Studio Legale Tamos & Partners
sito web: www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
e-mail: lorenzo.tamos@avvocatinteam.com

PRELIMINARE RIFLESSIONE CRITICA SULLA QUALIFICAZIONE SOGGETTIVA DELL'ORGANISMO DI VIGILANZA EX DLGS N. 231/2001 ALLA LUCE DELLA NORMATIVA SULLA CIRCOLAZIONE, TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI DELLE PERSONE FISICHE

o0o

Indice

Premessa

Senza pretesa di esaustività circa i molti aspetti giuridici che si potrebbero (meglio) approfondire con riguardo al tema posto in rubrica, pare però necessario compiere una breve **riflessione** critica che nasce anche grazie alla lettura di alcuni recenti analitici studi/contributi giuridici che si sono occupati della questione[1].

Si tratta di una riflessione collegata all'impossibilità di condividere in toto le considerazioni di chi ritiene si possa parlare di una conformazione *standard* dell'organo di vigilanza ex Dlgs n. 231/2001 (OdV), tanto da doversi ritenere che tale organismo, poiché ritenuto "*parte dell'impresa*", non debba essere qualificato come titolare del trattamento, né come responsabile del trattamento dei dati personali ai sensi e per gli effetti del Reg. UE 2016/679 (ex artt. 4, 24 e 28) in quanto organo "assorbito" dall'ente vigilato di cui sarebbe semplicemente "*parte*"[2].

Altro aspetto trascurato ma, si crede, meritevole di attenzione (critica ed esplorativa), è dato dalla **variegata** e delicata **tipologia di dati** che l'organismo di vigilanza ex Dlgs n. 231/2001 può e/o deve sistematicamente trattare in autonomia, tenuto conto del tipo di attività e funzione esercitata in concreto dall'ente controllato.

Si tratta di un aspetto che, in ultima analisi, potrebbe, anch'esso, in qualche misura, incidere sulla qualificazione soggettiva dell'OdV stesso.

---

1 Cfr., su tutti, reperibile in *info sfera*, "*Sulla qualificazione soggettiva dell'Organismo di Vigilanza ai fini privacy*": 21/03/2019, AODV, di L. Antonetto (con la consulenza di altri rinomati professionisti del settore).

2 Qui senza valutare il non esplorato fatto che, almeno in base a tale tesi, l'opzione soggettiva rimanente, ossia di designare e/o incaricare del trattamento l'OdV, non sarebbe invero praticabile posto che tale organo non potrebbe operare sotto la direzione ed il controllo (neppure minimo) del titolare del trattamento, tranne ovviamente nel caso in cui si tratti di organi mono-soggettivi apicali delle piccole realtà aziendali, essi stessi OdV (ex art. 6, co. 4, Dlgs 231/2001).

Studio Legale Tamos & Partners
sito web: www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
e-mail: lorenzo.tamos@avvocatinteam.com

Ad oggi, difatti, non pare vi siano approfonditi studi e/o contributi di commentatori che mettano in luce i rapporti (e/o le potenziali criticità) sussistenti tra l'attività di prevenzione, vigilanza e controllo obbligatoriamente posta in essere da (alcuni di) tali organismi e i c.d. "*trattamenti di dati personali di reato*" previsti, in particolare, dall'art. 10 del Reg. UE 2016/679 e, in modo più specifico ed analitico, dalla Direttive UE 2016/680, nonché dal Dlgs n. 51/2018 italiano di recepimento della stessa[3].

(1)

l'Organismo di Vigilanza tra necessità di indipendenza e "tentazioni" di generalizzato accorpamento all'interno dell'azienda[4] vigilata dallo stesso

Come noto l'istituzione dell'OdV è prevista dall'art. 6 del Dlgs n. 231/2001.

Tale norma, tuttavia – vale la pena ricordarlo per evitare di giungere a formalistiche conclusioni[5] – al comma 1, lettera b), parla esplicitamente di <<***autonomi poteri di iniziativa e controllo***>> da attribuire all'OdV (sebbene lo stesso sia) ivi individuato quale <<*organismo dell'ente*>> (individuazione che, tuttavia, non significa affatto solo "interno all'ente", ovvero "mero controllore formalistico" dell'attuazione del modello di auto-controllo predisposto dall'ente).

E, peraltro, il comma 2, lettera d) della medesima normativa dispone pure <<***obblighi di informazione*** *nei confronti*>> di tale organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli organizzativi preposti a prevenire i reati presupposto, senza peraltro escluderne l'accertamento in via di fatto.

Dovrebbe, quindi, essere piuttosto evidente che le variegate forme di vigilanza e controllo (davvero utili agli anzidetti scopi) non potranno che essere esercitate in modo autonomo, discrezionale, fattivo e, soprattutto, funzionale a verificare nella sostanza l'eventuale <<*violazioni delle prescrizioni*>> (art. 7, comma 4, lettera a del Dlgs n. 231/2001) che ben potrebbero ed, anzi, molto spesso si traducono nella rilevazione da parte dell'OdV di veri e propri **fatti** (e quindi dati) **di reato** presupposto, anche in forma di delitti commissivi e/o omissivi[6], ovvero

3 Quali dati che, ad esempio, potrebbero riguardare in particolare gli organismi incaricati di vigilare e controllare gli enti privati che si occupano di pubblici servizi e/o di funzioni pubblicistiche i quali, molto spesso, sono difatti sottoposti a procedure di accreditamento che, tra l'altro, prevedono l'obbligo normativo regionale di istituire funzionali e realmente operativi OdV nel pieno rispetto applicativo del Dlgs n. 231/2001.

4 Quando si parla di OdV pare opportuno non riferirsi (sempre ed in ogni caso) al concetto di "impresa" atteso che la disciplina normativa si applica a tutta una serie di soggetti – indicati dall'art. 1 dello stesso Dlgs 231/2001 – che pur non facendo sempre "impresa" hanno però, senza dubbio e sempre, una realtà aziendale nel senso più lato del termine.

