assonime

Associazione fra le società italiane per azioni

9/2020

Note e Studi

Trattamento dei dati relativi a condanne penali e reati da parte delle imprese:

verso l'attuazione dell'art. 2-octies del Codice privacy

Introduzione

Il trattamento dei dati relativi a condanne penali, a reati o alle connesse misure di sicurezza costituisce uno degli ambiti più delicati della disciplina europea a tutela dei dati personali.

Già prima del regolamento (UE) 2016/679 (GDPR), la direttiva 95/46/CE e la disciplina nazionale di recepimento avevano definito uno specifico insieme di regole per il trattamento di questi dati.

In particolare, l'articolo 27 del decreto legislativo n. 196/2003 (Codice privacy) consentiva il trattamento dei dati giudiziari da parte di privati o di enti pubblici economici soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specificasse le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

In quel contesto normativo, nell'autorizzazione generale n. 7/2016 il Garante aveva indicato una serie di ambiti nei quali, rispettando specifiche prescrizioni ivi contenute e fermi restando i principi generali della disciplina tra cui quello della minimizzazione del trattamento dei dati personali, il trattamento dei dati giudiziari era legittimo. Gli ambiti coperti dall'autorizzazione comprendevano, tra gli altri: i rapporti di lavoro; l'attività di associazioni e fondazioni; l'attività dei liberi professionisti; le imprese bancarie e assicuratrici; l'attività di investigazione privata; la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto; l'accertamento dell'idoneità morale di coloro che intendono partecipare a gare di appalto, ai sensi della normativa prevista in materia di appalti; l'adempimento degli obblighi previsti dalle disposizioni in materia di comunicazione e certificazioni antimafia; l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese.

1. L'attuale quadro normativo

Con il GDPR, le disposizioni europee riguardo al trattamento dei dati penali sono state rese più chiare rispetto a quanto previsto dalla direttiva 95/46/CE[1].

[1] L'articolo 8, paragrafo 5, della direttiva 95/46/CE prevedeva che i trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle connesse misure di sicurezza potessero essere effettuati solo sotto il controllo dell'autorità pubblica o se venivano fornite opportune garanzie specifiche sulla base del diritto nazionale, fatte salve le deroghe che potevano essere fissate dallo Stato membro in base ad una disposizione nazionale che prevedesse garanzie appropriate e specifiche. Anche in base alla formulazione

L'attuale articolo 10 del 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 è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati". Come noto, l'articolo 6, paragrafo 1, del GDPR richiamato dall'attuale formulazione individua le diverse possibili basi giuridiche per la liceità del trattamento.

Gli Stati membri hanno già adeguato o stanno adeguando la propria disciplina. In Italia, il decreto legislativo n. 101/2018, adottato per conformare la normativa nazionale a valle del GDPR, ha eliminato lo strumento dell'autorizzazione generale da parte del Garante per il trattamento dei dati giudiziari (art. 21) e ha introdotto nel Codice privacy un nuovo articolo 2-octies recante "Principi relativi al trattamento di dati relativi a condanne penali e reati".

Le prescrizioni dell'articolo 2-octies, che qui ricordiamo per comodità ai fini dell'analisi successiva, sono articolate in sei commi.

In base al primo comma, il trattamento dei dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'art. 6, comma 1, del GDPR, laddove non avviene sotto il controllo di un'autorità pubblica, è consentito ai sensi dell'articolo 10 del GDPR **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 libertà degli interessati[2].

Il secondo comma sancisce che, in mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati giudiziari di cui al comma 1 e le connesse garanzie sono individuati con **decreto del Ministero della Giustizia** da adottarsi sentito il Garante.

Il terzo comma aggiunge che, fermo restando quanto previsto dai commi 1 e 2, il trattamento dei dati personali relativi alle condanne penali e ai reati o alle connesse

della direttiva, come nel GDPR, un eventuale registro completo delle condanne può essere tenuto solo sotto il controllo dell'autorità pubblica.

[2] Viene fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, che è stato adottato in attuazione della direttiva 2016/680/UE e contiene la disciplina relativa al trattamento dei dati giudiziari da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati.

misure di sicurezza è consentito se autorizzato da una norma di legge o nei casi previsti dalla legge, di regolamento riguardanti **"in particolare" una serie di ambiti**[3].

Viene poi specificato che nei casi in cui le disposizioni di cui al comma 3 non individuano le **garanzie** appropriate per i diritti e le libertà degli interessati, tali garanzie sono previste con il decreto ministeriale (comma 4) e che se il trattamento avviene **sotto il controllo dell'autorità pubblica** si applicano le garanzie dell'art. 2-sexies del Codice (comma 5)[4].

Infine, l'articolo 2-octies, comma 6 prevede che con il decreto del Ministro della Giustizia di cui al comma 2 possono essere autorizzati i trattamenti dei dati relativi alle condanne penali, ai reati e alle connesse misure di sicurezza effettuati **in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità**

[3] Il testo completo dell'art. 2-octies, comma 3, è il seguente: "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] L'art. 2-sexies disciplina il trattamento dei dati particolari necessario per motivi di interesse pubblico rilevante, rispetto al quale le leggi devono specificare i dati , le operazioni e le misure a tutela dei diritti.

organizzata stipulati con il Ministero dell'Interno o con le prefetture. In relazione a tali protocolli, il decreto deve individuare le tipologie di dati trattati, gli interessati, le operazioni di trattamento eseguibili, anche in relazione all'aggiornamento e alla conservazione dei dati e prevedere le garanzie appropriate per i diritti e le libertà degli interessati. Per questi ambiti il decreto è adottato di concerto con il Ministro dell'Interno.

