguata verifica va commisurata al rischio in concreto rilevato, sulla base degli indici di cui all'articolo 23, commi 1 e 2, del D.Lgs. n. 90/2017;
- che in tali ipotesi, quali indici di basso rischio relativi a tipologie di clienti, possono individuarsi, a titolo esemplificativo, le seguenti tipologie di soggetti:
  1) società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva;
  2) pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea;
  3) clienti che sono residenti in aree geografiche a basso rischio, ai sensi della lettera c) dell'art. 23 del decreto stesso;

i soggetti sottoposti a vigilanza ai sensi del D.Lgs. 1° settembre 1993 n. 385, del D.Lgs. 24 febbraio 1998, n. 58, e del D.Lgs. 7 settembre 2005 n. 209 si considerano a basso rischio di riciclaggio.
Pertanto è possibile, qualora ricorrano in concreto i presupposti, applicare misure semplificate di adeguata verifica della clientela che consistono nella identificazione del rappresentante del soggetto, inclusa la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente.
In tal caso, l'obbligo di identificazione del titolare effettivo è da ritenersi assolto con l'acquisizione dei dati identificativi forniti dal cliente, con le modalità e nei termini di cui alla regola tecnica n. 5.
Gli obblighi di adeguata verifica sono attenuati ogniqualvolta i soggetti summenzionati intervengano in un atto per porre in essere un'operazione che la legge riserva espressamente ad essi in via esclusiva nonché con riferimento a tutti gli atti consequenziali o collegati a tali operazioni. A titolo di mera esemplificazione, è possibile far riferimento a contratti di mutuo, finanziamenti, aperture di credito, ivi compresi i patti aggiuntivi e modificativi degli stessi, gli atti di quietanza totale e parziale, di ristrutturazione e rinegoziazione, di erogazione, di surrogazione, di accollo, di delegazione e relativi atti connessi od accessori, ad atti e contratti che comportino la costituzione, la conferma, l'estensione, la rinnovazione, il frazionamento, la postergazione, la surroga, la riduzione, la cancellazione o lo svincolo di ipoteche, pegni o privilegi, fidejussioni e altre garanzie stabilite a favore dell'istituto, ad atti e contratti di cessione, a qualsiasi titolo, dei contratti di cui sopra e/o dei crediti nascenti dagli stessi, ai leasing mobiliari ed immobiliari.
Gli obblighi semplificati di adeguata verifica della clientela non si applicano qualora si abbia motivo di ritenere che l'identificazione effettuata non sia attendibile e qualora vi sia sospetto di riciclaggio o di finanziamento del terrorismo. I soggetti obbligati potranno dunque applicare misure semplificate di adeguata verifica solo qualora dalla valutazione emerga in concreto un basso rischio di riciclaggio.

Volendo quindi riassumere, *in caso di adeguata verifica semplificata*:

- sarà sufficiente identificare cliente e titolare effettivo (eventuale);

- per i soggetti non fisici iscritti in un registro pubblico si possono trarre le informazioni necessarie dalla consultazione del registro, confermate dal cliente;
- si procederà a raccogliere una dichiarazione scritta del cliente in ordine alla sua qualifica di non PEP e, nel caso di cliente non personificato, anche in ordine alla corrispondenza delle risultanze del registro pubblico con l'effettività;
- non occorre acquisire informazioni ulteriori sullo scopo e sulla natura della prestazione: è sufficiente la richiesta di stipula
- non occorre né verificare la consistenza patrimoniale del cliente né l'origine dei fondi.

L'ADEGUATA VERIFICA ORDINARIA

Il D.Lgs. si occupa di delineare i capi estremi dell'adeguata verifica (semplificata all'art. 23, rafforzata all'art. 24), senza dedicare adeguata attenzione all'adeguata verifica ordinaria: con riguardo a questa, quindi, il legislatore, oltre a non indicare il contenuto degli obblighi in cui si sostanzia l'adeguata verifica (come già per l'adeguata verifica semplificata), non indica nemmeno le condizioni in presenza delle quali il professionista debba procedere a tale forma di adeguata verifica.

Si può ritenere che ricorra un obbligo di adeguata verifica ordinaria allorquando, nonostante esistano tutte le condizioni per poter procedere con l'adeguata verifica semplificata, tuttavia l'operazione, in base alle linee guida interne adottate dallo Studio, è classificata a Medio Rischio o oggettivamente o in base al suo importo, ovvero è emerso, nel corso dell'istruttoria, qualche altro fattore soggettivo o oggettivo che richiede un approfondimento.

La norma nemmeno indica le modalità di esecuzione dell'adeguata verifica ordinaria; anche qui si potrebbe quindi ritenere che, oltre alle modalità di esecuzione previste per l'adeguata verifica semplificata, potrà essere necessario raccogliere, per iscritto, dal cliente, ulteriori informazioni sullo scopo e la natura dell'operazione e, quando l'operazione lo richiede, anche sulla sua consistenza patrimoniale; per quanto attiene ai fondi impiegati nell'operazione non dovrebbe essere necessario verificarne in ogni caso l'origine, almeno tutte le volte che il profilo economico del cliente sia tale da giustificare, dal punto di vista finanziario, l'operazione.

Il cliente/esecutore dovrà quindi fornire, all'occorrenza, per iscritto, sotto la propria responsabilità (art. 22, comma 1), i seguenti dati e informazioni:

a) informazioni sullo scopo e natura della prestazione professionale o dell'operazione richiesta al professionista anche con riferimento, in caso di titolare effettivo diverso dal cliente ovvero di prestazione o operazione resa tramite esecutore, delle relazioni intercorrenti tra il cliente e il titolare effettivo e tra il cliente e l'esecutore;

b) nel caso in cui si ritenga necessario verificare la provenienza dei fondi utilizzati dal cliente, se i medesimi provengono da: risparmi personali, redditi di attività propria, denaro fornito da familiari/terzi e a quale titolo, successione ereditaria, vendita di beni personali, finanziamento con indicazione della tipologia e del soggetto finanziatore, finanziamento soci, o altro (da specificare).

L'ADEGUATA VERIFICA RAFFORZATA

Circa l'**adeguata verifica rafforzata**, si ritiene la stessa ricorra in presenza delle presenti condizioni:

- quando sia emerso un fattore di rischio oggettivo o geografico;
- quando sia presente un Indicatore di Anomalia o una fattispecie prevista in uno degli Schemi UIF;

- quando ancora sia convolta una PEP, o un Trust o struttura simile.

L'adeguata verifica rafforzata si esegue, ai sensi dell'art. 25, acquisendo informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto e intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale; le criticità che emergono dalla nuova normativa si ravvisano nell'attuale assenza di un elenco ufficiale dei Paesi ad alto rischio nonché nella previsione che i PEP che abbiano cessato di esserlo da più di un anno siano ancora destinatari di particolare disciplina (norma che per questo specifico aspetto sembra di difficile attuazione, anche per la mancanza di elenchi consultabili).

Ai sensi dell'art. 24 comma 6, infatti, "i soggetti obbligati, in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo applicano misure di adeguata verifica rafforzata di clienti che, originariamente individuati come **persone politicamente esposte**, abbiano cessato di rivestire le relative cariche pubbliche da più di un anno."

Ne consegue che, in presenza delle condizioni per adeguata rafforzata, il professionista dovrà approfondire, acquisendo, sempre per iscritto dal cliente, informazioni aggiuntive, verificarne la congruenza in rapporto al profilo del cliente ed alla tipologia dell'operazione, esaminare la situazione patrimoniale del cliente e farsi dichiarare l'origine dei fondi impiegati; verificare la verosimiglianza di tutte le informazioni così raccolte.

Vediamo in concreto quali sono gli adempimenti ulteriori che si potrebbe ritenere debbano essere compiuti per una adeguata verifica rafforzata:

a) esaminare il contesto e la finalità di operazioni caratterizzate da importi insolitamente elevati ovvero rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate;

b) acquisire informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto e intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale;

c) applicare misure adeguate per stabilire l'origine del patrimonio e dei fondi impiegati nel rapporto continuativo o nell'operazione.

Esaminiamo in particolare l'attività di **acquisizione e valutazione delle informazioni** sullo scopo e sulla natura delle operazioni; in caso di adeguata verifica semplificata, lo standard è facilmente soddisfatto dalla stessa richiesta dell'operazione effettuata dal cliente al professionista: in sostanza essa sarà per così dire, autoportante; nel caso invece in cui non si possa applicare una modalità semplificata, ci troveremo per converso, nella condizione di dover approfondire, e quindi di dover richiedere, al cliente, di formalizzare, tendenzialmente per iscritto, informazioni aggiuntive; la norma in questo caso esemplifica tali informazioni quali quelle relative all'instaurazione del rapporto, alle relazioni intercorrenti tra il cliente e l'esecutore, tra il cliente e il titolare effettivo e quelle relative alla situazione economico-patrimoniale del cliente, acquisite o possedute in ragione dell'esercizio dell'attività; inoltre, nel caso di adeguata verifica rafforzata, occorrerà effettuare una puntuale comparazione tra le informazioni fornite dal cliente e le eventuali informazioni acquisite autonomamente, nei limiti del possibile, anche con riguardo ad eventuali precedenti operazioni con il medesimo cliente.

Altro dato che merita approfondimento, nel caso di adeguata verifica rafforzata, è quello relativo alla **verifica della provenienza dei fondi** e delle risorse nella disponibilità del cliente, sulla base di informazioni acquisite o possedute in ragione dell'esercizio dell'attività.

Qualora il rapporto con il cliente si protragga per una certa durata sarà necessario verificare anche il suo **complessivo comportamento**, vale a dire se la sua operatività nel tempo presenta caratteri di anomalia, ed anche qui, se non siamo in regime di adeguata verifica semplificata, occorre acquisire informazioni relative alla provenienza dei fondi e delle risorse nella sua disponibilità, sia pure sempre nell'ambito di quelle informazioni pertinenti alla attività del notaio.

GLI OBBLIGHI DI ASTENSIONE E SEGNALAZIONE

ASTENSIONE E SEGNALAZIONE PER LE OPERAZIONI SOSPETTE (art. 35 comma 2)

In presenza degli elementi di sospetto di cui al comma 1, i soggetti obbligati non compiono l'operazione fino al momento in cui non hanno provveduto ad effettuare la segnalazione di operazione sospetta. Sono fatti salvi i casi in cui l'operazione debba essere eseguita in quanto **sussiste un obbligo di legge di ricevere l'atto** ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini. **In dette ipotesi, i soggetti obbligati, dopo aver ricevuto l'atto o eseguito l'operazione, ne informano immediatamente la UIF.**

Nel caso in cui la prestazione richiesta al notaio non consista in una stipula, non sussiste la deroga dall'obbligo di astensione, e pertanto occorrerà, in presenza di sospetto, prima effettuare la segnalazione e, solamente dopo sarà possibile rendere la prestazione; ovviamente, come vedremo, occorre però che si sia compiuta positivamente l'adeguata verifica, altrimenti permarrebbe l'obbligo di astensione.

ASTENSIONE E SEGNALAZIONE PER LA MANCATA ADEGUATA VERIFICA (art. 42)

1. I soggetti obbligati che si trovano **nell'impossibilità oggettiva di effettuare l'adeguata verifica** della clientela, ai sensi delle disposizioni di cui all'articolo 19, comma 1, lettere a), b) e c), si astengono dall'instaurare, eseguire ovvero proseguire il rapporto, la prestazione professionale e le operazioni e valutano se effettuare una segnalazione di operazione sospetta alla UIF a norma dell'articolo 35.