5 Tra quelle che bisognerebbe evitare vi è quella in base alla quale l'OdV, giusto il disposto di cui al comma 1, lettera a) dell'art. 6 del Dlgs 231/2001 (id est: l'OdV ha il <<*compito di vigilare sul funzionamento e l'osservanza dei modelli di organizzazione e gestione*>>) si dovrebbe solo occupare di controllare in modo formalistico l'attuazione del modelli di auto-controllo.

6 Si pensi a tutti i reati presupposto previsti in materia di prevenzione sicurezza e sul lavoro, nonché, soprattutto, al riscontro da parte dell'OdV di quelli che si possono realizzare anche nella

Studio Legale Tamos & Partners
sito web: www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
e-mail: lorenzo.tamos@avvocatinteam.com

semplicemente tentati (qui rilevando, infatti, che il Dlgs n. 231/2001, giusto il disposto dell'art. 26 dello stesso, si applica anche ai reati posti in essere in modalità di tentativo, compiuto e/o incompiuto che sia[7]).

Detto in estrema sintesi ciò – anche al fine di introdurre il tema di cui alla seconda parte della riflessione critica anzidetta – pare il caso di evidenziare che l'OdV può essere costituito ***i)*** da chi dirige l'azienda negli enti di piccole dimensioni, oppure da ***ii)*** una pluralità di soggetti interni e/o esterni allo stesso ente, in altre realtà più complesse.

In entrambi i detti casi, seppure in modo radicalmente diverso, verranno comunque svolte le funzioni di vigilanza e controllo finalizzate alla verifica dell'attuazione dei modelli organizzativi atti a prevenire la realizzazione dei reati presupposto e, gioco forza, di tutte quelle attività necessariamente propedeutiche a prevenirli, ivi comprese o, almeno, non escluse quelle di accertamento, ovvero, per usare termini meno rituali, di riscontro diretto e sostanziale degli stessi.

L'OdV, pertanto, svolge una serie di compiti giuridici, tecnico pratici e, soprattutto, di vigilanza e controllo anche molto penetranti: tanto più penetranti quanto più consistenti saranno le risorse economiche e tecniche che tale organismo potrà utilizzare a rafforzamento della propria (dal legislatore e dalla giurisprudenza incentivata) piena autonomia[8].

Volendo anticipare parte delle conclusioni a cui questa **preliminare riflessione critica** ambisce, si può, quindi ed ovviamente condividere l'idea che, rispetto alla normativa in materia di trattamento dati, il "capo della piccola realtà aziendale" che svolge il ruolo di OdV, sia senza dubbio "parte dell'impresa".

E tuttavia, rispetto ad ambiti aziendali più complessi, ove tale organismo abbia caratteristiche collegiali di maggiore autonomia nell'espletare un fattivo controllo ed una reale vigilanza, la suddetta conclusione non sembra più sostenibile[9], ed anzi, di contro, parrebbe di gran lunga preferibile (se non doveroso)

---

forma omissiva (omesse misure di sicurezza; omessa formazione del personale etc.).

7 Chi ha un minimo di esperienza pratica quale componente di un qualunque OdV (di realtà aziendali complesse) ha ben presente che, nello svolgimento delle ordinarie attività di controllo e vigilanza, può capitare di rilevare, se non altro nella forma tentata o omissiva, alcuni reati presupposto che, inevitabilmente comportano il trattamento di dati personali dei soggetti coinvolti dagli stessi sia in senso attivo che passivo, ovvero omissivo.

8 Pare quindi di tutta evidenza che l'OdV non possa e (forse, sin anche ontologicamente) non debba essere studiato e trattato ogni volta nello stesso modo, come se si trattasse sempre dello stesso tipo di organismo più o meno grande e/o più o meno composito, non potendosi delineare uno standard di esso in questi termini: e ciò, men che mai, rispetto alla circolazione, al trattamento ed alla protezione dei dati personali delle persone fisiche coinvolte dalle inerenti finalità e attività di vigilanza e controllo poste in essere dalle **variegate** (soggettivamente diverse) **"specie" di OdV** che in concreto possono esistere e differentemente operare.

9 Quali funzioni che, invero, non possono prescindere dal trattamento autonomo e discrezionale di tutta una serie di dati personali per attuare finalità utili (*in primis*) all'ente presso cui l'organismo svolge la propria missione, ma distinte da esso e, semmai, poste in condivisione con quelle che ha e si propone di attuare l'OdV.

orientarsi verso la sussistenza della duplice (condivisa) titolarità del trattamento dati in capo all'ente e pure in capo all'OdV.

Difatti, almeno con riguardo alla suddetta seconda ipotesi di organismo (che, in realtà, in base alle rilevazioni di Confindustria del 2017, costituirebbe circa il 37% di quelle al tempo esistenti), non appare convincente la tesi proposta da alcuni secondo la quale la finalità del trattamento dei dati trattati e la base legittimante d'utilizzo degli stessi dati da parte dell'OdV, derivino e dipendano in toto da quella del soggetto controllato, ossia dall'ente sottoposto a controllo poiché da ritenersi unico vero titolare del complessivo trattamento dati in questione.

Ebbene, detto ciò, tornando alla tematica della sussistenza o meno della duplice titolarità e, quindi, della conseguente contitolarità dei dati trattati ex art. 26 Reg. UE 2016/679 (da alcuni esclusa), varrebbe la pena riferirsi al provvedimento del Garante Italiano in data 23 gennaio 2014, redatto e firmato dal suo Presidente *pro tempore* (A. Soro), in tema di servizi di firma digitale con autenticazione biometrica (spesso "dimenticato").

