

DATI PERSONALI

PROTEZIONE, LIBERA CIRCOLAZIONE
E *GOVERNANCE*

1. Principi

a cura di
Fabio Bravo


Pacini
Giuridica



DATI PERSONALI

PROTEZIONE, LIBERA CIRCOLAZIONE
E *GOVERNANCE*

1. Principi

a cura di
Fabio Bravo



© Copyright sull'Opera 2023 Prof. Avv. Fabio Bravo

Tutti i diritti riservati al Curatore Fabio Bravo, salvo quanto di seguito specificato. All'Editore è stato concesso il diritto esclusivo e senza limiti territoriali (con divieto di cessione a terzi) di pubblicazione a stampa e distribuzione dell'Opera. Gli ulteriori diritti restano in capo al Curatore in via esclusiva. L'Editore e il Curatore, ciascuno per quanto di propria spettanza, rilasciano la presente opera anche in formato digitale (PDF editoriale) ad accesso aperto in licenza Creative Commons CC BY ND 4.0, disponibile per il download gratuito sul sito cris.unibo.it, con il seguente identificativo persistente 11585/948658 | <https://hdl.handle.net/11585/948658>.



ISBN 978-88-3379-672-7

Realizzazione editoriale



Via A. Gherardesca
56121 Pisa

Responsabile di redazione
Gloria Giacomelli

Fotolito e Stampa
IGP Industrie Grafiche Pacini

Capitolo VII

Il principio di esattezza

*Francesco Avveduto - Carlo Basunti**

SOMMARIO: 1. Inquadramento normativo. – 2. Portata del principio. – 2.1. Il principio di esattezza: un’ipotesi ricostruttiva. – 2.2. Il principio di esattezza come baluardo a difesa dei diritti e degli interessi dell’interessato. – 2.3. Il principio di esattezza tra obblighi e interesse del titolare. – 2.4. L’esattezza dei dati nell’ambito dei diritti dell’interessato previsti dal GDPR. – 3. Applicazione del principio nella casistica. – 3.1. Il diritto di rettificare dati inesatti al vaglio della Corte di giustizia. Il caso dei documenti dei concorsi professionali e delle valutazioni dell’esaminatore. – 3.2. Il principio di esattezza nelle pronunce del Garante.

1. INQUADRAMENTO NORMATIVO

La tutela della vita privata e familiare di cui all’art 8 CEDU si è ramificata in varie forme di protezione, inclusa quella relativa alla protezione dei dati personali che, nelle sue diverse sfaccettature, declina anche il principio di *esattezza* dei dati per come oggi lo conosciamo e per come si trova contemplato nella normativa vigente¹.

* Pur essendo lo scritto frutto di riflessione comune, il par. 1 è da attribuire a Francesco Avveduto, i par. 2 e 3 sono da attribuire a Carlo Basunti.

¹ L’art. 8 CEDU contempla un generale diritto alla tutela della vita privata e familiare nei confronti di ingerenze pubbliche o private («Art. 8. *Diritto al rispetto della vita privata e familiare.* – 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell’esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell’ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui»), che reclama un bilanciamento con altri diritti fondamentali di pari rango. La Corte europea dei diritti dell’uomo ha interpretato tale diritto ricomprendendo nella sua tutela esigenze di protezione diverse, inclusa la tutela della riservatezza e dei dati personali, la tutela dell’immagine e del nome, la tutela dell’identità personale e, in particolare, la tutela dell’individuo alla rappresentazione veritiera delle vicende che interessano il soggetto. L’incidenza del diritto alla tutela della vita privata e familiare di cui all’art. 8 CEDU, come interpretato dalla Corte europea, non è stata immediata nel nostro ordinamento giuridico nazionale, né da parte del legislatore né da parte della giurisprudenza, che ha faticato a riconoscere il diritto alla riservatezza. Si pensi, ad esempio, alla celebre sentenza della Cass., n. 4487/1956, con riguardo alle vicende legate alla vita del celebre tenore Caruso, nei confronti delle quali i suoi eredi lamentavano l’illiceità della loro divulgazione, perché, anche se verificatesi al di fuori del domicilio, non avrebbero avuto diretto interesse per i terzi. Nel caso di specie tuttavia la S.C. si espresse sancendo che «chi non ha saputo o voluto tener celati i fatti della propria vita, non può pretendere che il segreto sia mantenuto dalla discrezione altrui; la curiosità ed anche un innocuo pettegolezzo, se pur costituiscono una manifestazione non elevata dell’animo, non danno luogo di per sé ad un illecito giuridico (...)», arrivando addirittura ad affermare che «(...) nell’ordinamento giuridico italiano non esiste un diritto

L'art. 5, par. 1, lett. *d*), del Reg. (UE) 2016/679 (GDPR), nel sancire che i dati debbano essere «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (“esattezza”)», pone in evidenza l'importanza riservata dal legislatore alla “qualità” del dato personale come fondamento per la tutela dei diritti del soggetto². Di fatto, solo salvaguardando la qualità delle informazioni, con riguardo all'esattezza delle stesse, è possibile assicurare che l'interessato sia reso incolume dal pregiudizio derivantegli da una falsa rappresentazione di sé o da altri aspetti, di natura personalistica o patrimonialistica, che lo riguardano.

Una prima importante tappa dell'evoluzione normativa che, a livello internazionale, ha reso evidente l'acquisita consapevolezza del principio di esattezza dei dati si ha con l'emanazione della *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* n. 108 del 28 gennaio 1981, con la quale – presa coscienza della sempre più rilevante mole di dati in circo-

alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto». Successivamente, una diversa sensibilità giuridica sulle nuove esigenze di protezione della sfera privata e, più recentemente, l'esponentiale aumento della mole di dati in circolazione ha portato a più recenti pronunce in cui si evidenzia la declinazione del diritto alla tutela della vita privata anche quale diritto alla *esatta* rappresentazione dell'individuo in elementi quali il nome e la sua immagine che compongono la sua identità che il singolo ha diritto a determinare e ad ottenere la giusta tutela. Si tratta di una nozione ampia, elaborata dapprima dalla giurisprudenza della Corte di Strasburgo, che consente, dunque, di includere numerosi aspetti dell'identità di un individuo (in tal senso cfr. M.G. PUTATURO DONATI, *Il diritto al rispetto della «vita privata e familiare» di cui all'art. 8 della CEDU, nell'interpretazione della Corte Edu: il rilievo del detto principio sul piano del diritto internazionale e su quello del diritto interno*, in *Europeanrights.eu*, articolo consultabile all'url http://www.europeanrights.eu/public/commenti/Commento_Putaturo.pdf visitato da ultimo in data 7 aprile 2023. Sul punto si vedano altresì le pronunce della Corte di Strasburgo ivi segnalate, tra le quali la sent. 5 dicembre 2013, sez. V, *Henry Kismoun contro Francia*, in tema di cambiamento del cognome e del nome delle persone fisiche, nonché la sent. 7 febbraio 2012, Grande Camera, *Von Hannover contro Germania*).

Più di recente la Corte EDU ha ribadito la portata di tale tutela che, giova dirlo, prescinde dalla lesione del diritto all'onore, dovendosi tenere a monte conto della necessità del diritto alla corretta rappresentazione del soggetto nel suo complesso ed in ogni aspetto della sua personalità (cfr., in tal senso, la decisione della Corte EDU del 21 febbraio 2017, *Rubio Dosamantes c. Espagne*, in tema di bilanciamento tra libertà di espressione e tutela della vita privata e familiare. La ricorrente lamentava la mancata tutela del proprio diritto innanzi all'autorità giudiziaria riguardo alla legittimità di dichiarazioni rese dal produttore della cantante, che aveva rivelato aspetti relativi alla presunta omosessualità della donna e ad una relazione affettiva ormai conclusasi. I giudici spagnoli avevano rigettato la domanda ritenendo che in tale vicenda non fosse rinvenibile una lesione all'onore della cantante. La Corte Edu ha invece ritenuto sussistente una violazione dell'art. 8 per non avere le Corti spagnole adempiuto al proprio obbligo positivo di protezione della vita privata della ricorrente). L'evoluzione del sistema di protezione della vita privata e familiare di cui all'art. 8 CEDU, giunto progressivamente a ricomprendere anche la tutela della persona contro una falsa rappresentazione della propria identità, ha portato alla progressiva affermazione del principio di esattezza, tutelato ora anche nell'ambito della puntuale disciplina in materia di protezione dei dati personali.

² Si veda anche il *considerando* n. 39 del GDPR, nella parte in cui prevede che «è opportuno adottare tutte le misure ragionevoli affinché i dati *inesatti* siano rettificati o cancellati».

lazione già nella società del tempo – si volle realizzare una prima tutela concreta con riguardo alle persone interessate dal trattamento³, prevedendo espressamente, all'art. 5, che «I dati a carattere personale oggetto di elaborazione automatica devono essere (...) *d*) esatti e, se necessario, aggiornati (...)»⁴. L'esattezza del dato rimane strettamente interconnessa con il principio di finalità, liceità e correttezza, poiché solo se il dato è esatto è possibile raggiungere il fine del trattamento, giustificando l'interferenza con la sfera privata del soggetto interessato; solo se il dato è esatto è possibile considerare il trattamento come lecito e corretto, perché svolto consentendo di avere una rappresentazione attendibile e non adulterata dell'identità personale dell'interessato⁵. L'esattezza del dato, ovviamente, incide anche su altri aspetti, non essendo confinabile al solo connotato dell'identità personale, come ben si comprende, a mero titolo esemplificativo, se si pensa all'esattezza dei dati delle movimentazioni bancarie nei conti correnti, in difetto della quale si hanno rischi di compromissione dei diritti patrimoniali o, ancora, all'esattezza dei dati di una cartella clinica, in difetto della quale sono evidenti i rischi sulla salute: si tratta dunque di diritti della personalità (quello alla vita e alla salute), diversi dal diritto all'identità personale. L'esattezza del dato, così come in generale l'intera disciplina sulla protezione dei dati personali, mantiene la sua vocazione ad essere precondizione per l'esercizio di altri diritti dell'individuo a cui i dati medesimi si riferiscono.

Tale consapevole interconnessione del principio di esattezza con quelli di finalità, liceità e correttezza del trattamento è stata la chiara ispirazione del legislatore comunitario nella redazione della dir. 95/46/CE (c.d. Direttiva Madre), da cui ha avuto origine la legislazione degli Stati membri in ambito del trattamento dati personali. Si legge infatti, all'art. 6, che «Gli stati membri dispongono che i dati personali devono essere (...) *d*) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati». Si tratta di un articolo che compone la Sezione I del Capo II del citato provvedimento comunitario, significativamente dedicata ai «*Principi relativi alla qualità dei dati*».

