LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Profilazione reputazionale e tutela del lavoratore: la parola al Garante della *Privacy*

ANNAMARIA DONINI
Università di Bologna

vol. 3, no. 1, 2017

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Profilazione reputazionale e tutela del lavoratore: la parola al Garante della *Privacy*

ANNAMARIA DONINI
Assegnista di ricerca in diritto del lavoro
Università di Bologna
annamaria.donini2@unibo.it

ABSTRACT

The Italian Data Protection Authority prohibited the activity of employees' (and users' in general) profiling implemented by a digital platform with the purpose of elaborating reputational profiles. This decision is the occasion to focus on risks for workers' dignity, personal identity and privacy resulting from profiling and other automated processing of personal data. The A. points out that "People analytics" activities are likely to breach the prohibition of the collection of belief-related information laid down in art. 8, Workers' Statute. To avoid this risk, new protection techniques "by design" are proposed, taking inspiration from art. 25, EU General Data Protection Regulation.

Keywords: big data analytics; dignity and personal identity; data protection; workers' statute; protection by design

Profilazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy

SOMMARIO: 1. L'affidabilità nelle relazioni giuridiche attraverso il *rating* reputazionale. – 2. Il provvedimento del Garante: La violazione dell'identità personale. – 3. (segue) I profili di contrasto con il Codice *Privacy*. – 4. Controlli "conoscitivi" tramite analisi dei dati e divieto di indagini sulle opinioni dei lavoratori. – 5. *Big data analytics* e rapporto di lavoro. Tutela della persona del lavoratore *by design*

1. L'affidabilità nelle relazioni giuridiche attraverso il *rating* reputazionale

La possibilità di elaborare e creare informazioni derivante dall'applicazione di strumenti di *analytics* ai dati disponibili sul *web* indirizza la riflessione giuridica su istanze di tutela della persona del lavoratore ulteriori rispetto a quelle sinora indagate. Tecniche informatiche sempre più sofisticate consentono di acquisire informazioni e di «capire quali conoscenze siano rilevanti [e] come acquisirle» ([1]), abilitando in tal modo una più documentata interazione con la realtà. Attraverso tali infrastrutture di calcolo, vengono creati profili degli utenti del *web* che combinano numerosi dati eterogenei e slegati in una sintesi dotata di contenuto informativo ulteriore, potenzialmente espressivo di ogni caratteristica personale o professionale degli individui (abitudini di consumo, rischi per la salute, affidabilità creditizia, reputazione…). L'aggregazione in una valutazione sintetica di una grande mole di informazioni riferite ad una determinata persona è in grado di soddisfare l'esigenza di ottenere elementi di conoscenza in merito alla credibilità e affidabilità nelle transazioni economiche e può rispondere al «"naturale desiderio" del datore di lavoro […] di essere onniveggente ed onnisciente» ([2]).

Il provvedimento del Garante emanato in data 24 novembre 2016 ([3]) si occupa per la prima volta di un sistema tecnologico finalizzato a fornire, a partire dall'analisi dei dati, elementi di conoscenza rilevanti sul piano giuridico ed economico tramite una sintesi espressa da un punteggio. La "profilazione reputazionale" offerta dalla struttura informatica oggetto del provvedimento non è limitata all'ambito lavorativo ma si propone di divenire «elemento di

([1]) M. Mazzotti, *Per una sociologia degli algoritmi*, *Rassegna italiana di sociologia*, 3-4, luglio-dicembre 2015, 465 ss.

([2]) M. Aimo, *Tutela della riservatezza e protezione dei dati personali dei lavoratori*, in *Contratto di lavoro e organizzazione*, tomo II, a cura di M. Marazza, in *Trattato di diritto del lavoro*, diretto da M. Persiani - F. Carinci, 2012, Cedam, 1775.

([3]) *Piattaforma web per l'elaborazione di profili reputazionali*, 24 novembre 2016, [doc. web n. 5796783]. Il provvedimento del Garante segue il testo del commento.

valutazione» in tutti i rapporti socio-economici al fine di realizzare «spazi negoziali più sicuri». La piattaforma elabora un *rating* per ogni utente in relazione ai profili relativi al settore penale, fiscale e civile (tra cui lavoro e impegno civile, studi e formazione) generando e mettendo a disposizione elementi di conoscenza, «rilevanti anche sotto il profilo etico», utili per la selezione e il controllo delle controparti negoziali tra cui vengono espressamente menzionati «appaltatori e subappaltatori, […] aspiranti dipendenti, dipendenti in forza» ([4]). L'infrastruttura digitale offre uno strumento verificabile e attendibile «avverso eventuali forme di mistificazione identitaria» per il tramite della combinazione di alcuni elementi: l'«assunzione di responsabilità da parte dei soggetti interessati», il «vaglio documentale realizzato dai […] consulenti reputazionali»; la «possibilità, riconosciuta gli utenti della piattaforma, di visionare in ogni tempo i documenti prodotti da altri … attuando una forma di controllo generalizzato e diffuso».

Il sistema sottoposto all'esame del Garante si inserisce in un contesto in cui le caratteristiche transnazionali, episodiche e spersonalizzate di numerose transazioni commerciali aumentano il rischio di comportamenti opportunistici e di conseguenza attribuiscono la massima importanza alla fiducia. In questo contesto le tecnologie di analisi automatizzata dei dati sono in grado di fornire elementi su cui fondare la fiducia degli operatori attraverso la costruzione di sistemi reputazionali nei quali un terzo «intermedia il rapporto tra chi fornisce notizie e chi le ricerca, raccogliendo i dati, organizzandoli e diffondendoli» ([5]), con effetti di condizionamento del funzionamento del mercato ([6]).

Altri sistemi trilaterali di "accreditamento" introdotti a livello legislativo, come il "*rating* di legalità" *ex* art. 5 *ter* d. l. n. 1/2012 e il "*rating* di impresa" *ex* art. 83, comma 10, d. lgs. n. 50/2016, perseguono l'obiettivo di fornire strumenti di valutazione sulla base di «requisiti e limiti, elementi di giudizio certi e oggettivi, nonché imparziali e affidabili». L'introduzione di tali procedure risponde all'esigenza di avere a disposizione informazioni relative all'etica, alla legalità e all'affidabilità degli operatori e conferma al contempo che l'accreditamento o la certificazione di tali qualità debbano essere fondate su «un'idonea fonte di regolazione» e affidate a «soggetti muniti di adeguate e comprovate garanzie di

([4]) Tra i cinque *sub-rating* in cui la valutazione reputazionale verrebbe articolata vi è anche «lavoro e impegno civile», v. punto 1.2, secondo cpv., Provv.

([5]) G. Smorto, *Reputazione, fiducia e mercati*, *Europa e diritto privato*, 2016, 1, 207.

([6]) E. Dagnino, *Una questione di fiducia: la reputazione ai tempi delle piattaforme online tra diritto alla privacy e prospettive di mercato*, *DRI*, 2017, 1, 247 ss.

terzietà e di indipendenza» (punto 2.2. ultimo cpv) ([7]). L'Autorità nazionale distingue le certificazioni di affidabilità inserite in un quadro legislativo all'uopo predisposto e considera invece con estrema cautela l'attività di profilazione realizzata dai privati perché priva di sufficienti garanzie di imparzialità e di un impianto normativo che garantisca conformità alle regole del Codice in materia di protezione di dati personali.

2. Il provvedimento del Garante: la violazione dell'identità personale.

Il Garante ha dichiarato illecito e contrario a numerose disposizioni del Codice della *privacy* il trattamento dati connesso ai servizi della "Infrastruttura immateriale Mevaluate per la qualificazione reputazionale", una «piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti le persone fisiche e giuridiche».

Il progetto di piattaforma sottoposto al vaglio dell'Autorità era volto a predisporre un servizio a pagamento avente ad oggetto sia la creazione di profili reputazionali a favore degli utenti interessati, che la creazione di profili «contro terzi» ([8]), attraverso il caricamento di documenti concernenti aspetti personali e professionali. A tali documenti, valutati da appositi "consulenti" al fine di garantirne genuinità e integrità, sarebbe stato applicato un algoritmo matematico, «in fase di brevettazione», in grado di generare un "*rating* reputazionale" per ogni interessato espressivo sia dell'affidabilità generale che di quella riferita a singoli settori (penale, civile, fiscale lavoro e impegno civile, studi e formazione). Nelle note presentate dalle società che hanno progettato la piattaforma sono elencati a titolo esemplificativo i documenti utilizzabili per l'elaborazione del *rating*: certificato del casellario giudiziario, provvedimenti giudiziari, diplomi e titoli di studio o di formazione, elementi che testimonino «fatti e circostanze legate … alla sfera morale dei soggetti o tecnico professionale» come documenti relativa alla «presenza/assenza di successi e/o insuccessi professionali», eventualmente acquisiti da articoli di stampa, radio e televisione. La volontarietà della procedura avrebbe richiesto il consenso dell'interessato per l'acquisizione, il trattamento e per la messa a disposizione dei dati, mentre i profili "contro terzi" sarebbero stati costruiti soltanto con i «dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da

([7]) Nel caso dei *rating* menzionati nel Provvedimento, l'AGCM (art. 5 *ter* d. l. n. 1/2012) e l'ANAC (*ex* art. 83, comma 10, d. lgs. n. 50/2016).

