Dati giudiziari e GDPR: un'*impasse* (ancora) in attesa di soluzione

Chiara Giannella
LL.M., Avvocato, Director dell'operating unit Intellectual Property, TMT & Digital Solution di PwC TLS Avvocati e Commercialisti

Luca Spada
LL.M., Avvocato, Senior Associate dell'operating unit Intellectual Property, TMT & Digital Solution di PwC TLS Avvocati e Commercialisti

Introduzione

Due anni sono trascorsi da quando, proprio in questo periodo (*i.e.*, tra agosto e settembre), specialisti *data protection*, esperti di *cybersecurity*, referenti privacy, DPO e addetti agli uffici competenti di titolari e responsabili iniziavano a familiarizzare e a fare i conti con le previsioni del (al tempo) appena emesso Decreto Legislativo 10 agosto 2018, n. 101 di adeguamento della normativa italiana in materia di protezione dei dati personali contenuta (principalmente) nel Decreto Legislativo 30 giugno 2003, n. 196 ("**Codice Privacy**") ai dettami del Regolamento (UE) 2016/679 ("**Regolamento**" o "**GDPR**"), divenuto pienamente applicabile pochi mesi prima, in quel 25 maggio 2018 che potrebbe essere considerato il giorno zero della nuova era della protezione dei dati personali in Europa. Sin da subito, tuttavia, ci si è resi conto di come il decreto attuativo, riproponendo alcune norme di principio mutuate dal disposto del GDPR, spesso demandasse a sua volta la soluzione di vari aspetti a successivi interventi normativi o regolamentari di maggiore dettaglio.
Tra i temi ancora non pienamente indirizzati a distanza di un biennio, spicca – se non altro, per la quasi completa assenza di suggerimenti "ufficiali" al riguardo – la pressoché irrisolta questione relativa alla possibilità o meno di

01_PwC_dicembre_2020.indd 151 09/12/20 15:58

trattare le informazioni di cui all'articolo 10, GDPR; tematica, questa, che tuttora disturba il sonno di consulenti e organizzazioni alla ricerca di appigli che permettano anche solo di ipotizzare una soluzione al problema e in trepidante attesa dell'emissione da parte del Ministero della giustizia – una volta sentito il Garante per la protezione dei dati personali (**Garante**) – di quel decreto ministeriale tramite il quale, ai sensi del comma 2 dell'articolo 2-*octies*, Codice Privacy, dovrebbero essere individuate le fattispecie in cui sarà possibile effettuare il trattamento di dati personali relativi a condanne penali e reati e le relative garanzie appropriate a salvaguardia dei diritti e delle libertà degli interessati.

Sono tuttavia molteplici le organizzazioni che nell'ambito della conduzione delle proprie routinarie operazioni effettuano attività da cui potrebbe in potenza derivare un trattamento di dati personali *ex* articolo 10, GDPR, e che, allo stato, scontano le conseguenze negative derivanti dall'assenza di chiarezza e di soluzioni sicuramente conformi alla normativa applicabile che siano al contempo funzionali alla soddisfazione degli interessi aziendali di fronte a quello che attualmente, nei fatti, si presenta in buona sostanza come un divieto generalizzato al trattamento di dati giudiziari.

Di rimedi – al cento per cento scevri da rischi – per far collimare una volta e per tutte esigenze aziendali e *compliance* normativa però non se ne vedono all'orizzonte.

Ad ogni modo, nelle more del tanto atteso decreto ministeriale, occorre fare i conti con quello che vi è sul tavolo, ricercando tra provvedimenti e prese di posizione dal Garante e tra le maglie della normativa dedicata a specifici settori, ambiti o attività, possibili indizi lasciati sul campo (più o meno di proposito), spunti e spiragli che aiutino a comprendere, da un lato, quali sono – sempreché allo stato ve ne siano – le ipotesi in cui parrebbe possibile già ora processare dati personali relativi a condanne penali e reati e, dall'altro, quali potrebbero essere eventuali accorgimenti alternativi per quei casi in cui, malgrado l'esistenza di interessi meritevoli in capo ai titolari, risultasse al contrario impedito il trattamento di tali informazioni.

La ricerca di soluzioni pratiche o di potenziali "vie di uscita" dalla situazione di stallo non può tuttavia che passare da uno stadio preliminare, ossia dall'identificazione del perimetro esatto dell'oggetto di una così stringente tutela e dalla piena comprensione del quadro normativo vigente.

Definizione dell'ambito di tutela

La corretta delimitazione del concetto di dato giudiziario riveste primaria importanza nell'ottica di individuare possibili accorgimenti che, *medio tem-*

01_PwC_dicembre_2020.indd 152 09/12/20 15:58

pore, potrebbero risultare fondamentali ai fini dell'appropriata gestione di determinati processi aziendali e dell'individuazione di soluzioni di compromesso tra gli interessi dei titolari e la loro parallela necessità di rispettare i dettami della normativa applicabile in materia di protezione dei dati personali. Un'indicazione al riguardo proviene direttamente dalla nostra autorità di controllo che definisce i "dati giudiziari" "quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza"[1]. La definizione fornita dal Garante, peraltro, non è mutata nel tempo; infatti già nel 1999, nel proprio Bollettino n. 8, la *authority* rilevava che per dati giudiziari dovessero intendersi solo quelli "idonei a rivelare taluni provvedimenti giudiziari di carattere penale (e cioè quelli previsti dall'art. 686, commi 1, lettere a) e d), 2 e 3 c.p.p.)"[2].

[1] Garante per la protezione dei dati personali, *Scheda di sintesi: Cosa intendiamo per dati personali?*, consultabile al seguente link: https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali.

[2] Garante per la protezione dei dati personali, *Bollettino n. 8, 1999* [doc. web: 1044626], p. 35, consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1044626. L'articolo 686 c.p.c. è stato dapprima modificato dall'articolo 31, Decreto-legge 14 gennaio 1991, n. 12, e, successivamente, abrogato dall'articolo 52 del D.P.R. 14 novembre 2002, n. 313. L'attuale definizione del contenuto del casellario giudiziario è prevista all'articolo 3, D.P.R. 14 novembre 2002, n. 313, che stabilisce: "Nel casellario giudiziale si iscrivono per estratto: a) i provvedimenti giudiziari penali di condanna definitivi, anche pronunciati da autorità giudiziarie straniere se riconosciuti ai sensi degli articoli 730 e seguenti del codice di procedura penale, salvo quelli concernenti contravvenzioni per le quali la legge ammette la definizione in via amministrativa, o l'oblazione limitatamente alle ipotesi di cui all'articolo 162 del codice penale, sempre che per quelli esclusi non sia stata concessa la sospensione condizionale della pena; b) i provvedimenti giudiziari definitivi concernenti le pene, compresa la sospensione condizionale e la non menzione, le misure di sicurezza personali e patrimoniali, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a delinquere; c) i provvedimenti giudiziari concernenti le pene accessorie; d) i provvedimenti giudiziari concernenti le misure alternative alla detenzione; e) i provvedimenti giudiziari concernenti la liberazione condizionale; f) i provvedimenti giudiziari definitivi che hanno prosciolto l'imputato o dichiarato non luogo a procedere per difetto di imputabilità, o disposto una misura di sicurezza, nonché quelli che hanno dichiarato la non punibilità ai sensi dell'articolo 131-*bis* del codice penale; g) i provvedimenti giudiziari definitivi di condanna alle sanzioni sostitutive e i provvedimenti di conversione di cui all'articolo 66, terzo comma, e all'articolo 108, terzo comma, della legge 24 novembre 1981, n. 689; h) i provvedimenti giudiziari del pubblico ministero previsti dagli articoli 656, comma 5, 657 e 663 del codice di procedura penale; i) i provvedimenti giudiziari di conversione delle pene pecuniarie; i-*bis*) l'ordinanza che ai sensi dell'articolo 464-*quater*

01_PwC_dicembre_2020.indd 153 09/12/20 15:58

Ragionando a contrario, sembrerebbe dunque lecito affermare che non rientrano nel perimetro della definizione di dato giudiziario tutte quelle informazioni inidonee a manifestare l'esistenza di provvedimenti penali a carico dell'interessato.