L'attenzione posta dal legislatore europeo sulla “qualità” del dato – ed in particolare sul connotato di esattezza – ha influenzato ovviamente gli ordinamenti nazionali, in occasione dell'emanazione della normativa di recepimento. Evidenza di ciò si ha già nella l. 31 dicembre del 1996 n. 675⁶, la quale, nel proprio *incipit*, esordiva

³ Già in quel contesto identificate dall'art. 2, lett. *a*), come persona fisica identificata od identificabile cui sono riferibili i dati personali fatti oggetto del trattamento.

⁴ *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* n. 108 del 28 gennaio 1981, art. 5.

⁵ Così P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione de dati personali*, Milano, 2003, I, pp. 455-460, dove nello specifico si rivolge l'attenzione al caso della tutela della identità in ambito giornalistico. In tali circostanze, infatti, la centralità della qualità della informazione data regge sulle proprie spalle la bontà dell'intero trattamento, perché da essa deriva la censurabilità o meno della condotta di chi diffonde una notizia.

⁶ L. n. 675 del 31 dicembre 1996 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* (testo consolidato con il d.lgs. 28 dicembre 2001, n. 467) (Pubblicato sulla Gazzetta

dichiarandosi come volta, tra l'altro, alla garanzia della tutela della riservatezza e dell'identità personale⁷ ed, all'art. 9 (rubricato «*Modalità di raccolta e requisiti dei dati*»), dettava alcuni requisiti qualitativi dei dati oggetto di trattamento, con lo scopo di assicurarne la completezza, l'esattezza, l'aggiornamento e la non eccedenza rispetto alla finalità perseguita⁸.

Anche nel nostro ordinamento, il principio di esattezza dei dati appare il frutto di un lento processo di sedimentazione normativa, dato che è possibile rinvenirlo anche in altri contesti, diversi da quello specificamente previsto in tema di *data protection*. Si pensi al d.p.r. n. 600/1973, al cui art. 33 si rinveniva una facoltà per gli uffici delle imposte, in caso di fondati sospetti sulla inesattezza dei dati, di disporre le opportune verifiche. Si pensi, ancora, alla l. n. 1/1991 («*Disciplina dell'attività di intermediazione mobiliare e disposizioni sull'organizzazione dei mercati mobiliari*») che all'art. 25 (rubricato «*Offerta e commercializzazione di servizi o prodotti informatici o telematici*») faceva esplicito riferimento alla necessità che i dati fossero «veritieri»⁹.

In materia di protezione dei dati personali, la completezza del dato e la conseguente esattezza dello stesso vanno considerate nell'ottica della finalità del trattamento di cui il dato medesimo è fatto oggetto. Infatti, non in astratto, ma in maniera direttamente e strettamente collegata con il contesto in cui il trattamento viene effettuato, sarà necessario calibrare l'attenzione volta alla completezza del dato, non potendosi, a titolo meramente esemplificativo, obbligare il titolare del trattamento ad acquisire anche notizie e dati ulteriori ed eccedenti rispetto a quelli necessari per l'attività di trattamento e le finalità della stessa¹⁰.

Ufficiale n. 5 dell'8 gennaio 1997, Suppl. Ordinario n. 3).

⁷ Cfr. art. 1, co. 1, della l. 675/96 cit., che, con riguardo alle finalità, prevedeva espressamente che «la presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale».

⁸ L'art. 9, co. 1, della l. 675/96 cit. prevedeva, testualmente, che «i dati personali oggetto di trattamento devono essere: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi; c) *esatti* e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati».

⁹ La l. n. 1/1991 cit. – successivamente abrogata dal d.lgs. 58/1998, T.U.I.F. – prevedeva espressamente, all'art. 25, co. 1, che «l'offerta o la commercializzazione di servizi, realizzati mediante strumenti informatici e telematici, aventi per oggetto la diffusione al pubblico di dati concernenti i corsi, le quantità scambiate, le condizioni di domanda ed offerta relative alle negoziazioni di valori mobiliari trattati nei mercati regolamentari ai sensi della presente legge, sono soggette ad autorizzazione da parte della Consob. La Consob può negare o revocare l'autorizzazione qualora ritenga che, in relazione alle modalità di acquisizione ed elaborazione dei dati ovvero alla natura ed ai fini del servizio offerto o commercializzato, sussista il rischio che i dati stessi non siano *veritieri* ovvero siano tali da *indurre in errore i destinatari*».

¹⁰ Sulla importanza dell'attenzione alla *qualità* dei dati si veda G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, pp. 265-270. Sempre sulla rilevanza della *qualità* del dato si veda anche G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 116-118, che pone l'attenzione sulle normative che regolamentano il trattamento

È con il codice della *privacy* (d.lgs. 196/2003) che il legislatore italiano compie un significativo passo in avanti verso la riorganizzazione sistematica dell'intera disciplina interna in materia di protezione dei dati personali, tenendo conto anche degli orientamenti giurisprudenziali e delle decisioni rese dal Garante per la *privacy* in tale materia. L'avvento del predetto codice non ha però modificato – nella forma e nella sostanza – quanto già previsto nella l. n. 675/96, rimanendo invariata, anche nella codificazione di inizio millennio, la formula usata dal legislatore nazionale nel recepire l'obbligo di mantenere i dati «esatti» ed «aggiornati», conformemente a quanto previsto dall'art. 6 della dir. 95/45/CE: quest'ultimo stabilisce che i dati debbano essere esatti e se necessario aggiornati e che devono essere prese tutte le misure ragionevoli necessarie affinché possa essere mantenuta tale esattezza; il codice della *privacy* nella sua versione originale del 2003 prevede all'art. 11, lett. e), che i dati debbano essere «esatti e, se necessario aggiornati», riprendendo in maniera letterale la previsione dell'art. 9, lett. c), dell'abrogata l. 675/96.

Il legislatore italiano, sia con la l. 675/1996 sia con il d.lgs. 196/2003 (codice in materia di protezione dei dati personali), in cui tale legge è confluita, ha voluto prevedere non solo l'obbligo di adozione di misure minime di sicurezza (art. 15, co. 2, l. 675/96 e art. 33 d.lgs. 196/2003, anteriforma del 2018), assistito da sanzioni penali, ma anche l'obbligo di adozione di misure “adeguate” (art. 15, co. 1, l. 675/96 e art. 31 d.lgs. 196/2003), finalizzate, tra l'altro, al mantenimento dell'*esattezza* dei dati personali nella dinamica dello svolgimento delle attività di trattamento.

Con il Reg. UE 679/2016 (GDPR) viene ripreso il fondamentale concetto di “adeguatezza” delle misure per il mantenimento della *esattezza* dei dati, già presente nella dir. 95/46 (senza alcuna specifica previsione di sanzioni penali per la mancata adozione di misure “minime” di sicurezza), viene esplicitato il principio di “esattezza” all'art. 5 (che da “requisito” del dato diviene “principio” a cui informare il trattamento) ed, altresì, viene affermato il nuovo principio di “responsabilizzazione” o *accountability* (in forza del quale il titolare del trattamento è tenuto ad adottare misure tecniche ed organizzative per garantire e per dimostrare la corretta applicazione dei principi in materia di protezione dei dati personali, ivi incluso il principio di *esattezza*)¹¹. Viene così in rilievo, in maniera uniforme per tutti gli altri ordinamenti

dei dati da parte di soggetti pubblici, evidenziando l'importanza dell'attenzione alla *esattezza* e completezza dei dati anche in tale contesto. Si pensi alla l. n. 35/1999 che all'art. 3, co. 3, prevedeva un obbligo per l'ente pubblico di effettuare una verifica periodica della *esattezza* dei dati, completezza e necessità rispetto alle finalità del trattamento, al fine di assicurare la pertinenza e non eccedenza dei dati rispetto al trattamento. Si pensi ancora al CAD, d.lgs. 235/2010, in cui si prevede per le amministrazioni di aggiornare tempestivamente gli archivi al fine di evitare una falsa rappresentazione dell'individuo e le conseguenze pregiudizievoli che da ciò potrebbero derivare allo stesso.

¹¹ Cfr. art. 5, par. 2, e 24 del Reg. UE 679/2016. Sulla rilevanza dell'*accountability* si veda G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 12 ss.; sul ruolo del principio di *esattezza* in prospettiva dinamica e della proporzionalità delle misure da adottare M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 208-213. Sul principio di *accountability* si veda anche, nel presente volume, il Capitolo XIII.

dei Paesi membri dell'UE, una nuova prospettiva della protezione dei dati personali nell'ottica della *accountability*, per la quale l'esattezza dei dati diventa fondamentale in quanto punto di contatto dei vari principi su cui si fonda la normativa stessa sul trattamento dei dati: l'esattezza del dato presuppone e impone l'adozione di adeguate misure tecniche e organizzative di sicurezza, incluse quelle che delineano efficaci procedure di gestione dei dati.

Con l'entrata in vigore del Reg. UE 679/2016 e, successivamente, con la sua effettiva applicazione (stabilita a far data dal 25 maggio 2018), s'è avvertita la necessità di riformare gli strumenti normativi interni e internazionali, per coordinarli con la nuova disciplina dell'UE.

Così, con il d.lgs. n. 108/2018 s'è avuta la riforma del codice in materia di protezione dei dati personali, dal quale sono stati espunti i riferimenti sia all'obbligo di esattezza e aggiornamento dei dati – in quanto previsti nel principio di esattezza di cui all'art. 5, par. 1, lett. e), del GDPR – sia all'obbligo di adozione di misure di sicurezza adeguate volte a garantire (anche) l'esattezza stessa dei dati personali oggetto di trattamento – perché già previsto nelle più articolate norme del GDPR, che impongono, su diversi livelli di operatività, l'adozione di adeguate misure tecniche e organizzative (cfr. artt. 24, 25 e 32 GDPR).

Sul versante internazionale, invece, l'applicazione del Reg. UE 679/2016, unitamente all'evoluzione sociale e tecnologica, ha portato il Consiglio d'Europa ad aggiornare anche la citata Convenzione n. 108 del 1981, con la previsione di un protocollo addizionale del 18 maggio 2018 (c.d. Convenzione 108+), che l'Italia ha provveduto a ratificare con l. 22 aprile 2021 n. 60. Il nuovo testo della Convenzione conserva sul punto una immutata previsione: all'attuale art. 5, par. 4, lett. d) della Convenzione 108+, così come nell'originario art. 5, par. 1, lett. d), della Convenzione 108 del 1981, si trova stabilito che «*Personal data undergoing processing shall be (...) accurate and, where necessary, kept up to date*». Cambia tuttavia il contesto in cui ora detto obbligo si inserisce, in quanto l'art. 5 viene ad essere arricchito di ulteriori paragrafi che trascendono il solo riferimento alla "qualità" dei dati, inserendo l'esattezza dentro un quadro normativo ben più vasto, in cui diviene evidente anche un più stretto collegamento con i principi di liceità, proporzionalità e finalità del trattamento¹².