L'impostazione dell'articolo 2-octies merita qualche breve considerazione a commento.

In sostanza, ferma restando la disciplina prevista dal decreto legislativo n. 51/2018 per le autorità pubbliche a fini di prevenzione, indagine, accertamento e perseguimento dei reati, l'ordinamento prevede due modalità per consentire il trattamento dei dati relativi a condanne penali, reati e connesse misure di sicurezza in attuazione dell'art. 10 del GDPR:

a. l'autorizzazione tramite norme di legge o, se previsto dalla legge, regolamenti;

b. l'autorizzazione tramite decreto ministeriale, adottato dal Ministro della Giustizia, sentito il Garante, che ha copertura a livello di normativa primaria nello stesso art. 2-octies, comma 2, del Codice privacy. Per i trattamenti associati a protocolli d'intesa con Ministero degli interni e prefetture, il decreto ministeriale è adottato di concerto con il Ministro dell'Interno.

Per quanto riguarda gli ambiti che, in base al comma 3, possono "in particolare" essere oggetto di autorizzazione normativa al trattamento dei dati giudiziari, è da ritenere che si tratti di un elenco esemplificativo e non esaustivo, ispirato all'autorizzazione generale n. 7/2016 e volto ad assicurare una certa continuità con il quadro previgente.

2. Importanza di una chiara base normativa per il trattamento dei dati penali da parte delle imprese

Con il venire meno dell'autorizzazione generale n. 7/2016 si è creata una situazione di transizione, che va ora superata con 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 autorizza il trattamento dei dati relativi a condanne penali e reati e da colmare le eventuali lacune.

Guardando alle imprese, va sottolineato che vi sono ambiti in cui il trattamento dei dati giudiziari di determinati soggetti è necessario per lo svolgimento dell'attività

economica, in una prospettiva che a volte è prevalentemente privatistica, a volte soprattutto di interesse pubblico.

Anzitutto, il trattamento di questi dati da parte dell'impresa può essere necessario per accertare l'idoneità degli interessati a svolgere compiti che presentano specifici profili di rischio, a tutela della stessa impresa o di terzi in una prospettiva di protezione.

In secondo luogo, sul piano giuridico la verifica dei dati giudiziari di determinati soggetti da parte delle imprese è indispensabile per accedere al mercato dei contratti pubblici e, simmetricamente, per operare come stazioni appaltanti laddove ve ne siano i presupposti, ma anche per rispettare la legge laddove l'impresa sia tenuta ad attuare gli obblighi antimafia e antiriciclaggio e per beneficiare dei trattamenti premiali previsti dall'ordinamento per gli operatori economici che assicurano il rispetto di elevati standard di legalità.

La verifica dell'assenza di condanne penali e reati nelle controparti contrattuali può risultare necessaria anche per gli appalti di natura privatistica, per una due diligence reputazionale a fini di prevenzione della corruzione e delle infiltrazioni criminali nell'attività economica.

Vi sono infine settori in cui il trattamento di dati relativi a condanne e reati può trovare giustificazione per risolvere problemi informativi specifici di una determinata attività economica (si pensi ad esempio alla prevenzione delle frodi nel settore assicurativo).

In questi vari ambiti, dunque, l'ordinamento dovrebbe consentire ('autorizzare') il trattamento dei dati relativi a condanne penali, reati e alle connesse misure di sicurezza che risulti necessario e proporzionato in relazione alle esigenze di protezione dell'impresa e alle varie esigenze di interesse pubblico coinvolte (tutela dei terzi, prevenzione delle infiltrazioni criminali nell'attività economica, ecc.).

Naturalmente, la circostanza che il trattamento dei dati penali venga autorizzato a livello normativo in attuazione dell'art. 2-octies non comporta che il trattamento di tali dati sia consentito tout court: occorre comunque rispettare tutte le regole e i principi del GDPR, che assicurano già una rigorosa base di tutela a cui potranno aggiungersi le specifiche garanzie previste dal decreto ministeriale.

È indubbio che, **laddove la normativa vigente obbliga l'impresa a raccogliere i dati in questione**, l'autorizzazione normativa richiesta dall'articolo 2-octies in aggiunta alla base giuridica di cui all'articolo 6, paragrafo 1, del GDPR già esista. Laddove invece la normativa nazionale esistente si limita a consentire, senza imporre, la raccolta di dati,

appare utile a fini di certezza giuridica che il decreto ministeriale (o, in alternativa, un intervento a livello di normativa primaria) sancisca senza ombra di dubbio che l'autorizzazione normativa per quel tipo di trattamento sussiste.

Una traccia per la ricognizione dei trattamenti da parte delle imprese che andrebbero indicati nel decreto ministeriale è fornita da un lato dalla previgente autorizzazione generale n. 7/2016 e dall'altro dall'elenco di cui all'articolo 2-octies, comma 3, che individua in via esemplificativa alcuni ambiti di interesse.