A sostegno di questa argomentazione, giova richiamare il parere reso dal Garante il 18 agosto 2017 su un'istanza di accesso civico, in relazione all'opportunità da parte del Ministero dello sviluppo economico di dare seguito positivamente alla richiesta di un parlamentare di accedere alla certificazione "in ordine alla insussistenza di incompatibilità, situazioni impeditive e conflitti d'interesse" fornita in sede di nomina da un commissario straordinario di una società ammessa alla procedura di amministrazione straordinaria[3]. Nello specifico, l'autorità di controllo non ha condiviso la ricostruzione del Ministero – che aveva inizialmente declinato la richiesta sul presupposto che la dichiarazione sostitutiva resa dall'interessato sarebbe consistita in "una autocertificazione in ordine al possesso dei requisiti di professionalità e onorabilità previsti dagli articoli 2 e 3 del DM 10 aprile 2013 e alla insussistenza delle cause impeditive e di incompatibilità di cui all'art. 4 del medesimo D.M., che per sua natura contiene 'dati sensibili e/o giudiziari'" – affermando che, nonostante in via puramente astratta e generale, nelle dichiarazioni fornite dai cittadini ai sensi degli artt. 46 e 47

del codice di procedura penale dispone la sospensione del procedimento con messa alla prova, nonché le sentenze che dichiarano estinto il reato per esito positivo della messa alla prova ai sensi dell'articolo 464-*septies* del codice di procedura penale; i-*ter*) i provvedimenti con cui il giudice dispone la sospensione del procedimento ai sensi dell'articolo 420-*quater* del codice di procedura penale; l) i provvedimenti giudiziari definitivi concernenti le misure di prevenzione della sorveglianza speciale semplice o con divieto o obbligo di soggiorno; m) i provvedimenti giudiziari concernenti la riabilitazione; n) i provvedimenti giudiziari di riabilitazione, di cui all'articolo 15 della legge 3 agosto 1988, n. 327; o) i provvedimenti giudiziari di riabilitazione speciale relativi ai minori, di cui all'articolo 24 dei regio decreto-legge 20 luglio 1934, 1404, convertilo, con modificazioni, dalla legge 27 maggio 1935, n. 835, e successive modificazioni; p) i provvedimenti giudiziari definitivi di interdizione e inabilitazione e quelli di revoca, nonché i decreti che istituiscono, modificano o revocano l'amministrazione di sostegno; q) [abrogato]; r) i provvedimenti giudiziari relativi all'espulsione a titolo di sanzione sostitutiva o alternativa alla detenzione, ai sensi dell'articolo 16 del decreto legislativo 25 luglio 1998, n. 286, come sostituito dall'art. 15 della legge 30 luglio 2002, n.189; s) i provvedimenti amministrativi di espulsione e i provvedimenti giudiziari che decidono il ricorso avverso i primi, ai sensi dell'articolo 13 del decreto legislativo 251uglio 1998, n. 286, come modificato dall'art. 12 della legge 30 luglio 2002, n.189; t) i provvedimenti di correzione, a norma di legge, dei provvedimenti già iscritti; u) qualsiasi altro provvedimento che concerne a norma di legge i provvedimenti già iscritti, come individuato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Ministro della giustizia".

[3] Garante per la protezione dei dati personali, *Parere su una istanza di accesso civico*, 18 agosto 2017 [doc. web: 6947348], consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6947348.

01_PwC_dicembre_2020.indd 154 09/12/20 15:58

del D.P.R. 445/2000 è possibile siano contenuti dati sensibili e/o giudiziari, nel caso di specie la certificazione prodotta dal commissario straordinario non conteneva alcun dato appartenente a quelle categorie particolarmente meritevoli di tutela. Ciò in quanto nel documento erano semplicemente riportati – oltre ai dati anagrafici e di contatto e alla firma dell'interessato – "le relative dichiarazioni circa: il possesso dei requisiti di professionalità e onorabilità [...]; l'inesistenza di cause impeditive e di incompatibilità previste dalla normativa di riferimento; la non conoscenza di situazioni personali o professionali di conflitto di interessi anche potenziale; l'inesistenza di condanne per i reati di cui alla lettera a) dell'art. 5, comma 1, del dm 10 aprile 2013 e dell'applicazione delle pene e misure previste dalle lettere b), c) e d) del citato articolo 5 del DM 10 aprile 2013; l'inesistenza di procedimenti penali pendenti per i reati di cui al comma 2, dell'art. 5 del D.M. 10 aprile 2013, dell'avvio di procedimenti per l'applicazione di misure di prevenzione di cui al D.Lgs. 159/2011 e di azioni giudiziarie civili e penali pendenti in relazione ad atti compiuti nell'esercizio di funzioni di amministrazione, direzione e controllo in enti o imprese"[4].

Il ragionamento della nostra *supervisory authority* parrebbe dunque a sostegno della tesi secondo la quale un documento – seppur potenzialmente contenente dati giudiziari – qualora "negativo" (ossia, laddove privo di evidenze circa l'esistenza di reati compiuti o procedimenti penali in corso) non implica di per sé un trattamento di dati giudiziari. Anche in queste circostanze, pertanto, dovrebbe trovare applicazione il principio della prevalenza della sostanza sulla forma[5]: a prescindere dalla sua denominazione "formale", è

[4] *Ibidem.*

[5] Come sostenuto da autorevole dottrina, il principio della prevalenza della sostanza sulla forma permeerebbe l'intero impianto del Regolamento, trovando la sua fonte nel dogma dell'*accountability* del titolare: "[...], l'introduzione dell'obbligo di dimostrare il rispetto dei predetti principi qualora le autorità di protezione dei dati ne facciano richiesta costituisce una ulteriore misura a garanzia del rispetto non solo dei principi di cui all'art. 5.1, ma anche del principio di responsabilizzazione stesso. Il WP29 aveva già rilevato, nell'op. 3/10, come il quadro giuridico allora vigente non fosse 'riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si [traducessero] in meccanismi efficaci atti a fornire una protezione reale' e per questa ragione aveva proposto alla Commissione di esaminare 'l'opportunità di introdurre meccanismi basati sulla responsabilità, con particolare accento sulla possibilità di includere un principio di 'responsabilità'". Il GDPR sembra aver dato concreta attuazione alle indicazioni del WP29, assicurando da un lato la responsabilizzazione come rispetto dei principi della protezione dei dati attraverso l'adozione di misure tecniche e organizzative funzionali alla loro messa in pratica concreta; dall'altro, introducendo l'obbligo di dimostrazione, su richiesta dell'autorità, di aver dato attuazione concreta ai principi di cui sopra. Dal momento che l'*accountability* pone l'accento su determinati risultati da raggiungere in termini di protezione dei dati, sembra che la ratio sottesa all'introduzione dell'*accountability* sia proprio quella di permettere il passaggio dalla teoria dei principi di protezione dei dati alla loro messa in pratica, traducendo così gli

01_PwC_dicembre_2020.indd 155 09/12/20 15:58

infatti innegabile che documenti quali l'attestazione resa dall'interessato nel caso in questione, ove "puliti", non riporterebbero nella sostanza alcuna informazione di per sé meritevole delle specifiche misure di tutela previste agli articoli 10, GDPR, e 2-*octies*, Codice Privacy.