([8]) Vedi punto 1.2, Provv. La piattaforma offre inoltre servizi per l'integrazione documentale di profili precedenti, la risposta documentata ad un profilo "contro" e la creazione di profili differenziati a seconda che siano basati o meno su documentazione e/o su certificazione dei documenti.

chiunque» sottoponibili a trattamento senza consenso secondo l'art. 24, comma 1, lett. d), d. lgs. n. 196/2003; salva in ogni caso la possibilità per l'interessato di intervenire a integrare o modificare (punto 1.5 terzo cpv) – ma non a cancellare – i profili.

All'esito dell'analisi delle caratteristiche della struttura informatica, il Garante ha riscontrato significative violazioni ai principi e alle regole del Codice *Privacy* e rilevanti rischi per la dignità e l'identità personale dei soggetti sottoposti a profilazione dichiarando pertanto illecita la realizzazione della piattaforma e il connesso trattamento dei dati. Le valutazioni e classificazioni cui Mevaluate è finalizzata sono infatti in grado di condizionare la proiezione sociale di un individuo, in considerazione sia della limitata qualità dei dati di partenza che della «oggettiva difficoltà di misurare situazioni, parametri e variabili non sempre agevolmente classificabili o quantificabili» (punto 2.5 ultimo cpv), come anzitutto la reputazione.

Dignità e identità personale compongono il fondamento valoriale della normativa per il trattamento dei dati, come ribadito in questa sede dal Garante ([9]), ma assumono una specifica e ulteriore rilevanza all'interno della relazione di lavoro. Se la tutela della dignità orienta larga parte dell'ordinamento giuslavoristico, la protezione dell'identità personale non ha assunto un autonomo ambito di affermazione a vantaggio dell'individuo coinvolto in un rapporto di lavoro. L'identità personale del prestatore emerge in combinazione con altri beni tutelati a livello costituzionale, come componente della personalità morale nelle vicende in cui con maggiore evidenza il lavoro si manifesta quale strumento per l'affermazione della personalità sul piano individuale e sociale ([10]), oppure in quelle in cui rileva la necessità di una adeguata protezione della sfera intima e privata anche nello svolgimento delle attività lavorative ([11]).

L'identità personale come «formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue specifiche

([9]) V. punto 2.2, Provv. che richiama l'art. 2, Codice *Privacy* e la sentenza della Cass. 8 agosto 2013, n 18981, *DJ*, nonché punto 2.5, ult. cpv., Provv., che richiama il Provv. Garante 9 marzo 2006, [doc. web n. 1269316] e la sentenza del T. Roma 7 dicembre 2015, a quanto consta inedita.

([10]) «Il lavoro non è solo un mezzo di sostentamento economico, ma anche una forma di accrescimento della professionalità e di affermazione dell'identità, personale e sociale, tutelata dagli artt. 1, 2 e 4 Cost.», Cass. 18 giugno 2012, n. 9965, *De&L Riv. Crit. Dir. Lav*. 2012, 3, 815 che nega la corrispondenza all'ordine giudiziale di reintegrazione della condotta del datore che «si limiti a versare al lavoratore la retribuzione e a consentirgli l'ingresso in azienda per lo svolgimento dell'attività sindacale, senza permettergli, tuttavia, di riprendere il lavoro»; v. Corte App. L'Aquila, 12 febbraio 2016; 12 maggio 2016, *dejure*.

([11]) Corte App. Venezia, 24 agosto 2010, n. 180, *dejure*, in relazione a condotte di *mobbing* che hanno determinato un danno non patrimoniale derivante dalla violazione di diritti di rango costituzionale, quali il diritto all'identità personale e il diritto all'onore e al decoro.

caratteristiche e manifestazioni» ([12]) e dunque la proiezione positiva del diritto a veder correttamente rappresentate le proprie scelte ha invece limitata rilevanza nella relazione di lavoro, perché le credenze e convinzioni che compongono tale diritto possono assumere rilevanza soltanto nella misura in cui siano connesse allo svolgimento della prestazione (per espressa previsione dell'art. 8 St. lav. e art. 10, d. lgs. n. 276/2003). Sarebbe pertanto irragionevole rivendicare la tutela nei confronti del datore di lavoro di un diritto che costituisce espressione di elementi a costui in larga parte inaccessibili.

Nel contesto tecnologico attuale, tuttavia, la tutela dell'identità personale potrebbe assumere una più ampia rilevanza nei confronti del prestatore di lavoro.

L'applicazione di sistemi di *big data analytics* comporta rilevanti rischi di compressione dell'identità personale del lavoratore, così come di ogni altro utente del *web*, dovuti alla limitatissima possibilità di contestualizzare e calare in un determinato momento storico le elaborazioni, sottraendo in tal modo veridicità alla rappresentazione digitale della persona ([13]). La possibilità di raccolta ed elaborazione dei dati professionali e personali diffusi nel *web* compromette la garanzia a che non sia travisato il patrimonio intellettuale, ideologico, etico, religioso e professionale dell'individuo ([14]) e al contrario è in grado di generare una falsata, inesatta ed eccessivamente sintetica rappresentazione della persona. Quando il trattamento automatizzato a scopo di profilazione riguarda il lavoratore, l'impropria proiezione delle sue caratteristiche, per un verso, potrebbe comportare una violazione di quella parte dell' identità personale che si riferisce alla professionalità e agli altri elementi rilevanti nella relazione di lavoro e, per altro verso, metterebbe a repentaglio le componenti "personalissime" del patrimonio intellettuale e valoriale del prestatore, che non dovrebbero entrare nella disponibilità del datore, e che invece gli vengono fornite in un declinazione imprecisa e parziale.

([12]) Secondo l'affermazione nella prima sentenza della Corte di cassazione che ha affermato il diritto all'identità personale, Cass. 22 giugno 1985, n. 3769, *FI*, 1985, 2211.

([13]) In merito ai pericoli per l'identità personale derivanti dall'esposizione sul *web*, v. M.F. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, in *Il diritto di famiglia e delle persone*, 2016, 3, 949 ss. "Aggiornamento" e "contestualizzazione" anche in relazione al tempo sono elementi necessari per salvaguardare l'identità sociale di un individuo messa a repentaglio in particolare negli archivi digitali e nei motori di ricerca, v. Cass. 5 aprile 2012, n. 5525, *Diritto dell'Informazione e dell'informatica*, 2012, 4-5, 910 ss.

([14]) Così in particolare, e Cass. civ., sez. I, 7 febbraio 1996 n. 978 e anche C. cost. 3 febbraio 1994, n. 13.

3. (segue) I profili di contrasto con il Codice *Privacy*

Il pregiudizio alla dignità e all'identità personale degli utenti derivante dall'attività di profilazione, a parere del Garante, si concretizza in maniera prevalente nel mancato rispetto delle regole che concernono la manifestazione del consenso in relazione al peculiare trattamento dati offerto dalla piattaforma in esame.

È anzitutto rilevata la violazione del principio della libera manifestazione del consenso *ex* art. 23 Cod. *Privacy*, sia nel caso in cui l'utente intervenga per contrastare un profilo creato da terzi, sia nelle ipotesi di inserimento di clausole all'interno di contratti di appalto, fornitura e lavoro che richiedano la concessione dell'autorizzazione alla pubblicazione delle informazioni a pena di risoluzione del contratto (v. 1.5 secondo cpv), per il condizionamento derivante, nel primo caso, dalla necessità di intervenire a correggere profili creati da altri; e, nel secondo caso, dal timore per la cessazione o la mancata costituzione del contratto. In secondo luogo, anche ove i dati derivino da documenti liberamente conoscibili (*ex* art. 24), secondo il Garante l'elaborazione realizzata dalla piattaforma fornisce «valutazioni reputazionali autonome, originali e del tutto distinte dalle informazioni originariamente acquisite» che richiedono un esplicito e autonomo consenso al trattamento (punto 2.3 secondo cpv). Da un punto di vista più ampio e in mancanza di adeguati argomenti forniti dalla società, l'illiceità del trattamento deriva altresì dalla dubbia conformità rispetto ai principi di pertinenza, indispensabilità, necessità e proporzionalità e nonché dalla dubbia qualità dei dati.

L'Autorità nazionale è intervenuta in materia di profilazione predisponendo delle Linee guida ([15]) dedicate all'«analisi e [l'] elaborazione di informazioni relative a utenti o clienti al fine di suddividere gli interessati in "profili", ovvero in gruppi omogenei per comportamenti o caratteristiche sempre più specifici, con l'obiettivo di pervenire all'identificazione inequivoca del singolo utente» indipendentemente dalle finalità perseguite, prese in considerazione soltanto a fine esemplificativo (predisposizione di servizi più adeguati, fornitura di pubblicità personalizzata, analisi e monitoraggio dei comportamenti, sfruttamento commerciale dei profili). Per garantire la conformità dell'attività di profilazione alle esigenze di protezione dei dati, le Linee guida hanno fornito parametri sull'adeguatezza dell'informativa, che dovrà garantire la preventiva consapevolezza circa i possibili impieghi delle

([15]) "Linee guida in materia di trattamento dei dati personali per profilazione *online*", 19 marzo 2015, [doc. web n. 3881513].

informazioni; sulle caratteristiche del consenso, che deve essere «libero, acquisito in via preventiva rispetto al trattamento medesimo, riferibile a trattamenti che perseguono finalità esplicite e determinate, informato e documentato per iscritto»; e sul rispetto del principio di finalità nella conservazione dei dati.