Nel seguito di questa nota presentiamo una serie di considerazioni su alcuni degli ambiti più rilevanti per le imprese in vista dell'attuazione dell'art. 2-octies. Ci soffermiamo in particolare su: rapporti di lavoro (par. 3); verifica di requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi (par. 4); appalti pubblici (par. 5); obblighi antimafia e antiriciclaggio (par. 6); rating di legalità (par. 7); attuazione delle norme per la prevenzione della responsabilità penale dell'impresa e il contrasto alla corruzione (par. 8). Verrà infine presentata qualche osservazione riguardo allo strumento dei protocolli di legalità con il Ministero dell'interno e le prefetture, alla luce della pronuncia del Consiglio di Stato n. 452/2020.

3. Rapporti di lavoro (art. 2-octies, comma 3, lett. a)

In specifici ambiti, la normativa italiana pone un obbligo sul datore di lavoro di raccolta di dati giudiziari nell'ambito di rapporti di lavoro (ad esempio, per le attività che prevedono un'interazione della persona con minori[5]).

In altri casi, indirettamente, l'articolo 8 dello Statuto dei lavoratori prevede la possibilità per il datore di lavoro di compiere indagini sul lavoratore nella misura in cui siano necessarie a verificare l'attitudine allo svolgimento della prestazione professionale. Tuttavia, non trattandosi di un obbligo ma di una facoltà, riconosciuta dall'ordinamento nel rispetto dei principi di necessità e proporzionalità delle informazioni richieste in relazione alla prestazione professionale prevista, appare opportuno che la sussistenza a questi fini dell'autorizzazione normativa al trattamento dei dati giudiziari nei rapporti di lavoro venga esplicitata nel decreto ministeriale.

Osserviamo che correttamente la formulazione dell'articolo 2-octies, comma 3, lettera a) non si limita a richiamare l'adempimento di obblighi, ma anche l'esercizio di diritti da parte del titolare o dell'interessato, nell'ambito dei rapporti di lavoro.

[5] Decreto del Presidente della Repubblica n. 313/2002.

Per i rapporti di lavoro il decreto ministeriale potrebbe quindi prevedere che il trattamento dei dati relativi alle condanne penali, ai reati e alle connesse misure di sicurezza è autorizzato per l'adempimento degli obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto di lavoro o comunque nell'ambito di rapporti di lavoro, salvi restando i limiti previsti da leggi, regolamenti e contratti collettivi, anche aziendali, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b) e 88 del GDPR.

Similmente, il decreto potrebbe precisare, in linea con l'autorizzazione generale n. 7/2016, che Il trattamento può essere effettuato, nel rispetto dei principi del GDPR, da persone fisiche e giuridiche, enti, associazioni e organismi che:

a. sono parte di un rapporto di lavoro;

b. utilizzano prestazioni lavorative anche atipiche, parziali o temporanee;

c. conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti e mandatari.

Si potrebbe specificare che il trattamento può riguardare in particolare dati attinenti a soggetti che hanno assunto o intendono assumere la qualità di:

a. lavoratori subordinati, anche se parti di un contratto di apprendistato o di formazione e lavoro, o di inserimento, o di lavoro ripartito, o di lavoro intermittente o a chiamata, ovvero prestatori di lavoro nell'ambito di un contratto di somministrazione, o in rapporto di tirocinio ovvero associati anche in compartecipazione o di titolari di borse di lavoro e di rapporti analoghi;

b. consulenti e liberi professionisti, agenti, rappresentanti e mandatari.

In linea con l'autorizzazione generale, si potrebbe inoltre indicare che è autorizzato anche il trattamento dei suddetti dati laddove tale trattamento sia indispensabile da parte di soggetti in relazione ad attività di composizione di controversie esercitate in conformità alla legge.

Il decreto ministeriale potrebbe infine indicare, sempre in linea con l'autorizzazione generale, che restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa dell´Unione europea che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute nell´art. 8 della legge 20 maggio 1970, n. 300, che vieta al datore di lavoro ai fini dell´assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche

a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell´attitudine professionale del lavoratore e nell´art. 10 del d. lgs. 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare indagini sulle opinioni e trattamenti discriminatori di preselezione di lavoratori. Si potrebbero richiamare anche gli obblighi di legge che vietano la rivelazione senza giusta causa e l´impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici o di buona condotta relativi alle singole figure professionali.

La formulazione proposta appare sufficientemente flessibile da consentire, **in relazione alla concreta prestazione lavorativa richiesta e al settore di attività**, l'accertamento dell'assenza di condanne penali o reati laddove questo accertamento sia necessario e proporzionato. Resta da valutare se sia o meno utile indicare espressamente, come avveniva nell'autorizzazione generale n. 7/2016, che è autorizzata la verifica, limitatamente ai dati strettamente necessari, dei requisiti di onorabilità dei dipendenti di società operanti nel settore del rating.

4. Requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi (art. 2-octies, comma 3, lett. c)

In questo ambito, espressamente richiamato dall'art. 2-octies e precedentemente disciplinato dalla autorizzazione generale n. 7/2016, appare sufficiente un richiamo, nel decreto ministeriale, al trattamento indispensabile per adempiere o esigere l'adempimento di specifici obblighi o eseguire specifici compiti previsti dalla legge, dalla normativa dell'Unione europea o da regolamenti, con particolare riferimento:

a. all'accertamento, nei casi previsti da leggi o regolamenti, dei requisiti di onorabilità dei soci, degli amministratori o dei membri degli organi esecutivi o di controllo, o di titolari di cariche direttive o elettive;

b. all'accertamento, nei casi previsti dalla legge, di requisiti soggettivi e presupposti interdittivi.

La necessità di accedere a dati relative a condanne penali o reati per accertare i requisiti di onorabilità esiste, ad esempio, per l'attività bancaria e creditizia e per l'attività assicurativa e dei fondi pensione, come richiamato dall'autorizzazione n. 7/2016, ma anche per le società quotate (art. 148 TUF e decreto ministeriale 30 marzo 2000, n. 172), per le società a controllo pubblico non quotate (in attuazione dell'art. 11

del decreto legislativo n. 175/2016), per gli enti di diritto privato in controllo pubblico per quanto attiene all'inconferibilità degli incarichi (in attuazione del decreto legislativo n. 39/2013).

5. Appalti (art. 2-octies, comma 3, lett. h seconda parte e lett. i)

L'articolo 2-octies, comma 3, indica tra gli ambiti in cui autorizzare il trattamento dei dati giudiziari "l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti".

Il riferimento principale è costituito dall'articolo 80 del Codice dei contratti pubblici, in base al quale le stazioni appaltanti (che possono anche essere imprese)[6] devono verificare per i contratti pubblici l'assenza di una serie di cause di esclusione degli operatori economici dalla partecipazione alla procedura di appalto o concessione. Il comma 3 dell'articolo 80 individua i soggetti rispetto ai quali occorre accertare l'assenza di tali motivi di esclusione (ad es. soci, amministratori, direttori tecnici). Questa attività comporta, per le stazioni appaltanti, il trattamento di dati giudiziari relativi a soggetti all'interno dell'impresa contraente e anche in relazione ai suoi eventuali subappaltatori.

Guardando alle ragioni sostanziali della disciplina, il trattamento dei dati giudiziari in questi ambiti è funzionale a perseguire la finalità indicata dalle direttive europee di "evitare l'aggiudicazione di appalti pubblici ad operatori economici che hanno partecipato a un'organizzazione criminale" o che si sono resi colpevoli di specifiche attività illecite[7].

Per questo motivo, si può ritenere che, anche al di là degli obblighi normativi, la possibilità di trattare i dati giudiziari per verificare se sussistano le cause di esclusione di cui all'art. 80 vada riconosciuta per tutti i contratti (c.d. contratti pubblici) ai sensi dell'art. 3, comma 1, lett. dd) del decreto legislativo n. 50/2016, ossia tutti i contratti di appalto o concessione posti in essere dalle stazioni appaltanti di cui all'art. 3, comma 1, lett. o del Codice, inclusi i contratti per i quali non è richiesto l'espletamento di procedure di gara.

[6] Decreto legislativo n. 50/2016, art. 3, lett. o).
[7] Direttiva 2014/24/UE, considerando 100.

A questo fine andrebbe incluso nel decreto ministeriale un riferimento generale al trattamento dei dati relativi alle condanne penali, ai reati e alle connesse misure di protezione necessari per l'accertamento da parte delle stazioni appaltanti, come definite dall'articolo 3, comma 1, lett. o) del Codice dei contratti pubblici, delle cause di esclusione di cui all'art. 80 del Codice dei contratti pubblici rispetto a coloro che, a qualsiasi titolo, intendono stipulare con esse un contratto pubblico per la fornitura di beni o servizi o per l'esecuzione di opere o lavori.

Simmetricamente, come già previsto dall'autorizzazione generale n. 7/2016, l'articolo 2-octies prevede che vada autorizzato **il trattamento dei dati giudiziari per produrre la documentazione prescritta dalla legge per partecipare a gare d'appalto**. In questo caso, i titolari del trattamento sono le imprese che già operano nel settore dei contratti pubblici o intendono accedervi in futuro. L'esigenza di interesse pubblico è quella di consentire alle imprese, in tutti i settori, di essere in grado di partecipare in tempi rapidi all'aggiudicazione di contratti pubblici assicurando l'assenza di motivi di esclusione ex articolo 80 del Codice connessi all'idoneità morale all'interno dell'impresa stessa e nella rete dei suoi fornitori.

A questo fine, appare opportuno che in attuazione dell'art. 2-octies il decreto ministeriale autorizzi le imprese a raccogliere ex ante e verificare periodicamente i dati giudiziari relativi alle cause di esclusione previste dall'articolo 80 del Codice dei contratti pubblici per le figure apicali al loro interno e per i fornitori che potrebbero fungere da subappaltatori.

6. Obblighi antimafia e antiriciclaggio (art. 2-octies, comma 3, lett. h) ed m)

Tra gli ambiti per cui l'articolo 2-octies prevede l'autorizzazione del trattamento dei dati relativi a condanne penali e reati vi sono le ipotesi in cui il trattamento è necessario per adempiere a:

- obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia, o di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti (lett. h, prima parte)
- obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (lett. m).