A riprova di ciò, basti pensare che nella fattispecie in analisi il Garante ha suggerito all'amministrazione di valutare l'opportunità di concedere un accesso parziale alla documentazione richiesta, limitandolo alla sola autodichiarazione del commissario straordinario previo oscuramento dei suoi dati personali "comuni" (*i.e.*: indirizzo, data e luogo di nascita, dati di contatto e firma autografa) considerati eccedenti l'interesse fondante l'istanza di accesso del parlamentare[6], riconoscendo pertanto una maggiore tutela a queste informazioni piuttosto che al contenuto negativo dell'autocertificazione dell'interessato; cosa che, al contrario, se la notizia circa l'inesistenza di condanne e carichi pendenti fosse stata essa stessa da considerare un dato giudiziario, probabilmente non sarebbe accaduta.

Del resto, se la logica sottostante il riconoscimento di cautele più stringenti in relazione al trattamento dei dati giudiziari è da ricercarsi nella necessità di garantire maggiore riservatezza a informazioni particolarmente sensibili – la cui conoscenza da parte di terzi potrebbe comportare per l'interessato conseguenze pregiudizievoli in termini, ad esempio, di future azioni nei suoi confronti o di situazioni che potrebbero determinarne l'estromissione o la discriminazione – si potrebbe ragionevolmente ritenere che la notizia circa l'assenza di procedimenti (siano essi in corso o conclusi) e di sanzioni penali non possa, all'opposto, causare pregiudizi specifici per l'individuo[7]. Essa

obiettivi giuridici in misure di protezione dei dati verificabili nei fatti e non solo sulla carta [...]". C. Bistolfi, *Le obbligazioni di compliance in materia di protezione dei dati personali*, in E. Pelino, L. Bolognini, C. Bistolfi (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, 2016, Giuffrè, p. 235.

[6] *Ibidem.*

[7] Per analogia, un ragionamento similare potrebbe valere anche per i dati personali relativi alla salute trattati nel contesto del rapporto di lavoro e, in particolare, all'informazione relativa all'idoneità o meno del dipendente a svolgere determinate mansioni che è comunicata al datore dal medico competente ai sensi della normativa in materia di salute e sicurezza. Il semplice dato relativo alla buona condizione fisica dell'interessato sembrerebbe infatti sottoposto, per certi versi, a minori garanzie di riservatezza rispetto, ad esempio, a quelli indicativi di una particolare patologia o della diagnosi di una malattia, proprio in ragione del fatto che la conoscenza di tale notizia non comporta, di per sé, un rischio di emarginazione né altre conseguenze negative per l'interessato. In dottrina è stato infatti osservato come la natura dei dati di cui all'articolo 9, Regolamento, evocherebbe con immediatezza l'immagine di esperienze concrete di emarginazione o di discriminazione legate all'appartenenza dell'interessato a determinati gruppi o etnie, fedi o religioni, posizioni politiche e altre espressioni della sua personalità che potrebbero contribuire alla costruzione di un disegno pubblico della persona potenzialmente foriero di discriminazioni o anche solo lesivo della sua identità. La disciplina giuridica dei dati "particolari" rappresenterebbe

01_PwC_dicembre_2020.indd 156 09/12/20 15:58

potrebbe infatti essere qualificata come un dato personale "comune" – la cui non particolare sensibilità dovrebbe derivare proprio dalla considerazione per cui parrebbe "normale" non essere sottoposto a misure o aver subito condanne rilevanti penalmente.

Ma se la *ratio* del sistema è presidiare la conoscenza di caratteristiche particolarmente delicate – siano esse dati sensibili, particolari o giudiziari – se ne deduce allora che l'informazione circa l'inesistenza di condanne penali, misure di sicurezza o carichi pendenti risultante da un casellario giudiziario "pulito" o da una autocertificazione "negativa", pur essendo potenzialmente un dato personale, non dovrebbe ontologicamente essere considerata alla stregua di una notizia meritevole di tutele aggiuntive quale lo sarebbe un dato giudiziario, proprio in quanto da tale conoscenza in sé non deriverebbe alcun rischio particolare di discriminazione per l'interessato.

In aggiunta al dato letterale, l'esito dell'interpretazione logica sembrerebbe quindi confermare a maggior ragione l'opportunità di escludere l'informazione negativa dalla definizione di dato giudiziario, permettendone il trattamento in presenza di una delle condizioni di liceità di cui all'articolo 6, GDPR[8].

infatti "una rilettura in chiave moderna del principio di eguaglianza" di cui all'articolo 3 della Costituzione, nel senso che la più "rigorosa assicurazione della disponibilità della circolazione dei dati sensibili al governo dell'interessato varrebbe a ristabilire una misura più equa o adeguata nell'equilibrio dei poteri costruiti o generati dal possesso delle informazioni personali nell'ambito della vita di relazione, contestualmente rinviando a ciascuno la libertà di regolare, secondo le proprie insindacabili scelte, le modalità della rappresentazione pubblica della propria identità, senza accettare il rischio di odiose discriminazioni, o anche solo la libertà di sottrarsi ai poteri di 'soggettivazione' tipici della società contemporanea". Quei dati personali che consentono l'identificazione in capo ad un soggetto di una situazione di debolezza o di disagio o che la storia ha dimostrato possano dare luogo a situazioni lesive dei suoi diritti sono pertanto prudenzialmente protetti in maniera più forte che qualunque altro dato attinente alla generica riservatezza della persona, proprio in ragione "della strutturale e ontologica pericolosità del disvelamento". M. Dell'utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. D'orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, 2019, G. Giappichelli Editore, pp. 239-241. Benché quanto sopra sia stato affermato in relazione ai dati appartenenti alle categorie particolari di cui all'articolo 9, Regolamento, si ritiene che il medesimo razionale potrebbe in buona sostanza giustificare anche le misure di maggiore tutela dedicate ai dati giudiziari, essendo queste informazioni, al pari dei dati sensibili, indicative di situazioni o caratteristiche dell'interessato che potrebbero, ove svelate, comportare il rischio di ingiustificate discriminazioni o altre ripercussioni particolarmente gravi sui diritti e le libertà dell'individuo.

[8] Ai sensi dell'articolo 6, paragrafo 1, GDPR: "Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

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;

01_PwC_dicembre_2020.indd 157 09/12/20 15:58

Identificazione della disciplina applicabile

Ferma restando la nozione di dato giudiziario come definita al precedente paragrafo, il *focus* dovrebbe quindi spostarsi sulle norme che ad oggi disciplinano il trattamento delle informazioni rientranti in tale perimetro.
In primis, l'articolo 10, GDPR, prevede che: "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica". Al riguardo, la Relazione 2018 del Garante, emessa il 7 maggio 2019, evidenzia come il nuovo quadro normativo demandi al legislatore nazionale o europeo l'individuazione delle casistiche in cui è possibile effettuare il trattamento dei dati giudiziari, nonché le relative cautele poste a tutela degli interessati[9].

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".