Tale provvedimento, *mutatis mutandis*, traendo spunto dai pareri del c.d. "WP29", afferma in sintesi che "*si è in presenza di una situazione di corresponsabilità* [oggi, *alias*: "contitolarità"] *quando varie parti determinano, per specifici trattamenti,* ***o la finalità o quegli aspetti fondamentali degli strumenti*** […]".

Provvedimento che, tra l'altro, ha sottolineato l'importanza di valutare bene "*la partecipazione delle parti alla determinazione congiunta [che]* ***può assumere varie forme*** *e non deve essere necessariamente ripartita in modo uguale",* ***potendo i vari titolari "occuparsi – e quindi rispondere – del trattamento di dati personali in fasi diverse e a gradi diversi"*** *(così Parere 1/2010 sui concetti di titolare e incaricato del trattamento, WP 169, adottato il 16 febbraio 2010, p. 19; per alcune pronunce in tal senso, v. Provv. Garante 3 dicembre 2009, doc. web n. 1692917; Provv. 30 maggio 2007, doc. web n. 1412610; Provv. 13 settembre 2012, doc. web n. 1927456)"*[10].

Con ciò l'Autorità nazionale, in buona sostanza, ha messo in luce che, seppur le finalità e, se vogliamo, la concezione (meramente) teorica di un servizio, o di una funzione, siano da ricondurre ad una sola entità, rispetto alla comunanza di finalità e mezzi di erogazione finale del servizio stesso, neppure la seconda entità si può considerare estranea al concetto di partecipazione nelle dette

10 Nel provvedimento vengono messi in luce i seguenti aspetti, qui esposti in sintesi: - la comunanza di esigenze tra le parti del rapporto di assicurare certezza e sicurezza alle operazioni intercorrenti con gli utenti nella loro complessità; - la determinazione da parte di una sola delle due entità (nel caso una Banca) delle finalità principali del trattamento e dei (teorici) mezzi di esecuzione dello stesso rispetto ai dati personali in questione (biometrici); - la determinazione da parte della seconda entità (tecnologica), in armonia con le esigenze della banca, delle finalità del trattamento da rapportare alla gestione del complessivo servizio di firma digitale fornito all'istituto, nonché delle modalità di esecuzione del trattamento unitamente alla determinazione quota parte congiunta delle procedure operative di trattamento dati.

determinazioni.

Determinazioni che, quindi, seppur in modo diverso, sia per concezione che per impostazione di trattamento, devono/possono di fatto (ed in base al buon senso pratico che pure caratterizza l'attuale normativa in materia di trattamento dati) considerarsi comuni ad entrambe le entità[11] e, quindi, come tali, da valutare alla luce dell'art. 26 del GDPR (e, in alcuni ambiti, probabilmente non solo[12]).

(2)

L'esistenza dell'obbligo di adottare validi modelli organizzativi previsti dal Dlgs 231/2001 e, di conseguenza, la sussistenza dell'obbligo di dotarsi di un Organismo di Vigilanza (OdV) efficace, autonomo ed in grado di svolgere reali funzioni di controllo e prevenzione dei delitti presupposto

La disciplina in oggetto è in continua **evoluzione** e le fattispecie delittuose che ricadono sotto la stessa sono sempre più estese.

Gli esempi sono molti: il reato di intermediazione illecita ed il lavoro non regolare; gli illeciti nell'area della sicurezza e prevenzione sul lavoro; alcuni reati ambientali; alcuni illeciti a matrice informatica; i reati di criminalità organizzata (che non sono solo quelli collegati ai fenomeni di mafia ma potrebbero tradursi nell'accertamento di pratiche concertate di c.d. "*cartello*" tese a turbare la regolarità degli incanti pubblici, ad esempio); il reato di corruzione nel settore privato; alcuni delitti c.d. societari; i reati contro l'industria ed il commercio; i delitti contro la proprietà industriale e molti altri ancora.

Non a caso varie istituzioni nazionali di controllo, al pari dei magistrati che si sono occupati delle nascenti responsabilità e pronunciati al riguardo nell'ultimo decennio, hanno sancito una sorta di "***obbligatorietà di fatto generalizzata***" di adottare modelli di auto-controllo e, di conseguenza di formare un efficace OdV[13].

Vediamo innanzitutto alcuni esempi meramente **incentivanti** l'assunzione delle dette misure di c.d. "auto-controllo":

---

11 Il Garante ha tratto le seguenti conclusioni: "*Alla luce di tali complessivi elementi, appare arduo// ipotizzare due distinti trattamenti di dati biometrici in capo alla banca e a //Technologies s.r.l. (**i quali, peraltro, autonomamente considerati, risulterebbero fini a sé stessi**), dovendo piuttosto ritenersi, anche in vista di un più agevole esercizio dei diritti di cui all´art. 7 del Codice da parte degli interessati, che le società coinvolte, ancorché operanti "in sequenza", pongano in essere – nell'ambito di un servizio definito "omogeneo"// – operazioni differenti di un unico trattamento preordinato all'autenticazione degli interessati, avvalendosi a tal fine di strumenti stabiliti congiuntamente (e operanti in forma "integrata") [ndr: non concepiti o realizzati congiuntamente] e rispondendo del medesimo trattamento solo per la parte di propria competenza (in tal senso, v. anche il parere del Gruppo art. 29, p. 21)"*.

12 Cfr. art. 17 del Dlgs n. 51/2018.

13 Invero il legislatore e le pubbliche amministrazioni, unitamente alla giurisprudenza, hanno progressivamente adottato provvedimenti con cui il comunemente detto "***Modello 231***" si è ampiamente stabilizzato in quasi tutti i campi dell'ordinamento.