2. I soggetti obbligati si astengono dall'instaurare il rapporto continuativo, eseguire operazioni o prestazioni professionali e pongono fine al rapporto continuativo o alla prestazione professionale già in essere di cui siano, direttamente o indirettamente, parte **società fiduciarie, trust, società anonime o controllate attraverso azioni al portatore aventi sede in Paesi terzi ad alto rischio**. Tali misure si applicano anche nei confronti delle ulteriori entità giuridiche, altrimenti denominate, aventi sede nei suddetti Paesi, di cui non è possibile identificare il titolare effettivo né verificarne l'identità.

3. I professionisti sono esonerati dall'obbligo di cui al comma 1, limitatamente ai casi in cui esaminano la posizione giuridica del loro cliente o espletano compiti di difesa o di rappresentanza del cliente in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, compresa la consulenza sull'eventualità di intentarlo o evitarlo.

4. È fatta in ogni caso salva l'applicazione dell'articolo 35, comma 2, nei casi in cui l'operazione debba essere eseguita in quanto **sussiste un obbligo di legge di ricevere l'atto**.

Per i notai non vi sono sostanziali cambiamenti, salvo che ora la segnalazione sembrerebbe pressoché automatica in caso di mancata o incompleta adeguata verifica, per effetto del richiamo fatto dal comma 4 dell'art. 42, che sembrerebbe non consentire una valutazione sulla opportunità o meno di effettuare la segnalazione; ciò potrebbe avere un rilevante impatto sull'attività notarile, in quanto, per effetto del rilevato difetto di coordinamento con la legge

notarile, in punto di modalità di identificazione del cliente, una lettura pedissequa della norma porterebbe a far ritenere incompleta l'adeguata verifica in tutti i casi in cui non si sia acquisito un valido documento di identità del cliente o dell'esecutore.

Va altresì rilevato che **le operazioni che investono fiduciarie, trust, società anonime o simili con sede in Paesi terzi ad alto rischio, devono essere segnalate pressoché automaticamente**.

Occorre ancora ricordare che **l'esonero dall'obbligo di astensione è limitato ai casi in cui sussiste un obbligo di legge di ricevere l'atto**, vale a dire quando la prestazione richiesta al notaio è un atto notarile; analoga deroga non vige per i casi in cui il notaio sia chiamato quale professionista per l'assistenza alla stipula di atti di natura privata, o per mere attività di consulenza.

Infine, come già rilevato, per valutare la sussistenza di un obbligo di astensione, della relativa deroga e del successivo obbligo automatico di segnalazione, occorre che si siano verificati i presupposti del conferimento dell'incarico e dell'esistenza di una prestazione professionale, in quanto le attività prodromiche esulano dal perimetro di applicazione della normativa ai sensi dell'art. 18, comma 4, che esonera da tutte le attività di adeguata verifica (salvo la mera identificazione) il professionista fin quando esamina la posizione giuridica del cliente; quindi, fermo restando che le operazioni di adeguata verifica possono avere un inizio antecedente (quanto meno per l'identificazione), dovrebbe ritenersi che il termine ultimo per la loro conclusione coincide, nel caso di atto notarile, con la stipula; l'obbligo di astensione, e la relativa deroga per gli atti notarili, non possono ragionevolmente quindi che essere riferiti al momento della stipula.

Nulla è mutato in ordine alle modalità di segnalazione delle operazioni sospette, ed in ordine alla possibilità di avvalersi dell'intermediazione del Consiglio Nazionale del Notariato, mentre infine la disciplina del nuovo D.Lgs. pare rafforzare ulteriormente la tutela dell'anonimato del segnalante; ciò dovrebbe indurre ad un minore timore nell'affrontare tale adempimento, anche nella considerazione che, a dieci anni dall'entrata in vigore della disciplina, non si sono segnalati episodi rilevanti di perdita di segretezza; conclusivamente è condivisibile la buona prassi di effettuare la segnalazione ogni qualvolta sia presente un ragionevole sospetto.

GLI OBBLIGHI DI CONSERVAZIONE E REGISTRAZIONE[8]

La prima rilevante novità è l'abolizione del registro della clientela, che, peraltro, era raramente utilizzato nella normale operatività dello studio notarile.

Viene ribadita l'equivalenza della conservazione informatica rispetto alla conservazione cartacea, e, intuitivamente, si possono utilizzare, per lo stesso fascicolo, i due metodi di conservazione alternativamente e congiuntamente; vale a dire, si possono conservare i documenti in parte in modalità cartacea ed in parte in modalità informatica; i documenti informatici devono comunque essere conservati in modalità non modificabile (statica).

Mentre i dati e le informazioni possono essere conservati in copia semplice, le scritture e le registrazioni inerenti le operazioni vanno conservati in originale o in copia autentica.

Per i dati relativi alla operazione, vale a dire la data di conferimento dell'incarico, la data dell'operazione, la natura e l'importo, il riferimento principale sarà il repertorio notarile.

E' da osservare che il sistema informatico dello studio notarile, per essere ritenuto idoneo alla conservazione ai fini della normativa in oggetto, dovrà essere munito di un sistema di controllo degli accessi, ed essere dotato di un valido sistema di protezione contro la perdita dei dati (antivirus e backup), mentre non sembrerebbero applicabili agli studi notarili, non essendo per loro natura deputati alla registrazione di operazioni, bensì di conservazione documentale, le disposizioni in materia di verifica della storicità delle operazioni.

Alla conservazione è dedicato il Capo V delle Regole Tecniche, e più precisamente le regole tecniche n. 9 e 10, di seguito riportate.

---

[8] Art. 31. Obblighi di conservazione

1. I soggetti obbligati conservano i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio e a consentire lo svolgimento delle analisi…

2. Per le finalità di cui al comma 1, i soggetti obbligati conservano copia dei documenti acquisiti in occasione dell'adeguata verifica della clientela e l'originale ovvero copia avente efficacia probatoria ai sensi della normativa vigente, delle scritture e registrazioni inerenti le operazioni. La documentazione conservata deve consentire, quanto meno, di ricostruire univocamente: a) la data di instaurazione del rapporto continuativo o del conferimento dell'incarico; b) i dati identificativi del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione; c) la data, l'importo e la causale dell'operazione; d) i mezzi di pagamento utilizzati.

3. I documenti, i dati e le informazioni acquisiti sono conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale.

Art. 32. Modalità di conservazione dei dati e delle informazioni

1. I soggetti obbligati adottano sistemi di conservazione dei documenti, dei dati e delle informazioni idonei a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità di cui al presente decreto.

2. Le modalità di conservazione adottate devono prevenire qualsiasi perdita dei dati e delle informazioni ed essere idonee a garantire la ricostruzione dell'operatività o attività del cliente nonché l'indicazione esplicita dei soggetti legittimati ad alimentare il sistema di conservazione e accedere ai dati e alle informazioni ivi conservati. Le predette modalità devono, altresì, assicurare: a) l'accessibilità completa e tempestiva ai dati e alle informazioni da parte delle autorità di cui all'articolo 21, comma 4, lettera a); b) la tempestiva acquisizione, da parte del soggetto obbligato, dei documenti, dei dati e delle informazioni, con indicazione della relativa data. E' considerata tempestiva l'acquisizione conclusa entro trenta giorni dall'instaurazione del rapporto continuativo o dal conferimento dell'incarico per lo svolgimento della prestazione professionale, dall'esecuzione dell'operazione o della prestazione professionale, dalla variazione e dalla chiusura del rapporto continuativo o della prestazione professionale; c) l'integrità dei dati e delle informazioni e la non alterabilità dei medesimi successivamente alla loro acquisizione; d) la trasparenza, la completezza e la chiarezza dei dati e delle informazioni nonché il mantenimento della storicità dei medesimi.

Art. 34. Disposizioni specifiche

2. Il fascicolo del cliente, conforme a quanto prescritto dagli articoli 31 e 32, e la custodia dei documenti, delle attestazioni e degli atti presso il notaio nonché la tenuta dei repertori notarili, a norma della legge 16 febbraio 1913, n. 89 , del regolamento di cui al regio decreto 10 settembre 1914, n. 1326 , e successive modificazioni, e la descrizione dei mezzi di pagamento ai sensi dell'articolo 35, comma 22 , decreto-legge 4 luglio 2006, n. 223 , convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248 costituiscono idonea modalità di conservazione dei dati e delle informazioni

REGOLA TECNICA N. 9

La conservazione, può essere sia cartacea che informatica. Il fascicolo cartaceo del cliente può rimandare ad alcuni documenti conservati elettronicamente come, a titolo esemplificativo, visure tratte dai pubblici registri conservate in formato statico e non modificabile così come fornite dal registro pubblico consultato, nel sistema informatico dello studio. Non vi è alcun limite, dunque, alla possibilità di avvalersi di modalità di conservazione dei documenti, dei dati e delle informazioni informatici piuttosto che cartacei, purché i soggetti obbligati adottino sistemi di conservazione idonei a garantire il rispetto dei principi di cui agli articoli 31 e 32 d.lgs. n. 231/07, delle norme dettate dal codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità di cui al citato decreto.
Le modalità di conservazione, in concreto, devono essere adottate in modo da prevenire qualsiasi perdita di dati e di informazioni ed essere idonee a garantire la ricostruzione dell'operatività o attività del cliente ai sensi di quanto disposto all'articolo 32, comma 2, del novellato D.Lgs. n. 231/2007.

REGOLA TECNICA N. 10

I sistemi di protezione contro la perdita dei dati e delle informazioni, quelli di autenticazione ed autorizzazione adottati per l'accesso al sistema informatico dello studio ed al relativo archivio cartaceo costituiscono idonea modalità di conservazione ai sensi dell'art. 32 del D.Lgs. n. 231/2007, come modificato dal D.Lgs. n. 90/2017. L'integrità dei dati e delle informazioni e la non alterabilità dei medesimi successivamente alla loro acquisizione si considera garantita qualora gli stessi si ricavino da un documento informatico conservato in formato statico e non modificabile o siano desumibili da un documento analogico correttamente conservato ai sensi della Legge notarile o ai sensi del D.P.R. n. 445/2000.

ANTIRICICLAGGIO

LE REGOLE TECNICHE DEL C.N.N. E LE BUONE PRASSI ORGANIZZATIVE

Notai Vincenzo Gunnella e Laura Piffaretti

Bergamo – 16 novembre 2018

QUADRO NORMATIVO

L'impianto normativo in materia di antiriciclaggio si basa, prima di tutto, sulla **Quarta Direttiva UE (2015/849)** del 20 maggio 2015.

Per recepirne i contenuti è intervenuta la **Legge Delega 12 agosto 2016 n. 170**, in esecuzione della quale il Governo ha emanato il **Decreto Legislativo Delegato 25 maggio 2017 n.90**; la tecnica prescelta dal Legislatore è stata quella di non abrogare il precedente testo normativo (D. Lgs. 21 novembre 2007 n.231), ma di intervenire sostituendone integralmente l'articolato, ed abrogandone gli allegati tecnici.

Peraltro, è stata pubblicata sulla G.U. dell'UE il 19 giugno 2018 la Direttiva UE 2018/843, che interviene a modificare alcuni articoli della IV Direttiva, anche se, per quanto riguarda la nostra professione, non in maniera rilevante; il termine per l'adeguamento della normativa interna è dato al 10 gennaio 2020.

La prima osservazione che emerge dall'esame del D. Lgs. 90/2017 è che si è deciso di mantenere un unico impianto normativo sia in materia di obblighi, anche organizzativi, dei soggetti coinvolti, sia in materia di sanzioni, non differenziandolo tra i soggetti di area bancaria e finanziaria ed i professionisti, come invece era stato richiesto con forza dalle categorie professionali.