[9] Garante per la protezione dei dati personali, *Relazione sull'attività 2018 e Discorso del Presidente, 7 maggio 2019* [doc. web: 9109075], consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9109075. Al riguardo, si segnala che il Garante, nel documento in questione (p. 127) dà atto di aver approvato quattro decisioni di diniego a fronte di altrettante richieste di autorizzazione al trattamento di dati contenuti nel certificato del casellario giudiziale relativo ai dipendenti, ritenendo insussistente un'idonea base giuridica (legislativa o regolamentare) per l'effettuazione dei trattamenti richiesti. In particolare, "Non è stato ritenuto criterio di legittimazione idoneo la circostanza che (in due dei casi sottoposti all'Autorità) il trattamento sarebbe stato necessario per adempiere a quanto previsto in un contratto di fornitura di servizi, né che ai dipendenti dei titolari fosse applicabile un contratto collettivo nazionale che prevede tale trattamento. Ciò sia in considerazione della disciplina europea di imminente piena applicazione al momento dell'adozione dei provvedimenti, sia in ragione della ritenuta genericità del richiamo contenuto nel contratto collettivo, in quanto sprovvisto di alcun riferimento a specifiche esigenze di onorabilità legate allo svolgimento di determinati incarichi (in relazione ad un comparto che ricomprende una grande varietà di mansioni, in gran parte non connotate da una particolare delicatezza). Inoltre, in alcuni casi non risultava essere stata effettuata, in applicazione del principio di indispensabilità, l'individuazione del novero delle fattispecie penali ritenute rilevanti per la valutazione di idoneità del lavoratore allo svolgimento di specifiche attività. In

01_PwC_dicembre_2020.indd 158 09/12/20 15:58

Coerentemente, l'articolo 2-*octies*, comma 2, Codice Privacy, stabilisce che, in mancanza di disposizioni di legge o di regolamento, i trattamenti di dati giudiziari e le relative "garanzie" sono individuati con decreto del Ministro della giustizia, da adottarsi (o meglio, che avrebbe dovuto essere adottato) entro 18 mesi dalla data di entrata in vigore del D.Lgs. 101/2018, anche con riferimento alla "*verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti*"[10].

Nelle more dell'emissione del menzionato decreto ministeriale, il legislatore ha previsto, all'articolo 22, comma 12, D.Lgs. 101/2018, che oltre alle ipotesi già espressamente individuate da disposizioni normative il trattamento dei dati giudiziari è consentito nel caso in cui costituisca specifica attuazione dei protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con le prefetture, sempre che sia stato acquisito il prescritto parere del Garante e che risultino specificati "*la tipologia dei dati trattati e le operazioni eseguibili*"[11].

Risultano al contempo abrogati gli articoli 21 e 27 del Codice Privacy, versione precedente alla riforma operata dal D.Lgs. 101/2018, che consentivano il trattamento di dati giudiziari da parte di enti pubblici o privati non solo in presenza di espressa disposizione di legge, bensì anche laddove autorizzato da un provvedimento dell'autorità di controllo che specificasse le finalità di rilevante interesse pubblico, le tipologie di informazioni trattabili e le specifiche operazioni eseguibili[12].

Coerentemente, è altresì venuta meno l'efficacia del Provvedimento generale di autorizzazione n. 7/2016[13], con il quale il Garante aveva in precedenza

uno dei casi è stata poi prospettata la comunicazione dei dati giudiziari ad un soggetto terzo (la stazione appaltante) in assenza, secondo quanto deciso dall'Autorità, di base giuridica. Il Garante ha infine ritenuto che le prospettate modalità del trattamento, consistenti nella consegna del certificato del casellario giudiziale al datore di lavoro, avrebbero consentito la visibilità di tutti i dati contenuti nel certificato, nonostante la dichiarata delimitazione delle fattispecie di reato ritenute rilevanti ai fini della valutazione di idoneità allo svolgimento delle mansioni (provv.ti 22 maggio 2018, n. 314, doc. web n. 9005845; 22 maggio 2018, n. 315, doc. web n. 9005857; n. 316, doc. web n. 9005869; n. 317, doc. web n. 9001980)".

[10] In ottemperanza alle tempistiche previste, il termine per l'emissione dell'atto amministrativo avrebbe dovuto essere il 19 marzo 2020; allo stato il documento risulta però ancora in lavorazione.

[11] Garante per la protezione dei dati personali, cit. *Relazione 2018*, p. 122.

[12] B. Bernabei, *Articolo 10 – Regolamento UE 2016/679 – Trattamento di dati personali relativi a condanne penali e reati,* in A. D'Agostino, L. R. Barlassina, V. Colarocco (a cura di), *Commentario al Regolamento UE 2016/679 e al codice della privacy aggiornato*, Top Legal Academy Edizioni, Milano, 2019, p. 100.

[13] Garante per la protezione dei dati personali, *Autorizzazione n. 7/2016 – Autorizzazione al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti*

01_PwC_dicembre_2020.indd 159 09/12/20 15:58

permesso il trattamento di dati giudiziari – a determinate condizioni – nell'ambito dei rapporti di lavoro, degli organismi di tipo associativo e fondazioni, della mediazione finalizzata alla conciliazione delle liti, della documentazione giuridica, nonché nel contesto delle operazioni di tratta-

pubblici, 15 dicembre 2016 [doc. web: 5803630], consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5803630. Nello specifico, il trattamento di dati giudiziari era in via generale autorizzato, *inter alia*, ove effettuato: (i) nel contesto di rapporti di lavoro (Capo I), con riferimento alle informazioni riguardanti lavoratori subordinati, amministratori o membri di organi esecutivi o di controllo, nonché consulenti e liberi professionisti, agenti, rappresentanti e mandatari, ove il trattamento fosse indispensabile per (a) "adempiere o esigere l'adempimento di specifici obblighi o eseguire specifici compiti previsti da leggi, dalla normativa dell'Unione europea, da regolamento o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro, anche autonomo o non retribuito od onorario", ovvero per (b) "verificare, limitatamente ai dati strettamente necessari, i requisiti di onorabilità dei dipendenti di società operanti nel settore del rating"; (ii) da organismi di tipo associativo (Capo II), incluse associazioni non riconosciute, "fondazioni, comitati e ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, nonché [...] cooperative sociali e società di mutuo soccorso" e "enti ed associazioni anche non riconosciute che curano il patrimonio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi", ove il trattamento avesse riguardato informazioni relative a (a) "associati, soci e aderenti, nonché, nei casi in cui l'utilizzazione dei dati sia prevista dall'atto costitutivo o dallo statuto, a soggetti che presentano richiesta di ammissione o di adesione", ovvero (b) "beneficiari, assistiti e fruitori delle attività o dei servizi prestati dall'associazione, dell'ente o dal diverso organismo", e fosse "indispensabile per perseguire scopi determinati e legittimi dall'atto costitutivo, dallo statuto o da un contratto collettivo"; (iii) da liberi professionisti (Capo III) – e, nello specifico da (a) gli iscritti "in albi o elenchi per l'esercizio di un'attività professionale, in forma individuale, associata o societaria", (b) "soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell´art. 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato", (c) "sostituti e ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, praticanti e tirocinanti" – ove il trattamento avesse riguardato dati attinenti ai clienti e – qualora strettamente indispensabile per eseguire specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi – a terzi; (iv) da organismi di mediazione (Capo IV); e (v) soggetti (Capo V – punto 1) (a) attivi nei settori bancario, assicurativo e dei fondi pensione ai fini di accertamento: "[...] del requisito di onorabilità nei confronti di soci e titolari di cariche direttive e elettive; [...] di requisiti soggettivi e di presupposti interdittivi; [...] di responsabilità in relazione a sinistri o eventi attinenti alla vita umana; [...] di situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa"; (b) "titolari di un trattamento di dati svolto nell'ambito di un'attività di richiesta, acquisizione e consegna di atti e documenti presso i competenti uffici pubblici, effettuata su incarico degli interessati"; (c) che si occupano (in forma societaria) di intermediazione mobiliare, investimento a capitale variabile, gestione del risparmio e dei fondi pensione e società di gestione dei mercati regolamentati o di gestione accentrata di strumenti finanziari, ai fini dell'accertamento dei requisiti di onorabilità; nonché alle (d) "società operanti nel settore del *rating*, limitatamente alle informazioni strettamente indispensabili a verificare la sussistenza o meno dei requisiti di onorabilità in capo ai soli soci responsabili di incarichi di revisione presso società italiane che abbiano emesso strumenti finanziari quotati