Nonostante tali cautele, l'utente coinvolto dall'attività di profilazione non ha il pieno controllo sulle informazioni relative alla propria persona. L'applicazione di tecniche automatizzate di elaborazione dei dati produce un «valore aggiunto informativo» ([16]) in grado di ledere la libertà di autodeterminazione informativa di cui il diritto alla protezione dei dati personali è strumento ([17]) – anche nel caso in cui informativa e consenso siano correttamente forniti. L'esito dell'elaborazione è infatti un'entità informativa, fuori dal dominio dell'individuo, che fissa le valutazioni in uno specifico momento senza possibilità di adattamenti o correzioni.

La peculiarità della profilazione rispetto ad altre modalità di trattamento dati è tenuta in debita considerazione dal Nuovo Regolamento *Privacy* europeo che in caso di profilazione estende gli oneri di informazione alla «logica utilizzata, nonché all'importanza e alle conseguenze previste di tale trattamento per l'interessato» (art. 13, comma 2 lett. f; art. 14, comma 2 lett. g, Reg. 679/2016 UE). L'attività che richiede un'informativa rafforzata non è soltanto la profilazione ma ogni "processo decisionale" o "trattamento" «automatizzato» in presenza del quale il destinatario ha il «diritto di non essere sottoposto a una decisione basata unicamente» su di esso «che produca effetti giuridici che lo riguardano o che incida […] significativamente sulla sua persona», tranne che nelle ipotesi in cui il trattamento sia necessario per la conclusione o lo svolgimento di un contratto, o si basi su consenso esplicito, o sia autorizzato dal diritto dell'Unione o di uno Stato membro. Anche nei casi di processo automatizzato a cui l'utente non può sottrarsi è comunque garantito il diritto all'intervento umano del titolare del trattamento ([18]), per evitare che le analisi o le previsioni aventi ad oggetto «il rendimento professionale, la situazione

([16]) P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, *RIDL*, 2009, I, 350, in relazione alle «operazioni compiute da altri (mediante accostamenti comparazione esame, analisi congiunzione o incrocio)». Secondo il provvedimento si tratta di «valutazioni reputazionali autonome, originale e del tutto distinte dalle informazioni originariamente acquisite» (2.3. secondo cpv., Provv.)

([17]) In quanto «diritto di un soggetto di controllare l'insieme delle informazioni che al medesimo di riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione», G. Finocchiaro, *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro*, in *Web e lavoro. Profili evolutivi e di tutela*, a cura di P. Tullini, Giappichelli, 2017, 53 che auspica un «bilanciamento, fra le ragioni dell'individuo e quelle dell'impresa», 60.

([18]) A cui si aggiunge il diritto di esprimere la propria opinione e di contestare la decisione, v. art. 22, commi 1 e 2 del Reg.

economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione e gli spostamenti» della persona (v. art. 4, comma 1, n.4, Reg. 679/2016 UE) siano conseguenza esclusiva delle approssimazioni e delle correlazioni derivanti dalle tecniche di analisi dei dati.

4. Controlli "conoscitivi" tramite analisi dei dati e divieto di indagini sulle opinioni dei lavoratori.

La piattaforma destinataria dell'intervento del Garante si proponeva di raccogliere informazioni relative a tutti gli aspetti della vita dell'utente e non solo quelle rilevanti per lo svolgimento del lavoro, fino a comprendere «fatti e circostanze legate ... alla sfera morale» con il fine di produrre una valutazione di affidabilità «riferito a tutte gli aspetti (a 360°) che concorrono a definire la reputazione» da cui trarre «importanti informazioni relative agli interessati rilevanti anche sotto il profilo etico».

Dalla finalità espressamente invasiva della sfera intima dell'utente e dall'utilizzo di dati rivelatori di opinioni personali discende senza dubbio una violazione dell'art. 8 St. lav. La contrarietà alla norma statutaria emerge altresì da un'altra caratteristica dell'attività di profilazione. Le tecniche di analisi dell'ingente mole di dati disponibili sul *web* producono entità informative sintetiche, inferenziali e predittive riferibili ad un singolo oppure ad un gruppo. L'opinione che si mira a ottenere è pertanto artefatta e costituisce un contenuto informativo che corrisponde alla "parziale" riproduzione tecnologica di alcuni tratti dell'esperienza personale o professionale riferibile ad un individuo. Se sono vietate le indagini sulle opinioni secondo una modalità di comunicazione diretta (informazione – ricezione), sarà a maggior ragione escluso il ricorso ad un *software* che elabori i dati in modo da generare un contenuto ulteriore rispetto al messaggio inviato. Attraverso le tecniche di *big data anlytics* gli elementi che compongono il patrimonio personale e valoriale del prestatore vengono forniti al datore in una declinazione imprecisa e parziale amplificando l'intensità della violazione dell'art. 8 St. Lav.

Stabilita l'incompatibilità con la norma statutaria di un sistema di trattamento dei dati finalizzato alla profilazione, resta da verificare la possibilità per il datore di realizzare l'operazione che costituisce l'antecedente logico di ogni trattamento ossia la raccolta e l'aggregazione delle informazioni relative al lavoratore disponibili sul *web*. Tale raccolta può avvenire con numerose modalità dirette e indirette, ad opera del datore di lavoro o dei suoi collaboratori, come forma di controllo riconducibile all'art. 3 o 4 St. lav. o come controllo difensivo.

In ossequio al carattere multilivello della tutela della riservatezza del lavoratore ([19]), le previsioni fissate nelle Linee Guida ([20]) relative alla raccolta di informazioni per finalità di profilazione devono integrarsi alle specificità delle regole e dei principi lavoristici, ricavabili dalle norme statutarie e declinate negli atti del Garante. La raccolta e il trattamento dati risultano ammessi ai sensi delle "Linee guida per l'utilizzo di Internet e della posta elettronica nel rapporto di lavoro" ([21]) se svolti per le finalità previste dall'art. 4, comma 2 St. lav. (nella versione in essere al momento dell'emanazione delle Linee guida, per «esigenze organizzative e produttive» e per la «sicurezza del lavoro»), pur se in tal modo si realizzi anche un controllo indiretto o preterintezionale. Per ciò che concerne i dati personali, l'"Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro"[22] ha inoltre scelto «un'impostazione finalistica che consente il trattamento dei dati sensibili ogniqualvolta risulti funzionale alla gestione – oltre che alla instaurazione e all'estinzione – del rapporto di lavoro»[23] (punto 3, lett. a). Quale che sia la fonte, e anche nel caso in cui siano stati "concessi" dal lavoratore che li ha caricati sulla piattaforma o li ha diffusi sul *web*, raccolta e utilizzo dei dati personali dei lavoratori deve altresì avvenire nel rispetto del divieto di indagini sulle opinioni politiche, religiose e sindacali o su fatti non rilevanti ai fini della valutazione della professionalità *ex* art. 8 St. lav.

Se si ritiene che il divieto dell'art. 8 St. lav. si applichi in via esclusiva alle attività commissive di indagine, la tutela delle opinioni che il datore "riceva" senza un intervento attivo (perché si tratta di flussi di dati ricavabili da altre attività o di informazioni in cui ci si imbatte nella navigazione sul *web*), sarà rimessa esclusivamente al rispetto delle regole del Codice *Privacy* e, qualora le

([19]) R. De Luca Tamajo, *Introduzione*, in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, a cura di P. Tullini, Cedam 2010, 1 ss.

([20]) "Linee guida in materia di trattamento dei dati personali per profilazione *online*", cit., v. § 2.

([21]) Delibera n. 13/2007: il trattamento lecito dei dati da parte del datore di lavoro può avvenire «per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi» (art. 24, comma 1, lett. g), del Codice). Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali. V. M. Paissan, E-mail *e navigazione in* internet: *le linee del Garante*, in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro* cit., 16 ss. In seguito alla novella dell'art. 4 St. lav. il presupposto su cui il Garante ha fondato il bilanciamento viene meno poiché per il controllo di cui al comma 2 non è sempre previsto l'accordo sindacale.

([22]) Autorizzazione n. 1/2016 del 15 dicembre 2016. Il contrasto con l'art. 8 St. lav. può essere ravvisato prevalentemente in riferimento ai dati sensibili *ex* art. art. 4, co. 1., lett. d), d. lgs. n. 196/2003, più idonei a fornire informazioni relative alle opinioni politiche sindacali e religiose.

([23]) L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, *RIDL*, 2016, I, 365 s.

informazioni derivino da attività di controllo, anche al rispetto dell'art. 4 St. lav. ([24]). In tal modo viene sottovalutata la rilevanza e la quantità di dati che può finire nella disponibilità del datore di lavoro ([25]), destinate ad aumentare in seguito alla novella dell'art. 4 St. lav. che ha introdotto un'area di esenzione dalla procedura autorizzativa per gli «strumenti per rendere la prestazione lavorativa». A ciò si aggiunga che la quantità e la varietà di dati che possono entrare nella disponibilità del datore di lavoro è massima nelle attività informatizzate e digitalizzate dei modelli organizzativi d'impresa riconducibili alla *smart industry* e *Industry* 4.0.