¹² L'originario art. 5, rubricato «*Quality of data*», stabiliva che «*Personal data undergoing automatic processing shall be: a) obtained and processed fairly and lawfully; b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are stored; d) accurate and, where necessary, kept up to date; e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*». L'attuale art. 5 della Convenzione 108+, riscritto a seguito del protocollo modificativo del 2018, è ora rubricato «*Legitimacy of data processing and quality of data*» e in esso si trova ora stabilito che «*1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. 2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law. 3. Personal data undergoing processing shall be processed lawfully. 4. Personal data undergoing processing shall be: a) processed fairly and in a transparent manner; b) collected*

2. PORTATA DEL PRINCIPIO

2.1. Il principio di esattezza: un'ipotesi ricostruttiva

Il principio di esattezza – nonostante i limitati contributi che lo hanno interessato, che tendono perlopiù a porlo in endiadi con altri principi, trattandolo solo incidentalmente ed in maniera unicamente connessa all'analisi di taluni diritti dell'interessato – riveste, in realtà, un ruolo tutt'altro che marginale nell'alveo dei principi del trattamento dei dati personali, che rappresentano il «denominatore comune minimo di garanzia»¹³ posto alla base della normativa *privacy*. L'esiguità delle analisi dedicate a tale principio da parte degli studiosi è probabilmente dovuta alla presunta (ma forse, almeno in parte, fuorviante) semplicità, nonché al suo essere autoesplicativo: del resto, come ha affermato l'*Information Commissioner's Office* (ICO), «*it will usually be obvious whether personal data is accurate*»¹⁴.

Posto che i dati trattati devono essere “esatti” affinché il trattamento possa considerarsi lecito, e che il parametro dell'esattezza di un dato può variare in base al contesto¹⁵, ci si deve domandare, in mancanza di una puntuale definizione da parte del legislatore, quando tali dati rispettino il principio in esame. E questo, prendendo le mosse da una definizione che se ne può dare sul piano interpretativo, in via di prima approssimazione, quale principio che sancisce l'obbligo di assicurare la ragionevole precisione e correttezza dei dati, trattati in rapporto diacronico con la realtà e con riferimento al contesto in cui il trattamento dei dati si inserisce. Ne consegue che il principio di esattezza, nel guidare l'operato del titolare del trattamento, impone un obbligo di «fedeltà contenutistica»¹⁶ dei dati che vengono trattati così da garan-

for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; e) preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed».

¹³ Così G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., p. 9.

¹⁴ Così si esprime l'*Information Commissioner's Office* (ICO) – l'autorità di controllo britannica – in merito al principio di esattezza (*accuracy* per utilizzare il lemma anglosassone) in una *Guide to the GDPR*. La guida, riferita al principio in esame, è rinvenibile al seguente link: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>.

¹⁵ Sottolinea come un dato possa essere considerato «*entirely accurate and sufficient*» in un contesto e, invece, «*wholly incomplete and misleading*» in un altro A.R. MILLER, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, in *Mich. Law Rev.*, 1969, p. 1115.

¹⁶ In questi termini si esprime M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., p. 210 in cui l'A. paragona il principio di esattezza a quello di minimizzazione dei dati e sottolinea come da questi principi derivi il dovere del titolare, al fine di tutelare l'interessato, di controllare costantemente la «corrispondenza del contenuto dei dati in suo possesso alla realtà dagli stessi rappresentata».

tire, almeno tendenzialmente, il minimo livello di interferenze nella sfera giuridica dell'interessato.

A parere di chi scrive, pare potersi enucleare una triplice declinazione dell'esattezza: (a) da un lato, sotto il profilo oggettivo, il principio si riferisce al dato in sé, richiamando quindi la qualità e l'accuratezza del dato stesso; (b) dall'altro, in una declinazione soggettiva, si riferisce al compito incombente sul titolare del trattamento (sulla scorta del principio di *accountability*)¹⁷ di provvedere ad una puntuale verifica dei dati trattati, anche senza la necessità di una precipua richiesta da parte dell'interessato o dell'autorità Garante; (c) infine, in una declinazione funzionale, il principio di esattezza appare configurabile in chiave prodromica all'esercizio di alcuni diritti da parte dell'interessato tra i quali spiccano sicuramente il diritto di limitazione del trattamento *ex art. 18 GDPR* ed il diritto di rettifica *ex art. 16 GDPR*.

Con riguardo al primo aspetto tratteggiato (a), pare opportuno sottolineare che se è vero che, al pari di un dato errato, un dato parziale potrebbe considerarsi inesatto (rendendo così inesatto e quindi illecito il trattamento posto in essere), altrettanto vero è che il dato, laddove sovrabbondante, rischia di porsi in contrasto con quanto sancito all'art. 5, par. 1, lett. *b*) e *c*) del GDPR, in riferimento alla limitazione delle finalità e al principio di minimizzazione. Si dovrà, pertanto, ricercare il più corretto bilanciamento, caso per caso, tra la non eccedenza rispetto alle finalità (determinate, esplicite e legittime) del trattamento e la presenza di un livello sufficiente di completezza tale da permettere il raggiungimento di dette finalità.

Il secondo profilo (b) ha, invece, riguardo al soggetto che, con valutazioni rigorose, deve occuparsi del necessario bilanciamento emerso *sub* (a). Nel nuovo assetto delineato dal GDPR, ricade nella discrezionalità e sotto la responsabilità del titolare del trattamento l'obbligo, ai fini dell'esattezza dei dati, di assicurarsi di trattare dati esatti, che possiedano le caratteristiche della qualità e della completezza, adottando inoltre, eventualmente e in modo tempestivo, tutte le misure che appaiono ragionevoli per cancellare o rettificare i dati inesatti.

L'ultima direzione in cui sembra si muova ed in cui pare quindi potersi inquadrare il principio di esattezza (c) fa riferimento ai casi in cui l'interessato agisca nei confronti del titolare quando quest'ultimo abbia trattato dati inesatti. Il *data subject* potrà infatti richiedere la rettifica dei dati inesatti (o la loro integrazione laddove incompleti) come pure la cancellazione o la limitazione del trattamento. Si nota come in quest'ultima accezione l'(in)esattezza dei dati rappresenti la condizione (o una delle condizioni) affinché l'interessato possa esercitare un suo diritto riconosciuto dal Regolamento.

Il principio di esattezza, nella cui essenza è rinvenibile un'eco del criterio di verità dell'informazione, deve essere rigorosamente rispettato proprio per garantire una piena tutela alla persona cui i dati trattati si riferiscono. I dati personali, strettamente legati alla persona umana, concorrono a formarne l'identità virtuale ed il di-

¹⁷ Il principio di *accountability*, una delle innovazioni più significative del GDPR, rappresenta un vero e proprio cambio di paradigma in ambito *privacy*, sul tema si rinvia a G. FINOCCHIARO, *Il principio di accountability*, in *Giur. it.*, 2019, 12, pp. 2778 ss., nonché al capitolo dedicato al principio di *accountability*, nel presente volume.

ritto alla loro protezione risulta, sotto vari aspetti, «cangiante nel tempo»¹⁸. Le ripercussioni negative che l'interessato può subire nel caso in cui i suoi dati siano inesatti possono, del resto, essere soggette ad un esponenziale aggravio dovuto alla possibile combinazione con ulteriori informazioni anch'esse inesatte, unite alle prime e trattate ad un tempo, eventualmente, con l'ausilio dei moderni sistemi automatizzati¹⁹.

2.2. Il principio di esattezza come baluardo a difesa dei diritti e degli interessi dell'interessato

In questo quadro, emerge l'inscindibile legame che unisce il principio di esattezza con il diritto all'identità personale dell'interessato che deve essere garantito (anche e soprattutto) attraverso un rigoroso rispetto del principio in esame. Come già storicamente affermato dalla Corte di Cassazione, ogni individuo ha «interesse a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale»²⁰. Il diritto all'identità personale deve pertanto essere inteso come il «diritto di essere sé stessi»²¹, il diritto alla propria identità attraverso la quale la persona si rappresenta liberamente con i propri principi, le proprie idee e la propria storia. In altri termini, il diritto a non vedere travisato, offuscato o contestato ciò che il soggetto esprime e rappresenta.

È quindi la proiezione sociale di ogni soggetto – determinante appunto per la sua identità personale – ad essere minata a causa di una circolazione di dati inesatti. Seguendo l'incontrovertibile pensiero di autorevole dottrina, «il diritto all'identità personale comporta una corretta rappresentazione della personalità del soggetto. La

¹⁸ In questo senso G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 18.

¹⁹ Sul punto vedi E. NAVARRETTA, *Art. 11: Modalità del trattamento e requisiti dei dati*, in C. M. BIANCA-F. D. BUSNELLI (a cura di), *La protezione dei dati personali, Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, Padova, 2007, p. 268, in cui l'A. afferma: «il singolo dato (...) è come la tessera di un complesso mosaico, la cui costruzione, affidata alla mente dell'operatore e alle connessioni informatiche, può facilmente sfuggire allo specchio della realtà».

²⁰ Il riferimento è alla celebre pronuncia Cass., 22 giugno 1985, n. 3769, tra le altre in *Foro it.*, 1985, 1, cc. 2211 ss., relativa al c.d. caso Veronesi: il noto oncologo aveva rilasciato una intervista in cui spiegava il nesso tra il fumo ed alcuni tumori maligni, specificando che alcune sigarette "light" potevano avere ripercussioni meno severe, ma concludendo comunque affermando come «tutto sarebbe più semplice se la gente si convincesse a non fumare»; in seguito a ciò una società produttrice di tabacco iniziò a pubblicizzare i propri prodotti "light" affermando che secondo il prof. Veronesi tali sigarette riducevano sostanzialmente il rischio di cancro; detta sentenza era stata preceduta dall'altrettanto nota pronuncia Pret. Roma, 6 maggio 1974, tra le altre in *Giur. it.*, 1975, 1, 2, pp. 514 ss., con nota di D'ANGELO, relativa alla vicenda di un uomo ed una donna che avevano visto una loro immagine (prodotta in un contesto del tutto estraneo) essere utilizzata in un manifesto per la propaganda del Comitato nazionale per il referendum sul divorzio senza alcuna autorizzazione; su entrambe le pronunce, ed in generale sul percorso giurisprudenziale che ha consacrato il diritto all'identità personale cfr. V. ZENO ZENCOVICH, *Identità personale*, in *Dig. disc. priv.*, 1993, p. 294 ss., spec. pp. 297 ss.

²¹ Sul punto v. G. ALPA, *Il diritto di essere se stessi*, Milano, 2021; in questi termini già Corte cost., 3 febbraio 1994, n. 13, tra le altre in *Giust. civ.*, 1994, 1, p. 2435 che parla dell'identità personale come «diritto ad essere sé stesso».

mancata o infedele rappresentazione integra una lesione del diritto»²², e ciò a prescindere dal fatto che la falsa rappresentazione del soggetto implichi una connotazione “in negativo”, dal momento che la semplice inesattezza in sé causa una lesione del diritto.