01_PwC_dicembre_2020.indd 160 09/12/20 15:58

mento poste in essere da liberi professionisti iscritti in albi o elenchi e da imprese bancarie e assicurative (l'"**Autorizzazione n. 7/2016**")[14].
L'Autorizzazione n. 7/2016, in realtà, nasceva già in origine con la veste di provvedimento di natura provvisoria con termine scadente il 21 maggio 2018 in attesa della piena applicabilità del GDPR[15]. Nelle more dell'adeguamento del quadro normativo nazionale al Regolamento, tuttavia, il Garante è dapprima intervenuto il 19 luglio 2018, stabilendo che "le garanzie e le misure appropriate e specifiche di cui alle Autorizzazioni generali, adottate in data 13 dicembre 2016 [...] per taluni trattamenti di categorie particolari di dati personali e di dati personali relativi a condanne penali e reati o a connesse misure di sicurezza, si intendono in vigore fino all'adozione di eventuali misure che potranno essere previste nel decreto di adeguamento della disciplina in materia, riservandosi ulteriori valutazioni all'esito del predetto percorso normativo"[16], per poi pronunciarsi nuovamente – in seguito all'emanazione del D.Lgs. 101/2018 – il 13 dicembre 2018 con un provvedimento volto ad individuare le prescrizioni delle autorizzazioni generali compatibili con il nuovo sistema legislativo in materia di protezione dei dati personali[17], dal

su mercati finanziari non nazionali, in relazione ai comportamenti penalmente rilevanti individuati dalla normativa nazionale [...]". L'autorizzazione è altresì rilasciata (Capo V – punto 2) a (vi) persone fisiche e giuridiche, istituti, enti ed organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia, ma soltanto ove il trattamento sia necessario "per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto di rango pari a quello del soggetto al quale si riferiscono i dati [...]" o "su incarico di un difensore in riferimento a un procedimento penale, per ricercare e individuare a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova"; nonché a (vii) chiunque per: "far valere un diritto anche da parte di un terzo" presso le sedi competenti (sempre che il diritto da far valere o difendere sia di rango pari a quello dell'interessato); "l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi e i regolamenti" applicabili; "adempiere gli obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso o di altre forme di manifestazione di pericolosità sociale [...] o per poter produrre la documentazione prescritta dalla legge per partecipare a gare d'appalto"; "l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gara d'appalto, in adempimento di quanto previsto dalla normativa applicabile in materia di appalti"; nonché per "l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese".

[14] B. Bernabei, *op. cit.*, p. 100.

[15] Garante per la protezione dei dati personali, cit. *Autorizzazione n. 7/2016*, Capo VII, punto 7) Efficacia temporale.

[16] Garante per la protezione dei dati personali, *Provvedimento in tema di Autorizzazioni generali del Garante per la protezione dei dati personali, 19 luglio 2018* [doc. web: 9026901], consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9026901.

[17] Garante per la protezione dei dati personali, *Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che*

01_PwC_dicembre_2020.indd 161 09/12/20 15:58

cui novero è stata esclusa *in toto* l'Autorizzazione n. 7/2016. Non avrebbe, del resto, potuto essere altrimenti, considerato che il combinato disposto dell'articolo 10, GDPR, e dell'articolo 2-*octies*, Codice Privacy, non lascia alcun margine di manovra al Garante in tema di dati giudiziari, essendo il trattamento limitato, con l'eccezione delle operazioni che avvengono sotto il controllo dell'autorità pubblica, ai soli casi previsti da previsioni di legge o regolamento, nonché alle ipotesi identificate dal Ministro della giustizia.

Alla ricerca di soluzioni *medio tempore*

Lecito quindi domandarsi come dovrebbero essere gestiti a fronte di un quadro normativo ancora incerto e, per certi versi, incompleto una serie di processi comuni alla stragrande maggioranza degli operatori economici – quali, ad esempio, la selezione del personale, la partecipazione a gare pubbliche, l'adempimento degli obblighi previsti dalla normativa antiriciclaggio ovvero ancora l'esecuzione di verifiche preliminari all'avvio di un rapporto contrattuale – nel cui contesto, vuoi per dar seguito a procedure interne, ovvero sulla (magari anche solo asserita) esistenza di un dovere o quantomeno di un bisogno specifico in capo al titolare – potrebbero palesarsi eventuali ipotesi di trattamenti di dati relativi a condanne penali o reati.
Il caso della selezione del personale è emblematico: facendo leva sull'esistenza di un interesse (se non di una necessità) del datore di verificare i "*requisiti di onorabilità*" dei collaboratori in entrata, molti titolari si chiedono come poter dare debito seguito a questa diffusa esigenza se non tramite la raccolta del casellario giudiziale e del certificato carichi pendenti dell'interessato. Al riguardo, tuttavia, l'odierno *framework* normativo sembrerebbe lasciar ben poco margine di manovra, risultando evidente come – in via generale – la regola imporrebbe loro di astenersi dal richiedere la produzione di quei tanto "ambiti" documenti, stante l'eventualità che al loro interno possano riportare informazioni qualificabili come dati giudiziari.
Una soluzione *medio tempore* di pronto impiego – pur sempre accettando un minimo di rischio – potrebbe anche esistere (forse): se è vero infatti che un'informazione circa la non esistenza di precedenti condanne o procedimenti penali in corso non rientra nella definizione di cui all'articolo 10, GDPR, allora, in luogo della raccolta del casellario o del certificato carichi pendenti, potrebbe essere valutata l'opportunità di limitarsi a richiedere al candidato

risultano compatibili con il Regolamento e con il D.Lgs. n. 101/2018 di adeguamento del Codice, 13 dicembre 2018 [doc. web: 9068972], consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972.