Per evitare che siano acquisite informazioni personali non rilevanti per la valutazione della professionalità del prestatore in caso di controllo lecito, è necessaria una lettura integrata della normativa a tutela della riservatezza e della normativa lavoristica, richiesta dagli artt. 113 e 184, co. 3, d. lgs. n. 196/2003 ([26]), che attribuisca all'art. 8 St. lav. la funzione di individuare «categorie di dati "supersensibili" dei quali è vietato in ogni momento il trattamento» ([27]). Sembra muoversi in una direzione simile la sentenza della Cassazione n. 18302/2016 ([28]) che interviene sulla vicenda, già sottoposta all'esame del Garante e del Tribunale di Roma ([29]), relativa al *software* di monitoraggio di ogni accesso e tentativo di

([24]) I dati lecitamente raccolti seguendo le regole del comma 1 o del comma 2 sono inoltre utilizzabili «a tutti i fini connessi al rapporto di lavoro» secondo quanto previsto dall'art. 4, comma 3, St. lav. Ricostruisce i «limiti normativi all'utilizzabilità dei dati registrati dallo strumento di controllo» I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della Privacy*, *LLI*, 2, 1, 2016, 27 ss. e in part. 29 ss. Secondo M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, *ADL*, 2016, 3, 507, invece, l'art. 4, comma 3, comporterebbe una «esplicita autorizzazione legislativa al trattamento dei dati rilevati mediante strumenti di controllo per "*tutti i fini connessi al rapporto di lavoro*" (art. 4, comma 3)» che «supera ogni diversa previsione del Codice *Privacy* in materia di consenso al trattamento e/o di finalitaà dello stesso».

([25]) Rileva nel panorama giurisprudenziale una tendenza a marginalizzare l'art. 8 rispetto all'art. 4 St. lav., L. Tebano, *La nuova disciplina dei controlli a distanza* cit., 355 ss.

([26]) Art. 113: «Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300»; art. 184, co. 3: «Restano ferme le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali».

([27]) A. Bellavista, *Poteri dell'imprenditore e* privacy *del lavoratore*, in *I poteri del datore di lavoro nell'impresa*, a cura di G. Zilio Grandi, 2002, Cedam, 47, che però fornisce una lettura elastica delle ragioni inerenti la valutazione dell'attitudine professionale del lavoratore, comprensiva delle informazioni «oggettivamente … rilevanti ai fini della gestione dello specifico rapporto di lavoro» e per assicurarne la funzionalità, 48. Storicamente connotata e più restrittiva l'impostazione di U. Romagnoli, *Sub* art. 8, in U. Romagnoli - L. Montuschi - G. Ghezzi. - G. F. Mancini, *Statuto dei diritti dei lavoratori*, Zanichelli, 1972, 138 «l'oggetto delle indagini private, pertanto, deve essere limitato ai presupposti dell'esatto adempimento diversi dall'idoneità fisica». S. Sciarra, *Sub* art. 8, in *Lo statuto dei lavoratori*, diretto da G. Giugni, Giuffrè, 1979, 94 ritiene l'attitudine professionale «un criterio interpretativo saldamente ancorato alla realtà del contratto di lavoro».

([28]) Cass. civ., sez. I, 19 settembre 2016, n. 18302, in corso di pubblicazione su *RIDL*, 2017, II, 2, nt. Ingrao.

([29]) Provvedimento 308 del 21 luglio 2011, [doc web 1829641]; T. Roma 4 aprile 2013 n. 1196.

accesso ai siti *web* da parte dei dipendenti. Secondo questa pronuncia, «acquisire e conservare dati che contengono (o possono contenere) simili informazioni importa già l'integrazione della condotta vietata, perchè si risolve in una indagine non consentita sulle opinioni e condotte del lavoratore, anche se i dati non sono successivamente utilizzati. Non è necessario sottoporre i dati raccolti ad alcun particolare trattamento per incorrere nell'illecito, poiché la mera acquisizione e conservazione della disponibilità di essi comporta la violazione della prescrizione legislativa» ([30]).

In tal modo è possibile tracciare una nozione di "indagini" che si estenda fino alla raccolta e conservazione di dati non riconducibili alle esigenze oggettive di svolgimento della prestazione di lavoro. Considerando il valore economico dei dati degli utenti del *web* e la crescita dei sistemi per l'analisi e la profilazione, soltanto la sottrazione di ogni materiale informativo può garantire il rispetto delle prerogative fondamentali che afferiscono al lavoratore di cui la norma dell'art. 8 St. lav. è fondamentale misura di tutela (libertà di manifestazione del pensiero, dignità e identità personale, prevenzione delle condotte discriminatorie).

5. *Big data analytics* e rapporto di lavoro. Tutela della persona del lavoratore *by design*

L'analisi realizzata dalla piattaforma Mevaluate per la creazione di un profilo espressivo della reputazione del lavoratore non è che una delle numerose possibilità di elaborazione tecnologica dei dati conservati sul *web*. Si diffondono infatti metodi di organizzazione d'impresa e di gestione delle risorse umane basati sui risultati della *big data analytics* ([31]), sia in relazione alle politiche di mercato che a quelle relative alle relazioni commerciali e di lavoro ([32]). Tale tendenza è presente in particolare nelle grandi imprese multinazionali e in quelle che operano nel settore digitale e ICT che dunque sono già in possesso delle tecnologie, competenze e professionalità necessarie per la *big data anlytics*.

La disponibilità di enormi quantità di dati variegati consente la produzione di una nuova tipologia di informazioni, fondata su correlazioni, schemi, ricorrenze e proiezioni relative all'evoluzione di una situazione o alla

([30]) Anche il provvedimento del Garante "Accesso alla posta elettronica dei dipendenti" 22 dicembre 2016 assume una posizione simile richiamando la stessa sentenza (punto 3.5 ultimo cpv).

([31]) Forme di *automatic management* costituiscono inoltre la struttura portante delle piattaforme digitali di lavoro. «a salient feature of crowdwork infrastructure is the predomincance of code in mediating work relations», M. Cherry, *Beyond misclassification: the digital transformation of work*, *Comparative labor law and policy journa*l, 2016, 37, 3, 596.

([32]) World economic forum, *Big data big impact: new possiiblities for international development*, 2012.

concretizzazione di un comportamento. Dall'analisi statistica a base causale dei comportamenti si passa all'individuazione di collegamenti inferenziali, che forniscono una conoscenza sufficiente per prendere decisioni, ma generano nuove problematiche relative all'adeguatezza dei modelli teorici attraverso i quali analizzare questi *set* di dati ([33]) e all'introduzione e diffusione di soggettività artefatte. Le correlazioni che sono generate dagli algoritmi di *people analytics* infatti non sono espressione di un individuo specifico ma nemmeno sono riconducibili ad un gruppo in considerazione del fatto che il flusso di dati sottoposti al trattamento non corrisponde ad un insieme di soggetti individuato e stabile ma è generato da una popolazione definita «in maniera dinamica e variabile» ([34]).

Non è pertanto sufficiente selezionare la forma di elaborazione dei dati che presenti una "valida correlazione" ([35]) rispetto agli elementi legittimamente sottoponibili ad indagine, come quelli attinenti l'"attitudine professionale", dal momento che l'uso della *people analytics* sia nella fase di massiva e indistinta acquisizione dei dati, che nella fase di elaborazione ed applicazione del modello, determina una violazione dei diritti di libertà, dignità ed identità personale del prestatore, poiché il datore entra in possesso di informazioni relative alla sfera personale riconducibili solo in via eventuale al prestatore ([36]).

Dati i pericoli relativi alla produzione e circolazione di elementi di conoscenza personali e professionali inaccurati derivanti dalla diffusione delle tecniche di *big data analytics*, una protezione adeguata per gli utenti del *web* esposti a tali forme di trattamento potrebbe ispirarsi al principio di *privacy by design* e *by default* ([37]) introdotto dal nuovo Regolamento europeo. La consacrazione nella normativa europea di tali principi ([38]) impone a tutti i responsabili del

([33]) D. Bollier, *The promise and peril of big data*, *Communications and Society Program*, 2010, The Aspen Institute, 16 ss. che riporta l'esempio di Sense Network Inc.

([34]) A. Mantelero, *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, *Contratto e impresa. Europa*, 2015, 1, 147 che auspica un modello di tutela collettivo ad opera di enti esponenziali che siano in grado di esercitare «diversi e autonomi diritti inerenti alla dimensione collettiva della protezione dei dati», tra cui anche la valutazione del rischio.

([35]) Così E. Dagnino, People analytics: *lavoro e tutele al tempo del* management *tramite* big data, LLI, 3, 1, 2017.

([36]) Per il possibile impatto discriminatorio di tali tecniche, v. A. Rota, *Rapporto di lavoro e* big data analytics: *profili critici e risposte possibili*, *LLI*, vol. 3, 1, 2017.

([37]) Sulla distinzione vedi A. Principato, *Verso nuovi approcci alla tutela della* privacy: privacy by design *e* privacy by default settings, *Contratto e impresa. Europa*, 2015, 1, 197 ss.

([38]) Assieme a nuove tecniche che meglio si adattano alla elevata velocità, varietà e volume dei dati che transitano sulla rete, quali l'anonimizzazione, la pseudonimizzazione e criptazione, v. *The EU Data Protection Reform and Big data*, facsheet aprile 2015, 4. In dottrina, G. D'acquisito - M. Naldi, *Big data e protezione dei dati personali*, in *Big data e privacy by design, anonimizzazione, pseudonimizzazione, sicurezza*, in *I diritti nella "rete" della rete*, diretto da F. Pizzetti, 2017, Giappichelli, 5 ss. e per alcuni profili rilevanti dal

trattamento di adottare e scegliere strumentazioni tecnologiche che siano in grado di realizzare una protezione dei dati «per impostazione predefinita» (art. 25, Regolamento), senza lasciare alcuna discrezionalità nel momento successivo del trattamento dei dati. Secondo l'art. 25, par 2, inoltre, «il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento» e pertanto gli strumenti tecnologici utilizzati devono essere in grado di escludere sia i dati che non possono essere lecitamente trattati e quelli che non corrispondono al principio di necessità.