Una delle principali critiche volte al precedente articolato del decreto 231/2007, era, infatti, quella di essere una normativa nata per destinatari con una forte specificità (principalmente i soggetti di area bancaria e finanziaria), poi estesa anche a soggetti differenti, con adeguamenti del tutto insufficienti: le sanzioni non erano differenziate nel loro ammontare tra gli intermediari finanziari e i professionisti, il dettato normativo era eccessivamente generico per quanto attiene ai confini degli obblighi imposti ai destinatari, in particolare gli obblighi di adeguata verifica e di segnalazione; infine, tutto l'impianto normativo sembrava presupporre una possibilità, per il soggetto obbligato di dotarsi di una struttura organizzativa dedicata per poter assolvere al meglio ai suoi doveri.

Va, tuttavia, riconosciuto che il Decreto Delegato ha cercato di porre un rimedio a questi difetti, operando una precisa scelta di politica legislativa, che tuttavia non deriva né dalla direttiva comunitaria né dalla legge delega: si è deciso di delegare alle autorità di vigilanza (per i soggetti di

area bancaria e finanziaria) ed agli organismi di autoregolamentazione (per i professionisti), il compito di integrare la norma primaria ed adeguarla alle specificità dei singoli soggetti obbligati; ciò in particolare con riferimento all'adozione di presìdi e metodologie volti ad individuare ed a mitigare il rischio di riciclaggio, e ad organizzare la propria struttura per assolvere agli obblighi di adeguata verifica, di registrazione e di conservazione.

Oltre a questa normativa regolamentare proveniente dall'organismo di autoregolamentazione, il quadro normativo cui in concreto il soggetto obbligato dovrà riferirsi, è completato da un ulteriore livello di regole più di dettaglio, di produzione per così dire endogena: la norma prevede infatti che i soggetti obbligati effettuino una valutazione concreta dei rischi a cui la propria struttura è esposta e si organizzino di conseguenza, dandosi regole interne e protocolli operativi.

Riassumendo, il quadro normativo viene ad essere composto da:

a) la Direttiva Comunitaria, da leggersi unitamente ai suoi Considerando, e dalla quale andranno estrapolati i Principi Generali della materia, che sono di diretta applicazione, avendo contenuto precettivo[1];
b) la legge delega ed il decreto legislativo delegato;
c) le Regole Tecniche, emanate da parte dell'organismo di autoregolamentazione, previo parere favorevole del Comitato di Sicurezza Finanziaria:
d) le circolari ministeriali;
e) le linee guida e le direttive interne, proprie di ogni singolo soggetto obbligato, e rivolte alla sua stessa struttura.

In materia di modalità applicative da seguire nell'esecuzione dell'adeguata verifica, il primo riferimento naturale è il testo del Decreto Delegato; trattandosi di normativa di recepimento di direttiva comunitaria, hanno comunque rilevanza anche i principi generali della materia, nonché il dettato della legge delega; il Decreto Delegato poi, dovendosi riferire a soggetti del tutto eterogenei fra loro, rimanda, come si è detto, per concretizzare il suo precetto, da un lato, alla autovalutazione che il soggetto obbligato è tenuto a compiere in ordine al rischio cui la sua attività è esposta ed alla definizione di conseguenti protocolli organizzativi interni, e dall'altro, alle regole tecniche che l'organismo di autoregolamentazione (nel caso del professionista) adotta per definire sia le modalità di esecuzione dell'adeguata verifica che le procedure interne da adottare in funzione del rischio.

[1] Nel testo del Decreto è l'articolo 2 che definisce i principi, che vengono poi declinati nel corpo di successivi articoli:

a) **Proporzionalità** - le misure da adottare per adempiere agli obblighi devono essere proporzionate sia in rapporto all'attività dimensioni e complessità dell'obbligato che in rapporto al rischio in relazione al tipo di cliente, al rapporto continuativo, alla prestazione professionale, al prodotto o alla transazione (art. 8 della Direttiva)

(Art. 16, comma 1) I soggetti obbligati adottano i presidi e attuano i controlli e le procedure, adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi di riciclaggio...

b)**Circoscrizione dell'attenzione alle circostanze conosciute in ragione delle funzioni esercitate -** Il soggetto obbligato deve tener conto dei dati e delle informazioni acquisiti o posseduti nell'esercizio della propria attività istituzionale o professionale (art. 18 comma 1, lett. d))

c) **Approccio basato sul rischio** - v. Art. 22 Considerando, art. 8 Direttiva, numerosi articoli del D.Lvo

I SOGGETTI COINVOLTI
(nell'ambito dell'organizzazione del notariato)

1) IL CONSIGLIO NAZIONALE DEL NOTARIATO

L'organo esponenziale della categoria (organismo di autoregolamentazione), come si evince dalla lettura delle norme[2], ha il compito di adottare regole tecniche che riguardano:
a) l'adeguata verifica, in particolare per definire ambito di applicazione e modalità di esecuzione dell'adeguata verifica semplificata;
b) la conservazione;

[2] Art.1 - Definizioni

2. aa) organismo di autoregolamentazione

l'ente esponenziale, rappresentativo di una categoria professionale, ivi comprese le sue articolazioni territoriali e i consigli di disciplina cui l'ordinamento vigente attribuisce poteri di regolamentazione, di controllo della categoria, di verifica del rispetto delle norme che disciplinano l'esercizio della professione e di irrogazione, attraverso gli organi all'uopo predisposti, delle sanzioni previste per la loro violazione.

Art. 11

2. Gli organismi di autoregolamentazione sono responsabili dell'elaborazione e aggiornamento di regole tecniche, adottate in attuazione del presente decreto previo parere del Comitato di sicurezza finanziaria, in materia di procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo cui i professionisti sono esposti nell'esercizio della propria attività, di controlli interni, di adeguata verifica, anche semplificata della clientela e di conservazione .....

Art.15

1. Gli organismi di autoregolamentazione dettano criteri e metodologie, commisurati alla natura dell'attività svolta e alle dimensioni dei soggetti obbligati, per l'analisi e la valutazione dei rischi di riciclaggio e di finanziamento del terrorismo, cui sono esposti nell'esercizio della loro attività.

2. I soggetti obbligati, adottano procedure oggettive e coerenti rispetto ai criteri e alle metodologie di cui al comma 1, per l'analisi e la valutazione dei rischi di riciclaggio e di finanziamento del terrorismo.

4. La valutazione di cui al comma 2 è documentata, periodicamente aggiornata e messa a disposizione degli organismi di autoregolamentazione, ai fini dell'esercizio delle rispettive funzioni e dei rispettivi poteri in materia di prevenzione del riciclaggio e di finanziamento del terrorismo.

Art.16

2. Gli organismi di autoregolamentazione, ai sensi dell'articolo 11, comma 2, individuano i requisiti dimensionali e organizzativi in base ai quali i soggetti obbligati, rispettivamente vigilati e controllati adottano specifici presidi, controlli e procedure per:

a) la valutazione e gestione del rischio di riciclaggio e di finanziamento del terrorismo;

b) l'introduzione di una funzione antiriciclaggio, ivi comprese, se adeguate rispetto alle dimensioni e alla natura dell'attività, la nomina di un responsabile della funzione antiriciclaggio e la previsione di una funzione di revisione indipendente per la verifica delle politiche, dei controlli e delle procedure.

c) le procedure e metodologie di analisi e valutazione del rischio e di controlli interni; nel dettaglio dovranno essere individuati requisiti dimensionali e organizzativi per mettere in grado i soggetti obbligati di auto-valutare e gestire il rischio di riciclaggio.

2) I CONSIGLI NOTARILI DISTRETTUALI

Le articolazioni periferiche degli organismi di categoria, hanno il compito di:
a) adottare misure idonee a sanzionare l'inosservanza delle regole tecniche in materia di procedure e metodologie di analisi e valutazione del rischio;
b) applicare sanzioni disciplinari a fronte di violazioni gravi, ripetute o sistematiche, ovvero plurime: si tratta di attività ordinaria del consiglio distrettuale che venga a conoscenza di tali violazioni nell'ambito della sua attività istituzionale;
c) comunicare annualmente i dati dei procedimenti disciplinari: i dati devono essere tempestivamente comunicati al consiglio nazionale, affinché questi possa a sua volta comunicarli al CSF entro il 30 marzo di ogni anno;
d) effettuare, insieme al Consiglio Nazionale del Notariato, la formazione per i propri iscritti.

2) IL NOTAIO

Il Notaio:
a) adotta procedure oggettive e coerenti per l'analisi e la valutazione del rischio, il che tradotto in termini pratici, vuol dire effettuare una valutazione interna delle proprie procedure;
b) adotta i presidi e attua i controlli e le procedure adeguati: in sostanza deve definire delle linee guida e dei protocolli operativi interni alla sua struttura;
c) documenta periodicamente al suo consiglio distrettuale di avere effettuato la valutazione ed adottato i presidi;
d) forma il suo personale.

L'ADEGUATA VERIFICA IN GENERALE

Perimetro di applicazione e obbligo di adeguata verifica - Regola Tecnica n.1

REGOLA TECNICA N. 1

Non rientrano tra le operazioni di cui all'art. 3, comma 4, lettera c) del D.Lgs. 231 del 2007 novellato tutti i negozi di natura non patrimoniale.
Alla luce di ciò, fermo restando l'approccio *risk based* e l'accertamento della concreta natura non patrimoniale dell'operazione, è possibile enucleare un elenco, indicativo e non esaustivo, riferito all'attività notarile di prestazioni professionali escluse dal novero di quelle che fanno sorgere gli obblighi di adeguata verifica:
- gli atti notori;
- gli atti *mortis causa*;
- la pubblicazione di testamento;
- il passaggio nel fascicolo degli atti tra vivi del testamento pubblico;
- la costituzione di fondo patrimoniale senza trasferimento di beni;
- le convenzioni matrimoniali, in quanto atti meramente programmatici;
- le rinunce meramente abdicative;
- il verbale di apertura di una cassetta di sicurezza;
- gli inventari in generale;
- la levata del protesto (in quanto atto di accertamento che non implica alcuna movimentazione di denaro), restando invece soggetto agli obblighi antiriciclaggio il servizio di "cassa cambiali", salvo la possibilità di ricevere pagamenti superiori alle soglie limite di utilizzo del denaro contante, come precisato nella nota MEF dell'8 aprile 2009, prot. 28107.

Per le procure ed i mandati, è da ritenere che esse diano luogo al sorgere degli obblighi di adeguata verifica se generali, ovvero se contengono un'espressa autorizzazione a contrarre con se stessi, se sono irrevocabili o a termine, ovvero se sono conferite per il compimento di un atto giuridico avente ad oggetto mezzi di pagamento, beni o utilità di valore pari o superiore ad 15.000 euro ovvero di valore non determinato o determinabile.