01_PwC_dicembre_2020.indd 162 09/12/20 15:58

di autocertificare l'assenza di procedimenti a suo carico (siano essi pendenti o conclusi). Il contenuto della dichiarazione "negativa" essendo privo di informazioni meritevoli di particolare tutela non comporterebbe infatti il trattamento di dati giudiziari e, al contempo, risulterebbe funzionale ad assicurare la conformità dell'operazione di trattamento ai principi di limitazione della finalità e di minimizzazione dei dati di cui all'articolo 5, GDPR[18].
Nonostante questo *escamotage* possa risultare tanto banale quanto efficace, a dire il vero parrebbero ancora residuare ipotesi in cui la richiesta di una certificazione sostitutiva potrebbe non essere sufficiente a mettere del tutto al riparo il titolare da possibili vicoli ciechi o, addirittura, da responsabilità: cosa succederebbe infatti se il candidato rifiutasse di rendere la dichiarazione? E se questa risultasse palesemente falsa o, ancor peggio, vi fosse il dubbio che potesse esserlo? E poi, come comportarsi nel caso di interessati che siano dipendenti in posizione apicale e che potrebbero agire in qualità di legali rappresentanti o procuratori del proprio datore di lavoro?
Altro ambito in cui potrebbero essere effettuati trattamenti (non leciti) di dati giudiziari è quello della partecipazione a gare pubbliche soggette all'applicazione del Decreto legislativo 18 aprile 2016, n. 50 ("**Codice Appalti**"). In questo contesto, infatti, alla sussistenza in capo all'operatore economico dell'obbligo di dichiarare l'assenza delle cause di esclusione previste dall'articolo 80, Codice Appalti, mediante la compilazione del DGUE e delle eventuali dichiarazioni integrative richieste dalla stazione appaltante, viceversa, non sembrerebbe corrispondere un dovere di produrre i certificati attestanti il possesso dei requisiti dichiarati in sede di gara: l'articolo 43, D.P.R. 28 dicembre 2000, n. 445, imporrebbe infatti alle stazioni appaltanti – e non ai partecipanti alla gara – l'onere di acquisire autonomamente presso i competenti uffici pubblici le documentate informazioni oggetto delle dichiarazioni sostitutive rese in precedenza dai concorrenti.
Di conseguenza, malgrado l'esistenza di precisi obblighi dichiarativi in capo al concorrente e del connesso rischio di possibili conseguenze di natura penale a carico del legale rappresentante nel caso fossero rilasciate *"dichiarazioni mendaci",* stante l'assenza di un esplicito vincolo di legge relativo alla produzione del casellario giudiziale e del certificato carichi pendenti da

[18] Ai sensi dell'articolo 5, paragrafo 1, lett. b) e c), GDPR: "i dati sono: [...] raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»)" e "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati») [...]".

01_PwC_dicembre_2020.indd 163 09/12/20 15:58

parte di tutti i legali rappresentanti e procuratori del soggetto partecipante alla gara pubblica, non parrebbero – nemmeno in questo caso – ricorrere le condizioni di cui all'articolo 10, Regolamento, per il legittimo trattamento dei dati giudiziari dei soggetti in questione. E ora? Come si esce dal *deadlock*[19]? In questo caso, alla luce della pluralità di rischi per l'organizzazione concorrente e, soprattutto, della possibile responsabilità penale del legale rappresentante in ordine alla falsa attestazione resa dall'interessato, sembrerebbe ancor di più sussistere un legittimo interesse in capo al titolare di ottenere anche la documentazione necessaria a comprovare la veridicità di quanto (auto)dichiarato dai procuratori. Eppure, i termini della questione non cambiano: a rigore di norma, in assenza di obbligo normativo ovvero di disposizioni di legge o regolamento che lo permettano, raccogliere un casellario giudiziale o un certificato carichi pendenti da cui risultasse l'esistenza di dati giudiziari comporterebbe una violazione degli articoli 10, GDPR, e 2-*octies*, Codice Privacy, con tutto ciò che ne consegue.

Potenziali aperture circa la possibilità di conoscere legittimamente dati giudiziari sembrerebbero potersi individuare in una certa misura anche in relazione (i) all'adempimento degli obblighi prescritti ai soggetti rientranti nel campo di applicazione della disciplina in materia di *anti-money laundering* di cui al Decreto legislativo 21 novembre 2007, n. 231, nel testo da ultimo modificato ai sensi del Decreto legislativo 4 ottobre 2019, n. 125 ("**Decreto antiriciclaggio**")[20] – integrata per ciascuna "tipologia" di Soggetti obbligati dalle disposizioni di maggiori dettaglio previste nei provvedimenti di autorità di vigilanza di settore[21] e organismi rappresentativi di categorie

[19] Termine inglese con il quale si identifica una situazione di stallo derivante dall'azione di due forze uguali ed opposte, in cui nessun progresso risulta possibile.

[20] L'articolo 3, Decreto antiriciclaggio, individua all'articolo 3 un'ampia platea di soggetti obbligati al rispetto delle sue disposizioni, tra cui rientrano non soltanto intermediari bancari e finanziari (quali banche, Poste Italiane S.p.A., gli istituti di moneta elettronica, *etc*.) e altri operatori finanziari (*e.g.*: società fiduciarie, mediatori creditizi, *etc*.), ma anche professionisti – tra cui, nello specifico: (a) gli iscritti all'albo dei dottori commercialisti o in quello dei consulenti del lavoro, (b) "ogni altro soggetto che rende i servizi forniti da periti, consulenti e altri soggetti che svolgono in maniera professionale, anche nei confronti dei propri associati o iscritti, attività in materia di contabilità e tributi [...]", (c) i notai e gli avvocati quando compiono operazioni di natura finanziaria o immobiliare e quando assistono i clienti nella predisposizione o nella realizzazione di determinate operazioni, (d) i revisori legali e le società di revisione legale, "altri operatori non finanziari" (*e.g.*: i "soggetti che svolgono attività di recupero stragiudiziale dei crediti per conto di terzi, in presenza della licenza di cui all'articolo 115 TULPS [...]" –, altri operatori non finanziari (*e.g.*: *provider* di servizi relativi a società e trust, soggetti che esercitano l'attività di case d'asta, commercianti di cose antiche, *etc*.) nonché i c.d. prestatori di servizi di gioco ("Soggetti obbligati").

[21] Il riferimento è, in particolare, ai seguenti testi: Commissione nazionale per le società e la borsa, *Regolamento recante disposizioni di attuazione del Decreto legislativo 21 novembre 2007, n.*

01_PwC_dicembre_2020.indd 164 09/12/20 15:58

professionali[22] – e (ii) alle attività inerenti (e similari a) le verifiche che molte organizzazioni svolgono preliminarmente all'instaurazione di rapporti contrattuali con fornitori, clienti o *partner* commerciali.

Con riferimento all'adempimento degli obblighi imposti dalle norme vigenti in materia di prevenzione del riciclaggio e del finanziamento al terrorismo, in effetti – pur dovendosi evidenziare come anche in tali circostanze (salvo il caso di commercialisti ed esperti contabili[23]) la raccolta e archiviazione del casellario giudiziale o del certificato carichi pendenti non risulti espressamente consentita – vi sono specifiche disposizioni a livello di normativa secondaria che (con i limiti di volta in volta precisati[24]) parrebbero giustificare

231 e successive modifiche ed integrazioni per i revisori legali e le società di revisione con incarichi di revisione su enti di interesse pubblico o su enti sottoposti a regime intermedio adottato con Delibera n. 20570 del 4 settembre 2018, disponibile al link: http://www.consob.it/documents/46180/46181/reg_consob_2018_20570.pdf/61495c49-c4aa-42c5-b839-c591e249471d; Banca d'Italia, *Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo*, 30 luglio 2019, disponibili al link: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/20190730-dispo/index.html; Istituto per la Vigilanza sulle Assicurazioni, *Regolamento IVASS n. 44 del 12 febbraio 2019, recante disposizioni attuative volte a prevenire l'utilizzo delle Imprese di assicurazione e degli intermediari assicurativi a fini di riciclaggio e di finanziamento del terrorismo in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela, ai sensi dell'articolo 7, comma 1, lettera a) del Decreto legislativo 21 novembre 2007, n. 231*, disponibile al link: https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2019/n44/index.html.