Il riconoscimento della tecnica di protezione dei dati fin dalla progettazione potrebbe comprendere forme di filtro e tutela *by desing* delle prerogative personali del cittadino e del prestatore, come quelle ricavabili dall'art. 8 St. lav. Gli stessi sistemi di *advanced data analytics* possono dunque fornire adeguati strumenti di tutela dei diritti fondamentali, se finalizzati alla *compliance* normativa. Per raggiungere tale obiettivo, è utile orientare la progettazione delle strumentazioni informatiche in modo da stralciare ogni dato rilevatore delle attitudini personali del lavoratore, sperimentando in tal modo una regolazione veicolata dai codici informatici ([39]) che attribuisca alla tecnologia una funzione indiretta ma essenziale di tutela delle posizioni giuridiche.

punto di vista giuslavoristico, C. Del Federico, *Il trattamento dei dati personali dei lavoratori e il Regolamento 2016/679/UE. Implicazioni e prospettive*, in *Web e lavoro* cit., 61 ss.

[39] V. anche Comunicazione "*A European Agenda for the collaborative economy*" (SWD(2016) 184 final) che richiede alle piattaforme di assicurarsi che i service providers che queste intermediano rispetto le regole europee per la tutela dei consumatori e il commercio «by designing their web structures to make it possible for third party traders to identify themselves as such to platform users». Tale prospettiva amplifica il problema del controllo sulla tecnica, v. G. Finocchiaro, Lex mercatoria *e commercio elettronico: il diritto applicabile ai contratti conclusi su internet*, in *Il contratto telematico*, a cura di V. Ricciuto - N. Zorzi, Cedam 2002, 44 s.

Bibliografia

M. Aimo, *Tutela della riservatezza e protezione dei dati personali dei lavoratori*, in *Contratto di lavoro e organizzazione*, tomo II, a cura di M. Marazza, in *Trattato di diritto del lavoro*, diretto da M. Persiani - F. Carinci, 2012, Cedam, 1771 ss.

I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della* Privacy, *LLI*, 2, 1, 2016, 27 ss.

A. Bellavista, *Poteri dell'imprenditore e privacy del lavoratore*, in *I poteri del datore di lavoro nell'impresa*, a cura di G. Zilio Grandi, 2002, Cedam, 41 ss.

D. Bollier, *The promise and peril of big data*, *Communications and Society Program*, 2010, The Aspen Institute.

M. Cherry, *Beyond misclassification: the digital transformation of work*, *Comparative labor law and policy journa*l, 2016, 37, 3, p. 577 ss.

M.F. Cocuccio, *Il diritto all'identità personale e l'identità digitale*, *Il diritto di famiglia e delle persone*, 2016, 3, 949 ss.

G. D'acquisito - M. Naldi, *Big data e protezione dei dati personali*, in *Big data e privacy by design, anonimizzazione, pseudonimizzazione, sicurezza*, in *I diritti nella "rete" della rete*, diretto da F. Pizzetti, 2017, Giappichelli, 5 ss.

E. Dagnino, *Una questione di fiducia: la reputazione ai tempi delle piattaforme online tra diritto alla privacy e prospettive di mercato*, *DRI*, 2017, 1, 247 ss.

E. Dagnino, People analytics: *lavoro e tutele al tempo del management tramite* big data, *LLI*, 3, 1, 2017.

R. De Luca Tamajo, *Introduzione*, in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, a cura di P. Tullini, Cedam 2010, 1 ss.

C. Del Federico, *Il trattamento dei dati personali dei lavoratori e il Regolamento 2016/679/UE. Implicazioni e prospettive*, in *Web e lavoro. Profili evolutivi e di tutela*, a cura di P. Tullini, Giappichelli, 2017, p. 61 ss.

G. Finocchiaro, Lex mercatoria *e commercio elettronico: il diritto applicabile ai contratti conclusi su internet*, in *Il contratto telematico*, a cura di V. Ricciuto - N. Zorzi, Cedam 2002, p. 15 ss.

G. Finocchiaro, *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro*, in *Web e lavoro. Profili evolutivi e di tutela*, a cura di P. Tullini, Giappichelli, 2017, p. 51 ss.

A. Mantelero, *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, *Contratto e impresa. Europa*, 2015, 1, 137 ss.

M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, *ADL*, 2016, 3, 483.

M. Mazzotti, *Per una sociologia degli algoritmi*, *Rassegna italiana di sociologia*, 3-4, luglio-dicembre 2015, 465 e ss.

M. Paissan, E-mail *e navigazione in* internet: *le linee del Garante*, in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, a cura di P. Tullini, Cedam 2010, 11 ss.

A. Principato, *Verso nuovi approcci alla tutela della* privacy: privacy by design *e* privacy by default settings, *Contratto e impresa. Europa*, 2015, 1, 197 ss.

A. Rota, *Rapporto di lavoro e* big data analytics: *profili critici e risposte possibili*, LLI, vol. 3, 1, 2017.

U. Romagnoli, sub art. 8, in U. Romagnoli, L. Montuschi, G. Ghezzi. G. F. Mancini, *Statuto dei diritti dei lavoratori*, Zanichelli, 1972, p. 135 ss.

S. Sciarra, sub art. 8, in *Lo statuto dei lavoratori* diretto da G. Giugni, Giuffrè, 1979, p. 88 ss.

G. Smorto, *Reputazione, fiducia e mercati*, *Europa e diritto privato*, 2016, 1, 199 ss.

L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, *RIDL*, 2016, I, 345 ss.

P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, RIDL, 2009, I, 323 ss.

Documenti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI,
24 novembre 2016, Reg. n. 488. *Piattaforma web per l'elaborazione di profili reputazionali*

Omissis. – 1. Le comunicazioni di Mevaluate Holding Ltd., Mevaluate Italia s.r.l. e Associazione Mevaluate Onlus [d'ora in poi Mevaluate Holding Ltd et alia] in relazione all'"Infrastruttura Immateriale Mevaluate per la Qualificazione Reputazionale".

1.1. Con note del 4 giugno 2015, del 19 gennaio, del 18 marzo e del 4 ottobre 2016, Mevaluate Holding Ltd et alia hanno manifestato l'intenzione di voler procedere alla realizzazione di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti persone fisiche e giuridiche. Il sistema, volto anzitutto a contrastare fenomeni basati sulla creazione di profili reputazionali "artefatti" o "inveritieri", permetterebbe di calcolare in maniera imparziale, affidabile e oggettivamente misurabile il "rating reputazionale" dei soggetti censiti, sì da consentire a eventuali terzi di poter verificare la loro reale credibilità.

In particolare, attraverso la facoltà riconosciuta agli iscritti di documentare la posizione (propria o altrui) rispetto a fatti ritenuti rilevanti sul piano reputazionale, il sistema permetterebbe, tra l'altro, di rendere "più efficaci i processi di valutazione e classificazione delle controparti (appaltatori e subappaltatori, fornitori, distributori, business partner, aspiranti dipendenti, dipendenti in forza e clienti)", incrementando il livello di fiducia nei singoli interlocutori e incentivando l'adozione di comportamenti virtuosi da parte di enti pubblici e privati. Nel valorizzare, quindi, l'aspetto reputazionale quale possibile elemento di valutazione nei rapporti socio-economici, i predetti soggetti ritengono di poter realizzare "spazi negoziali più sicuri", promettendo efficaci azioni di contrasto avverso eventuali forme di mistificazione identitaria e garantendo, in pari tempo, maggiore trasparenza e certezza nelle relazioni interpersonali e di business; ciò, attraverso un servizio che, premiando i soggetti più meritevoli, contribuirebbe altresì allo sviluppo di "buone prassi" presso i singoli operatori economici, ponendosi, nei fatti, quale possibile volano per la promozione di più diffuse forme di legalità.

1.2. Il processo di valutazione degli interessati, per come descritto, prenderebbe avvio dal volontario "caricamento" sulla piattaforma, da parte degli utenti, di documenti contenenti informazioni ritenute significative sul piano reputazionale (v. infra). Tali documenti, prodotti in base alla tipologia di servizio richiesto −1) creazione di un profilo non documentato e non certificato (…); 2) creazione di un profilo documentato, ma non certificato (…); 3) certificazione di documenti e dati successivamente alla creazione di un profilo (…); 4) creazione di un profilo a favore di se stesso (…); 5) creazione di un profilo contro terzi (…); 6) integrazione documentale dei profili precedenti (…); 7) risposta documentata avverso un profilo "contro" (…)−, verrebbero previamente valutati da appositi "consulenti reputazionali" al fine di garantirne la genuinità e l'integrità. All'esito delle operazioni di verifica, il sistema provvederebbe a calcolare, mediante un sofisticato algoritmo matematico (in fase di asserita brevettazione), un "punteggio" complessivo da assegnare agli interessati (c.d. "rating reputazionale") atto a determinarne il grado di affidabilità.