Trattandosi di obblighi normativi, in linea di principio non occorre una apposita previsione da parte del decreto ministeriale per fornire la base normativa che autorizza il trattamento. Il decreto potrebbe semplicemente richiamare questi ambiti, anche al fine dell'applicazione del regime delle garanzie che verrà specificato dal decreto stesso.

E' utile soffermarsi brevemente sul contenuto degli obblighi in materia di documentazione antimafia previsti dal decreto legislativo n. 159/2011, per i collegamenti con quanto si dirà in seguito riguardo ai protocolli di intesa con Ministero dell'Interno e Prefetture. Anche in questo caso, come per i contratti pubblici, i soggetti destinatari dell'obbligo sono un insieme predeterminato (più ampio rispetto alle stazioni appaltanti di cui all'art. 3, comma 1, lett. o). Gli obblighi si rivolgono infatti a pubbliche amministrazioni, enti pubblici anche costituiti in stazioni uniche appaltanti, enti e aziende vigilati dallo Stato o altro ente pubblico, società o imprese comunque controllate dallo Stato o da altro ente pubblico, concessionari di lavori e servizi pubblici e contraenti generali (art. 83, commi 1 e 2).

Tali soggetti, prima di stipulare, approvare o autorizzare contratti e subcontratti relativi a lavori, servizi e forniture pubblici di valore superiore a 150 000 euro, ovvero prima di rilasciare o consentire i provvedimenti indicati nell'articolo 67 (ad esempio, un'autorizzazione) sono tenuti ad acquisire la documentazione antimafia relativa ad alcune persone (legale rappresentante, componenti del consiglio di amministrazione e così via). Anche in questo caso le fattispecie penali rilevanti ai fini dell'interdizione sono puntualmente determinate.

La documentazione antimafia consiste nell'attestazione della sussistenza o meno di una delle cause di decadenza, sospensione o divieto di cui all'articolo 67. L'informazione antimafia prevede invece, in aggiunta a tale attestazione, anche l'attestazione della sussistenza o meno di eventuali tentativi di infiltrazione mafiosa tendenti a condizionare le scelte e gli indirizzi delle società o imprese interessate, desunti da una serie di indicatori.

La disciplina prevede anche, in alcune ipotesi, la possibilità di acquisire un'autocertificazione con cui l'interessato accerta che nei suoi confronti non sussistono le cause di divieto, decadenza o esclusione di cui all'articolo 67.

7. Rating di legalità (art. 2-octies, comma 3, lettera l)

L'articolo 2-octies, in linea con la precedente autorizzazione generale n. 7/2016, prevede la possibilità del trattamento di dati giudiziari per l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese, di cui all'articolo 5-ter del decreto legge n. 1/2012, convertito con modificazioni dalla legge n. 27/2012.

Ricordiamo che per ottenere il rating di legalità dall'Autorità garante della concorrenza e del mercato l'impresa deve dichiarare l'assenza di condanne per determinati reati da parte dei titolari dell'impresa e delle figure apicali (requisiti necessari per l'attribuzione del rating). L'impresa, quindi, deve potere chiedere a tali soggetti informazioni relative alle condanne per i reati rilevanti. Se non fosse consentito il trattamento di questi dati giudiziari, l'impresa non potrebbe accedere al rating di legalità.

Ottenere il rating di legalità non è un obbligo per l'impresa, ma una mera facoltà, a cui corrispondono per l'impresa stessa benefici in termini di immagine e vantaggi di tipo premiale (nell'accesso ai finanziamenti pubblici e al credito bancario). L'ordinamento attribuisce una valenza positiva al conseguimento del rating di legalità "ai fini della promozione dell'introduzione dei principi etici nei comportamenti aziendali" (art. 5-ter, d.l. 1/2012).

Dato che richiedere il rating non è un obbligo giuridico, occorre che il decreto ministeriale autorizzi espressamente il trattamento dei dati relativi a condanne penali, reati e connesse misure di sicurezza in questo contesto. L'autorizzazione deve riguardare sia i dati che sono necessari per accedere al rating, sia quelli necessari per conseguire un punteggio superiore al punteggio base, a cui si associa un trattamento premiale rafforzato.

Al fine di una visione completa dei rapporti tra le diverse discipline, va ricordato che tra le condizioni per conseguire un punteggio superiore a quello base vi sono:

- l'adozione di una funzione o struttura organizzativa, anche in outsourcing, che espleti il controllo di conformità delle attività aziendali a disposizioni normative applicabili all'impresa o di un modello organizzativo ai sensi del decreto legislativo 8 giugno 2001, n. 231;
- essere iscritti in uno degli elenchi di fornitori, prestatori di servizi ed esecutori di lavori non soggetti a tentativi di infiltrazione mafiosa istituiti ai sensi delle vigenti disposizioni di legge (white list);

- aver adottato modelli organizzativi di prevenzione e di contrasto della corruzione;
- l'adesione ai protocolli o alle intese di legalità finalizzati a prevenire e contrastare le infiltrazioni della criminalità organizzata nell'economia legale, sottoscritti dal Ministero dell'Interno o dalle Prefetture-UTG con associazioni imprenditoriali e di categoria[8].