Il diritto all'identità personale quale prisma di elementi che compongono l'io di un determinato individuo, inteso come autonomo diritto della personalità «trovato»²³ dal diritto oggettivo e tutelato dalla clausola a fattispecie aperta di cui all'art. 2 Cost.²⁴, pare richiedere, in concreto ai fini della sua tutela, un comportamento attivo del titolare del trattamento che deve assicurarsi di trattare dati esatti e rispondere celermente ad eventuali segnalazioni da parte dell'interessato, proprio per non travisare la proiezione sociale della persona i cui dati vengono trattati.

Tale diritto esplica la sua importanza in forza della sua natura relazionale: i terzi in buona fede che si rapportano con il soggetto titolare del diritto devono considerarlo come è o come, anche idealmente, ritiene di essere. Ogni persona deve quindi potersi presentare all'esterno nel rispetto della identità (o delle identità) con cui ha deciso di mostrarsi, indossando anche, magari, diverse “maschere” in diversi contesti ed assumendo così differenti identità, come del resto ci suggerisce anche l'etimologia greca del termine “persona”, *pròsopon*, il cui significato è anche (e primariamente) quello di “maschera”.

Proprio la massiccia circolazione dei dati in rete, nuovo scenario dell'agire umano e nuovo contesto in cui l'individuo sviluppa la sua personalità, rischia di danneggiare la persona nella più vulnerabile delle sue proiezioni, quella digitale²⁵ nel caso in cui non si prevedano misure idonee a garantire l'esattezza delle informazioni in tutte le loro vicende circolatorie. L'identità digitale è particolarmente esposta proprio perché relativa all'esplicazione della persona su Internet dove, come è noto, è assai arduo eliminare determinate informazioni una volta diffuse, nonostante il tempo le abbia, eventualmente, rese non più attuali e non corrispondenti all'identità aggiornata del soggetto cui si riferiscono.

Il tempo gioca, infatti, un ruolo cruciale per l'identità personale di ognuno, destinata, appunto, a mutare senza rimanere staticamente relegata ad un preciso momento storico²⁶. L'esattezza del dato è strettamente collegata alla sua attualità e contestualizzazione: un dato non attuale non potrà certo essere considerato esatto.

²² Così G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Dig. disc. priv. agg.*, 2010, p. 726; analogamente F. GALGANO, *Trattato di Diritto civile*, vol. I, Padova, 2015, pp. 191 s. afferma: «il diritto all'identità personale è lesa anche se le azioni o convinzioni attribuite al soggetto non sono di per sé disonorevoli e lesive della sua reputazione».

²³ La fortunata espressione è di F. GALGANO, *Trattato di Diritto civile, supra cit.*, p. 171 in cui l'Autore sostiene che vi siano «diritti soggettivi che si dicono ‘trovati’ dal diritto oggettivo: sono i diritti dell'uomo, che si considerano esistenti indipendentemente da ogni norma giuridica che li riconosca e che il diritto oggettivo si limita a garantire».

²⁴ Sull'art. 2 Cost. quale norma a fattispecie aperta cfr. A. BARBERA, *Commento all'art. 2 Cost.*, in G. BRANCA (a cura di), *Commentario alla Costituzione italiana*, Bologna, 1975, spec. pp. 96 ss.

²⁵ In questo senso M. TAMPIERI, *L'identità personale: il nostro documento esistenziale*, in *Eur. dir. priv.*, 2019, 4, p. 1223.

²⁶ Sul punto v. G. ALPA, *Il diritto di essere se stessi*, cit., p. 229 in cui l'Autore sottolinea «l'evoluzione della personalità nel corso del tempo, e il graduale mutamento dell'immagine e dell'identità

Se in passato, la società si preoccupava di preservare la propria storia, la propria memoria e le proprie informazioni attraverso la scrittura o la diffusione orale di notizie, oggi la situazione appare ribaltata, dal momento che lo sviluppo tecnologico, e soprattutto l'avvento di Internet, ha reso sempre più difficile dimenticare, obbligando, spesso anche contro la volontà degli interessati, al ricordo. Tra le problematiche che emergono nella c.d. società dell'informazione è sicuramente presente quella relativa alla contestualizzazione delle informazioni: il terreno dal quale è sorto il diritto all'oblio.

Senza volere, in questa sede, analizzare il diritto all'oblio nella sua evoluzione legislativa (si ricorda che solo con il GDPR il diritto all'oblio ha conosciuto una puntuale previsione all'art. 17) e nel dibattito dottrinale e giurisprudenziale, incentrato sul difficile bilanciamento tra diritto di informazione e di cronaca da un lato e diritto alla protezione dei dati personali e alla riservatezza dall'altro, basti sottolineare come tale diritto risulti di primaria importanza affinché l'identità personale dell'interessato, nel costante divenire che la caratterizza, sia fedelmente rappresentata all'esterno. Si fa quindi riferimento al rapporto tra fatti che, seppur realmente accaduti e lecitamente diffusi nella loro esattezza, devono essere relegati nel passato di un soggetto e avvenimenti più recenti che hanno alterato la situazione pregressa. Il diritto all'oblio non rappresenta, in realtà, un nuovo diritto della personalità: si tratta infatti di un diritto funzionale e strumentale alla realizzazione e all'esercizio di altri consolidati diritti, quali il diritto all'identità personale e quello alla protezione dei dati personali²⁷. Esso permette quindi di evitare che l'identità di un soggetto venga travisata ed opera, per così dire, in concerto con il principio di esattezza affinché l'identità personale dell'interessato venga tutelata da un punto di vista diacronico, nei mutamenti che la riguardano.

Il principio di esattezza, relativo ai dati pubblicati in rete, anche in rapporto al diritto all'oblio, non pare però potersi spingere al di là di quello che può essere ragionevolmente richiesto ai gestori degli archivi *online*, nei quali le notizie (esatte al momento della pubblicazione) sono contenute. Posto infatti che le informazioni devono certamente rispettare, tra gli altri, il principio di esattezza ed essere aggiornate nel momento in cui vengono immesse in rete, l'esigenza di un costante aggiornamento di tali informazioni (per la tutela dell'identità dell'interessato) deve essere proporzionalmente bilanciata con i costi e gli sforzi ragionevolmente richiedibili ai gestori degli archivi. A differenza di quanto sembrava affermare la Corte di Cassazione²⁸,

“ideale” di ogni persona»; ID., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impr.*, 2017, 3, pp. 723 ss.; e G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. inf.*, 2012, 3, spec. p. 389 in cui l'Autrice afferma: «la persona è ciò che è in un determinato momento storico e l'identità muta col tempo. Divengono essenziali la storicizzazione e la contestualizzazione. Eventi occorsi in una certa epoca possono non corrispondere più alla personalità di un soggetto in un diverso momento storico»; ID., *Identità personale (diritto alla)*, cit., spec. p. 735.

²⁷ In questo senso, cfr. G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf.*, 2014, 4-5, pp. 600 ss.

²⁸ Cass., 5 aprile 2012, n. 5255, tra le altre in *Resp. civ. e prev.*, 2012, 4, pp. 1147 ss.; e sulla quale vedi la ricostruzione operata da G. ALPA, *Il diritto di essere se stessi*, cit., pp. 233 ss.

non pare potersi richiedere al gestore di un archivio *online* un costante impegno di ricerca, indirizzato a qualsivoglia ulteriore informazione che rappresenti un aggiornamento di notizie pubblicate precedentemente, al fine di attualizzarle e contestualizzarle così da renderle aderenti alla attuale identità del soggetto interessato²⁹. Non sembra, infatti, che si possa chiamare a rispondere un soggetto che, una volta pubblicata una notizia, non vi abbia successivamente (ricercato e) inserito il riferimento ad eventuali fatti sopravvenuti che abbiano reso la notizia a monte non più attuale. Va da sé che laddove l'interessato richiedesse l'aggiornamento o la cancellazione di una determinata notizia perché non più attuale e lesiva della sua identità, nonché priva di un pubblico interesse, il titolare dell'archivio dovrà, previa valutazione della fondatezza dell'istanza ricevuta, impegnarsi in tal senso. Analogamente, nel caso in cui si intendano pubblicare ulteriori informazioni sulla medesima vicenda, mutata nel tempo, o, più semplicemente ripubblicare la questione in sé (anche se, in realtà, nel mondo digitale è difficile parlare di una vera e propria "ripubblicazione" dato che, come si è detto, la rete difficilmente dimentica)³⁰, ci si dovrà adoperare affinché le notizie siano esatte e quindi, certamente, attuali e contestualizzate. Richiederebbe parimenti un intervento del gestore dell'archivio il caso in cui lui stesso si accorgesse di un'inesattezza a monte della notizia pubblicata: si tratterebbe però in questo

²⁹ Diverse sono state le voci critiche con riferimento ad un simile obbligo imposto sui gestori di archivi *online*, cfr. F. DI CIOMMO-R. PARDOLESI, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!*, in *Danno e resp.*, 2012, 7, pp. 701 ss., e spec. a p. 704 s. in cui gli Autori affermano che una simile soluzione non terrebbe in considerazione «i notevoli costi che la gestione di un sistema del genere richiederebbe, oltre che le oggettive difficoltà tecniche di realizzazione di una banca dati che, dunque, deve essere costantemente aggiornata e si deve alimentare di notizie che non è nemmeno detto siano inserite nel circuito informativo in cui "pesca" il suo gestore», aggiungendo che «il problema è di carattere più generale. Pensare che ognuno debba, a pena di responsabilità civile ed eventualmente penale, organizzare i propri archivi *on-line* in modo tale da renderli sempre aggiornati all'attualità vuol dire, per un verso, postulare una missione davvero impossibile, per l'altro trascurare la realtà della rete Internet»; M. BELLANTE, *Diritto all'identità personale e obbligo di aggiornamento degli archivi storici di testate giornalistiche*, in *Giur. it.*, 2013, 5, pp. 1073 ss.; G. CITARELLA, *Aggiornamento degli archivi online tra diritto all'oblio e rettifica «atipica»*, in *Resp. civ. e prev.*, 2012, 4, pp. 1155 ss., spec. p. 1159 in cui, secondo l'A. «garantire il rispetto dell'identità personale negli archivi *on-line* aperti al pubblico dei quotidiani, apportando aggiornamenti che scolorano nella rettifica, fino al limite della cancellazione e quindi dell'oblio, finisce per imporre agli editori una serie di problemi realmente insormontabili, e prima ancora comporta rilevanti conseguenze giuridico/sistematiche»; C. SCARPELLINO, *Contorsionismi del diritto all'oblio e criticità degli archivi on line*, in *Danno e resp.*, 2020, 3, pp. 405 ss. la quale, pur commentando la decisione del Trib. Venezia, 26 settembre 2019, richiama criticamente la citata pronuncia della Corte di Cassazione; *contra* A. DI MAJO, *Il tempo siamo noi...*, in *Corr. giur.*, 2012, 6, pp. 769 ss., spec. p. 771 secondo cui «non sembra infatti fondato né convincente distinguere le due operazioni (pubblicazione della notizia e sua permanenza nell'archivio) (...). Va ribadito ancora una volta che la collocazione in un sito, destinato alla memoria storica, non può costituire impedimento acché la memoria da esso custodita, e a cui si accede via internet, subisca tutti i limiti e condizioni che incontra il "trattamento" dei dati personali, (...). Ancora una volta si viene a sezionare artificialmente un fenomeno che è unitario e la cui sezionabilità non può costituire una cortina fumogena, tale da far dimenticare che l'elemento da salvaguardare è pur sempre il diritto della persona acché il governo dei suoi "dati" corrisponda ai valori ad essa immanenti».