Tale punteggio, variabile nel tempo e in funzione degli elementi trasmessi, sarebbe suddiviso in cinque sub-rating ("penale", "fiscale" e "civile", oltre, eventualmente, a "lavoro e

impegno civile" e, limitatamente alle persone fisiche, "studi e formazione") e verrebbe reso disponibile agli altri utenti della piattaforma, in eventuale associazione ai relativi documenti "giustificativi", mediante apposite "interrogazioni" del sistema, diversamente strutturate in funzione del grado di dettaglio di volta in volta richiesto ("query semplice"/"query dettagliata").

1.3. In base agli elementi trasmessi, il "rating" elaborato dal sistema consentirebbe di ricevere una rappresentazione tendenzialmente completa dei soggetti censiti, perchè riferito a "tutti gli aspetti (a 360°) che concorrono a definire la [loro] reputazione" (cfr. all. 8, nota 18 marzo 2016, cit.). Tale obiettivo sarebbe perseguito, in particolare, attraverso l'allegazione di numerosissimi documenti −in parte obbligatori e in parte facoltativi− in grado di rivelare, nei distinti ambiti considerati ("civile"; "penale"; "fiscale"; ecc.), importanti informazioni relative agli interessati, rilevanti anche sotto il profilo etico.

Tali documenti −tra cui figurano, a titolo esemplificativo: certificati del casellario giudiziale; certificati di regolarità fiscale; certificati relativi ad abilitazioni; diplomi; denunce; querele; provvedimenti giudiziari; ecc.− proverrebbero esclusivamente da fonti diverse dagli interessati (non essendo ammesso, al riguardo, materiale in autocertificazione, potenzialmente distorsivo del sistema) e atterrebbero a fatti e circostanze legate, tra l'altro, alla "sfera morale" dei soggetti censiti (certificati di riconoscimento al valor civile; partecipazione ad attività di volontariato; encomi; premi; referenze; ecc.) e a quella "tecnico-professionale" (presenza/assenza di successi e/o insuccessi professionali); inoltre, verrebbero eventualmente acquisite informazioni tratte da "articoli stampa, radio/TV", laddove prodotte facoltativamente dagli interessati (v. all. B1, E-H, nota 4 giugno 2015, cit., nonché all. 8, nota 18 marzo 2016, cit.).

1.4. L'attendibilità dei profili reputazionali, secondo quanto riferito, sarebbe garantita da una molteplicità di fattori. All'assunzione di responsabilità da parte degli interessati −chiamati a sottoscrivere un'apposita dichiarazione di completezza e accuratezza delle informazioni e di autenticità dei documenti inseriti nel sistema − si aggiungerebbe il vaglio documentale realizzato dai predetti consulenti reputazionali e la possibilità, riconosciuta agli stessi utenti della piattaforma, di visionare in ogni tempo i documenti prodotti da altri; ciò consentirebbe di verificare periodicamente la correttezza e l'integrità delle informazioni presenti a sistema, attuando una forma di controllo generalizzato e diffuso sui dati raccolti. Inoltre, quale ulteriore presidio a garanzia delle informazioni acquisite, verrebbe istituito un apposito "Comitato di Controllo" incaricato di vigilare sull'operato dei medesimi consulenti reputazionali. Infine, verrebbe riconosciuta agli interessati la possibilità di integrare, modificare o aggiornare in ogni tempo i profili a sè riferiti, allegando a tal fine idonea documentazione a supporto (con relativo inserimento, per contro, in un'apposita "black list" o "grey list" in caso, rispettivamente, di allegazione di documenti falsi o di omesso tempestivo aggiornamento dei documenti incidenti sul "rating").

Tale complessivo meccanismo, basato su procedure, accorgimenti e misure asseritamente in grado di assicurare elevati standard di completezza, esattezza e integrità dei dati, porta le proponenti a ritenere che i profili reputazionali elaborati dal sistema presentino, tra gli altri, idonei requisiti di affidabilità e accuratezza (in quanto frutto esclusivo di calcoli matematici basati su documenti autentici, aggiornati e previamente validati), nonché di oggettività e imparzialità (perché non influenzabili da condizionamenti esterni e/o considerazioni personali).

1.5. Il servizio, che presuppone l'iscrizione ad Associazione Mevaluate Onlus e l'adesione ai "valori" espressi dalla "community", opererebbe principalmente su base volontaristica. Le informazioni e i documenti caricati dagli aderenti, infatti, verrebbero raccolti, verificati e resi disponibili agli altri utenti della piattaforma, unitamente ai relativi profili reputazionali, solo a seguito della preventiva raccolta del consenso da parte degli interessati, che "coprirebbe" anche le successive operazioni di trattamento effettuate da terzi (visualizzazione, estrazione e riutilizzo dei dati e dei documenti); il medesimo consenso, inoltre, verrebbe acquisito per giustificare eventuali operazioni di trattamento collegate a presunte

"irregolarità" documentali segnalate da altri, nonchè per pubblicare atti e documenti attinenti a controversie giudiziarie pendenti o future.

Nell'eventualità in cui taluni soggetti (committenti; datori di lavoro; fornitori) fossero già membri del sodalizio associativo, l'"autorizzazione" alla pubblicazione di atti e documenti relativi alle controparti (appaltatori; lavoratori; clienti) verrebbe acquisita, a pena della mancata stipula del negozio o di risoluzione del vincolo in caso di sua revoca, per effetto di apposite clausole che le proponenti vorrebbero inserite nell'ambito dei rapporti contrattuali tra loro intercorrenti.

In presenza di "profili contro terzi" non iscritti alla "piattaforma", il trattamento verrebbe effettuato, qualora fondato su documenti ritenuti liberamente utilizzabili (ad esempio, le sentenze), ai sensi dell'art. 24, co. 1, lett. c), Codice; in ogni caso, non concorrerebbero alla determinazione del rating, n. formerebbero oggetto di condivisione con gli altri utenti della "community", gli atti endo-procedimentali o precontenziosi eventualmente acquisiti dal sistema (v. all. 1, nota 19 gennaio 2016, p. 11). Resterebbe peraltro salva, per costoro, la possibilità di aderire in ogni tempo alla piattaforma e presentare nuovi documenti volti a integrare e/o modificare i profili a sè riferiti.

Nessuna autorizzazione specifica, ai sensi degli artt. 26 e 27 del Codice, richiederebbe il trattamento dei dati sensibili e giudiziari eventualmente presenti o desumibili dai documenti prodotti dagli utenti, trattandosi di informazioni, a detta delle proponenti, liberamente disponibili dagli interessati. In ogni caso, tale trattamento risulterebbe già autorizzato dal Garante attraverso le autorizzazioni generali nn. 3 e7 dell'11 dicembre 2014.

Le caratteristiche dei trattamenti svolti verrebbero rese note agli iscritti in occasione della loro adesione al servizio, attraverso l'apposita informativa riportata sul sito web della piattaforma; in caso di soggetti censiti per effetto di segnalazioni altrui, l'informativa verrebbe resa alla prima occasione utile di contatto, di norma in sede di notifica dell'avviso agli interessati.

1.6. Il servizio verrebbe configurato per operare in conformità al "Codice della reputazione universale" (dichiaratamente ispirato alla "Dichiarazione Universale dei Diritti dell'Uomo"), elaborato da Mevaluate Holding Ltd. al fine di disciplinare i principi per l'individuazione della reputazione di persone fisiche e giuridiche e definire, attraverso l'accluso regolamento, i criteri e le modalità della relativa misurazione. L'affidabilità e l'autorevolezza dei "rating" elaborati a livello nazionale verrebbero garantiti da un apposito organismo tecnico (denominato "Comitato etico mondiale") che, attraverso "note-paese" specificamente elaborate sulla base dei singoli contesti socio-culturali, ne assicurerebbe un'interpretazione coerente con i principi sopra richiamati.

1.7 La soluzione descritta troverebbe giustificazione, a detta delle proponenti, in alcuni indici normativi specificamente individuati (art. 1, co. 1, lett. uu, l. n. 11/2016; d.lgs. n. 460/1997; art. 118 Cost.), oltre che nell'esigenza di contrastare i predetti fenomeni di "ingegneria reputazionale" sovente legati alla commissione di fattispecie delittuose (corruzione; riciclaggio; terrorismo; ecc.), e si affiancherebbe agli strumenti normativi già esistenti −su tutti, il "rating di legalità" di cui all'art. 5-ter d.l. n. 1/2012− con l'intenzione di migliorarne taluni limiti applicativi. Il sistema, inoltre, arrecherebbe significativi vantaggi agli interessati, permettendo loro di valorizzare (e promuovere) la propria immagine sul piano morale, professionale e relazionale, nonchè alla collettività, attraverso il contributo fornito allo sviluppo di prassi "compliant" alla normativa vigente. Il tutto, dietro versamento, da parte degli aderenti e dei fruitori della piattaforma (con alcune eccezioni), di un corrispettivo variabile in funzione dei servizi richiesti e con possibilità per gli stessi iscritti di garantirsi futuri ritorni economici, attraverso "royalties" commisurate al numero di accessi registrato sui singoli "profili" da loro stessi creati.

1.8. Titolare dei trattamenti sarebbe l'Associazione Mevaluate Onlus, che si avvarrebbe a tal fine di Mevalutate Italia s.r.l. nella veste di responsabile ex art. 29 del Codice e della collaborazione di Mevaluate Italia Advisory s.r.l., compagine associativa dei consulenti reputazionali. Questi ultimi, unitamente agli altri soggetti aventi accesso ai dati per conto

dell'associazione, verrebbero designati incaricati ai sensi dell'art. 30 del Codice.