La Regola Tecnica n.1 interviene a chiarire la portata dell'art. 3 comma 4, lettera c), che definisce il perimetro di applicazione della normativa ai notai, da leggere, per quanto attiene all'insorgenza degli obblighi di adeguata verifica, in uno con l'art. 17, comma 1.
Secondo l'art. 3, comma 4, lettera c), la normativa si applica ai notai quando compiono operazioni[3] finanziarie o immobiliari in nome o per conto dei propri clienti, o quando li assistono nella predisposizione o nella realizzazione di una serie di operazioni economiche, tra le quali il trasferimento di diritti reali su immobili o realtà economiche, e la costituzione di società, enti, trust, o soggetti giuridici analoghi.
Se la prestazione rientra nel perimetro di applicazione della normativa, l'art. 17 comma 1 fa sorgere l'obbligo di procedere all'adeguata verifica in occasione del conferimento dell'incarico per l'esecuzione della prestazione professionale[4].
Opportunamente la Regola Tecnica n.1 chiarisce che sono esclusi dal perimetro di applicazione della normativa "tutti i negozi di natura non patrimoniale"; a fortiori devono parimenti intendersi esclusi tutti gli atti notarili aventi contenuto non negoziale.
Va comunque rimarcato che in tutte tali ipotesi, in base alla legge notarile una serie di adempimenti in ordine alla identificazione delle parti ed all'adeguamento della loro volontà a norme di legge è comunque sempre dovuta.
I casi di esenzione dall'obbligo di adeguata verifica sono disciplinati dall'Art.17 comma 7 (Gli obblighi di adeguata verifica della clientela non si osservano in relazione allo svolgimento

[3] Dalle Definizioni contenute nell'art.1: l'attività consistente nella movimentazione, nel trasferimento o nella trasmissione di mezzi di pagamento o nel compimento di atti negoziali a contenuto patrimoniale; costituisce operazione anche la stipulazione di un atto negoziale, a contenuto patrimoniale, rientrante nell'esercizio dell'attività professionale o commerciale
[4] Dalle Definizioni contenute nell'art.1: una prestazione intellettuale o commerciale resa in favore del cliente, a seguito del conferimento di un incarico, della quale si presume che abbia una certa durata;

dell'attività di mera redazione e trasmissione ovvero di sola trasmissione delle dichiarazioni derivanti da obblighi fiscali) e dall'art.18 comma 4 (Fermi gli obblighi di identificazione, i professionisti, limitatamente ai casi in cui esaminano la posizione giuridica del loro cliente ..., sono esonerati dall'obbligo di verifica dell'identità del cliente e del titolare effettivo fino al momento del conferimento dell'incarico).

Gli elementi di cui si compone l'adeguata verifica - Art.18

a) l'identificazione del cliente e la verifica della sua identità [5] - Regola Tecnica n. 7

REGOLA TECNICA N. 7

Nelle ipotesi in cui ricorra un basso rischio di riciclaggio e di finanziamento del terrorismo, esista, ai sensi dell'ordinamento vigente, l'obbligo per il notaio di ricevere l'atto ed egli sia certo, ai sensi della legge 16 febbraio 1913, n. 89 dell'identità personale del cliente o dell'esecutore, la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo, fermo l'obbligo di acquisizione dei dati identificativi, può essere posticipata ad un momento successivo al conferimento dell'incarico per lo svolgimento della prestazione professionale, secondo quanto prescritto dall'articolo 18, comma 3, d.lgs. n. 231/07.
In dette ipotesi, l'indisponibilità di un documento di riconoscimento in corso di validità costituisce presupposto per l'effettuazione, da parte del notaio, dell'aggiornamento dei dati e delle informazioni necessarie all'adeguata verifica della clientela, senza rappresentare, di per sé elemento idoneo e sufficiente a fondare un sospetto meritevole di segnalazione, in assenza di concomitanti ulteriori evidenze relative al profilo soggettivo del cliente o a quello oggettivo della prestazione.
In caso di prestazioni professionali non occasionali, il notaio provvederà ad aggiornare i documenti di identità in base al rischio: ogni 2 anni se a basso rischio, ogni anno se a rischio ordinario, con frequenza inferiore e comunque calibrata al rischio, per le ipotesi di elevato rischio di riciclaggio e di finanziamento del terrorismo.
Ai sensi dell'articolo 19, comma 1, lettera a) l'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, per i clienti i cui dati identificativi risultino da atti pubblici o da scritture private autenticate.
Nel caso in cui sia materialmente impossibile, per il notaio, effettuare l'adeguata verifica e fuori dalle ipotesi in cui sussista l'obbligo giuridico di ricevere l'atto, egli deve astenersi dall'esecuzione della prestazione e valutare se sussistano gli estremi per l'effettuazione di una segnalazione di operazioni sospette alla UIF, senza che possa ravvisarsi alcun automatismo tra astensione e segnalazione.
Ai sensi del combinato disposto dell'art. 18, comma 1, lett. a), e dell'art. 19, comma1, lettera a) n. 1 del D.Lgs. n. 231/2007 gli atti notarili da cui risultano i dati identificativi dei soggetti persone fisiche o non fisiche sono sempre considerati una fonte affidabile e indipendente ai fini dell'espletamento degli obblighi di adeguata verifica e ciò anche nel caso di intervento in atto di un

[5] attraverso riscontro di un documento d'identità o di altro documento di riconoscimento equipollente ai sensi della normativa vigente nonché sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. Le medesime misure si attuano nei confronti dell'esecutore, anche in relazione alla verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente

esecutore dotato di procura notarile.
Ai sensi del degli articoli 18, comma 1, lettera a) e 19, comma 1, lettera a) n. 1, il solo obbligo di identificazione del cliente può ritenersi assolto, senza la presenza fisica del medesimo, per i clienti i cui dati identificativi risultino, tra gli altri, da atti pubblici o scritture private autenticate e che, ai sensi del citato articolo 18, comma 1, lettera a), l'identificazione dell'esecutore non si esaurisce nel riscontro dei rispettivi dati identificativi ma abbraccia la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome del cliente.

L'**identificazione**, attività sempre obbligatoria, deve essere effettuata in presenza del cliente (ovvero dell'esecutore) che deve esibire un **documento di identità** per consentire al soggetto obbligato di acquisire i suoi dati identificativi[6]; l'identificazione del titolare effettivo, invece, non richiede né la presenza fisica del medesimo né l'acquisizione del suo documento di identità;

l'identificazione può anche essere effettuata, senza la presenza fisica del cliente, in alcuni casi previsti nell'art. 19, tra i quali il caso in cui i dati identificativi del cliente risultano da un atto pubblico o una scrittura privata autenticata (è il caso ad esempio della **procura notarile** conferita all'esecutore) ed il caso in cui il soggetto obbligato abbia già provveduto, per altra prestazione, all'identificazione;

l'identificazione può anche essere compiuta attraverso dipendenti o collaboratori, e **il documento deve essere acquisto in copia** (cartacea o informatica), salvo, appunto, il caso dell'acquisizione dei dati identificativi da altro atto notarile.

La verifica dell'identità del cliente (e ciò vale anche per il titolare effettivo), è una **attività eventuale**, da compiersi solo quando sussistono dubbi, incongruenze e incertezze in ordine alla veridicità dei dati e dei documenti acquisiti all'atto della identificazione; con riferimento ai clienti diversi dalle persone fisiche e ai fiduciari di trust espressi, la verifica dell'identità del titolare effettivo impone l'adozione di misure, commisurate alla situazione di rischio, idonee a comprendere la struttura di proprietà e di controllo del cliente.

La Regola Tecnica n. 7 viene a colmare, almeno in parte, un difetto di coordinamento tra la legge notarile ed il nuovo decreto[7], dall'altro chiarisce che resta rimessa alla valutazione del notaio l'opportunità di effettuare una segnalazione di operazione sospetta qualora non riesca ad acquisire il documento di identità del cliente o dell'esecutore, avendo, tuttavia, raggiunto la certezza sull'identità personale del medesimo secondo la normativa di settore del Notariato.

Occorre ricordare che, infatti, è stato abrogato l'allegato tecnico al vecchio testo del D.Lvo 231/07, che, all'art. 3, prevedeva che l'identificazione potesse essere svolta anche da un "pubblico ufficiale a ciò abilitato", con ciò dando una logica soluzione di sistema alle ipotesi in cui il notaio fosse comunque certo dell'identità personale del cliente, pur non disponendo di un documento di identità.

[6] Dalle Definizioni dell'art.1: il nome e il cognome, il luogo e la data di nascita, la residenza anagrafica e il domicilio, ove diverso dalla residenza anagrafica, gli estremi del documento di identificazione e, ove assegnato, il codice fiscale o, nel caso di soggetti diversi da persona fisica, la denominazione, la sede legale e, ove assegnato, il codice fiscale.

La Regola Tecnica n.7 indica che il notaio potrà procedere alla stipula, pur in assenza del documento di identità; ove ritenesse di dover procedere alla verifica dell'identità del cliente, dell'esecutore o del titolare effettivo, potrà farlo in un secondo momento, come previsto dall'art. 18, comma 3; in ogni caso il notaio, ricorda la Regola Tecnica n.7, dovrà aggiornare i dati identificativi, e, in presenza di clienti ricorrenti (prestazioni professionali non occasionali), con ricorrenza calibrata al rischio.

E' importante rilevare che i dati identificativi possono essere rilevati, anche in assenza del cliente, da atti pubblici o scritture private autenticate, in quanto fonti affidabili ed indipendenti e ciò anche quando consistano in procure notarili.

Infine la Regola Tecnica n.7 chiarisce che l'impossibilità di completare la procedura di identificazione richiesta dall'art. 17, da un lato non impedisce di ricevere l'atto, se sussiste un obbligo per il notaio di riceverlo, e dall'altro non costituisce di per sè elemento idoneo e sufficiente a far nascere l'obbligo di segnalazione di operazione sospetta.

b) l'identificazione del titolare effettivo e la verifica della sua identità[8] - Regole Tecniche n. 5 e 6

REGOLA TECNICA N. 5

Ai fini dell'identificazione del titolare effettivo, rileva il disposto di cui all'articolo 19 comma 1 lettera a) ai sensi del quale il cliente, all'atto dell'identificazione, fornisce "le informazioni necessarie a consentire l'identificazione del titolare effettivo".

La verifica dell'identità del (cliente, dell'esecutore e) titolare effettivo, necessaria qualora sussistano dubbi, incertezze o incongruenze in relazione ai dati acquisiti in sede di identificazione, può essere effettuata, ai sensi dell'articolo 19, comma 1, lettera b) anche attraverso il riscontro di tali dati con quelli riportati da fonti attendibili e indipendenti. Con riferimento alla titolarità effettiva di imprese dotate di personalità giuridica, tenute all'iscrizione nel registro delle imprese, il riscontro dei dati acquisiti in sede di identificazione può avvenire anche attraverso l'accesso alla sezione del registro delle imprese, ad hoc istituita, ai sensi dell'articolo 21, d.lgs. n. 231/07.

Resta fermo quanto stabilito dal comma 7 del medesimo articolo 20 in ordine alla circostanza che la consultazione dei registri di cui al presente articolo non esonera i soggetti obbligati dal valutare il rischio di riciclaggio e finanziamento del terrorismo cui sono esposti nell'esercizio della loro attività e dall'adottare misure adeguate al rischio medesimo.

Fermo quanto sopra, e fermo restando che ai sensi dell'art. 19 del medesimo decreto, non si è tenuti all'acquisizione del documento di identità del titolare effettivo, qualora il titolare effettivo sia individuato attraverso la consultazione di pubblici registri, salva la valutazione del rischio e la conseguente applicazione di misure ad esso proporzionate, l'identificazione può essere ritenuta correttamente eseguita mediante la sola acquisizione dei dati e delle informazioni risultanti dai pubblici registri stessi, confermati nella loro validità dal cliente.

Ai fini dell'individuazione del titolare effettivo, nelle ipotesi in cui sia possibile la consultazione di un pubblico registro, tale consultazione è da ritenersi idonea ai fini dell'espletamento dell'obbligo di identificazione dello stesso titolare effettivo, salvo che ci si trovi in presenza di elementi oggettivi che mettano in dubbio o rendano palesemente incerti o incongrui i dati e le informazioni pubblicate.

Detti dati e informazioni sono, infatti, da ritenere affidabili a fronte dell'obbligo giuridico a carico dei responsabili delle imprese, persone giuridiche e trust, di comunicare notizie vere, aggiornate e complete, ferma restando la possibilità di acquisire, in funzione del rischio, ulteriori informazioni.

Ai sensi dell'articolo 18, comma 1, lettera b, l'identificazione del titolare effettivo deve essere attuata nel contesto dell'adozione di regole comportamentali proporzionate al rischio.