- la relazione ministeriale al Dlgs. n. 231/2001, al paragrafo 3.5., stabilisce che l'adozione del Modello sia un <<"*onere*">> rimesso alle valutazioni discrezionali delle persone giuridiche (non si tratta quindi, di una facoltà, ma di una "scelta pre-indirizzata" che l'amministratore della società dovrà compiere nell'interesse della stessa);

- le decisioni dei tribunali di merito nelle cui motivazioni si enuncia il seguente principio "*per quanto attiene all'omessa adozione di un adeguato modello organizzativo// risulta incontestabile il concorso di responsabilità di parte convenuta che, quale Amministratore Delegato e Presidente del C.d.A., aveva il dovere di attivarsi in tal senso*"[14];

- l'art. 93 del c.d. Codice dei Contratti Pubblici (D.lgs. n. 50/2016) ha previsto che nei contratti pubblici di servizi e forniture, l'importo della garanzia fideiussoria da garantire alla PA e del suo eventuale rinnovo è ridotto del 30%, in favore degli operatori economici in possesso della attestazione del modello organizzativo ai sensi del Dlgs. n. 231/2001;

- l'Autorità Garante della Concorrenza e del Mercato, a partire dal 2012, ha il potere di rilasciare in favore dell'Impresa il c.d. *Rating* di legalità. La relativa valutazione premiante avviene sulla base di diversi parametri incentrati sull'adeguamento da parte della società alle disposizioni di cui al Dlgs. 231/2001. Il Ministero dello Sviluppo Economico ha evidenziato che il detto *Rating* di legalità connesso ad un concreto adeguamento è funzionale al conseguimento di finanziamenti pubblici e di agevolazioni per l'accesso al credito bancario;

- con delibera del 2016, l'ANAC ha previsto che «*le stazioni appaltanti devono verificare l'osservanza, da parte degli organismi no-profit, delle disposizioni di cui al D.lgs. 231/2001 applicabile agli stessi in ragione, sia del tenore letterale delle relative previsioni (rivolte agli enti forniti di personalità giuridica, alle associazioni anche prive di personalità giuridica e alle società private concessionarie di un pubblico servizio) sia della natura dei servizi erogati*»;

- diverse Autorità (*cfr.*, ad es., il Comando Generale GdF, circolare n. 83607/2012), hanno costantemente sancito il principio secondo cui l'impresa soggetta a controllo deve dimostrare di aver attuato un sistema organizzativo *ex* Dlgs. n. 231/2001 efficace ed idoneo a prevenire la commissione di illeciti attraverso una procedura comprovabile.

14 Una delle prime sentenze di condanna per omessa adozione dei modelli è stata pronunciata dal Tribunale di Milano (sent., sez. VIII civile, 13/02/2008, n. 1774) ove, difatti, è stata sancita la responsabilità per inadeguata attività amministrativa legittimante un'azione di responsabilità in base all'art. 2392 c.c. e l'insorgenza dell'obbligo risarcitorio, in quanto: *<<l'amministratore delegato e presidente del CdA è tenuto al risarcimento della sanzione di cui all'art. 10 D.lgs. n. 231/2001, nell'ipotesi di condanna dell'ente a seguito di reato, qualora non abbia adottato un modello organizzativo>>.*

Studio Legale Tamos & Partners
sito web: www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
e-mail: lorenzo.tamos@avvocatinteam.com

Ma, al di là di tali estensioni "pretorie", in determina casi, **esiste** un **vero e proprio obbligo normativo** di adeguarsi alle previsioni del Dlgs n. 231/2001 che determina il dovere di **nominare l'OdV**.

Vediamone alcuni:

- il Decreto n. 5808/2010 della regione Lombardia, rubricato "*Approvazione dei requisiti e delle modalità operative per la richiesta di iscrizione all'albo regionale degli operatori pubblici e privati per i servizi di istruzione e formazione professionale e per i servizi al lavoro in attuazione della D.G.R. N. VIII del 23 dicembre 2009*" ha imposto dal 31/12/2010 l'adozione del Codice Etico, la nomina dell'OdV e la relativa comunicazione alla Regione Lombardia, nonché, dal 31/03/2011 l'adozione del modello organizzativo D.lgs. 231/2001;

- la Delibera GR n. 3540/2012 della Regione Lombardia ha imposto ai soggetti accreditati (o agli enti richiedenti per il sistema di accreditamento regionale), in relazione ad alcuni settori, di procedere all'adozione del modello ex D.lgs. n. 231/2001 e alla nomina dell'OdV;

- con DGR n. 2120/2015 la Regione Veneto ha aggiornato il meccanismo di accreditamento prevedendo, in capo agli enti accreditati e per quelli che faranno istanza, l'obbligo di adozione di modelli organizzativi ai sensi di legge;

- la legge n. 15/2008 della Regione Calabria, all'art. 54, addirittura, obbliga da circa dieci anni tutte le imprese che operano in regime di convenzione con la stessa (nei servizi sanitari e dei trasporti) di adottare i modelli organizzativi previsti dal Decreto dandone comprovabile comunicazione ai competenti uffici regionali[15].

Tale obbligo normativo, oltre ad essere utile per introdurre l'aspetto più specifico che verrà nel seguito trattato, sposta ancora di più (almeno ad avviso di chi scrive) il "baricentro" della possibile qualificazione soggettiva di una certa "specie" di OdV verso la titolarità ed autonomia nel trattamento dei dati a cui lo stesso può e deve accedere in originaria autonomia per svolgere (efficacemente) la propria funzione di prevenzione, vigilanza e controllo (rispetto ai reati presupposto).

E ciò pare essere tanto più vero laddove, ad esempio, l'OdV svolga funzioni di controllo e vigilanza rispetto ad enti accreditati dalle istituzioni poiché destinatari di risorse pubbliche funzionali ad **attuare un servizio pubblico** primario o secondario. E' il caso, ad esempio, degli enti gestori dei servizi socio-sanitari assistenziali accreditati dalle regioni di competenza.