8. Evitare la responsabilità penale dell'impresa e prevenire la corruzione

In generale, se l'autorizzazione normativa del trattamento dei dati giudiziari si giustifica quando l'ordinamento riconosce una premialità alle imprese che accedono al rating di legalità, a fortiori dovrebbe essere riconosciuta quando l'ordinamento chiede alle imprese di organizzarsi per evitare la commissione di reati.

Il decreto ministeriale dovrebbe quindi considerare direttamente, e non solo attraverso la disciplina del rating di legalità, il trattamento di dati giudiziari necessario in attuazione di altri istituti previsti dall'ordinamento a cui viene riconosciuto un valore nell'interesse generale, con particolare riferimento al decreto legislativo n. 231/2001 e alle norme a livello nazionale, europeo e internazionale volte alla prevenzione dell'illegalità e della corruzione.

In particolare, il decreto legislativo n. 231/2001 in tema di responsabilità amministrativa degli enti richiede all'operatore economico di adottare presidi organizzativi adeguati a prevenire la commissione di una serie di reati all'interno dell'impresa, che comporterebbero responsabilità penali per l'impresa stessa. Tra le varie modalità per adempiere ed evitare la responsabilità, il modello organizzativo rappresenta lo strumento generalmente adottato dalle imprese di medio-grande dimensione, all'interno di un più ampio sistema di gestione e controllo dei rischi.

Inoltre molte imprese, soprattutto quelle che operano nei mercati internazionali, adottano modelli organizzativi di prevenzione e contrasto della corruzione in attuazione di normative di altri ordinamenti, ispirate perlopiù alla disciplina statunitense (Foreign Corrupt Practices Act - FCPA) e alla Convenzione OCSE su "Combating Bribery of Foreign Officials in International Business Transactions". In particolare, a partire dal 2011 diversi Stati europei (ad esempio, Francia, Irlanda, Regno Unito) ed extra europei (Stati Uniti, Messico, Brasile, Argentina, Uruguay, Giappone) hanno adottato normative

[8] Autorità garante della concorrenza e del mercato, delibera 27165 del 15 maggio 2018, art. 3.

anticorruzione che richiedono l'adozione di programmi di *compliance* o riconoscono riduzioni delle pene o esimenti alle persone giuridiche che dimostrino di avere adottato ed efficacemente applicato un tale programma. Queste normative hanno un ambito di applicazione extraterritoriale, talvolta molto esteso, che le rende applicabili a qualsiasi persona giuridica che svolga parte del proprio business o le cui operazioni abbiano qualche tipo di collegamento con tali Stati, e alle loro capogruppo, nella misura in cui agiscono mediante società controllate ricadenti nell'ambito di applicazione di tali normative. In Italia, per le società a controllo pubblico non quotate, l'adozione delle misure di prevenzione della corruzione costituisce un obbligo ai sensi della legge n. 190/2012.

Queste normative sul piano organizzativo equivalgono alla disciplina 231, anche se non si limitano a prevenire i reati commessi 'nell'interesse dell'impresa'. Per quanto riguarda il contenuto, le buone pratiche OCSE su controlli interni, etica e compliance prevedono che i programmi di compliance anticorruzione includano una "due diligence ben documentata" relativa alla selezione delle controparti a rischio.

E' evidente che nell'attuazione dell'articolo 2-octies del Codice privacy occorre tenere conto di queste realtà, dati l'interesse pubblico sotteso alla prevenzione dei reati e le responsabilità delle imprese a fronte delle normative sopra indicate.

Anche altri Stati membri stanno cercando di elaborare soluzioni per consentire, in conformità a quanto prescritto dal GDPR, l'effettuazione di una due diligence reputazionale. La legge austriaca permette il trattamento se fondato su un obbligo di due diligence o necessario ai fini del perseguimento di un interesse legittimo del titolare del trattamento o di un terzo ai sensi dell'art. 6(1) del GDPR, purché il modo in cui i dati sono trattati salvaguardi gli interessi dei soggetti interessati[9]. La legge danese autorizza il trattamento dei dati relativi a condanne penali e reati se necessario ai fini di salvaguardare un interesse legittimo e tale interesse prevale chiaramente su quelli dell'interessato[10]. In Irlanda sono in via di definizione regolamenti governativi che autorizzano i trattamenti di dati penali necessari per valutare o prevenire il rischio di corruzione[11].

In Italia, l'autorizzazione normativa al trattamento potrebbe essere fornita direttamente dal decreto ministeriale, facendo riferimento al trattamento dei dati relativi a condanne penali o reati o alle connesse misure di detenzione che risulti **necessario per la**

[9] Art. 4(3)2 della LPD austriaca..
[10] Art. 8(3) della LPD danese.
[11] Art. 55(3) della LPD irlandese.

prevenzione della responsabilità penale dell'impresa ai sensi del decreto legislativo n. 231/2001 oppure in attuazione di modelli organizzativi per la prevenzione e il contrasto della corruzione.

Ciò consentirebbe alle imprese di acquisire dati giudiziari, analogamente a quanto già avviene per gli appalti pubblici, anche per attività di tipo privatistico e di potere esercitare un maggiore controllo nel contesto dei processi di qualificazione dei fornitori, ossia nell'ambito di quelle procedure dirette a identificare le imprese e/o i professionisti e a verificarne il possesso degli standard qualitativi, dei requisiti oggettivi e soggettivi previsti dalle policy aziendali. Ovviamente, a valle della copertura normativa in attuazione dell'articolo 2-octies, resta ferma l'esigenza di rispettare i principi del GDPR, tra cui in particolare quello della minimizzazione del trattamento, previa verifica della necessità e proporzionalità dello stesso.