L'obbligo di identificazione del titolare effettivo può ritenersi assolto attraverso l'acquisizione delle informazioni fornite dal cliente (direttamente o tramite conferma, ove già acquisite o in possesso del notaio nel contesto del rapporto con il cliente) in ordine al nome, cognome, luogo e data di nascita del titolare effettivo, unitamente all'indicazione della fonte, attendibile e indipendente, da cui tali informazioni sono attinte.

REGOLA TECNICA N. 6

Fermo restando quanto previsto dall'articolo 20 d.lgs. n. 231/07 e successive modificazioni per l'individuazione del titolare effettivo di clienti diversi dalle persone fisiche, nelle società di persone e consorzi e negli enti privati non riconosciuti, può assumere rilievo, ai fini dell'individuazione del titolare effettivo, la figura della persona fisica che agisce quale tramite di essi, in qualità di legale rappresentante.

Nell'individuazione del titolare effettivo delle società di persone e consorzi, è consentita l'utilizzazione dei dati dei soci, risultanti dal Registro delle Imprese, salvo che sussistano dubbi, incertezze o incongruenze sull'identità dello stesso e salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni.

Nell'individuazione del titolare effettivo degli enti privati non riconosciuti, in assenza di indici che rivelino l'esistenza di associati che ne detengano di fatto il controllo, ovvero di beneficiari determinati, si farà riferimento ai soggetti titolari di funzioni di direzione e/o amministrazione.

E' l'art. 20 che detta i criteri per l'identificazione del titolare effettivo di soggetti diversi dalle persone fisiche[9], mentre l'art. 19 indica che è il cliente che deve fornire sotto la sua responsabilità,

[8] attraverso l'adozione di misure proporzionate al rischio ivi comprese, con specifico riferimento alla titolarità effettiva di persone giuridiche, trust e altri istituti e soggetti giuridici affini, le misure che consentano di ricostruire, con ragionevole attendibilità, l'assetto proprietario e di controllo del cliente;

[9] Nel caso in cui il cliente sia una società di capitali: a) costituisce indicazione di proprietà diretta la titolarità di una partecipazione superiore al 25 per cento del capitale del cliente, detenuta da una persona fisica; b) costituisce indicazione di proprietà indiretta la titolarità di una percentuale di partecipazioni superiore al 25 per cento del capitale del cliente, posseduto per il tramite di società controllate, società fiduciarie o per interposta persona.

Nelle ipotesi in cui l'esame dell'assetto proprietario non consenta di individuare in maniera univoca la persona fisica o le persone fisiche cui è attribuibile la proprietà diretta o indiretta dell'ente, il titolare effettivo coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile il controllo del medesimo in forza: a) del controllo della maggioranza dei voti esercitabili in assemblea ordinaria; b) del controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria; c) dell'esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante.

Qualora l'applicazione dei criteri di cui ai precedenti commi non consenta di individuare univocamente uno o più titolari effettivi, il titolare effettivo coincide con la persona fisica o le persone fisiche titolari di poteri di amministrazione o direzione della società.

Nel caso in cui il cliente sia una persona giuridica privata, sono cumulativamente individuati, come titolari effettivi: a) i fondatori, ove in vita; b) i beneficiari, quando individuati o facilmente individuabili; c) i titolari di funzioni di direzione e amministrazione.

al soggetto obbligato, tutte le informazioni necessarie a consentire l'identificazione del titolare effettivo.
Abbiamo già osservato che l'identificazione del titolare effettivo non richiede né la presenza fisica del medesimo né l'acquisizione del suo documento di identità, e che la verifica delle informazioni ricevute dal cliente è attività solo eventuale, da compiersi quando emergano dubbi o incongruenze.

La Regola Tecnica 5 conferma tali indicazioni e indica, in primis, come fonte attendibile ed indipendente da consultare per la verifica dell'identità del titolare effettivo, il "pubblico registro", ricordando che, in particolare, è istituita una sezione ad hoc del Registro delle Imprese ai sensi dell'art. 21 del D.Lvo 231/07.
Sempre la regola tecnica in questione, consente di procedere alla identificazione del titolare effettivo, mediante acquisizione dei dati del pubblico registro, confermati nella validità dal cliente, ovvero mediante acquisizione del nome, cognome, luogo e data di nascita, come forniti dal cliente direttamente o tramite conferma ove già acquisiti o in possesso del notaio nel contesto del rapporto con il cliente; vedremo in seguito come tale indicazione verrà coniugata, nel caso di adeguata verifica semplificata da eseguirsi per soggetti che per definizione possono definirsi a basso rischio, quali, tra gli altri, le Banche, i soggetti vigilati e le PA.

La Regola Tecnica n.6, invece, ha lo scopo di colmare un vuoto normativo in quanto nel nuovo decreto non sono rappresentate le modalità di individuazione del titolare effettivo per le società di persone ed i consorzi privi di personalità giuridica nonché per gli enti privati non riconosciuti.
Per i primi (società di persone e consorzi), coerentemente con quanto previsto nella regola tecnica n. 5, si prevede la possibilità di fare riscorso alle risultanze del Registro delle Imprese, nel quale risultano, in chiaro, le generalità dei soci e degli amministratori, consentendo in tal modo, il ricorso ad una fonte affidabile ed indipendente.
Per i secondi (enti privati non riconosciuti), si è previsto di verificare se emergano indici che rivelino l'esistenza di associati con posizione di controllo di fatto dell'ente ovvero di beneficiari determinati; in assenza di tali indici, si è previsto il ricorso ad un criterio coerente con quello adottato dal decreto per le persone giuridiche private, vale a dire, la titolarità di funzioni di amministrazione o direzione, stante la generale impossibilità di acquisire il dato del fondatore o del beneficiario.

Alcune osservazioni riassuntive a margine del dettato normativo come integrato dalle Regole Tecniche n.5 e 6:

a) Quando il cliente è una **persona fisica**, sia esso presente di persona o per il tramite di un procuratore (esecutore), è opportuno richiedere espressamente se agisce nel proprio esclusivo interesse o per conto di un terzo che non compare nell'atto ("titolare effettivo").
b) Quando il cliente **non è una persona fisica**, saremo **sempre** in presenza di un esecutore e dovremo sempre individuare un **titolare effettivo**; l'individuazione potrà essere effettuata, a discrezione del notaio, o richiedendo l'informazione relativa all'esecutore, ovvero attingendo a

pubblici registri o altra fonte affidabile e facendone confermare le risultanze all'esecutore; infatti la consultazione di un pubblico registro è da ritenersi idonea, trattandosi di fonte affidabile, salvo che le circostanze di fatto presenti al momento dell'identificazione possano far sorgere un dubbio o rendano palesemente incerti o incongrui i dati e le informazioni presenti nel registro.

c) I criteri per l'individuazione del titolare effettivo delle persone non fisiche sono in parte individuati in chiaro dalla norma (per le società di capitali e per le persone giuridiche private), in parte adombrati dalla norma in maniera non espressa (per i trust) ed in parte da ricavare per interpretazione (per tutti gli altri soggetti) sulla base della definizione contenuta nell'art. 20.1:
   - nell'individuazione del titolare effettivo delle società di persone e consorzi, appare consentita l'utilizzazione dei dati dei soci, risultanti dal Registro delle Imprese, salvo che sussistano dubbi, incertezze o incongruenze sull'identità dello stesso e salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni;
   - nell'individuazione del titolare effettivo degli enti privati non riconosciuti, in assenza di indici che rivelino l'esistenza di associati che ne detengano di fatto il controllo, ovvero di beneficiari determinati, si dovrebbe fare riferimento ai soggetti titolari di funzioni di direzione e/o amministrazione.
d) Resta fermo il principio per cui non è da ritenersi necessaria l'acquisizione del documento di identità del titolare effettivo, qualora il titolare effettivo sia individuato attraverso la consultazione di pubblici registri, in quanto l'identificazione può essere ritenuta correttamente eseguita mediante la sola acquisizione dei dati e delle informazioni risultanti dai pubblici registri stessi, confermati nella loro validità dal cliente.
e) Quando l'operazione coinvolge un trust, occorre anzitutto prendere in considerazione lo schema UIF relativo a queste fattispecie, per verificarne la fisiologicità. L'analisi richiederà l'esame della normativa di riferimento, e l'acquisizione di tutta la documentazione relativa alla costituzione ed al regolamento del Trust, dei dati identificativi di tutti i soggetti coinvolti e dei beni che costituiscono il fondo in trust; si potrà così giungere alla comprensione degli scopi perseguiti e concludere se si è in presenza di una struttura di natura fisiologica o patologica: è in questo senso che deve intendersi la lettura dell'art. 22, 5^ comma. Dall'esame della documentazione acquisita emergerà chi debba considerarsi "titolare effettivo" ai sensi del primo comma dell'art. 20.
f) Quando l'operazione coinvolge società fiduciarie che intervengono nell'esplicazione delle loro attività e quindi per conto di fiducianti, dovrà essere consentito al notaio di identificare i medesimi per poter eseguire i relativi adempimenti di adeguata verifica. Una notazione a parte va fatta per le Fiduciarie iscritte all'Albo di cui all'art. 106 TUB, che, in base al precedente testo del D.Lvo 231 erano considerate esentate da obblighi di adeguata verifica, al pari delle Banche; nel testo novellato tale esenzione è scomparsa sia per le Banche che per le Fiduciarie ex art. 106.

c) l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale[10] - Regola Tecnica n.4

REGOLA TECNICA N. 4

Sono considerate idonee misure semplificate di adeguata verifica della clientela l'acquisizione delle informazioni sullo scopo e sulla natura della prestazione effettuata in contestualità della stipula, mediante la richiesta delle medesime, fermo restando l'obbligo della loro valutazione da parte del notaio.
Allo scopo di definire l'idoneità delle misure semplificate di adeguata verifica della clientela nell'ambito dell'attività notarile, si precisa che lo scopo e la natura della prestazione professionale dei notai coincidono, per la quasi totalità dei casi, con il negozio giuridico oggetto dell'incarico, e che, a differenza delle operazioni finanziarie, negli atti notarili, scopo e natura delle prestazioni risultano manifesti nell'atto stesso, pertanto, salva diversa valutazione da parte del notaio, non è necessario formalizzare in autonomo documento l'acquisizione di tali informazioni dal cliente. Occorre comunque considerare le ipotesi di più atti, anche della stessa specie, che possono risultare collegati e rispetto alle quali va fatta salva la valutazione del complesso di operazioni compiute.

L'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto devono essere declinate in funzione del rischio, e di queste si tratterà in dettaglio in occasione dell'esposizione delle modalità di esecuzione dell'adeguata verifica semplificata o rafforzata.