[22] In particolare: Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, *Linee guida per la valutazione del rischio, adeguata verifica della clientela, conservazione dei documenti, dei dati e delle informazioni ai sensi del D.Lgs. 231/2007 (come modificato dal D.Lgs. 25 maggio 2017, n. 90)*, 23 maggio 2019, disponibili al link: https://commercialisti.it/visualizzatore-articolo?_articleId=1345302&plid=323242; Consiglio Nazionale Forense, *Regole tecniche in materia di procedure e metodologia 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*, 20 settembre 2019, disponibili al link: https://www.consiglionazionaleforense.it/documents/20182/644108/Regole+tecniche.pdf/7aba2d29-22a2-4db4-95ea-bc2d06734299; Consiglio Nazionale Forense, *Criteri e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo, con particolare riferimento all'adeguata verifica semplificata*, 20 settembre 2019, disponibili al link: https://www.consiglionazionaleforense.it/documents/20182/644108/Criteri+e+metodologie.pdf/e7c2ecd9-1866-4a18-b1b1-8d8e376e6a9a.

[23] Per i soli commercialisti ed esperti contabili, ove ciò fosse necessario per valutare la rilevanza rispetto alla prestazione richiesta dal cliente di notizie relative a precedenti penali di cui fosse venuto a conoscenza, sembrerebbe infatti persino possibile richiedere all'interessato la prestazione di attestazioni sostitutive o di certificati rilasciati dal Tribunale (sul punto, Allegati AV.0 e AV.2 alle *Linee guida Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili*).

[24] Tanto il Decreto antiriciclaggio quanto le disposizioni di attuazione di cui ai regolamenti e linee guida predisposti dalle autorità di vigilanza di settore e dagli organismi di autoregolamentazione stabiliscono la necessità di svolgere l'adeguata verifica con un'estensione e un approfondimento variabili in ragione dei fattori di rischio propri del caso concreto.

01_PwC_dicembre_2020.indd 165 09/12/20 15:58

nell'ambito delle procedure di profilatura e adeguata verifica della clientela il trattamento di notizie relative a procedimenti a rilevanza penale, a condizione che queste siano notorie o comunque note al Soggetto obbligato.
La disciplina in questione impone di fatto di effettuare una preliminare identificazione e profilatura della clientela alla luce di una serie di fattori sintomatici del rischio (basso o elevato) di riciclaggio o di finanziamento del terrorismo, all'esito della quale il Soggetto obbligato sarà poi tenuto a svolgere l'adeguata verifica, a seconda dei casi, semplificata o rafforzata. Già nella fase di profilazione preventiva, la normativa secondaria sembra quindi richiedere/permettere di effettuare delle verifiche (ad esempio, sulle liste antiterrorismo stilate da UE, Nazioni Unite o Dipartimento del Tesoro U.S.A.) che potrebbero portare alla conoscenza di dati giudiziari riferiti al cliente o al titolare effettivo del caso. E ciò prima ancora che tali informazioni siano "validate" nell'ambito dell'adeguata verifica e a prescindere dal fatto che la tipologia di cliente, l'operazione o l'area geografica interessata risultino tali da far sorgere un rischio "significativo" comportante l'obbligo di porre in essere misure rafforzate di valutazione. Il che è dunque sufficiente, come parrebbe, a legittimare un trattamento di dati giudiziari? Oppure la norma su cui dovrebbe trovare fondamento la possibilità di conoscere tali informazioni dovrebbe essere maggiormente esplicita e definire altresì le misure di sicurezza a protezione di notizie così delicate?
Sempre facendo leva sulla lettura combinata di disposizioni di legge e testi valevoli quali standard di settore, si potrebbe potenzialmente giungere a conclusioni in parte simili anche con riguardo alle verifiche precontrattuali, ossia a quei c.d. *background check* preliminari alla sottoscrizione di accordi con terze parti previsti dalle *policy* in vigore presso diverse organizzazioni. Si pensi, ad esempio, alle società che offrono servizi di revisione legale: ebbene, dalle disposizioni dedicate alla garanzia della qualità dell'operato del revisore (su tutte, l'articolo 10, Decreto Legislativo 17 luglio 2016, n. 135[25], e le norme contenute nel principio internazionale sul controllo della

[25] L'articolo 10, D.Lgs. 39/2010, prevede espressamente che il revisore nonché ogni persona fisica in grado di influenzare in qualsiasi maniera l'esito della revisione debbano essere indipendenti rispetto all'organizzazione revisionata e non coinvolti in alcun modo nel suo processo decisionale per il periodo a cui si riferiscono i bilanci da verificare e per l'intera durata dell'incarico. A questo fine, il revisore è tenuto ad adottare ogni misura ragionevole per evitare che la sua indipendenza sia influenzata da conflitti di interessi – anche soltanto potenziali – o da relazioni d'affari o di altro genere, siano esse dirette o indirette, riguardanti la sua organizzazione in quanto tale, la sua rete, i membri dei suoi organi di gestione, i suoi dirigenti, revisori e dipendenti, nonché qualsiasi persona direttamente o indirettamente collegata all'*auditor* o alla società di revisione, dovendo esimersi dallo svolgere la revisione legale ove sussistano pericoli di auto-riesame, di interesse personale o rischi derivanti dall'esercizio del patrocinio

01_PwC_dicembre_2020.indd 166 09/12/20 15:58

qualità ISQC 1[26]) emerge la necessità per la rete di cui fa parte il revisore di munirsi di procedure funzionali a garantire indipendenza e assenza di conflitto di interessi, volte, *inter alia*, a valutare l'integrità del cliente (anche) sulla scorta di fattori significativi tra cui la sua identità e reputazione commerciale, la natura delle attività da esso svolte (incluse le sue prassi aziendali) e l'esistenza di eventuali "*indizi sul possibile coinvolgimento del cliente nel riciclaggio di denaro o in altre attività illecite*", facendo affidamento su comunicazioni con altri fornitori, indagini svolte presso terzi (banche, consulenti legali e altri operatori) e ricerche su banche dati specializzate. Pur in assenza di una specifica disposizione che ammetta espressamente la legittimità dell'eventuale trattamento di dati personali relativi a condanne o procedimenti pendenti, l'adozione di un'interpretazione estensiva dei principi di cui sopra potrebbe condurre a ritenere legittimo in questo contesto lo svolgimento di verifiche di portata similare a quelle effettuate in ambito AML, arrivando con ciò ad ammettere la possibilità di processare notizie rientranti nella definizione di dato giudiziario purché siano note o notorie. A questo proposito, tuttavia, è doveroso segnalare che – con riferimento al tema delle verifiche precontrattuali (almeno per ciò che concerne l'ipotesi richiamata) ancor più che con riguardo all'assolvimento degli obblighi imposti dalla normativa antiriciclaggio – la tesi che porterebbe a ritenere

legale, da familiarità ovvero minacce di intimidazione, determinati da relazioni finanziarie, di business, personali, di lavoro o di altro genere instaurate tra il cliente (potenziale o attuale) revisionato e il revisore, il *network* di cui questo fa parte, o qualsiasi persona fisica in grado di influenzare l'esito dell'audit; onere di astenersi dall'assunzione dell'incarico che dovrebbe trovare applicazione ogniqualvolta che, date le circostanze, "un terzo informato, obiettivo e ragionevole, tenendo conto delle misure adottate, trarrebbe la conclusione che l'indipendenza del revisore legale o della società di revisione legale risulti compromessa".