Infine, va ricordato che le imprese che operano come stazioni appaltanti ai sensi della disciplina dei contratti pubblici, siano esse a partecipazione pubblica o meno, attivano normalmente anche appalti e meccanismi di gara di tipo privatistico dovendo soddisfare le necessità ordinarie determinate dall'attività d'impresa. Se la ratio delle norme sui contratti pubblici è quella di contrastare l'infiltrazione della criminalità organizzata nell'attività d'impresa, lo stesso approccio che è obbligatorio per i contratti pubblici (applicare le cause di esclusione dell'art. 80) dovrebbe essere consentito più in generale per tutti gli appalti relativi a lavori, servizi e forniture.

Sebbene tale obiettivo sia importante per la generalità delle imprese, l'esigenza di svolgere tali trattamenti è particolarmente sentita da alcune tipologie di società: le società a controllo partecipazione pubblica, le società che prestano servizi di interesse economico generale e le società che operano in ambiti strategici (infrastrutture, telecomunicazioni, oil & gas, ecc.), inclusi gli operatori di servizi pubblici essenziali ai sensi della disciplina nazionale attuativa della direttiva NIS 2016/1148 (d.lgs. n. 65/2018) e del Cybersecurity Act[12]. Con riferimento a tali imprese, infatti, si presenta un particolare rischio di infiltrazioni criminali ed è proprio in relazione ad esse che lo Stato dovrebbe rafforzare gli opportuni presidi, quantomeno fornendo alle stesse imprese adeguati strumenti di autotutela preventiva.

Andrebbe quindi considerata la possibilità di fornire espressa copertura normativa anche al trattamento di dati relativi a condanne penali, reati e connesse misure di sicurezza **negli appalti di natura privatistica,** almeno per i soggetti sopra indicati, **al**

[12] Sul quadro europeo e nazionale in materia di cibersicurezza, cfr. la circolare Assonime n. …/2019.

fine della verifica su base volontaria delle cause di esclusione di cui all'art. 80 del Codice appalti.

9. I protocolli d'intesa

L'articolo 2-octies, comma 6 prevede espressamente la possibilità di autorizzare con il decreto ministeriale (da adottare per questi profili di concerto con il Ministro dell'Interno) i trattamenti dei dati relativi a condanne penali, reati o connesse misure di sicurezza effettuati **in 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**.

Questi protocolli costituiscono, come noto, uno strumento di collaborazione tra imprese (o associazioni di imprese) e autorità pubbliche per il contrasto delle infiltrazioni della criminalità organizzata nell'attività economica. Tipicamente, le imprese aderenti si impegnano su base volontaria a condizionare la stipula di contratti di forniture, lavori e servizi con terze parti all'assenza delle condizioni ostative evidenziate dalla documentazione antimafia di cui al d. lgs n. 159/2011. Le cautele antimafia vengono così estese anche ad imprese private, al di fuori dei contratti pubblici, con riguardo a tutti i fornitori nelle aree a rischio o, in ogni caso, al di sopra di determinate soglie di valore del contratto.

L'interesse pubblico all'utilizzo di questo tipo di strumenti è evidenziato dalla stessa disponibilità del Ministero dell'Interno (o delle Prefetture) ad adottarli. Appare quindi appropriato prevedere che, laddove per l'attuazione di uno di questi protocolli sia necessario il trattamento di dati giudiziari da parte delle imprese, questo trattamento venga autorizzato in attuazione dell'art. 2-octies. Peraltro, il sistema dei protocolli di legalità già incorpora alcune cautele nella prospettiva del trattamento dei dati personali. Infatti, fermo restando che in alcuni casi l'impresa può chiedere al terzo contraente un'autodichiarazione, l'informazione che viene trasmessa all'impresa dalla prefettura è esclusivamente l'esito della verifica antimafia (liberatorio o interdittivo), senza dettaglio sui dati penali relativi ai singoli soggetti.

Proprio per questo motivo, lo strumento del protocollo d'intesa con il Ministero dell'Interno o la Prefettura può costituire un canale appropriato per la minimizzazione del trattamento dei dati penali da parte delle imprese negli ambiti in cui esse spontaneamente pongono in essere misure di prevenzione della criminalità che vanno oltre gli obblighi di legge.

Riguardo all'utilizzo dei protocolli di legalità va segnalato un ostacolo di natura normativa, a monte della tutela dei dati personali, che è stato evidenziato dalla pronuncia n. 452/2020 del Consiglio di Stato, pubblicata lo scorso 20 gennaio. In seguito a un intervento normativo di modifica del Codice antimafia del 2012[13], la possibilità di richiedere la documentazione antimafia è stata limitata ai soggetti obbligati al rispetto della disciplina, escludendo la possibilità di una richiesta da parte di soggetti privati.