Come vedremo, trattando delle varie modalità di esecuzione dell'adeguata verifica, occorre declinare variamente, nelle varie ipotesi, le informazioni sulla situazione economico-patrimoniale del cliente sono da acquisire in funzione del rischio, e comunque sono quelle acquisite o possedute in ragione dell'attività.
La Regola Tecnica n. 4, allo scopo di definire l'idoneità delle misure semplificate di adeguata verifica della clientela nell'ambito dell'attività notarile, parte dal presupposto che nell'ambito dell'attività dei notai lo scopo e la natura della prestazione professionale coincidono, per la quasi totalità dei casi, con il negozio giuridico oggetto dell'incarico, tenuto conto del fatto che, a differenza delle operazioni finanziarie, negli atti notarili, scopo e natura delle prestazioni risultano manifeste nell'atto stesso, e pertanto risulta superfluo formalizzare in autonomo documento l'acquisizione di tali informazioni dal cliente.

d) il controllo costante del rapporto con il cliente

Il controllo costante del rapporto va eseguito per tutta la sua durata, attraverso l'esame della complessiva operatività del cliente medesimo, la verifica e l'aggiornamento dei dati e delle informazioni acquisite nello svolgimento delle attività di adeguata verifica, anche riguardo, se necessaria in funzione del rischio, alla verifica della provenienza dei fondi e delle risorse nella

[10] per tali intendendosi, quelle relative all'instaurazione del rapporto, alle relazioni intercorrenti tra il cliente e l'esecutore, tra il cliente e il titolare effettivo e quelle relative all'attività lavorativa, salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni, ivi comprese quelle relative alla situazione economico-patrimoniale del cliente, acquisite o possedute in ragione dell'esercizio dell'attività. In presenza di un elevato rischio di riciclaggio e di finanziamento del terrorismo, i soggetti obbligati applicano la procedura di acquisizione e valutazione delle predette informazioni anche alle prestazioni o operazioni occasionali;

disponibilità del cliente, sulla base di informazioni acquisite o possedute in ragione dell'esercizio dell'attività.
Nel controllo costante, si esamineranno quindi la complessiva operatività del cliente, e, solo se necessario in funzione del rischio rilevato, la provenienza dei fondi, sempre sulla base delle informazioni acquisite o possedute in ragione dell'esercizio dell'attività

La tempistica dell'adeguata verifica - Regola Tecnica n.8

REGOLA TECNICA N. 8

Il termine ultimo per la conclusione delle operazioni di adeguata verifica coincide, nel caso di atto notarile, con la stipula del medesimo, che costituisce il momento ultimo per l'esecuzione degli adempimenti prescritti in funzione di adeguata verifica della clientela, fermo restando che il complesso dei presidi antiriciclaggio si attiva al momento del conferimento dell'incarico per lo svolgimento della prestazione professionale, secondo il combinato disposto delle definizioni di cui all'articolo 1, comma 2, lettere h) e gg) del D.Lgs. n. 231/2007, come modificato dal D.Lgs. n. 90/2017. L'incarico per la stipula non sempre viene conferito da tutte le parti dell'atto, congiuntamente e nello stesso momento, al notaio, che pertanto potrà effettuare gli adempimenti di adeguata verifica della clientela anche in momenti diversi, purché si concludano alla stipula, in quanto è in quel momento che lo stesso notaio può concludere la valutazione della prestazione professionale per cui l'incarico è stato conferito.
Ai sensi dell'art. 32, comma 2, lettera b), è comunque considerata tempestiva l'acquisizione dei dati e delle informazioni relativi all'adeguata verifica del cliente conclusa entro trenta giorni dall'instaurazione del rapporto continuativo o dal conferimento dell'incarico per lo svolgimento della prestazione professionale, dall'esecuzione dell'operazione o della prestazione professionale, dalla variazione e dalla chiusura del rapporto continuativo o della prestazione professionale.

L'art.18 indica[11] che le attività di identificazione e verifica dell'identità vanno compiute **prima del conferimento dell'incarico**, ma che, in presenza di basso rischio, e qualora ciò sia funzionale all'ordinato svolgimento dell'attività del soggetto obbligato, possono essere posticipate nel loro completamento fino a trenta giorni.

[11] 2. Le attività di identificazione e verifica dell'identità del cliente, dell'esecutore e del titolare effettivo, di cui alle lettere a) e b) del comma 1, sono effettuate prima ... del conferimento dell'incarico per lo svolgimento di una prestazione professionale ovvero prima dell'esecuzione dell'operazione occasionale.
3. In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo può essere posticipata ad un momento successivo all'instaurazione del rapporto o al conferimento dell'incarico per lo svolgimento di una prestazione professionale, qualora ciò sia necessario a consentire l'ordinaria gestione dell'attività oggetto del rapporto. In tale ipotesi, i soggetti obbligati, provvedono comunque all'acquisizione dei dati identificativi del cliente, dell'esecutore e del titolare effettivo e dei dati relativi alla tipologia e all'importo dell'operazione e completano le procedure di verifica dell'identità dei medesimi al più presto e, comunque, entro trenta giorni dall'instaurazione del rapporto o dal conferimento dell'incarico.

Nel caso dell'attività notarile è ragionevole ritenere che il **termine ultimo** per l'esecuzione delle operazioni di adeguata verifica coincide con la **stipula**, che viene a costituire quindi il momento in cui devono usualmente concludersi tali attività.
Tuttavia, in un ragionevole ed ordinato svolgersi delle attività istruttorie, è corretto prevedere che il complesso dei presidi antiriciclaggio si attivi al momento del conferimento dell'incarico per lo svolgimento della prestazione professionale, e ciò anche in funzione dell'analisi occorrente a determinare la tipologia di adeguata verifica da compiere;
è da ritenere pertanto legittimo effettuare gli adempimenti di adeguata verifica della clientela anche in momenti diversi, e fino al momento della stipula, in quanto è in quel momento che può concludersi la valutazione della prestazione professionale per cui l'incarico è stato conferito.
A conferma di ciò la Regola Tecnica n. 8 prevede che, fermo restando che le operazioni di adeguata verifica possono avere un inizio antecedente, quanto meno per l'identificazione, il termine ultimo per la loro conclusione coincide, nel caso di atto notarile, con la stipula, in quanto è in quel momento che si verifica il complessivo conferimento dell'incarico al notaio; l'art. 18, comma 4, esonera infatti da tutte le attività di adeguata verifica (salvo la mera identificazione) il notaio fin quando esamina la posizione giuridica del cliente.
Si può infine osservare che anche gli articoli 35 e 42, in materia di obbligo di astensione, hanno necessariamente come termine di riferimento, per l'attività notarile, il giorno della stipula, potendo essere riferita la relativa deroga dall'astensione solo a tale momento.

Gli obblighi del cliente per consentire l'adeguata verifica

Sono disciplinati dall'art. 22, che stabilisce anzitutto il principio che le informazioni debbano essere rese per iscritto, debbano essere complete e aggiornate e fornite sotto la propria responsabilità.
Viene introdotto un ulteriore nuovo obbligo a carico degli amministratori e simili, rispetto ai soggetti non personificati, che consiste nel procurarsi le informazioni in ordine alla titolarità effettiva, in modo da poterle rendere disponibili ai soggetti obbligati in occasione dell'adeguata verifica; sempre a carico degli amministratori viene previsto (art. 21) un obbligo di comunicare al Registro delle Imprese le medesime informazioni, destinate a confluire in un istituendo registro pubblico per le informazioni relative al titolare effettivo di persone giuridiche e trust.

LE TIPOLOGIE DI ADEGUATA VERIFICA

I presupposti per la scelta - la valutazione e mitigazione del rischio

Il contesto delle Regole Tecniche emanate dal CNN, e sottoposte al parere del CSF con esito positivo, ci consente di definire con sufficiente determinazione quei dettagli in tema di contenuto

dell'adeguata verifica semplificata e sue modalità di esecuzione, che dal testo normativo non erano stati disciplinati nel dettaglio; rimane tuttavia in gran parte scoperta l'area di definizione dei presupposti in base ai quali il notaio debba eseguire una adeguata verifica semplificata, piuttosto che ordinaria o rafforzata.

Il quadro verrà completato quando il CNN avrà dettato i criteri e le metodologie per la valutazione del rischio da parte dei notai (art. 15, comma 1) e avrà individuato ai sensi dell'art.16, i requisiti dimensionali e organizzativi in base ai quali i notai adottano presidi, controlli e procedure per la valutazione del rischio.

In linea generale rileviamo che è il soggetto obbligato a dover effettuare, anche secondo le indicazioni date dall'organismo di autoregolamentazione, la valutazione del rischio e una attività di organizzazione della propria struttura volta a mitigare il rischio; ciò si traduce in una serie di operazioni, alcune preliminari, altre connesse alla prestazione che è chiamato a rendere al cliente.

Anzitutto il notaio dovrebbe, ai sensi degli artt.15 e 16, aver valutato se abbia organizzato la propria struttura perchè costituisca un valido presidio "oggettivo" per il rischio di riciclaggio; in una parola, il notaio che abbia adottato tutti gli accorgimenti opportuni in materia di formazione del personale e formalizzazione di idonee procedure interne, potrà ragionevolmente orientare la valutazione del rischio verso in maniera più *soft*, consapevole che la propria organizzazione già di per sè è valido strumento per mitigarlo.

Eseguita questa operazione preliminare, si procede a valutare il c.d. **rischio inerente** di riciclaggio e finanziamento del terrorismo.

Questa operazione consiste nell'attribuire un "peso" oggettivo all'operazione considerata in astratto, e riferita alla ordinaria tipologia di clientela ed all'area geografica di operatività del notaio; gli atti andrebbero suddivisi per tipologia e classificati anche in base alla loro rilevanza economica, ed occorre anche classificare le aree geografica di destinazione.
Una precisazione appare opportuna per quanto attiene alle aree geografiche: il precedente testo del D.Lvo (art. 25, comma 2) prevedeva l'emanazione di un decreto del MEF che individuasse la c.d. White List, vale a dire una lista di Paesi extracomunitari il cui regime in materia di normativa AR poteva ritenersi equivalente.[12]
Nel testo attuale del D.Lvo, gli indici di basso e alto rischio riferibili alle aree geografiche sono rappresentati rispettivamente negli artt. 23 e 24; fermo restando che viene definita area geografica di basso rischio l'UE, non è più prevista una espressa individuazione con decreto ministeriale dei Paesi a basso rischio.
Entrambi gli articoli fanno, in maniera simmetrica, riferimento all'essere, o meno, dotato, il Paese, di un "efficace sistema di prevenzione del riciclaggio", ovvero dall'essere, o meno, il Paese, valutato da "fonti autorevoli ed indipendenti a basso rischio di corruzione" ovvero abbiano, o meno, dato, sulla base di fonti attendibili ed indipendenti, "effettiva applicazione alle raccomandazioni del GAFI in materia"; l'art. 24 infine indica come Paesi ad altro rischio anche

[12] L'ultima di tali White List comprende: 1. Australia 2. Brasile; 3. Canada; 4. Hong Kong; 5. India; 6. Giappone; 7. Repubblica di Corea, 8. Messico; 9. Singapore; 10. Stati Uniti d'America; 11. Repubblica del Sudafrica; 12. Svizzera. 13. San Marino

quelli soggetti a sanzioni o embargo o che finanziano o sostengono organizzazioni terroristiche o nei quali operano organizzazioni terroristiche.
Dal punto di vista del soggetto obbligato appare evidente la difficoltà di dare attuazione al dettato normativo in assenza di indicazioni più precise da parte dei soggetti (italiani, comunitari?) preposti all'individuazione dei Paesi a basso o alto rischio.
Per il momento si può suggerire di continuare a fare affidamento sulla precedente lista (White List) benché non venga più aggiornata, dei Paesi che hanno obblighi equivalenti, e di consultare le Black List disponibili, anche con un occhio alle c.d. Black List fiscali.

Infine si valuta il c.d. **rischio specifico,** e si rileva il **rischio effettivo.**

Il collaboratore o il notaio completerà la valutazione del rischio, in base agli elementi oggettivi e soggettivi, concretamente presenti, e verificherà se emergano indicatori di anomalia o schemi rappresentativi UIF, ed infine se siano presenti fattori di rischio[13].

A conclusione di queste operazioni, sarà possibile classificare l'operazione a basso, medio o alto rischio, e conseguentemente optare per il corrispondente regime di adeguata verifica (semplificata, ordinaria o rafforzata).
L'attribuzione della classe di rischio può, tuttavia, essere rivista nel corso dell'istruttoria ed anche in sede di stipula, in dipendenza di ulteriori informazioni aggiornate e/o del comportamento tenuto dal cliente, ovvero ancora dall'emergere di altre circostanze.