[26] Con specifico riferimento all'accettazione e al mantenimento del rapporto con il cliente, il paragrafo 26 del Principio ISQC 1 prevede, per quanto qui rilevante, che "il soggetto abilitato deve stabilire direttive e procedure per l'accettazione ed il mantenimento del rapporto con il cliente e dei singoli incarichi, configurate per conseguire una ragionevole sicurezza che il soggetto abilitato ponga in essere o mantenga unicamente i rapporti e gli incarichi per i quali: [...] c) abbia considerato l'integrità del cliente e non disponga di informazioni che possano indurlo a concludere che il cliente manchi di integrità" (par. 26 con rimandi ai parr. A18-A20 e A23). Al riguardo, il Principio in esame propone al par. A19 un elenco non esaustivo di fattori da tenere nel debito conto nella valutazione dell'integrità del cliente, che include, *inter alia*, "l'identità e la reputazione commerciale dei principali proprietari del cliente, dei membri della direzione con responsabilità strategiche e dei responsabili delle attività di governance; la natura delle attività del cliente, incluse le sue prassi aziendali, e informazioni sull'atteggiamento dei principali proprietari del cliente, dei membri della direzione con responsabilità strategiche e dei responsabili delle attività di governance in relazione ad aspetti quali l'interpretazione aggressiva dei principi contabili e l'ambiente di controllo interno" nonché "indizi sul possibile coinvolgimento del cliente nel riciclaggio di denaro o in altre attività illecite".

01_PwC_dicembre_2020.indd 167 09/12/20 15:58

lecito il trattamento di dati di cui all'articolo 10, GDPR, sembrerebbe trovare fondamento soltanto su pochi appigli testuali, prestando dunque il fianco all'eventualità che l'autorità di controllo possa assumere posizioni in senso difforme, stante, se non altro, l'assenza a livello normativo e nei principi di revisione internazionali di alcun indicatore chiaro e specifico in relazione alla possibilità/necessità per i destinatari di tali prescrizioni di trattare informazioni in merito all'esistenza di condanne procedimenti penali. L'ambito in questione, nelle more del decreto del Ministero della giustizia, sembrerebbe dunque destinato a inserirsi in una sorta di zona grigia, risultando tutt'altro che semplice identificare precise indicazioni in un verso o nell'altro all'interno della disciplina applicabile. E ora?

Note conclusive e appuntamento alla prossima pubblicazione

Salva l'ipotesi eccezionale dell'attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con le prefetture, in attesa dell'emissione di un decreto ministeriale che – come il Signor Godot del teatro dell'assurdo – sembra non voler apparire mai sulla scena, oggi il trattamento dei dati giudiziari è permesso soltanto laddove autorizzato da una norma di legge o di regolamento, che prevedano appropriate garanzie in conformità agli articoli 10, GDPR, e 2-*octies*, Codice Privacy.

In aggiunta, non vi è alcuna presa di posizione ufficiale ed inequivoca da parte del Garante nel senso di considerare al di fuori dal novero delle informazioni relative a condanne penali e reati le notizie circa l'inesistenza di tali circostanze, che si apprenderebbero qualora il casellario giudiziale, il certificato carichi pendenti, o un'autocertificazione fornita dallo stesso interessato fossero "puliti".

L'esclusione di queste informazioni "negative" dal concetto di dato giudiziario, quindi, è una conclusione al momento raggiungibile solamente in chiave interpretativa (i) rifacendosi al *wording* della definizione adottata dall'autorità di controllo, ove il riferimento è a informazioni che "*possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale [...] o la qualità di imputato o di indagato*", (ii) richiamando le considerazioni fatte proprie dal Garante con il parere reso il 18 agosto 2017 in merito all'istanza di accesso civico ricevuta dal Ministero dello sviluppo economico, e (iii) ontologicamente ragionando *a contrario* dal presupposto per cui se una maggiore tutela è da riconoscere a questa tipologia di notizie (così come ai dati "sensibili" o "particolari",

01_PwC_dicembre_2020.indd 168 09/12/20 15:58

che dir si voglia, di cui all'articolo 9, GDPR) in quanto la loro rivelazione potrebbe comportare un rischio concreto di discriminazioni o pregiudizi per l'interessato, nel momento in cui l'informazione è invece assente – ossia, non vi è evidenza di alcun carico pendente o sanzione penale – verrebbe meno anche il rischio che giustifica il divieto al trattamento.

Ciò posto, attesa la particolare natura dei dati giudiziari – e proprio in virtù dell'incertezza che vi sarà sulla questione sino all'emissione del provvedimento del Ministro della giustizia – risulta sicuramente opportuno adottare un approccio estremamente cautelativo.

A questo proposito, per mesi abbiamo lavorato con l'obiettivo di individuare potenziali vie d'uscita ad una situazione che continua a destare preoccupazione tra titolari ed esperti del settore[27]. Le fattispecie e i quesiti menzionati in precedenza sono solo alcuni tra quelli sui quali abbiamo a lungo ragionato, ipotizzando soluzioni che, nel rispetto del disposto e dei principi del Regolamento e del Codice Privacy e in conformità alle indicazioni del Garante, potessero trovare un equo bilanciamento tra gli interessi in gioco e fossero suscettibili di eventuale immediata implementazione nelle more del provvedimento ministeriale.

Non resta dunque che darsi appuntamento a breve, quando sarà pubblicata una versione completa e approfondita delle risultanze del nostro lavoro.

[27] Le voci provenienti dal mercato sono unanimi nel rilevare l'esigenza per molti operatori di procedere alla raccolta di dati giudiziari nel contesto di svariate attività aziendali (soprattutto nell'ottica di assicurare la propria conformità a specifiche richieste normative) e la conseguente necessità che si faccia presto chiarezza. Nel dettaglio, Assonime richiede che la situazione di transizione venutasi a creare con la perdita di efficacia dell'Autorizzazione n. 7/2016 sia quanto prima superata mediante "un adeguato intervento del legislatore, in attuazione dell'articolo 2-*octies*, tale da rimuovere ogni incertezza sulla sussistenza o meno, nei vari contesti, di una base normativa che autorizzai il trattamento dei dati relativi a condanne penali e reati e da colmare le eventuali lacune". L'Associazione fra le società italiane per azioni precisa che il trattamento di dati giudiziari è necessario – in una prospettiva che a volte è prevalentemente privatistica, a volte di interesse pubblico – per lo svolgimento dell'attività economica delle imprese e, nello specifico, per accertare l'idoneità di alcuni soggetti a svolgere compiti che presentano particolari profili di rischio, per accedere al mercato dei contratti pubblici, per operare come stazioni appaltanti e anche per rispettare eventuali obblighi in materia antimafia o antiriciclaggio. Nella circolare recentemente pubblicata, Assonime presenta dunque una serie di considerazioni in merito ad alcuni tra gli ambiti maggiormente rilevanti per le organizzazioni (*i.e.*: rapporti di lavoro, verifica dei requisiti di onorabilità, appalti pubblici, adempimento di obblighi antimafia e antiriciclaggio, *rating* di legalità, attuazione delle norme per la prevenzione delle responsabilità penale dell'impresa e il contrasto alla corruzione) individuando possibili soluzioni che il Ministero della giustizia dovrebbe tenere nel debito conto per andare incontro alle esigenze delle imprese. Assonime, *Note e Studi 9/2020 – Trattamento dei dati relativi a condanne penali e reati da parte delle imprese: verso l'attuazione dell'art. 2-*octies *del Codice privacy*, in www.assonime.it, 17 marzo 2020, disponibile al seguente link: http://www.assonime.it/attivita–editoriale/studi/Pagine/note–e–studi–9–2020.aspx.

01_PwC_dicembre_2020.indd 169 09/12/20 15:58