15 La Regione Calabria, in base a tale legge, dovrebbe peraltro stipulare convenzioni e rinnovare quelle già in essere solo con le imprese che dimostrino di essersi adeguate al Dlgs 231/2001 ed abbiano nominato l'OdV.

In tali delicati ambiti **l'esercizio della funzione pubblica** si "sposta" sull'ente privato determinandone anche la qualificazione soggettiva che, in un certo senso, "deborda" verso quella pubblicistica (o "para-pubblicistica") in ragione del servizio pubblico in concreto erogato/svolto[16].

Acciocché, anche l'OdV di tali enti espleterà la (ancor più delicata e maggiormente connessa a quella primaria) funzione pubblicistica di vigilanza e controllo dell'ente incaricato del pubblico servizio di cui trattasi, posto che non esiste alcuna ragione logico-giuridica per escluderla in capo al medesimo organismo di controllo ed, anzi, ne esisterebbero molte evidenti di segno contrario.

(3)

La qualificazione soggettiva dell'OdV in base alla tipologia dei dati trattati. Un tema (aperto e da esplorare e) che, in base alla normativa sovranazionale sul trattamento dei dati, meriterebbe attenzione

Da quanto esposto emerge in sostanza che, almeno in certi casi, l'OdV:

- ***i)*** è nominato in base ad una norma che lo impone all'ente privato (o pubblico economico) come obbligatorio;

- ***ii)*** vigila e controlla l'ente che può, in base ad un delegatogli servizio/funzione a matrice pubblica, svolgere una missione pubblicistica;

- ***iii)*** è composto da soggetti esterni dotati di capacità di vigilanza e mezzi per poterla attuare in concreto rispetto ai reati c.d. presupposto previsti dalla disciplina;

- ***iv)*** può/deve trattare fatti di reato (nelle varie declinazioni giuridiche possibili) e, quindi, gioco forza, anche "*dati personali di reato* afferenti a persone fisiche"[17].

Orbene, relativamente al suddetto ultimo punto, come noto agli "addetti ai lavori", il trattamento di dati di reato è disciplinato mediante una serie di cautele e limiti che non si ritrovano solo nell'art. 10 del Reg. UE 2016/679, bensì, anche, nella Direttiva UE 2016/680, nelle normative nazionali di recepimento della stessa,

16 Oltretutto, posto che nel GDPR non è dato rinvenire alcuna definizione di «autorità pubblica» o «autorità competente» e che, quindi, tale definizione dovrebbe conformarsi alle (variegate) interpretazioni del diritto nazionale, lo svolgimento di funzioni a carattere pubblicistico (o assimilabili) porta pure a dover considerare le raccomandazioni di cui alle linee guida del Gruppo di lavoro ex art. 29 rispetto alla necessità di nominare un responsabile per la protezione dei dati o c.d. DPO (linee guida WP29 del 13/12/2016, emendate il 05/04/2017, punto 2.1.).

17 Il tema è quello del trattamento dei c.d. "dati di reato" relativi alle persone fisiche quando e se non immediatamente ("d'acchito") rientranti nell'ambito di applicazione della Direttiva UE 2016/680 recepita in Italia dal Dlgs n. 51/2016 poiché, ad esempio, non riferibili a dati personali di un individuo contenuti in una sentenza penale di condanna quale ipotesi di trattamento pacificamente rientrante nell'ambito applicativo (soggettivo e materiale) della normativa nazionale d'attuazione della stessa Direttiva UE 2016/680.

nonché in quelle regolamentari di specificazione delle legislazioni adottate da ogni singolo Stato membro dell'Unione[18].

E posto che, senza dubbio, anche i fatti umani costituenti reato possono costituire dati personali riferibili a persone fisiche e, come tali, rappresentare una parte significativa del diritto fondamentale di protezione dell'uomo previsto dall'art. 8 della Carta dei Diritti Fondamentale dell'Unione Europea (Carta di Nizza), l'aspetto centrale della questione afferente a tale tipo di trattamento è, dunque, quello di capire non solo quando ci si trovi (un OdV si trovi) ad avere a che fare con un "dato di reato" ma anche **quale normativa** (primaria e secondaria) applicare esattamente per il corretto trattamento di tale tipologia di dato.

Ebbene, se nella previgente normativa domestica sussisteva una maggiore specificità lessicale e i riferimenti normativi avevano una più definita delimitazione applicativa (se non altro terminologica) con riferimento particolare al concetto di "dato giudiziario" e ambito di polizia, oggi, non pare essere più così o, almeno, non sembra possa sostenersi che sia ancora così[19].

Vediamo alcuni dei molti spunti normativa che si potrebbero analizzare positivamente a tale proposito.

L'art. 4 del Dlgs 196/2003, ante novella 2018, ad esempio, alla sua lettera «e) indicava quali "*dati giudiziari*", quei dati personali idonei a rivelare provvedimenti di cui all'art. 3, co. 1, lett. da a) ad o) e da r) a u), del DPR n. 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt 60 e 61 del cpp» e, all'art. 22, forniva i «*principi applicabili al trattamento di dati sensibili e giudiziari*>> ivi specificando che <<*i soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari*».

Il non ancora effettivamente abrogato DPR n. 15/2018 (G.U. n. 61 14-03-2018) in materia di «//*trattamento dei dati effettuato per le finalità di polizia, da organi, uffici e comandi di polizia*» era/è molto esplicito nell'individuare il proprio ambito applicativo soggettivo.