³⁰ Sull'argomento, cfr. G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, cit., pp. 391 s.

caso di un'azione richiesta al titolare non per un aggiornamento, ma per correggere l'informazione primigenia, sulla base dell'obbligo legale inscritto nel principio di esattezza, rafforzato dall'operatività del principio di *accountability*.

Se infatti da un lato, una informazione completa e vera in origine, successivamente non aggiornata, diviene «parziale e non esatta, e pertanto sostanzialmente non vera»³¹, dall'altro non si può richiedere a colui che ha pubblicato tale informazione o a chi gestisce l'archivio in cui tale notizia è conservata, uno sforzo che, se non impossibile, appare di sicuro eccessivamente oneroso. I costi che deriverebbero da un obbligo di aggiornamento imposto *tout court*, ai fini del rispetto del principio di esattezza, in capo a chi pone a disposizione degli utenti uno strumento conoscitivo, verrebbero poi riallocati sugli utenti stessi.

A quanto detto, si aggiunga che il principio di esattezza presenta importanti ricadute anche su interessi e diritti ulteriori rispetto a quello all'identità personale.

Si pensi, ad esempio, ai dati contenuti all'interno delle cartelle cliniche: se tali dati fossero inesatti, il personale medico dedito alla cura del paziente-interessato non si ritroverebbe nelle condizioni di porre in essere le terapie corrette ed adeguate alla cura di cui il soggetto è bisognoso. Emergerebbe, in una simile fattispecie, un rischio per il diritto alla salute, finanche per la vita della persona.

Già nel 2015, il Garante per la protezione dei dati personali aveva pubblicato delle Linee guida relative ai *dossier* sanitari³². L'autorità Garante, pienamente consapevole della delicatezza dei dati sanitari, muove dall'esigenza di garantirne l'esattezza, l'integrità e la disponibilità. Nel settore in questione, del resto, oltre ai profili di responsabilità inerenti alla protezione dei dati personali, assumono rilievo gli aspetti relativi alla responsabilità deontologica e professionale. È quindi senz'altro presente un dovere, particolarmente incisivo data l'assolutezza dei diritti della persona che si rischia di ledere, in capo al titolare del trattamento: quello di garantire l'esattezza e l'aggiornamento dei dati sanitari, adottando ogni misura idonea a ridurre il rischio di cancellazione, manipolazione o estrapolazione dei dati.

L'esattezza del dato non rileva però unicamente nell'ambito dei diritti fondamentali della persona, ma anche con riguardo a diritti e interessi patrimoniali dell'interessato. Mi riferisco in particolar modo ai dati relativi ai conti correnti, alle movimentazioni bancarie e, più in generale, ai rapporti sussistenti tra gli istituti bancari e la clientela, anch'essi oggetto di Linee guida del Garante per la protezione dei dati personali³³. Così, nell'esecuzione di ordini di pagamento, spetterà alla banca del debitore-interessato verificare l'esattezza dei dati trattati relativi alle coordinate bancarie e al conto corrente, mettendo in atto, in caso di dubbio, incongruenza o discordanza, adeguati controlli preventivi, contattando direttamente il cliente prima di eseguire un pagamento (eventualmente non dovuto) a carico dell'interessato.

Si aggiunga poi la rilevanza rivestita dal principio di esattezza con riferimento ai dati immessi nei sistemi di autenticazione biometrici, finalizzati all'accesso a

³¹ Così Cass., 5 aprile 2012, n. 5255, cit.

³² GPDP, Provv. 4 giugno 2015, doc. *web* n. 4091542; in argomento, di recente, cfr. GPDP, Provv. 15 dicembre 2022, doc. *web* n. 9870788.

³³ GPDP, Provv. 25 ottobre 2007, doc. *web* n. 1457247.

dispositivi, sistemi informatici, locali o ambienti fisici e così via. Tali sistemi che si basano sull'intelligenza artificiale si nutrono, per loro natura, di dati e tali dati devono essere esatti. L'importanza di immettere dati esatti in tali sistemi è finalizzata a contenere il più possibile l'indice FAR (*False Acceptance Rate*) con cui si misura la frequenza con la quale viene permesso un accesso non autorizzato; l'indice FRR (*False Rejection Rate*) con cui si misura la frequenza con la quale il sistema autorizza utenti il cui accesso non doveva, invece, essere autorizzato; e l'indice FIR (*False Identification Rate*) con cui si misura la frequenza con la quale il sistema riconosce l'utente, ma lo associa ad un'altra identità. Se solo idealmente tali indici possono essere pari a zero, in presenza di un sistema biometrico sostanzialmente perfetto, nella realtà, risulta comunque fondamentale diminuirli massimamente e, sul punto, l'esattezza dei dati alla base del sistema gioca un ruolo fondamentale.

Si aggiunga che, a maggior ragione alla luce delle concorrenti istanze di tutela poste alla base del GDPR, l'esattezza dei dati assume rilievo non solo ai fini della tutela della persona dell'interessato, dei suoi diritti ed interessi, ma anche per garantire un corretto funzionamento del mercato dei dati nel suo insieme³⁴.

2.3. Il principio di esattezza tra obblighi e interesse del titolare

Nonostante si tratti di un principio dalle origini ormai risalenti, le cui radici affondano nella Risoluzione (73) 22 del Consiglio d'Europa³⁵, è proprio nel contesto attuale, caratterizzato da un ampio utilizzo delle nuove tecnologie, capaci di permettere (o, talvolta, causare) una massima diffusione delle informazioni nella rete, che l'esattezza dei dati assume a principio fondamentale della *data protection law*.

Si deve infatti ribadire che i recenti sviluppi della tecnologia presentano un margine di rischio particolarmente più elevato nel caso in cui i dati siano inesatti: la raccolta massiva di dati porta, infatti, a profili minuziosamente dettagliati, ma non sempre in linea con il principio di esattezza (oltre che con gli altri principi contenuti nel GDPR). Sebbene l'infinita mole di dati che i moderni sistemi permettono di raccogliere e trattare non rappresenti nemmeno un costo di particolare rilievo per i

³⁴ In questo senso, cfr. N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in ID. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 92 in cui l'Autrice afferma che: «è evidente, a titolo indicativo, che se i dati di carattere personale sono inesatti, non è lesa solo il diritto della persona fisica a cui i dati si riferiscono, ma anche il corrispondente mercato risulta falsato».

³⁵ Si ricorda che il principio di esattezza veniva già menzionato dal *Council of Europe* nella *Resolution (73) 22 On the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies*, nella quale, all'art. 1, si legge «*the information stored should be accurate e and should be kept up to date*». L'importanza di mantenere una buona qualità dei dati, dato l'elevato rischio di danno presente nel trattamento dei dati personali viene anche sottolineato nell'*explanatory report* della Risoluzione. Di un solo anno successivo è il *Privacy Act of 1974* degli Stati Uniti in cui si rinviengono vari riferimenti all'*accuracy* dei dati; con riferimento a questa ultima fonte normativa e alle radici americane del principio di qualità dei dati v. T. HOEREN, *Big Data and Data Quality*, in ID., B. KOLANY-RAISER (a cura di), *Big Data in Context. Legal, Social and Technological Insights*, Cham, 2018, pp. 3 ss.

titolari³⁶, allo stato dell'arte, sorgono spesso problemi relativi alla (mancata) analisi e verifica dei dati raccolti che si traduce poi in ricadute qualitative sul trattamento effettuato. In altri termini, nonostante la quantità di dati disponibile sia attualmente sconfinata (anzi, forse proprio anche per questa ragione), tali dati necessitano di un adeguato processo di *data mining* e di una puntuale analisi, al fine di evitare distorsioni. Si pensi, ad esempio, alle *fake news*, a dati relativi ad insolvenze per crediti contestati che possono incidere sulla qualificazione di un soggetto come cattivo pagatore³⁷, come pure alla gestione dei profili reputazionali³⁸, in grado di determinare importanti pregiudizi sui diritti fondamentali dell'interessato e, in generale, incidere negativamente sulla sua sfera giuridica da un punto di vista sociale, lavorativo, etc.

Nell'odierna società, calata nel contesto della c.d. *data driven economy*, in cui sempre più spesso i dati personali, come è noto definiti il "nuovo petrolio", assumono un ruolo preminente nel contesto delle imprese che ne sfruttano sempre più sapientemente le potenzialità, il principio di esattezza esplica la sua centralità.

A livello europeo, è ormai chiaro il potenziale economico che lo sfruttamento dei dati personali racchiude ed anzi, tende ad essere sempre più incentivato, come dimostra, tra le altre, la Comunicazione della Commissione europea, intitolata «Strategia europea per i dati»³⁹. Il valore economico dei dati personali ed il loro utilizzo nel mondo degli affari non devono indurre a sgretolare la «convinzione che l'essere umano sia e debba rimanere l'elemento centrale»⁴⁰: non pare infatti corretto qualificare i dati personali come «"beni giuridici" in senso tecnico, quale "merce" che forma oggetto di commercializzazione, rimanendo pur sempre attributi della personalità, sui quali è possibile l'esercizio di diritti, anche nel senso di un uso di carattere patrimoniale»⁴¹. Proprio in questa direzione, il principio di esattezza rappresenta una

³⁶ Cfr., J. CHEN, *The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle*, in *Eur. Data Prot. Law Rev.*, 2018, 1, p. 40.

³⁷ F. BRAVO, *I sistemi privati di informazione creditizia*, in G. CONTE (diretto da), *Arbitrato Bancario e Finanziario*, Milano, 2021, pp. 229 ss.

³⁸ Con particolare riguardo ai sistemi che si offrono di elaborare i profili reputazionali di persone fisiche e giuridiche in modo da arrivare ad un vero e proprio *rating*, cfr. Cass. ord., 25 maggio 2021, n. 14381, in *Dir. inform.*, 2021, 6, pp. 1001 ss., sulla quale cfr. il commento di F. BRAVO, *Rating reputazionale e trasparenza dell'algoritmo. Il caso «Mevaluate»*, *ivi*, pp. 1005 ss.; per la ricostruzione della vicenda cfr. GDP, Prov. 24 novembre 2016, doc web n. 5796783; e successivamente l'impugnazione cui è seguita la pronuncia Trib. Roma, 4 aprile 2018, in *Dir. inform.*, 2019, 2, pp. 520 ss., con nota di G. GIANNONE CODIGLIONE.

³⁹ COMMISSIONE EUROPEA, *Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Una strategia europea dei dati*, Bruxelles, 19 febbraio 2020, COM (2020) 66 final.

⁴⁰ *Idem*, p. 5.