I dati e i documenti utilizzati per l'elaborazione dei "rating" verrebbero messi a disposizione degli utenti della piattaforma per essere successivamente utilizzati da costoro a vario titolo (indagini su fornitori, appaltatori, consulenti; selezione di personale; accertamenti su dipendenti; verifiche sulla clientela; controlli su soci, legali rappresentanti, consiglieri di amministrazione; ecc.). In caso di recesso, i medesimi dati e documenti, insieme ai connessi profili reputazionali, verrebbero cancellati dal sistema, fatta eccezione per quelli relativi ai "profili contro terzi" e quelli inseriti in "black list", conservati per un ulteriore periodo di dodici mesi dalla loro messa a disposizione (v. all. 1, nota 19 gennaio 2016, cit., p. 14 e nota 18 marzo 2016, cit., p. 35).

Tra le misure (minime) indicate a tutela dei dati (v. notifica del 20 gennaio 2016, allegata alla nota interlocutoria del 28 settembre 2016; v., altresì, nota 18 marzo 2016, pp. 28 e ss.), figurano: forme di autenticazione basate su "user id" e "password"; sistemi di tracciamento degli accessi; software antivirus aggiornati semestralmente; meccanismi di cifratura dei dati giudiziari.

I dati, secondo la documentazione trasmessa, non formerebbero oggetto di trasferimento in Paesi non appartenenti all'Unione europea (v. nota 18 marzo 2016, cit., p. 36; v. anche notifica del 20 gennaio 2016, cit.). – *Omissis*.

La suddetta piattaforma, alla data del 18 marzo 2016, sarebbe stata ancora in fase di allestimento (v. nota 18 marzo 2016, cit., p. 1); nessun trattamento ad essa correlato, pertanto, avrebbe avuto luogo, quantomeno fino a tale data, in ordine ai dati personali degli utenti.

Il sistema, inoltre, ha già formato oggetto di alcune prime considerazioni da parte dell'Autorità (v. nota del 21 ottobre 2015, inviata a Mevaluate Holding Ltd.), sia pure in riferimento a presupposti e modalità di implementazione parzialmente differenti da quelle descritte nel presente provvedimento.

2. Le considerazioni dell'Autorità.

2.1. L'"Infrastruttura Immateriale Mevaluate – *Omissis*. –, è costituita da una piattaforma web (con annesso archivio informatico) preordinata all'assegnazione, previa raccolta, verifica, ed elaborazione di numerosi dati personali contenuti in documenti prodotti dagli utenti, di indicatori alfanumerici asseritamente in grado di misurare l'affidabilità reputazionale dei soggetti censiti (persone fisiche e giuridiche). Tale sistema, come già anticipato a Mevaluate Holding Ltd. nella nota sopra citata, comporta rilevanti problematiche sotto il profilo della disciplina di protezione dei dati personali – qui considerate unicamente in rapporto alle persone fisiche (art. 40, d.l. n. 201/2011, convertito, con modificazioni, dalla l. n. 214/2011) – in ragione della delicatezza delle informazioni che si vorrebbero utilizzare, del pervasivo impatto sugli interessati, nonchè dei presupposti e delle modalità di trattamento prospettate.

2.2. Ed infatti, pur essendo legittima, in linea di principio, l'erogazione di servizi che possano contribuire a rendere maggiormente efficienti, trasparenti e sicuri i rapporti socio-economici, si osserva che il sistema in esame presuppone la raccolta di dati personali suscettibili di incidere significativamente, per tipologia e quantità, sulla rappresentazione economica e sociale di un'ampia platea di soggetti (clienti; dipendenti; candidati; imprenditori; liberi professionisti; fornitori; cittadini; ecc.). Il "rating" da questo elaborato, infatti, potrebbe ripercuotersi pesantemente sulla vita (anche privata) degli individui censiti, influenzandone scelte e prospettive e condizionando la loro stessa ammissione a (o esclusione da) specifiche prestazioni, servizi o benefici; occorre, pertanto, estrema cautela nell'affrontare tematiche così delicate, anche in considerazione del fatto che la "reputazione" che si vorrebbe qui misurare, in quanto strettamente correlata alla considerazione delle persone e alla loro stessa "proiezione" sociale, risulta intimamente connessa con la loro dignità, elemento cardine della disciplina di protezione dei dati personali (art. 2 del Codice; v. anche Cass. 8 agosto 2013, n. 18981 secondo cui "la dignità dell'interessato […], [in quanto] è valore sommo a cui è ispirata la legislazione sul trattamento dei dati personali – il cui disegno è funzionale alla difesa della persona e dei suoi fondamentali diritti, [tendendo] ad impedire che l'uso, astrattamente

legittimo, del dato personale avvenga con modalità tali da renderlo lesivo di quei diritti […]– è [comunque] preminente rispetto all'iniziativa economica privata" tutelata dall'art. 41 Cost.).

Tale doverosa premessa porta il Garante a ritenere, anche alla luce di quanto già evidenziato, sia pure in ambiti parzialmente differenti, dal Gruppo di lavoro dei Garanti europei istituito ai sensi dell'art. 29 della direttiva 95/46/CE (cfr. Parere del 3 ottobre 2002, "Documento di lavoro sulle liste nere", WP65), che la costituzione di siffatta piattaforma (e il connesso trattamento di dati personali), in ragione delle sue peculiari caratteristiche –tali da incidere, come detto, sulla stessa dignità degli interessati–, non sia, allo stato, lecita.

Al riguardo, non può trascurarsi, infatti, che gli altri sistemi di "accreditamento" riconosciuti attualmente dall'ordinamento derivano da previsioni di legge che ne individuano espressamente, salvo il rinvio a discipline più di dettaglio, le principali caratteristiche (v., ad esempio, il già citato "rating di legalità", ovvero il "rating di impresa" di cui all'art. 83, co. 10, d.lgs. n. 50/2016); ciò appare coerente, del resto, con l'obiettivo di rendere disponibili alla collettività strumenti di valutazione universalmente riconosciuti, in grado di fornire agli utenti, attraverso un avallo formale che ne stabilisca puntualmente i requisiti e i limiti, elementi di giudizio certi e oggettivi, nonchè imparziali e affidabili.

In tale quadro, i riferimenti addotti da Mevaluate Holding Ltd. Et alia – tenuto conto del tipo di trattamento che si intende realizzare - appaiono generici e, comunque, inidonei a giustificare la costituzione della prefigurata banca di dati.

Anche il richiamo alla citata l. n. 11/2016 (per la cui attuazione v., in parte qua, il summenzionato art. 83, co. 10, d.lgs. n. 60/2016), lungi dal corroborare la tesi delle proponenti, appare piuttosto avvalorare l'impostazione sopra evidenziata, sia in relazione alla necessità di un'idonea fonte di regolazione di siffatte tipologie di strumenti, sia in merito all'opportunità di demandarne la gestione in capo a soggetti muniti di adeguate e comprovate garanzie di terzietà e indipendenza. E ciò, a tacere del fatto che il richiamo al menzionato "Codice della reputazione universale", peraltro assimilabile a un codice di condotta o autoregolamentazione (ancorchè liberamente ispirato, secondo quanto sostenuto, ai principi della "Dichiarazione Universale dei Diritti dell'Uomo") e in sè privo di valenza normativa certa, appare invero inidoneo rispetto ai fini sopra evidenziati.

2.3. In disparte l'assenza di un'idonea cornice normativa (rilevante anche ai sensi dell'art. 11, co. 1, lett. a), del Codice), vale poi osservare, sempre sul piano della liceità dei trattamenti, che il consenso degli interessati, per essere conforme a legge, deve essere manifestato liberamente (art. 23 del Codice). Tale presupposto non ricorre se il consenso risulta manifestato –come nel caso di profili creati da altri– dietro necessità di contrastare gli effetti negativi derivanti da eventuali valutazioni avverse (in tal senso, v. pure il "Parere 15/2011 sulla definizione di consenso" adottato dal Gruppo di lavoro articolo 29 per la protezione dei dati in data 13 luglio 2011, WP 187, secondo cui il consenso non può essere considerato libero se le conseguenze dello stesso "minano la libertà di scelta dell'individuo"). Parimenti, e per le stesse ragioni, non apparirebbe frutto di libera autodeterminazione il consenso espresso da appaltatori, lavoratori e clienti in conseguenza della clausola contrattuale che l'associazione vorrebbe inserita nell'ambito dei rapporti intercorrenti con le controparti, non potendo considerarsi tale la volontà manifestata dagli interessati dietro "minaccia" della mancata stipula del contratto o quale condizione per la permanenza del vincolo negoziale.

Ancora, non risulterebbe giustificato il trattamento che l'associazione vorrebbe effettuare con riferimento ai soggetti non iscritti alla piattaforma, posto che i relativi dati personali, ove anche tratti da documenti liberamente conoscibili, verrebbero comunque elaborati da quest'ultima per ottenere valutazioni reputazionali autonome, originali e del tutto distinte dalle informazioni originariamente acquisite; ragion per cui il loro lecito trattamento potrebbe avvenire solo sulla base del "libero" consenso degli interessati, ovvero di altro idoneo presupposto alternativo (artt. 23 e 24 del Codice), allo stato non ravvisabile. Analogamente, nessun presupposto giustificherebbe il trattamento (fosse anche nella forma della sola raccolta e conservazione: v. nota 18 marzo 2016, cit., p. 26) dei dati sensibili eventualmente riconducibile ai medesimi soggetti, che potrebbe avvenire unicamente con il "libero" consenso

(scritto) di costoro o in presenza di altro adeguato equipollente (artt. 23, co. 4 e 26, co. 1 e 4, del Codice), comunque non ricorrente.