L'autorizzazione generale n. 7/2016 (15/12/2016 n. 5803630) che, invero, si riferiva e si riferisce, esplicitamente, al trattamento dei dati giudiziari (sebbene) da parte di privati, enti pubblici economici e soggetti pubblici, parla espressamente di

18 Qui evidenziando che, sia ai sensi del GDPR che ai sensi della Direttiva UE 2016/680, per fonte normativa (in grado di incidere e/o giustificare il trattamento dei dati personali) non deve intendersi esclusivamente una legge emanata da un parlamento nazionale bensì, una qualsiasi

19 Se sino al 2016 si poteva ancora sostenere (non sempre a ragione) che il dato personale afferente ai reati era esclusivamente quello c.d. "giudiziario" e l'ambito di trattamento era solo quello riservato alle forze dell'ordine per l'attuazione delle finalità (dirette o indirette) di polizia, attualmente tale tesi interpretativa non pare più granitica sia sotto il profilo normativo, sia avuto riguardo al modo pratico in cui i dati di reato sono (sempre più) utilizzati anche da parte di chi non è *tout court* autorità pubblica o autorità competente (e nemmeno un qualificato professionista, o un giurista iscritto in un albo professionale).

<<dati giudiziari>>.

Oggi, invece, alla luce del GDPR e della Direttiva UE 2016/680, tale (sopra esemplificata) delimitazione terminologica ed applicativa si assottiglia molto sino a "quasi" scomparire del tutto.

Infatti, il considerando n. 19 e l'art. 10 del GDPR confermano ad esempio che (a certe condizioni) i dati afferenti ai dati di reato possono essere trattati anche da chi non è autorità pubblica.

L'art. 1, par. 1 della Direttiva 2016/680 parla di «*reati o esecuzioni di sanzioni penali*» così rafforzando il significato "umanistico" e materiale da attribuire al concetto di dato di reato (collegandolo al fatto di reato e) rendendolo indipendente da un accertamento giurisdizionale da parte di un organo istituzionale.

Il considerando n. 11 della predetta Direttiva pare[20] considerare le entità (private) che si occupano per conto degli istituti di credito di svolgere attività di indagine ed accertamento di reati (finanziari) soggette alla medesima direttiva per come ovviamente recepita dagli stati membri.

Il considerando n. 12 (sempre della Direttiva 2016/680) si riferisce alle attività di polizia e delle altre autorità preposte anche qualora non vi sia previa conoscenza della rilevanza penale di un fatto e «*ad altre autorità incaricate dell'applicazione della legge*» a prevenzione e tutela degli interessi della società tanto da, quindi, ulteriormente scollegare il detto concetto di (dato di) reato sia dall'accertamento giudiziale (anzi, addirittura, dalla previa conoscenza della rilevanza penalistica dello stesso), sia dalle sole autorità istituzionali che, a vari livelli, possono contribuire a prevenirlo o accertarlo.

Il considerando n. 13 della Direttiva in parola si riferisce al reato quale «*concetto autonomo*» del diritto dell'unione europea e, oltretutto, sia gli artt. 6 e 7 della stessa, che l'art. 4 del Dlgs n. 51/2018, pongono la eloquente distinzione tra categorie di interessati al trattamento di dati di reato (rei; potenziali rei; vittime; persone informate) e, addirittura, tra dati afferenti a reati fondati su fatti e dati di reato basati su valutazioni personali ponendo un obbligo di distinzione tra gli uni e gli altri.

Il considerando n. 16 della Direttiva, nel trattare il diritto di accesso ai documenti ufficiali (pure potenzialmente contenenti "dati di reato"), parla anche espressamente di <<// ***organismo privato per l'esecuzione di un compito svolto nell'interesse pubblico***>>.

Ed ancora e difatti, l'art. 3, parag. 7, lett. b, della più volte citata Direttiva, nonché l'art. 2, parag. 1, lett g 2 del Dlgs n. 51/2018, si riferiscono alle "autorità competenti" anche nei seguenti significativi termini: «***qualsiasi altro organismo o***

20 Vi è da dire però che tale considerando non è scritto in modo del tutto chiaro.

entità *incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di* ***prevenzione****, indagini, accertamento e perseguimento di reati*//» con ciò, pertanto, erodendo definitivamente l'egemonia nel possibile trattamento di "dati di reato" che si poteva in tale materia attribuire alle sole forze di polizia o autorità pubbliche intese in senso squisitamente istituzionale.

Esposti tali esempi, si può quindi evidenziare che se, da un lato, rimane indubbio che le forze dell'ordine oggi, in Italia, debbano applicare il Dlgs n. 51/2018 nel mentre eseguono, ad esempio, l'identificazione di una persona per porre in esecuzione un ordine giudiziario relativo alla commissione di un reato accertato, esiste, da un altro lato, un vasto ambito di **trattamento "atipico"** di "dati di reato" (nel senso giuridico del termine) che sfugge a tale pacifica ipotesi applicativa della normativa e che non costituisce affatto una mera ipotesi di scuola.

E poiché per reato si può e si deve in generale intendere un fatto umano antigiuridico a cui un ordinamento ricollega una sanzione penale[21] ecco che, allora, niente esclude che anche chi non faccia parte delle forze dell'ordine (o non sia un operatore professionale del diritto o un investigatore *tout court*) si trovi a poter trattare dati di reato concernenti persone fisiche identificate o identificabili[22] sulla base della funzione che deve svolgere.

Al riguardo, difatti, non pare oggi possibile "licenziare" l'argomento sostenendo che il dato di reato sarebbe solo quello "assistito/caratterizzato" da una sentenza penale di condanna, ovvero trattato da parte dell'autorità pubblica, né, come visto, dalle sole forze di polizia istituzionali[23].

Detta visione, invero, appare limitata e, peraltro, nemmeno corrispondente al contenuto e significato (letterale e comprensibile) della normativa europea che, notoriamente, andrebbe in ogni caso interpretata estensivamente e non in modo restrittivo[24].