L'adeguata verifica semplificata - Regola Tecnica n.3

REGOLA TECNICA N. 3

In tema di adeguata verifica semplificata, tenuto conto:

[13] Art. 24 comma 2
a) fattori di rischio relativi al cliente quali: 1) rapporti continuativi o prestazioni professionali instaurati ovvero eseguiti in circostanze anomale; 2) clienti residenti o aventi sede in aree geografiche ad alto rischio secondo i criteri di cui alla lettera c); 3) strutture qualificabili come veicoli di interposizione patrimoniale; 4) società che hanno emesso azioni al portatore o siano partecipate da fiduciari; 5) tipo di attività economiche caratterizzate da elevato utilizzo di contante; 6) assetto proprietario della società cliente anomalo o eccessivamente complesso data la natura dell'attività svolta;
b) fattori di rischio relativi a prodotti, servizi, operazioni o canali di distribuzione quali: 1)servizi con un elevato grado di personalizzazione, offerti a una clientela dotata di un patrimonio di rilevante ammontare;2)prodotti od operazioni che potrebbero favorire l'anonimato; 3)rapporti continuativi, prestazioni professionali od operazioni occasionali a distanza non assistiti da adeguati meccanismi e procedure di riconoscimento; 4)pagamenti ricevuti da terzi privi di un evidente collegamento con il cliente o con la sua attività; 5)prodotti e pratiche commerciali di nuova generazione, compresi i meccanismi innovativi di distribuzione e l'uso di tecnologie innovative o in evoluzione per prodotti nuovi o preesistenti;
c) fattori di rischio geografici quali quelli relativi a: 1)Paesi terzi che, sulla base di fonti attendibili e indipendenti quali valutazioni reciproche ovvero rapporti pubblici di valutazione dettagliata, siano ritenuti carenti di efficaci presidi di prevenzione del riciclaggio e del finanziamento del terrorismo coerenti con le raccomandazioni del GAFI; 2) Paesi terzi che fonti autorevoli e indipendenti valutano essere caratterizzati da un elevato livello di corruzione o di permeabilità ad altre attività criminose; 3)Paesi soggetti a sanzioni, embargo o misure analoghe emanate dai competenti organismi nazionali e internazionali; 4)Paesi che finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche.

- che il notaio potrà applicare misure semplificate di adeguata verifica della clientela nelle ipotesi in cui, alla stregua di un processo valutativo ricostruibile e dimostrabile, emerga in concreto un basso rischio di riciclaggio e di finanziamento del terrorismo, in quanto l'estensione dell'adeguata verifica va commisurata al rischio in concreto rilevato, sulla base degli indici di cui all'articolo 23, commi 1 e 2, del D.Lgs. n. 90/2017;
- che in tali ipotesi, quali indici di basso rischio relativi a tipologie di clienti, possono individuarsi, a titolo esemplificativo, le seguenti tipologie di soggetti:
1) società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva;
2) pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea;
3) clienti che sono residenti in aree geografiche a basso rischio, ai sensi della lettera c) dell'art. 23 del decreto stesso;
i soggetti sottoposti a vigilanza ai sensi del D.Lgs. 1° settembre 1993 n. 385, del D.Lgs. 24 febbraio 1998, n. 58, e del D.Lgs. 7 settembre 2005 n. 209 si considerano a basso rischio di riciclaggio.
Pertanto è possibile, qualora ricorrano in concreto i presupposti, applicare misure semplificate di adeguata verifica della clientela che consistono nella identificazione del rappresentante del soggetto, inclusa la verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente. In tal caso, l'obbligo di identificazione del titolare effettivo è da ritenersi assolto con l'acquisizione dei dati identificativi forniti dal cliente, con le modalità e nei termini di cui alla regola tecnica n. 5.
Gli obblighi di adeguata verifica sono attenuati ogniqualvolta i soggetti summenzionati intervengano in un atto per porre in essere un'operazione che la legge riserva espressamente ad essi in via esclusiva nonché con riferimento a tutti gli atti consequenziali o collegati a tali operazioni. A titolo di mera esemplificazione, è possibile far riferimento a contratti di mutuo, finanziamenti, aperture di credito, ivi compresi i patti aggiuntivi e modificativi degli stessi, gli atti di quietanza totale e parziale, di ristrutturazione e rinegoziazione, di erogazione, di surrogazione, di accollo, di delegazione e relativi atti connessi od accessori, ad atti e contratti che comportino la costituzione, la conferma, l'estensione, la rinnovazione, il frazionamento, la postergazione, la surroga, la riduzione, la cancellazione o lo svincolo di ipoteche, pegni o privilegi, fidejussioni e altre garanzie stabilite a favore dell'istituto, ad atti e contratti di cessione, a qualsiasi titolo, dei contratti di cui sopra e/o dei crediti nascenti dagli stessi, ai leasing mobiliari ed immobiliari.
Gli obblighi semplificati di adeguata verifica della clientela non si applicano qualora si abbia motivo di ritenere che l'identificazione effettuata non sia attendibile e qualora vi sia sospetto di riciclaggio o di finanziamento del terrorismo. I soggetti obbligati potranno dunque applicare misure semplificate di adeguata verifica solo qualora dalla valutazione emerga in concreto un basso rischio di riciclaggio.

La Regola Tecnica n.3 ha avuto una gestazione particolarmente travagliata; nella sua versione originaria tendeva a ripristinare una elencazione di soggetti già contenuta nel precedente testo dell'art. 25 del D.Lgs. n. 231/2007, in tema di obblighi semplificati di adeguata verifica, nei confronti dei quali si disponeva che i destinatari della normativa antiriciclaggio non fossero del tutto tenuti all'osservanza degli obblighi di adeguata verifica, tuttavia prendendo atto del

mutamento del quadro normativo, che non prevede più possibilità di esonero da tale obbligo; la precedente versione della Regola Tecnica n.3, indicava, come modalità di adempimento degli obblighi di adeguata verifica, la sola identificazione dell'esecutore e la verifica dei suoi poteri, ritenendo superflua, in una interpretazione teleologica della norma, l'identificazione del titolare effettivo, riferita a soggetti vigilati, o simili o a Pubbliche Amministrazioni: difatti, da un lato, per tali soggetti si tratta di dati comunemente reperibili, e dall'altro, appare del tutto irrilevante la valutazione del soggetto cui compete la titolarità effettiva ai fini di orientare l'adeguata verifica verso forme ordinarie o rafforzate, in quanto la modalità di esecuzione dell'adeguata verifica nei loro confronti, nel contesto della loro ordinaria attività istituzionale, sarà sempre semplificata: solo per fare un esempio, non avrebbe senso prevedere una adeguata verifica rafforzata nei confronti di un Istituto di Credito, in quanto porterebbe a dover verificare, tra l'altro, l'origine dei fondi impiegati nell'operazione.

Tuttavia, la versione finale di tale Regola Tecnica n.3, prevede comunque che si debba procedere anche nei confronti di tali soggetti, all'individuazione del titolare effettivo.
La Regola, nel suo complesso, può essere utile per dare alcune indicazioni sulle modalità di svolgimento dell'adeguata verifica semplificata, in quanto:
- identifica a titolo esemplificativo alcune categorie di soggetti a basso rischio
- per tali soggetti ribadisce che l'identificazione del titolare effettivo si può svolgere con i criteri di cui alla Regola Tecnica n.5
- effettua una elencazione di operazioni, riferibili ai soggetti di area bancaria e finanziaria, da considerarsi a basso rischio di default

CONDIZIONI

Si può ritenere che si possa procedere ad adeguata verifica semplificata, se concorrono le seguenti condizioni:

a) deve essere presente almeno un **indice di basso rischio**, quale, usualmente, sarà la presenza di soli clienti residenti in UE o in Paesi a basso rischio ;

b) **non devono emergere fattori di rischio**; nella rilevazione del rischio, oltre che i fattori indicati dal Decreto (v. art.24), andranno tenuti presenti, come detto, anche gli Indicatori di anomalia, in quanto, benché emanati in vigenza del precedente testo di legge, come anche risulta da comunicazione dell'UIF pubblicata su CNN Notizie del 6 luglio 2017, sono da considerare ancora efficaci e/o applicabili in via transitoria, e gli Schemi di Comportamento emanati dall'UIF.

A queste due pre-condizioni, dal complessivo tenore del D.Lgs, e da una prudente applicazione della norma che preveda l'adozione di linee guida interne che ne integrino il suo contenuto, individuando aree e situazioni di alto e basso rischio nella concreta realtà dello studio professionale, si aggiungeranno:

a) **l'inesistenza di fattori di dubbio**, incongruenza o incertezze nell'acquisizione di informazioni in sede di adeguata verifica;

b) **la persistenza**, in base alle linee guida interne, **delle condizioni** per cui si possa effettuare l'adeguata verifica semplificata; in sostanza nelle linee guida interne si saranno individuate preventivamente le operazioni che, oggettivamente o per il loro importo, richiedono una adeguata verifica che va oltre la modalità semplificata.

Pare quindi possibile autodeterminare, in via interpretativa, sulla base dei principi generali di sostenibilità e approccio basato sul rischio, una minore estensione degli adempimenti di adeguata verifica, in presenza delle condizioni di cui sopra; è comunque utile ricordare che, per poter escludere la presenza di indici di rischio, leggendo le norme relative alla rilevazione e valutazione del rischio, sembrerebbe opportuno acquisire, sempre e comunque, il dato relativo all'attività svolta dal cliente, quando esso possa essere significativo in rapporto al tipo di prestazione richiesta ed al suo ammontare.

MODALITÀ DI ESECUZIONE

In base al complessivo tenore delle Regole Tecniche, si possono individuare le seguenti modalità di esecuzione dell'adeguata verifica semplificata:

a) In ordine alla individuazione del **titolare effettivo di soggetti non fisici iscritti in un registro pubblico**, si ritiene equipollente, all'acquisizione delle informazioni scritte fornite dal cliente, l'acquisizione delle informazioni tratte dal registro pubblico confermate dal cliente, qualora il professionista, per praticità, scelga tale modalità.

b) Si ritiene sufficiente l'acquisizione delle **informazioni sullo scopo e sulla natura della prestazione** effettuata in contestualità della stipula, senza che sia necessario formalizzare e conservare documentazione informativa autonoma al riguardo.

c) Fermo restando che occorre comunque valutare il profilo lavorativo e economico del cliente e confrontarlo con l'operazione richiesta e il suo ammontare, non sembra necessario verificare **l'origine dei fondi impiegati** dal cliente nell'operazione; le informazioni sulla situazione economico-patrimoniale del cliente sono comunque da acquisire in funzione del rischio, sia pure limitate a acquisibili o possedute in ragione dell'attività professionale svolta.

d) nel controllo costante, si esamineranno la complessiva operatività del cliente, e solo se necessario in funzione del rischio, la provenienza dei fondi, sempre sulla base delle informazioni acquisite o possedute in ragione dell'esercizio dell'attività professionale svolta.

Riassumendo, sarà sufficiente:

- identificare cliente e titolare effettivo (eventuale);
- per i soggetti non fisici iscritti in un registro pubblico si possono trarre le informazioni necessarie dalla consultazione del registro
- raccogliere una dichiarazione scritta del cliente in ordine alla sua qualifica di non PEP e, nel caso di cliente non personificato, anche in ordine alla corrispondenza delle risultanze del registro pubblico con l'effettività

- non occorre acquisire informazioni ulteriori sullo scopo e sulla natura della prestazione: è sufficiente la richiesta di stipula
- non occorre né verificare la consistenza patrimoniale del cliente né l'origine dei fondi.

L'adeguata verifica ordinaria

CONDIZIONI

Esisterebbero tutte le condizioni per poter procedere con l'adeguata verifica semplificata, tuttavia l'operazione, in base alle linee guida interne adottate dallo Studio, è classificata a Medio Rischio o oggettivamente o in base al suo importo, ovvero è emerso, nel corso dell'istruttoria, qualche altro fattore soggettivo o oggettivo che richiede un approfondimento.