⁴¹ Così, condivisibilmente, F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impr. Eur.*, 2021, 1, p. 14; in giurisprudenza sul tema v. Tar Lazio, 10 gennaio 2020, nn. 260 e 261 e le serrate critiche avanzate da F. BRAVO, *La «compravendita» di dati personali?*, in *Dir. Internet*, 2020, 3, pp. 521 ss.; nonché Cass., 2 luglio 2018, n. 17278, tra le altre in *Giur. it.*, 2019, 3, pp. 530 ss., con nota di S. THOBANI, i cui risvolti vengono ampiamente affrontati da F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impr.*, 2019, 1, pp. 34 ss.; e su cui sia anche consentito il rinvio a C. BASUNTI, *La (perduta) centralità del*

condizione affinché il titolare ne possa sfruttare al meglio il potenziale economico e, al contempo, un presidio che permette all'interessato di tutelarsi da rappresentazioni distorte della sua personalità e da altri pregiudizi anche di carattere patrimoniale.

Il dato, per acquisire importanza per il titolare e per essere quindi da lui utilizzato in chiave economica, deve essere necessario e finalizzato allo scopo da perseguire, come pure esatto e pertanto capace di fornire all'impresa tutte quelle informazioni utili ad instaurare una relazione *lato sensu* "personalizzata" tra impresa/titolare e soggetto interessato, quale possibile cliente. Si deve infatti tener ben presente che non è (solo) la quantità di dati che una impresa possiede e tratta, ma (anche e soprattutto) la loro qualità ed esattezza a rendere tali dati un *asset* strategico per operare sul mercato.

Il titolare del trattamento ha, pertanto, un assoluto interesse a trattare dati esatti, specialmente nell'ambito della profilazione dei soggetti (utilizzata prevalentemente per finalità di *marketing* che mirano a creare proposte commerciali mirate sui singoli consumatori). Tale interesse deve però rapportarsi, da un lato, con la pleora di dati disponibile al giorno d'oggi che caratterizza l'era dei *Big Data* (e quindi con la difficoltà di "estrarre" dati esatti) e, dall'altro, con l'eventualità che un soggetto fornisca (consapevolmente o inconsapevolmente) dati inesatti. Sotto quest'ultimo aspetto, oltre all'evidente contrasto con i principi di correttezza e buona fede relativi alla "cessione" (di un consenso al trattamento) di dati inesatti, si deve sottolineare come il titolare del trattamento, una volta scoperta l'inesattezza dei dati in questione sia tenuto ad intervenire, rettificandoli o cancellandoli. Il titolare non può, infatti, essere chiamato a trattare (consapevolmente) dati inesatti, essendo tenuto al rispetto dei principi di esattezza e *accountability*. Egli risulterebbe, quindi, responsabile nel caso in cui trattasse dati che ha riconosciuto essere inesatti, anche laddove lo facesse in seguito ad una specifica richiesta dell'interessato in tal senso. L'interessato potrà, tutt'al più revocare il consenso prestato (art. 7, par. 3 GDPR) ed il titolare dovrà interrompere ogni operazione di trattamento (senza pregiudizio per le operazioni effettuate prima della revoca), sempre che non sussista una condizione di liceità alternativa al consenso, e quindi non basata sulla volontà dell'interessato, su cui fondare il trattamento.

Il principio di esattezza rappresenta un obbligo che il titolare è tenuto a rispettare e che supera l'eventuale interesse del *data subject* al trattamento di dati inesatti sul suo conto perché a lui più congeniali. Una differente impostazione condurrebbe del resto ad inaccettabili ricadute di sistema: in tema di solvibilità del debitore; in materia fiscale; in ambito giudiziario; in materia assicurativa; con riguardo alle banche dati per la valutazione del merito creditizio⁴²; con riferimento all'obbligo

consenso nello specchio delle condizioni di liceità del trattamento dei dati personali, in *Contratto e impr.*, 2020, 2, spec. pp. 886 ss.

⁴² In argomento cfr. F. BRAVO, *I sistemi privati di informazione creditizia*, cit., pp. 229 ss.; F. BRAVO, *La centrale di allarme interbancaria (CAI) e la centrale dei rischi (CR)*, in G. CONTE (diretto da), *Arbitrato Bancario e Finanziario*, cit., pp. 265 ss.; R. DI RAIMO, *Accesso al credito e valutazione del merito creditizio*, in G. CONTE (diretto da), *Arbitrato Bancario e Finanziario*, cit., pp. 211 ss.; A.A. DOLMETTA, *Disciplina di trasparenza e principio di trasparenza*, in G. CONTE (diretto da), *Arbitrato Bancario e Finanziario*, cit., pp. 193 ss.

di verità oggettiva che, nel diritto di cronaca si somma al dovere di utilità sociale dell'informazione e contenenza dell'esposizione dei fatti⁴³ e così via.

Al fine di evitare pericolose derive soggettivistiche del trattamento dei dati personali, risulta di massima importanza che il titolare del trattamento operi nel pieno rispetto del principio di esattezza (rafforzato da quelli di *accountability* e correttezza) per essere *compliant* con la normativa *privacy* e per raggiungere più efficacemente le proprie finalità di natura (anche) economica.

2.4. L'esattezza dei dati nell'ambito dei diritti dell'interessato previsti dal GDPR

Il principio di esattezza, *rectius*, il mancato rispetto di tale principio è, per l'interessato, il fondamento che consente l'esercizio di taluni diritti riconosciutigli dal Regolamento, e precisamente l'inesattezza del dato viene richiamata all'art. 16 GDPR sul diritto di rettifica; la contestazione dell'esattezza del dato si rinviene all'art. 18 GDPR inerente al diritto di limitazione di trattamento; e rileva inoltre nell'art. 17 GDPR sul diritto alla cancellazione (o all'oblio). Si tratta di diritti definibili come "dinamici", in quanto permettono all'interessato di intervenire sul trattamento posto in essere⁴⁴. Tale dinamicità, propria della tutela, è necessaria per salvaguardare, come si è detto, i diritti fondamentali della persona come il diritto all'identità personale (diritto altrettanto dinamico che richiede una fedele rappresentazione del soggetto all'esterno e la correzione di eventuali rappresentazioni distorte)⁴⁵ o il diritto alla salute (si pensi al menzionato tema della gestione dei dati contenuti nelle cartelle cliniche), ma anche diritti di carattere patrimoniale (come ad esempio quelli inerenti alla correttezza delle operazioni bancarie ed ai conti correnti).

Precisamente, l'art. 16 del Regolamento sancisce il diritto dell'interessato di «ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo» (tale diritto alla rettifica si rinviene anche all'art. 8, par. 2, della Carta di Nizza) nonché «il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa».

Proprio tale diritto all'integrazione rappresenta una novità del Regolamento rispetto alla normativa previgente dal momento che la direttiva 95/46/CE prevedeva

⁴³ Sul punto il riferimento è alla nota decisione della Cass., 18 ottobre 1984, n. 5259, tra le altre in *Giur. it.*, 1985, 1, pp. 1099 ss. che contiene una sorta di decalogo per il giornalista nell'esercizio del diritto di cronaca; sul tema cfr. per tutti M. FRANZONI, *Dalla colpa grave alla responsabilità professionale*, Torino, 2017, pp. 175 ss.

⁴⁴ Cfr. F. CALISAI, *I diritti dell'interessato*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 344.

⁴⁵ Cfr. A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Nuove leggi civ. comm.*, 2019, 3, p. 593 che afferma: «si potrebbe, semplificando, affermare che i diritti dell'interessato consentono alla persona di invocare una più generale pretesa all'esatta rivelazione della propria identità» e sottolinea come «attraverso il riconoscimento dei diritti dell'interessato si dà attuazione ai principi di base che ispirano la disciplina in materia di trattamento dei dati personali, così da poter conformare le attività poste in essere ai diritti e alle libertà fondamentali della persona».

semplicemente giusta l'art. 12, lett. *b*), il diritto alla rettifica, alla cancellazione o al congelamento dei dati nei casi di incompletezza o inesattezza dei dati, senza appunto menzionare (almeno esplicitamente) alcuna possibilità di integrazione⁴⁶.

Il diritto di rettifica è esercitabile dall'interessato nei confronti del titolare – che si potrà poi, eventualmente, avvalere di responsabili o altri soggetti – in modo gratuito, ma, nel caso in cui la richiesta sia manifestamente infondata o eccessiva, in particolare per la ripetitività della stessa, il titolare potrà addebitare all'interessato un ragionevole contributo per le spese di carattere amministrativo e finanche rifiutare la richiesta (art. 12, par. 5, GDPR). Inoltre, l'inadempimento del titolare è soggetto ad una sanzione fino a venti milioni di euro e, per le imprese, fino al 4% del fatturato annuo dell'esercizio precedente laddove superiore [art. 83, par. 5, lett. *b*), GDPR].

La rettifica riguarda, si è detto, dati inesatti, ma l'inesattezza deve far riferimento, come ha indicato l'*European Data Protection Supervisor* (EDPS), a dati oggettivi e fattuali, non a giudizi e valutazioni di carattere soggettivo che, ontologicamente, non possono essere fattualmente inesatte⁴⁷. L'EDPS ha anche provveduto a tipizzare determinate fattispecie particolarmente significative per il diritto di rettifica (selezioni per assunzioni di personale, procedure di valutazione, dati di carattere medico-sanitario, procedure amministrative e disciplinari, *blacklisting* e *asset freezing*), indicando i limiti e le modalità di esercizio del diritto⁴⁸.

Pare corretto evidenziare come il diritto di rettifica e aggiornamento rappresenti per l'interessato una mera libertà e non un obbligo, come invece è per il titolare

⁴⁶ Dà conto di questa innovazione A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, p. 403 in cui l'A. sottolinea che, in effetti, «l'integrazione poteva, vigente la Direttiva, considerarsi implicita nel diritto alla rettifica, il cui esercizio di fatto si traduce in un intervento sui dati, giustificato dalla perdita di attualità dei dati medesimi, e finalizzato a colmare l'inesattezza che, in generale, si manifesta in un'assenza di qualità dell'informazione».

⁴⁷ Cfr. EDPS, *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data*, del 25 febbraio 2014, p. 18; v. anche sul punto GRUPPO DI LAVORO EX ART. 29, *Guidelines on the implementation of the Court of Justice of the European Union judgment on the "Google Spain and Inc. v. Agencia Española de protección de datos (AEPD) and Mario Costeja González" C-131/12*, p. 15. Sull'applicabilità del principio di accuratezza alle opinioni cfr. D. HALLINAN-F. ZUIDERVEEN BORGESIU, *Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle*, in *Int. Data Privacy Law*, 2020, 1, pp. 1 ss.