Il Consiglio di Stato, nel riconoscere che l'attuale formulazione del Codice antimafia non consente a un privato o a un'associazione di categoria di chiedere alla Prefettura la documentazione antimafia, invita a riflettere sull'opportunità di un intervento normativo correttivo. La sentenza osserva in particolare che "Occorre (…) interrogarsi (…) se per rafforzare il disegno del Legislatore con una sapiente disciplina antimafia che sta portando in modo tangibile i suoi risultati, non possano le Istituzioni a ciò preposte valutare il ritorno alla originaria formulazione del Codice antimafia, nel senso che l'informazione antimafia possa essere richiesta anche da un soggetto privato e anche per rapporti esclusivamente tra privati. Soltanto un tale intervento potrebbe, in vicende come quella oggi in esame, permettere l'applicabilità generalizzata della documentazione antimafia che non a caso questo Consiglio ritiene pietra angolare del sistema normativo antimafia (..) in presenza di una serie di elementi sintomatici da cui evincere l'influenza, anche indiretta, delle organizzazioni mafiose sull'attività d'impresa (…). In tal modo si riuscirebbe, chiudendo gli spazi che oggi esistono, da un lato ad emarginare completamente tali soggetti rendendoli vulnerabili nel loro effettivo punto di forza e dall'altro lasciare il mercato economico agli operatori che svolgono l'attività affidandosi esclusivamente al proprio lavoro nel rispetto delle regole (…). E, su questo terreno, non vi è dubbio che il devastante impatto della infiltrazione mafiosa si manifesta nei rapporti tra privati come in quelli tra privati e P.A. ".

A monte della disciplina del trattamento dei dati personali, occorrerebbe quindi un intervento sulla disciplina antimafia, volto a consentire anche a privati la richiesta della documentazione antimafia per la prevenzione della criminalità. Come visto, la documentazione antimafia non contiene in realtà dati giudiziari relativi a singoli interessati e pertanto un sistema di prevenzione delle infiltrazioni criminali incentrato su questo tipo di informazione è virtuoso anche dal punto di vista della minimizzazione del trattamento dei dati personali.

[13] Modifica dell'art. 87, comma 1, del decreto legislativo n. 159/2011 introdotta dall'articolo 4 del decreto legislativo n. 218/2012.

10. Conclusioni

L'attuazione dell'articolo 2-octies del Codice privacy è di grande importanza per rimuovere ogni incertezza e colmare le lacune riguardo alla copertura normativa del trattamento dei dati personali relativi alle condanne penali, ai reati e alle connesse misure di sicurezza dopo il superamento dell'autorizzazione generale n. 7/2016. In questa nota ci siamo soffermati su alcuni degli ambiti di maggiore interesse per la generalità delle imprese. Dall'analisi emergono alcuni auspici.

In particolare, viene auspicato che il decreto autorizzi espressamente il trattamento necessario per verificare la sussistenza dei requisiti di idoneità morale previsti dal Codice dei contratti pubblici per le figure apicali dell'impresa e dei suoi potenziali subappaltatori per tutti i contratti pubblici di lavori, servizi e forniture da parte di stazioni appaltanti ex art. 3, lett. o) del decreto legislativo n. 50/2016, a prescindere dalla sussistenza o meno di un obbligo di procedura a evidenza pubblica. Anche per gli appalti in ambito privatistico dovrebbe essere consentito ciò che è obbligatorio per i contratti pubblici, ossia contrastare l'infiltrazione della criminalità organizzata nell'attività d'impresa applicando le cause di esclusione dell'articolo 80 del Codice dei contratti pubblici relative all'idoneità morale del contraente. Tale esigenza è particolarmente sentita per le imprese a partecipazione pubblica, i prestatori di servizi pubblici e le società che operano in ambiti strategici, inclusi gli 'operatori di servizi essenziali' di cui alla disciplina sulla cibersicurezza. Con riferimento a tali imprese, infatti, si presenta un particolare rischio di infiltrazioni criminali e in relazione ad esse appare fondamentale che lo Stato rafforzi gli opportuni presidi, quantomeno fornendo alle stesse imprese adeguati strumenti di autotutela preventiva.

In secondo luogo, l'analisi pone in evidenza la necessità di autorizzare il trattamento necessario per conseguire non solo il punteggio base, ma anche un punteggio superiore al punteggio base per il rating di legalità. Più in generale, viene sottolineata l'esigenza di autorizzare il trattamento necessario per prevenire la responsabilità penale dell'impresa ai sensi del decreto legislativo n. 231/2001 e per attuare programmi e misure di prevenzione dei reati di corruzione.

Lo strumento dei protocolli di legalità con il Ministero dell'interno e con le Prefetture è un importante ausilio nell'azione di contrasto alla criminalità, in cui le imprese si impegnano ad applicare determinate cautele, anche oltre gli obblighi di legge, nella

selezione dei fornitori. Per promuovere l'impiego di questi strumenti occorre, a monte della disciplina a tutela dei dati personali, rivedere la normativa antimafia ripristinando la possibilità per i privati di richiedere la documentazione antimafia, attualmente esclusa. Ottenere determinate informazioni mediante la documentazione antimafia (liberatoria o interdittiva) è positivo anche nella prospettiva della tutela dei dati personali, in quanto il richiedente non accede al dato giudiziario sul singolo soggetto, ma è posto a conoscenza solo dell'esito complessivo della verifica.