MODALITÀ DI ESECUZIONE

oltre alle modalità di esecuzione previste per l'adeguata verifica semplificata, potrà essere necessario raccogliere, per iscritto, dal cliente, ulteriori informazioni sullo scopo e la natura dell'operazione e, quando l'operazione lo richiede, anche sulla sua consistenza patrimoniale; per quanto attiene ai fondi impiegati nell'operazione non dovrebbe essere necessario verificarne in ogni caso l'origine, almeno tutte le volte che il profilo economico del cliente sia tale da giustificare, dal punto di vista finanziario, l'operazione.

Il cliente/esecutore dovrà quindi fornire, all'occorrenza, per iscritto, sotto la propria responsabilità (art. 22, comma 1), i seguenti dati e informazioni:

a) informazioni sullo scopo e natura della prestazione professionale o dell'operazione richiesta al professionista anche con riferimento, in caso di titolare effettivo diverso dal cliente ovvero di prestazione o operazione resa tramite esecutore, delle relazioni intercorrenti tra il cliente e il titolare effettivo e tra il cliente e l'esecutore;

b) nel caso in cui si ritenga necessario verificare la provenienza dei fondi utilizzati dal cliente, se i medesimi provengono da: risparmi personali, redditi di attività propria, denaro fornito da familiari/terzi e a quale titolo, successione ereditaria, vendita di beni personali, finanziamento con indicazione della tipologia e del soggetto finanziatore, finanziamento soci, o altro (da specificare).

L'adeguata verifica rafforzata

CONDIZIONI

E' emerso un fattore di rischio oggettivo o geografico, ovvero è presente un Indicatore di Anomalia o una fattispecie prevista in uno degli Schemi UIF, ovvero ancora è convolta una PEP, o un Trust o struttura simile[14].

MODALITÀ DI ESECUZIONE

Occorre approfondire, acquisendo sempre informazione scritta dal cliente, informazioni aggiuntive, verificarne la congruenza in rapporto al profilo del cliente ed alla tipologia dell'operazione, esaminare la situazione patrimoniale del cliente e farsi dichiarare l'origine dei fondi impiegati; verificare la verosimiglianza di tutte le informazioni così raccolte.

Questi in concreto gli adempimenti ulteriori da compiere per una adeguata verifica rafforzata:

a) esaminare il contesto e la finalità di operazioni caratterizzate da importi insolitamente elevati ovvero rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate;

b) acquisire informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto e intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale;

c) applicare misure adeguate per stabilire l'origine del patrimonio e dei fondi impiegati nel rapporto continuativo o nell'operazione.

Esaminiamo in particolare l'attività di **acquisizione e valutazione delle informazioni** sullo scopo e sulla natura delle operazioni; in caso di adeguata verifica semplificata, lo standard è facilmente soddisfatto dalla stessa richiesta dell'operazione effettuata dal cliente al professionista: in sostanza essa sarà per così dire, autoportante; nel caso invece in cui non si possa applicare una modalità semplificata, ci troveremo per converso, nella condizione di dover approfondire, e quindi di dover richiedere, al cliente, di formalizzare, tendenzialmente per iscritto, informazioni aggiuntive; la norma in questo caso esemplifica tali informazioni quali quelle relative all'instaurazione del rapporto, alle relazioni intercorrenti tra il cliente e l'esecutore, tra il cliente e il titolare effettivo e quelle relative alla situazione economico-patrimoniale del cliente, acquisite o

[14] le operazioni che investono fiduciarie, trust, società anonime o simili con sede in Paesi terzi ad alto rischio, devono essere, all'atto pratico, segnalate quasi automaticamente:
Art. 35
2. In presenza degli elementi di sospetto di cui al comma 1, i soggetti obbligati non compiono l'operazione fino al momento in cui non hanno provveduto ad effettuare la segnalazione di operazione sospetta. Sono fatti salvi i casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto ovvero nei casi in cui l'esecuzione dell' operazione non possa essere rinviata tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini. In dette ipotesi, i soggetti obbligati, dopo aver ricevuto l'atto o eseguito l'operazione, ne informano immediatamente la UIF.
Art. 42
2.I soggetti obbligati si astengono dall'instaurare il rapporto continuativo, eseguire operazioni o prestazioni professionali e pongono fine al rapporto continuativo o alla prestazione professionale già in essere di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime o controllate attraverso azioni al portatore aventi sede in Paesi terzi ad alto rischio. Tali misure si applicano anche nei confronti delle ulteriori entità giuridiche, altrimenti denominate, aventi sede nei suddetti Paesi, di cui non è possibile identificare il titolare effettivo né verificarne l'identità.
4.È fatta in ogni caso salva l'applicazione dell'articolo 35, comma 2, nei casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto.

possedute in ragione dell'esercizio dell'attività; inoltre, nel caso di adeguata verifica rafforzata, occorrerà effettuare una puntuale comparazione tra le informazioni fornite dal cliente e le eventuali informazioni acquisite autonomamente, nei limiti del possibile, anche con riguardo ad eventuali precedenti operazioni con il medesimo cliente.

Altro dato che merita approfondimento, nel caso di adeguata verifica rafforzata, è quello relativo alla **verifica della provenienza dei fondi** e delle risorse nella disponibilità del cliente, sulla base di informazioni acquisite o possedute in ragione dell'esercizio dell'attività.

Qualora il rapporto con il cliente si protragga per una certa durata sarà necessario verificare anche il suo **complessivo comportamento**, vale a dire se la sua operatività nel tempo presenta caratteri di anomalia, ed anche qui, se non siamo in regime di adeguata verifica semplificata, occorre acquisire informazioni relative alla provenienza dei fondi e delle risorse nella sua disponibilità, sia pure sempre nell'ambito di quelle informazioni pertinenti alla attività del notaio.

La formazione del personale e l'organizzazione dello studio[15]

Il Decreto in più parti ribadisce la necessità per i soggetti obbligati di curare l'organizzazione della propria struttura, formando il personale e dotandosi di procedure interne "oggettive", per l'analisi e la valutazione in materia di adeguata verifica. Già nel vigore della precedente normativa il Mod.6 (Modulo Operativo della Guardia di Finanza) prevedeva, tra i primi adempimenti in sede di ispezione, la verifica del grado di organizzazione dello studio in materia.

L'attuale testo normativo prevede che gli adempimenti di adeguata verifica possano essere svolti anche da dipendenti o collaboratori dello studio, e, in applicazione dei principi generali di proporzionalità, approccio basato sul rischio ed in ragione della specificità della professione, è riconosciuto che l'adeguata verifica non deve essere svolta sempre con lo stesso grado di approfondimento, e comunque deve essere tenuto conto della dimensione della struttura.

[15] Art.15 - VALUTAZIONE DEL RISCHIO DA PARTE DEI SOGGETTI OBBLIGATI

2.I soggetti obbligati, adottano procedure oggettive e coerenti rispetto ai criteri e alle metodologie di cui al comma 1, per l'analisi e la valutazione dei rischi di riciclaggio e di finanziamento del terrorismo. Per la valutazione del rischio di riciclaggio o di finanziamento del terrorismo, i soggetti obbligati tengono conto di fattori di rischio associati alla tipologia di clientela, all'area geografica di operatività, ai canali distributivi e ai prodotti e i servizi offerti.

Art. 16 - PROCEDURE DI MITIGAZIONE DEL RISCHIO

1.I soggetti obbligati adottano i presidi e attuano i controlli e le procedure, adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi di riciclaggio e di finanziamento del terrorismo, individuati ai sensi degli articoli 14 e 15.

3.I soggetti obbligati adottano misure proporzionate ai propri rischi, alla propria natura e alle proprie dimensioni, idonee a rendere note al proprio personale gli obblighi cui sono tenuti ai sensi del presente decreto, ivi compresi quelli in materia di protezione dei dati personali. A tal fine, i soggetti obbligati garantiscono lo svolgimento di programmi permanenti di formazione, finalizzati alla corretta applicazione delle disposizioni di cui al presente decreto, al riconoscimento di operazioni connesse al riciclaggio o al finanziamento del terrorismo e all'adozione dei comportamenti e delle procedure da adottare.

Qui di seguito alcune possibili prime indicazioni, per avviare una verifica di idoneità della propria organizzazione di studio e formare una linea guida interna:[16]

a) formare almeno i collaboratori e dipendenti addetti all'istruttoria delle pratiche e mantenere documentazione dell'attività di formazione;

b) dotarsi di una guida interna all'adeguata verifica, o quanto meno di un set di documentazione da consultare, con il materiale normativo e regolamentare (in primis gli indicatori di anomalia ministeriali e l'elenco dei Paesi in Black e nella precedente White List);

c) suddividere, mediante una tabella interna, le operazioni in base al rischio inerente, vale a dire nella loro astrattezza, e individuare soglie di rilevanza economica, anche riferite al profilo del cliente, che impongano un diverso livello di attenzione nell'esecuzione dell'adeguata verifica;

d) dotarsi di adeguata modulistica, eventualmente differenziata in base alla tipologia di adeguata verifica, da poter utilizzare all'occorrenza per raccogliere informazioni scritte dal cliente;

e) all'apertura della pratica, formare un sotto-fascicolo, da tenere riservato per contenervi la documentazione raccolta, le note, e quanto altro pertinente all'attività di adeguata verifica, in modo da tenere separato tale materiale dal restante fascicolo del cliente e renderla disponibile in sede di ispezione;

f) acquisire al primo momento utile, i documenti di identità delle parti e le informazioni in ordine alla loro attività lavorativa, per valutarne, se necessario, la congruità con l'operazione richiesta, in modo da verificare la permanenza delle condizioni per procedere con una adeguata verifica semplificata;

g) nel caso di intervento in atto di soggetti non personificati, individuare sempre il titolare effettivo, secondo criteri che vanno indicati in maniera esemplificativa ai collaboratori;

h) nel caso di ricorrenza di adeguata verifica rafforzata, acquisire per iscritto dal cliente informazioni in ordine alla origine del patrimonio, e dei fondi impiegati nell'operazione e valutarne l'attendibilità; acquisire informazioni aggiuntive sul cliente per eseguire una ulteriore verifica;

i) al più tardi al momento della stipula, o del compimento dell'operazione, acquisire dichiarazione scritta dal cliente in ordine alla non sussistenza di PEP e/o titolari effettivi rispetto alle persone fisiche intervenute, sempre che non si sia deciso di ricorrere ad altre modalità di rilevazione di tali situazioni;

l) dopo la stipula o il compimento dell'operazione, effettuare una verifica finale della completezza del fascicolo, che dovrà contenere, in genere, documenti di identità e codici fiscali, mezzi di pagamento (sempre), visure camerali, delibere autorizzative, dichiarazione di assenza di PEP o altri interessati (titolari effettivi), scheda di valutazione interna.

[16] Ricordiamo che l'art.56, comma 2 indica che ...la gravità della violazione è determinata anche tenuto conto: a) dell'intensità e del grado dell'elemento soggettivo, anche avuto riguardo all'ascrivibilità, in tutto o in parte, della violazione alla carenza, **all'incompletezza o alla non adeguata diffusione di prassi operative e procedure di controllo interno...**

SEGRETERIA ORGANIZZATIVA
Consiglio Notarile di Bergamo
V.le Vittorio Emanuele, 44 - 24121 Bergamo
Tel. 035.224065 - Fax 035.244578
www.notaibergamo.it
consigliobergamo@notariato.it

PATROCINI

Fondazione Italiana del Notariato

SCUOLA DI NOTARIATO DELLA LOMBARDIA