⁴⁸ Cfr. EDPS, *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data*, *supra cit.*, pp. 19-20 in cui, precisamente, con riferimento alle procedure di assunzione del personale, si sottolinea che una volta spirati i termini per l'invio delle domande, il diritto di rettifica è limitato ai soli dati inerenti ai criteri di ammissibilità (limitazione necessaria per la correttezza della procedura); con riferimento alle procedure di valutazione, si afferma che non possono essere sottoposte a rettifica le valutazioni soggettive fatte da un superiore in un *report* di valutazione, laddove ogni altro dato oggettivo e fattuale (come il nome) può essere rettificato; con riferimento ai dati di carattere medico-sanitario, stante la difficoltà di valutare esattezza e correttezza di tali dati, il diritto di rettificarli è in un certo qual modo limitato: si riconosce pertanto all'interessato il diritto di integrare la documentazione aggiungendo ulteriori opinioni mediche; con riferimento alle procedure amministrative, viene data all'interessato la possibilità di aggiungere suoi commenti al fascicolo disciplinare per assicurarne la completezza; con riferimento ai meccanismi di *blacklisting*, si sottolinea come il diritto alla rettifica abbia un'importanza chiave per garantire la qualità dei dati trattati, connessi al diritto di difesa.

del trattamento sia qualora gli venga richiesto dall'interessato sia qualora si renda conto lui stesso del difetto di esattezza del dato. Il titolare ha infatti un obbligo legale di intervento (che appunto discende dal principio in esame unito a quello di *accountability*) laddove si accorga che i dati da lui trattati siano inesatti, e questo anche senza preventiva richiesta dell'interessato come pure contro la sua eventuale volontà contraria, nei modi e nei termini che *supra* si sono tratteggiati. Il diritto in questione, solo da parte del *data subject* e solo entro determinati limiti, può quindi essere inteso quale «scelta soggettiva»⁴⁹ di cui egli può avvalersi durante il trattamento.

Si aggiunga che devono, comunque, essere sempre fatti salvi i doveri di correttezza e buona fede. Il rapporto tra titolare ed interessato non pare, infatti, poter prescindere dai principi generali di buona fede e correttezza – disciplinato, quest'ultimo, anche nel GDPR *ex art.* 5, par. 1, lett. *a)* – che rafforzano senza dubbio il principio di esattezza che non può certo essere interpretato in maniera unidirezionale, ossia valevole per il titolare nei confronti dell'interessato e non viceversa. In altri termini, la correttezza e la buona fede, così come codificate, tra gli altri, nel nostro codice civile, permeano l'intero diritto delle obbligazioni e dei contratti, ed incidono e governano anche l'agire sia del titolare sia dell'interessato.

Come si è accennato, il principio di esattezza rileva anche nell'ambito dell'art. 18 del Regolamento che, innovando rispetto alle previgenti fonti normative dell'ambito *privacy*, sancisce il diritto dell'interessato di ottenere dal titolare la limitazione del trattamento al ricorrere di una serie di ipotesi tassative⁵⁰ tra le quali figura, alla lett. *a)*, quella in cui l'interessato contesti l'esattezza dei dati personali. In tale fattispecie la limitazione dovrà essere concessa per il periodo di tempo necessario al titolare per operare una verifica in merito all'esattezza dei dati.

Il secondo paragrafo della norma, nel disporre che in caso di limitazione del trattamento, i dati siano trattati unicamente per la loro conservazione richiama la definizione che l'art. 4, par. 1, n. 3), fornisce di limitazione quale «contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro». I dati, infatti, non vengono cancellati, ma conservati dal titolare per un determinato lasso temporale; potranno essere trattati solo fondando il trattamento sul consenso dell'interessato o, senza necessità di consenso, ai fini di accertamento, esercizio o difesa di un diritto in sede giudiziaria o anche al fine di tutelare i diritti di un'altra persona fisica o giuridica, o infine per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro (art. 18, par. 2, GDPR).

⁴⁹ È questa la tesi sostenuta da E. PELINO, *I diritti dell'interessato*, in L. BOLOGNINI-E. PELINO-C. BISTOLFI (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 257.

⁵⁰ Le ulteriori ipotesi contenute nella norma in oggetto sono: «*b)* il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; *c)* benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; *d)* l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato».

Nell'ambito delle previsioni normative inerenti alla limitazione del trattamento⁵¹, si inserisce inoltre il *considerando* n. 67 del Regolamento che prevede le modalità attraverso le quali il titolare potrebbe (si tratta, del resto, di un *considerando* e non di una norma dotata di pieno valore precettivo)⁵² procedere alla limitazione del trattamento⁵³. Di particolare interesse risulta il richiamo agli archivi automatizzati che conoscono, al giorno d'oggi, un largo impiego.

Dunque, laddove l'interessato ritenga che i suoi dati siano inesatti – al di là della richiesta di una loro rettifica o eventuale cancellazione – avrà il diritto di chiedere al titolare di limitare il trattamento posto in essere (la limitazione, infatti, non opera automaticamente), senza dover fornire alcuna motivazione: ricadrà infatti, eventualmente, sul titolare l'onere di provare l'infondatezza della domanda avanzata⁵⁴. In simili fattispecie, risulta ancora imprescindibile un sapiente utilizzo dei principi di buona fede e correttezza che devono, in tal caso, permeare, particolarmente, le azioni dell'interessato cui viene offerta una tutela tutt'altro che priva di costi per il titolare nelle more della verifica.

È proprio nell'ipotesi di richiesta di esercizio del diritto di limitazione del trattamento per inesattezza dei dati – così come nel caso *sub* lett. *d*) – che emerge la natura eminentemente cautelare⁵⁵ del diritto in questione (limitato nel tempo e suscettibile di revoca), la cui finalità è quella di evitare, per mezzo della conservazione, che si elimini un dato la cui verifica approfondita ne potrebbe delineare la liceità del trattamento posto in essere.

Anche il diritto alla limitazione del trattamento appare utile per sottolineare la centralità dell'esattezza dei dati personali e del connesso principio nell'ambito *privacy*.

⁵¹ Non pare questa la sede per operare anche un confronto con la normativa previgente: a tal fine si rinvia però a A. RICCI, *I diritti dell'interessato*, cit., p. 430 s.; ed a F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 369.

⁵² Sottolinea l'attenuata portata precettiva della disposizione F. DI CIOMMO, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, cit., pp. 368-369, che sottolinea come, oltre al fatto che la previsione sia contenuta in un *considerando*, in essa si possono leggere le parole «in linea di massima» che «riconoscono e lasciano, dunque, ai titolari del trattamento la possibilità di valutare, in relazione alla propria situazione concreta, le misure migliori per attuare la limitazione eventualmente richiesta dall'interessato».

⁵³ Ai sensi del *considerando* n. 67 del Regolamento «le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito *web*. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato».

⁵⁴ Cfr. G. BUTTARELLI, *op. cit.*, p. 310, in cui l'A. prospetta la possibilità per il titolare di effettuare in prima persona la sua richiesta all'interessato; ed anche la possibilità di una previsione pattizia delle parti sul punto.

⁵⁵ Ne evidenzia tale natura unitamente ai profili procedurali A. RICCI, *I diritti dell'interessato*, cit., p. 431.

Il titolare dovrà provvedere immediatamente⁵⁶ a marcare i dati di cui si contesta l'esattezza, sottoponendoli a inutilizzabilità e inaccessibilità, limitandone, pertanto, il trattamento al fine di iniziare le verifiche del caso. Sempre nell'ottica di una piena tutela dell'interessato e della sua autodeterminazione informativa, devono essere inquadrati gli obblighi informativi in capo al titolare verso quest'ultimo nei casi di revoca della limitazione (art. 18, par. 3 GDPR) e verso i destinatari cui vengono trasmessi i dati sottoposti a limitazione (art. 19 GDPR). Sono, infatti, evidenti le ripercussioni fortemente negative, sia nell'ambito personale sia patrimoniale, che l'interessato i cui dati vengono trattati in modo inesatto può subire.

Per quanto non espressamente richiamato all'art. 17 GDPR, non si può ritenere che il principio di esattezza (precisamente, la sua violazione) non rilevi per il diritto alla cancellazione. Già nel rispetto dell'art. 5, par. 1, lett. *d*), il titolare del trattamento è tenuto ad adottare tutte le misure ragionevoli per cancellare (oltre che rettificare) in modo tempestivo i dati di cui ha scoperto l'inesattezza. Tale dovere, oltre ad essere pienamente rispondente al principio di *accountability*, viene richiamato anche al *considerando* n. 39 GDPR. L'obbligazione che sorge in capo al titolare in caso di (fondata) richiesta da parte dell'interessato è comunque una obbligazione di mezzi e non di risultato, essendo chiamato ad adottare le misure che secondo ragionevolezza ci si può legittimamente attendere, avuto anche riguardo ai costi che l'operazione comporta e alla tecnologia a disposizione⁵⁷.

Il mancato rispetto del principio di esattezza sembra poter rientrare nel disposto dell'art. 17, par. 1, lett. *d*), GDPR che sancisce il diritto dell'interessato di ottenere la cancellazione dei dati nel caso in cui siano stati «trattati illecitamente». Pare, infatti, che l'illiceità qui richiamata non attenga unicamente alla mancanza di una delle condizioni di liceità previste dal Regolamento *ex* art. 6 (la cui mancanza porta per certo ad una illiceità), ma debba essere letta in maniera più ampia, ricomprendendo anche la violazione di uno dei principi fondamentali del trattamento, e sicuramente quello di esattezza.

Si sottolinea come il titolare – che, si ricorda, deve (aggiornare, rettificare o) cancellare i dati trattati anche se si accorge *ex se* della relativa inesattezza – sia chiamato ad un compito particolarmente delicato nell'esercizio di questo diritto da parte dell'interessato. Il titolare è, infatti, chiamato a bilanciare gli altri diritti che emergono nel caso concreto (come, ad esempio, il diritto alla libertà di informazione)⁵⁸ per poi decidere di conseguenza quale diritto prevalga nella fattispecie.

⁵⁶ Tale immediatezza viene richiesta nelle *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data* dell'EDPS, cit., p. 21.

⁵⁷ A. RICCI, *I diritti dell'interessato*, cit., p. 412 aggiunge che «la cancellazione deve essere definitiva e deve riguardare ogni singola copia o riproduzione dei dati personali. A tale scopo i dati personali possono essere distrutti o anche anonimizzati, a condizione che non sia possibile la loro re-identificazione e non è sufficiente, ai fini della cancellazione, la pseudonimizzazione».

⁵⁸ Fattispecie prevista *ex* art. 17, par. 3 lett. *a*), GDPR unitamente all'esercizio del diritto alla libertà di espressione; la disposizione prevede anche altri casi che non conducono alla cancellazione dei dati e precisamente: «*b*) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; *c*) per motivi di interesse pubblico nel settore della sanità pubblica

3. APPLICAZIONE DEL PRINCIPIO NELLA CASISTICA

3.1. Il diritto di rettificare dati inesatti al vaglio della Corte di giustizia. Il caso dei documenti dei concorsi professionali e delle valutazioni dell'esaminatore

Il principio di esattezza ed il connesso diritto di rettifica rivestono particolare rilevanza in una decisione della Corte di giustizia dell'Unione europea divenuta ormai nota: il caso *Nowak*⁵⁹. In tale pronuncia, è stata infatti riconosciuta l'applicabilità del diritto di rettifica dei dati inesatti con riguardo ai documenti contenenti le correzioni di un esame pubblico.