Non risultano documentati, infine, i criteri di stretta pertinenza e indispensabilità richiesti dalle autorizzazioni generali nn. 3 (punto 7) e 7 (capo VII, punto 4) del 2014 ai fini di una lecita pubblicazione dei dati sensibili e giudiziari degli interessati, non potendosi ritenere per ciò solo legittimante, come pure sostenuto dalle proponenti, il mero consenso espresso dagli interessati (v. nota 18 marzo 2016, cit., pp. 25 e ss.).

2.4. Il descritto trattamento, per altro verso, desta perplessità anche con riferimento ai principi di necessità e proporzionalità (artt. 3 e 11, co. 1, lett. d), del Codice).

Premesso che il funzionamento del sistema si basa su modalità di raccolta (massiva) di dati e documenti che non risultano in linea con l'art. 3 del Codice (il quale impone, come noto, di configurare i sistemi informativi e i programmi informatici in modo da ridurre al minimo l'utilizzo di dati personali e identificativi degli interessati), occorre evidenziare, da altro angolo di visuale, che la rilevanza e pertinenza di detti dati e documenti (parte dei quali, peraltro, in grado di rivelare aspetti anche molto delicati della vita privata delle persone) appare in taluni casi dubbia e, comunque, indimostrata. E ciò, non solo in ragione dei criteri (discrezionali) individuati come basi per il calcolo del rating reputazionale, ma anche per l'assenza di circostanziati elementi in grado di comprovare, empiricamente, l'effettiva incidenza di talune dinamiche etico-comportamentali sull'"affidabilità" dei soggetti censiti (a titolo esemplificativo, non è detto che l'aver ricevuto attestati di merito o riconoscimenti al valor civile garantisca –di per sè– una maggiore "credibilità" rispetto a soggetti che ne sono privi, come pure l'appartenere ad associazioni di volontariato o l'aver conseguito successi e/o insuccessi sul piano professionale). Sicchè, essendo il sistema preordinato, per l'appunto, a valorizzare "il bene più prezioso di ciascuno: la reputazione" (cfr. all. "A", nota 4 giugno 2015, cit.) attraverso l'allegazione di detti documenti, sarebbe stato preciso onere delle proponenti presentare rigorosi elementi in tal senso.

A ciò, si aggiunga che il trattamento riguarderebbe un numero potenzialmente molto elevato di soggetti, con attendibili significative ripercussioni per i diritti individuali degli interessati in caso di violazione delle misure di sicurezza (v. infra), di accessi non autorizzati o di utilizzo abusivo delle informazioni, anche da parte di terzi. Dacchè appaiono sproporzionate anche le modalità con cui si è stabilito di dare libero e indiscriminato accesso a tutti i numerosi documenti presenti sulla piattaforma, considerati i rischi che corrono gli interessati in relazione al loro successivo riutilizzo per finalità non necessariamente lecite (si pensi, ad esempio, al riuso dei dati per finalità di indagine su fatti non attinenti alla valutazione dell'attitudine professionale di candidati e lavoratori, potenzialmente confliggente con l'art. 8, l. n. 300/1970, richiamato dall'art. 113 del Codice).

2.5. Anche con riferimento al principio di qualità dei dati (art. 11, co. 1, lett. c), del Codice), il sistema pare scontare alcune criticità. Dall'esame delle risultanze in atti, infatti, non si evincono documentati elementi idonei a comprovare un'elevata affidabilità del sistema descritto. Al di l. delle mere dichiarazioni concernenti una sua presunta brevettazione (v., su tutti, all. "I" alla nota del 4 giugno 2015, cit.), le proponenti non sono state in grado di dimostrare l'efficacia del non meglio identificato algoritmo che regolerebbe la determinazione dei "rating" e al quale dovrebbe essere rimessa, peraltro senza possibilità di contestazione (v. all. 1 alla nota del 19 gennaio 2016, cit.), la valutazione reputazionale dei soggetti censiti; e ciò, verosimilmente, anche a causa dell'assenza di riconosciuti criteri, a livello nazionale o internazionale, sulla base dei quali poter "misurare" la reputazione degli individui in modo realmente oggettivo, affidabile e imparziale.

In ogni caso, si nutrono perplessità, più in generale, sull'opportunità stessa di rimettere a un sistema automatizzato ogni determinazione in merito ad aspetti particolarmente delicati e complessi quali quelli connessi alla reputazione dei soggetti coinvolti. A prescindere, infatti, dall'oggettiva difficoltà di misurare situazioni, parametri e variabili non sempre agevolmente "classificabili" o "quantificabili", occorre evidenziare che la suddetta (acritica) valutazione potrebbe fondarsi su atti, documenti o certificati viziati ex ante da falsità ideologica, ovvero

caratterizzati da alterazioni materiali non facilmente riscontrabili da parte di pur esperti "consulenti" reputazionali (peraltro non esenti, contrariamente a quanto sostenuto, da pericoli di errore o tentativi di corruzione); con il rischio, neanche tanto remoto, di creare profili reputazionali inesatti e non rispondenti alla reale rappresentazione – e, quindi, all'identità personale, intesa anche quale immagine sociale (art. 2 del Codice; Provv. 9 marzo 2006 [doc. web n. 1269316]; Trib. Roma 7 dicembre 2015) − dei soggetti censiti. E ciò, a tacere del fatto che gli stessi interessati potrebbero non essere in condizione, per molteplici ragioni, di aggiornare tempestivamente i propri profili reputazionali, con evidenti, ulteriori ricadute in termini di effettiva qualità dei dati.

2.6. Senza voler entrare nel merito del prefigurato meccanismo remunerativo, che pur potrebbe alimentare, in concreto, pericolosi impulsi delatori in danno di un'estesa platea di soggetti, esposti al rischio di "censimento" per il solo fatto di avere pendenti controversie giudiziarie di varia natura, si osserva, da altro angolo di visuale, che suscitano dubbi anche le misure di sicurezza indicate dalle proponenti (v. punto 1.8).

Dall'esame delle risultanze istruttorie, infatti, è emerso che tali misure sarebbero basate, prevalentemente, su sistemi di autenticazione "debole" (user id e password) e su meccanismi di cifratura dei (soli) dati giudiziari, invero inadeguate −specie se rapportate all'elevato numero di soggetti che potrebbero essere coinvolti e all'ingente quantitativo di informazioni, anche molto delicate, che verrebbero registrate all'interno della piattaforma− a garantire idonei standard di tutela degli interessati. Al contrario, sistemi quali quello in esame dovrebbero offrire rigorose garanzie in termini di sicurezza e affidabilità dei dati, basate su misure e accorgimenti che vadano ben oltre quelle minime dichiarate in corso di istruttoria e che prevedano certificazioni od omologazioni rilasciate da appositi organismi qualificati e indipendenti. Gli elementi in atti, invece, hanno denotato significative lacune in tal senso, evidenziando rischi con riferimento a possibili situazioni di violazione dei dati e di furto di identità, sia in fase di visualizzazione delle informazioni (accessi a dati non pertinenti; accessi non autorizzati) che di invio dei documenti da parte degli utenti (alterazione di profili a seguito di furto delle credenziali).

2.7. Ulteriori criticità, ancora, si ravvisano nei tempi di conservazione dei dati e nell'informativa da rendere agli interessati.

Quanto al primo profilo, si rileva che nessun elemento giustificativo. stato addotto con riferimento agli ulteriori tempi di conservazione (dodici mesi dall'intervenuto recesso) delle informazioni relative ai profili "contro" o contenute nella "black list"; tale conservazione, in assenza di idonea motivazione, risulta in violazione dell'art. 11, comma 1, lett. e), del Codice.

Per quanto riguarda, invece, l'informativa agli interessati, la stessa non risulta adeguata rispetto al trattamento che si intenderebbe svolgere. Posto che il testo in atti reca riferimenti a "finalità connesse all'esecuzione di procedure selettive indette" dall'associazione o da società collegate che nulla hanno a che vedere con i servizi offerti agli utenti, si rileva, sotto a ltro profilo, che la stessa informativa, contrariamente a quanto sostenuto in sede istruttoria (cfr. nota 16 marzo 2016, cit., p. 36; v. notifica 20 gennaio 2016, cit.), richiama possibili trasferimenti all'estero dei dati; dal relativo testo, inoltre, si desume la raccolta di un consenso facoltativo in merito a non meglio identificate finalità commerciali, nemmeno menzionate tra gli scopi perseguiti dal titolare. Ciò ingenera notevole confusione circa le effettive caratteristiche del trattamento, con conseguente violazione dell'art. 13 del Codice.

2.8. Alla luce delle considerazioni che precedono, si ritiene, conclusivamente, che il trattamento di dati personali connesso ai servizi offerti tramite l'"Infrastruttura Immateriale Mevaluate per la Qualificazione Reputazionale", per le ragioni di cui in motivazione, non possa essere considerato conforme alla disciplina di protezione dei dati personali (artt. 2, 3, 11, 13, 23, 24 e 26 del Codice); ne consegue che qualunque operazione di trattamento (presente o futura) al riguardo, ove effettuata sulla base dei presupposti e delle modalità indicate, deve essere considerata illecita e, quindi, vietata in riferimento ai dati personali degli interessati (art. 154, co. 1, lett. d), del Codice). – *Omissis*.