21 Tra i molti giuristi cfr., F. Mantovani, Principi di diritto penale, 2ª ed., CEDAM, 2007, pag. 56.
22 Gli esempi reali di tali fattispecie sono da considerarsi diffusissimi in tutta Europa.
23 Parlando espressamente la normativa di altre entità delegate e/o preposte.
24 Sovviene il "caso František Ryneš" (richiamato anche dalle embrionali Linee Guida n. 3 del 12/07/2019 del EDPB), ove la Corte di Giustizia UE si è occupata dei dati raccolti da un proprietario di una abitazione che aveva ripreso con il sistema di sorveglianza domestico (CCTV) l'immagine riconoscibile (e, poi, difatti, identificata) di chi gli stava mandando in frantumi alcune finestre. La CGUE ha stabilito che la videosorveglianza con registrazione e conservazione di tali dati personali costituisce trattamento automatico di dati (sentenza C-212/13, František Ryneš v Úřad pro ochranu osobních údajů , 11/12/2014). Ma ciò che occorre bisognerebbe chiedersi è se tale trattamento (indubbiamente) di dati costituisca, anche, un "*trattamento di dati personali di reato*"? A questa domanda si dovrebbe rispondere di sì poiché un simile caso di trattamento costituisce in primo luogo la video-ripresa di un fatto umano antigiuridico violativo della legge penale (riconducibile a persone identificabili) a cui il/un legislatore ricollega come conseguenza una pena.

Studio Legale Tamos & Partners
sito web: www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
e-mail: lorenzo.tamos@avvocatinteam.com

(5)

La questione del controllo rispetto alla funzione pubblicistica

Ebbene, ciò posto in termini generali ed introduttivi, tornando all'esempio dell'OdV di cui alle ***i)*** realtà aziendali più complesse, ***ii)*** con riferimento particolare agli enti privati che esercitano pubbliche funzioni e che hanno ***iii)*** l'obbligo giuridico di nominarlo, non pare potersi escludere a priori che tali "specie" di OdV, oltre ad essere considerate entità autonome titolari del trattamento dati, possano "*dover fare i conti*", quali "**entità o organismi competenti**"[25], con l'applicazione della normativa nazionale di recepimento della Direttiva 2016/680, ossia il citato Dlgs n. 51/2018: e questo poiché essi, come accennato, debbono, in definitiva, porre in essere attività di prevenzione, vigilanza e controllo a tutela della missione pubblicistica di cui l'ente controllato si è fatto carico e che, inevitabilmente, è dagli stessi condivisa (missione che porta gli OdV a trattare dai personali di reato).

In generale, coloro che si trovano ad essere considerati incaricati di un pubblico servizio hanno obblighi analoghi a quelli dei pubblici ufficiali senza, però, averne gli stessi poteri.

Rispetto a tale definizione si può ricorrere alla (generale) nozione di cui all'art. 358 del codice penale, secondo cui: «*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata, dalla mancanza dei poteri tipici*[26] *di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*»[27].

Tale ruolo, qualora da ritenersi sussistente e (caso per caso effettivamente) assunto, comporta delle conseguenze poiché, appunto, trasferisce in quota parte ad un privato l'attuazione e/o il controllo (anche parziale) di un interesse pubblico.

Con lo svolgimento di mansioni riconducibili a pubblico servizio[28] anche il privato dovrà agire sempre a piena tutela del detto interesse, ossia imparzialmente nonché in stretta osservanza delle norme poste a protezione del buon andamento dell'azione pubblica, essendo questi, difatti, i concetti tipici, basilari e generali che sorreggono l'agire di quest'ultima.

---

25 Se non altro finché non subentrerà un provvedimento ad hoc dell'Autorità Garante.

26 Non di ogni potere ma solo quelli «*tipici*».

27 Si tratta di una nozione poco precisa e a portata ampia e che genera incertezza pure in quanto interpretata dalla giurisprudenza nel corso degli anni con una certa varietà di orientamenti che, difatti, cambiano da caso a caso, da settore a settore (Cfr., sul tema, V. Manes, "Servizi pubblici e diritto penale. L'impatto delle liberalizzazioni sullo statuto penale della pubblica amministrazione", Ed. Giappichelli, Torino, 2010).

28 «*Per la qualifica di incaricato di pubblico servizio non rileva l'assenza di un rapporto di dipendenza con l'amministrazione e la gratuità dell'attività prestata, ma solo la natura dell'attività esercitata*» (Cass. pen. Sez. VI, 21/11/2017, n. 594).

Studio Legale Tamos & Partners
sito web: www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
e-mail: lorenzo.tamos@avvocatinteam.com

o0o

Il tema non è semplice. Proviamo ad esaminare alcune norme che, se ben lette e calate nella realtà pratica, porterebbero ad escludere che le predette "specie" di OdV possano (applicare ed) essere soggette solo al Reg. UE 2016/679.

Ed, invero, l'art. 2ter del novellato Codice italiano ex Dlgs n. 196/2003, riporta nella propria rubrica un concetto che riguarda la «*base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*».

Per i dati personali relativi a reati[29] (e condanne penali), ex art. 10 del GDPR, si prevede che il trattamento possa avvenire solo sotto il controllo dell'autorità pubblica, ovvero se il trattamento è autorizzato dal diritto dell'Unione o del singolo Stato membro. E ciò è previsto nonostante la lettera e), del parag. 1, dell'art. 6 del GDPR, in generale, legittimi il trattamento dei dati per l'attuazione di una attività di interesse pubblico o connessa all'esercizio di pubblici poteri di cui è investito il titolare: quale potrebbe essere quella svolta da chi svolge le attività di OdV (per come sopra individuate, ossia a controllo di un ente incaricato di pubblico servizio).

Sennonché, trovandoci in detto caso a che fare con un (dato di) reato[30], si dovrebbe agire solo sotto il controllo dell'autorità pubblica o in base ad una legge (o regolamento) che lo consenta e che, oltretutto, come visto, preveda adeguate garanzie e procedure specifiche di trattamento.

Peraltro il par. 2 dell'art. 2ter del Dlgs 196/2003, ritiene lecita la comunicazione di questi tipi di dati (particolari e afferenti a reati), tra i titolari non inclusi nelle categorie autorizzate a trattarli di cui agli artt. 9 e 10, solo in presenza di una legge (interna o europea), ovvero di un regolamento previsto dalla legge che lo consentano.

L'art. 2-octies individua poi i casi in cui, il trattamento di dati personali (anche) relativi a reati, possa avvenire al di fuori del controllo dell'autorità pubblica ma solo se autorizzato da una norma di legge o di regolamento che

29 Quale sostantivo maschile che identifica il comportamento cui il legislatore ricollega una sanzione penale, a causa dell'aggressione recata ad un bene giuridico meritevole di tutela: il furto in una abitazione; lo scassinamento di un cancello; uno scippo etc. Cfr. anche "Diritto Penale parte generale" - Giovanni Fiandaca ed Enzo Musco, settima edizione, Zanichelli Ed., 2014: «***Il reato è definibile come un fatto umano tipico, antigiuridico e colpevole***».

30 Non potendosi allo stato condividere l'opinione (ingiustificatamente restrittiva) di chi ritiene dati personali afferenti a reati solo quelli contenuti, ad esempio, nelle sentenze penali di condanna, ovvero nell'informazione di garanzia spiccate da un pubblico ministero, posto che la normativa non ha una simile portata ristretta circa la detta nozione di reato, men che mai sotto il profilo del significato meramente letterale della specifica disposizione di cui trattasi (l'art. 10 del GDPR).

preveda garanzie appropriate per i diritti e le libertà degli interessati. In mancanza di tali disposizioni le garanzie predette saranno individuate con Decreto dal Ministro della giustizia previo parere del Garante.

Al proposito si potrebbe ritenere che esista una base giuridica che consente il trattamento di detti dati per l'esecuzione di un compito connesso all'esercizio di pubblici poteri (lettera e, parag. 1 art. 6 GDPR) di cui è investito il titolare. E si potrebbe pensare di trovare una giustificazione ricorrendo alla lettera g) dell'art. 2-octies del Codice che, invero, consente un simile trattamento per «*l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi*»: ma tanto è consentito solo «ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza» e, perciò, bisognerebbe comunque essere autorizzati.

(6)

Ruolo, funzione e definizioni normative: un tema aperto?

Insomma, l'intricata normativa ad oggi in divenire, soprattutto quella concernente l'utilizzo di dati afferenti «***a reati***», ha diversi spigolosi profili da considerare e, anche per questo, appare piuttosto complicata e delicata da applicare.

Ma, in definitiva, preso come paradigma l'esempio di certi OdV, si potrebbe riassumere la questione dicendo che, un trattamento di dati finalizzato e connesso a prevenire e riscontrare fatti umani costituenti reato può aver luogo senza criticità solo in presenza di un adeguato e preciso fondamento giuridico derivante dalla legge nazionale o europea la cui applicazione dipende – o può dipendere in tutto, o in parte – dalla qualificazione giuridica soggettiva da attribuite all'entità che tali dati tratta (o potrebbe sistematicamente trattare) nel rispetto della propria missione, nonché conformemente alla legge che ne prevede il trattamento.

Ebbene, la lettera g) dell'art. 2 del Dlgs n. 51/2018, sotto la rubrica, «definizioni», offre una nozione (in pratica identica a quella di cui alla Direttiva UE 2016/680) piuttosto ampia di cosa debba intendersi per autorità competente soggetta all'applicazione del medesimo decreto.

Tale definizione ricomprende: «**1)** *qualsiasi autorità pubblica dello Stato, di uno Stato membro dell'Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*//»; «**2)** *qualsiasi* ***altro organismo*** *o* ***entità*** *incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione della sicurezza pubblica*».

Qui interessa, in particolare, la seconda specificazione: «***qualsiasi altro organismo o entità*** *incaricato dagli ordinamenti interni di esercitare l'autorità*

pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati», poiché, non potendo sussistere svolgimento di funzione pubblica senza un minimo di potere correlato, essa potrebbe ampliare il novero delle possibili «***entità***» (o organismi) a cui si dovrebbe applicare la normativa in esame.

E, sempre da questo angolo visuale, rileverebbe dunque il tema dell'incarico di pubblico servizio svolto da parte di un organismo, o entità privata che, in definitiva, esercita un compito/"potere" ad ausilio **pubblicistico**: come ad esempio le – in alcuni casi e*x lege* rese obbligatorie – funzioni di vigilanza e controllo che gli OdV svolgono (in particolare nelle realtà aziendali complesse) a tutela dell'erogazione corretta del servizio e/o della fornitura pubblica da parte dell'ente privato dagli stessi controllato.

(7)

Conclusioni "preliminari"

Tanto valutato ed esposto, almeno rispetto al tema qui introdotto, si potrebbe quindi ritenere (o, almeno, teorizzare) che alcuni OdV, oltre ad essere dei veri e propri titolari del trattamento di dati personali, ove esercitino funzioni di prevenzione, vigilanza e controllo rispetto ad enti incaricati di pubblico servizio, siano anche da qualificare «*organismi o entità competenti*»[31] ex Direttiva UE 2016/680 ed, in Italia, ex Dlgs n. 51/2018.

La questione su cui riflettere è, dunque, posta.

o0o

04/10/2019

(avv. Lorenzo Tamos)

31 Cfr., tra l'altro, il "***Draft Data sharing code of practice***" ICO, ove, a pag. 63, si legge che per autorità competente si può intendere, anche <<*qualsiasi altro soggetto se, e nella misura in cui, ha compiti stabiliti dalla legge per esercitare poteri pubblici o poteri pubblici ai fini dell'applicazione della legge (articolo 30, paragrafo 1, lettera b), del DPA 2018).*>>.