La vicenda origina dal rifiuto del Garante per la protezione dei dati personali irlandese di consentire al sig. *Nowak*, l'accesso alla copia della propria prova di esame da esperto contabile, sostenuta in Irlanda con esito sfavorevole. Tale rifiuto veniva giustificato sul presupposto che le informazioni ivi contenute non fossero considerabili alla stregua di dati personali ai sensi della normativa sulla *privacy*.

Nonostante il rifiuto dell'autorità Garante fosse stato giustificato dalla *Circuit Court* prima, nonché dalla *High Court* e, in seguito, dalla *Court of Appeal*, la questione, sottoposta alla *Supreme Court*, veniva considerata ricevibile, ma il giudizio veniva sospeso e la questione rinviata al vaglio della Corte di Giustizia dell'Unione europea per la soluzione di pregiudiziali⁶⁰. La Corte di Giustizia emana, pertanto, una sentenza che offre un'attenta disamina della normativa irlandese (*Data Protection Act* del 1988 come modificato dal *Data Protection Amendment Act* del 2003) di recepimento della direttiva 95/46/CE, tenendo altresì in considerazione la disciplina del GDPR che, all'epoca, non era ancora entrato in vigore.

La direttiva madre, così come anche il successivo Regolamento, accolgono una accezione ampia di dato personale, cuore della *data protection law*, anche laddove non riferibile a questioni private o familiari: «qualsiasi informazione» è oggetto della disciplina⁶¹. L'ampiezza delle definizioni rappresenta il fondamento per il giu-

in conformità dell'articolo 9, paragrafo 2, lettere *h*) e *i*), e dell'articolo 9, paragrafo 3; *d*) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o *e*) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

⁵⁹ CGUE, 20 dicembre 2017, II sezione, C-434/16, *Peter Nowak c. Data Protection Commissioner*, in <http://www.curia.europa.eu>. Per un commento cfr. K. PODSTAWA, *Peter Nowak v. Data Protection Commissioner. You Can Access Your Exam Script Because It Is Personal Data*, in *European, in Data Prot. Law Rev.*, 2018, 2, pp. 252 ss.; e D. JOVE, *Peter Nowak v Data Protection Commissioner: Potential Aftermaths Regarding Subjective Annotations in Clinical Records*, in *Data Prot. Law Rev.*, 2019, 2, pp. 175 ss.

⁶⁰ Nella specie, dati i dubbi sul punto, si chiedeva alla Corte di Giustizia se le informazioni contenute nelle risposte del candidato durante un qualsivoglia esame professionale costituiscono dati personali e, in caso di risposta affermativa, quali fattori risultino determinanti per considerare la prova d'esame come dato personale e che peso tali fattori debbano avere.

⁶¹ Con definizioni che riprendono quelle della direttiva 95/46/CE (art. 2 a e b), ai sensi dell'art. 4, 1), del Regolamento è qualificabile come "dato personale" «qualsiasi informazione riguardante una

dice al fine di stabilire che i documenti di un esame professionale e, in particolare, le valutazioni *ivi* contenute, debbano essere considerate dati personali.

È certamente pacifico che un candidato ad un esame pubblico sia una persona fisica che può (*rectius*, deve) essere identificata direttamente, attraverso il suo nome, o indirettamente, attraverso un codice identificativo, a nulla rilevando, come sostenuto invece dall'autorità Garante, il fatto che l'esaminatore possa o meno identificare il candidato al momento della correzione della prova, rimanendo sempre possibile del resto per l'ente organizzatore (nel caso di specie l'organizzazione professionale degli esperti contabili) la possibilità di identificare il candidato al fine di attribuire le risposte ad un soggetto ben determinato⁶². Le informazioni in questione sono connesse alla persona del candidato: il contenuto delle risposte rispecchia il suo livello di conoscenze e preparazione; di più, nel caso di esame redatto a mano, contengono anche informazioni grafologiche. La raccolta delle risposte, al fine di valutare l'idoneità del candidato alla professione, incide sui diritti e sugli interessi del soggetto.

Appare, quindi, corretto secondo il convincente ragionamento della Corte – la quale non si pone solo in linea con le finalità normative di tutela dell'interessato e con l'orientamento dell'autorità Garante⁶³, ma che dimostra, anche in questa sede, il suo cruciale ruolo interpretativo e creativo⁶⁴ – qualificare come dati personali le

persona fisica identificata o identificabile»; all'art. 4, 2), si definisce poi come “trattamento”, «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali». Data l'ampiezza di queste definizioni, la natura della normativa è da considerarsi onnicomprensiva; sul tema si rinvia alle considerazioni di M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ.*, 2017, 2, pp. 165 ss.

⁶² Inoltre, come affermato in CGUE, 19 ottobre 2016, *Breyer*, C- 582/14, EU:C:2016:779, punto 43, affinché una informazione costituisca un dato personale non è necessario che tutte le informazioni che consentono di identificare l'interessato siano in possesso di una singola persona.

⁶³ Il Garante per la protezione dei dati personali ha da tempo sottolineato l'esigenza di una ampia concezione di “dato personale”: si richiama per tutti GDPR, Provv. 17 giugno 1999, doc. web n. 48067, uno dei primissimi e più celebri provvedimenti dell'autorità Garante in cui si afferma come si possano intendere alla stregua di “dati personali” le valutazioni che concorrono a formare il giudizio annuale di rendimento di un lavoratore dipendente, le c.d. note di qualifica, dal momento che «ogni notizia o elemento che fornisce un contributo aggiuntivo di valutazione rispetto ad un soggetto identificato o identificabile. E questo in riferimento sia ad informazioni oggettive sia a descrizioni, giudizi, analisi o ricostruzioni di profili personali (riguardanti attitudini, qualità, requisiti o comportamenti professionali) che danno origine a valutazioni complessive del soggetto interessato», tali informazioni devono pertanto essere messe a disposizione dell'interessato che ne faccia richiesta.

⁶⁴ Per quanto non sia il tema centrale della presente indagine, la pronuncia permette di sottolineare l'importanza dell'intervento della Corte di Giustizia dell'Unione europea nell'ambito *privacy*, su cui v. per tutti G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir. inform.*, 2015, 4-5, pp. 779 ss.; e F. ROSSI DAL POZZO, *La tutela dei dati personali nella giurisprudenza della Corte di Giustizia*, in *Eurojus*, 27 dicembre 2018, pp. 8 ss. in cui l'A., oltre ad analizzare la protezione dei dati personali come nuova competenza dell'Unione europea e come autonomo diritto fondamentale, pone in luce il fondamentale apporto di pronunce come *Nowak* e *Breyer* per la concezione di “dato personale”. Come autorevolmente già sostenuto da F. GALGANO, *La globalizzazione nello specchio del diritto*, Bologna, 2005, p. 119, la funzione creativa del diritto in capo ai giudici, soprattutto europei, è infatti da tempo considerata come «dato di cultura giuridica ormai acquisito», v. anche p. 115 in cui l'A. sottolinea come «il giudice non possa più essere, quale lo aveva pensato Montesquieu, la *bouche qui prononce les paroles de la loi*».

informazioni contenute sia nelle risposte del candidato sia nelle annotazioni dell'esaminatore⁶⁵, in ragione del loro contenuto, delle loro finalità e dei loro effetti. La scelta del Garante per la protezione dei dati irlandese si tradurrebbe quindi in una indebita costrizione della concezione di "dato personale" e, di conseguenza, dei diritti dell'interessato che non riceverebbe protezione in situazioni, come quella in esame, meritevoli di tutela⁶⁶.

Dovendosi pertanto ammettere l'esercizio dei diritti legislativamente previsti tra i quali il diritto di rettifica su tali dati e posto che tale diritto non può certo consentire al candidato di modificare *ex post* una o più risposte sbagliate, i giudici di Lussemburgo pongono l'accento sull'esattezza e la completezza dei dati personali, per la cui valutazione ci si deve rifare alle finalità con le quali i dati in questione sono stati rilevati. Nel caso di un concorso pubblico, la «finalità consiste (...) nel poter valutare il livello di conoscenza e di competenza di tale candidato al momento dell'esame. Orbene, tale livello si riflette proprio in eventuali errori in tali risposte. Di conseguenza, errori del genere non costituiscono affatto un'inesattezza, ai sensi della direttiva 95/46, che conferisca un diritto di rettifica ai sensi dell'articolo 12, lett. b), della stessa. Per contro, è possibile che si presentino, situazioni nelle quali le risposte di un candidato a un esame e le annotazioni dell'esaminatore ad esse relative si rivelano inesatte, ai sensi dell'art. 6, par. 1, lett. d), della direttiva 95/46, per esempio per il fatto che, per errore, le prove di esame sono state scambiate in modo tale che le risposte di un altro candidato siano state attribuite al candidato interessato, o che una parte dei fogli contenenti le risposte di tale candidato è stata smarrita con la conseguenza che tali risposte sono incomplete o, ancora, che le eventuali annotazioni dell'esaminatore non documentano correttamente la valutazione da esso effettuata delle risposte del candidato interessato»⁶⁷.

In argomento ci si limita a richiamare le considerazioni di S. ROMANO, *L'ordinamento giuridico*, Firenze, 1946, e di P. GROSSI, *Ritorno al diritto*, Roma-Bari, 2015, pp. 34 ss.; ID., *Il diritto civile tra le rigidità di ieri e le mobilità di oggi*, in M. LOBUONO (a cura di), *Scienza giuridica privatistica e fonti del diritto*, Bari, 2009; vedi anche il commento del pensiero di Grossi offerto da G. CONTE, *L'eredità della "modernità giuridica". In margine a un recente volume di Paolo Grossi sulla storia giuridica europea*, in *Riv. trim. dir. e proc. civ.*, 2009, 1, pp. 376 ss. in cui secondo l'A., Grossi non mira ad un "esilio dell'attività legislativa", ma sottolinea la non esclusività, in capo alla legge, della funzione nomopoietica, ciò anche in ragione dell'attuale presenza di vari centri di produzione del diritto che sempre più spesso non hanno un preciso radicamento territoriale; v. poi A. RICCIO, *La giurisprudenza è, dunque, fonte del diritto*, in *Contratto e impr.*, 2017, 3, pp. 857 ss.; *amplius* sul tema vedi F. BRAVO, *Ubi societas ibi ius e fonti del diritto nell'età della globalizzazione*, in *Contratto e impr.*, 2016, 6, pp. 1344 ss.

⁶⁵ Secondo CGUE, 20 dicembre 2017, II sezione, C- 434/16, *Peter Nowak c. Data Protection Commissioner*, cit., punti 42 ss., anche le annotazioni dell'esaminatore riferite alle risposte del candidato costituiscono informazioni a quest'ultimo riferibili e ciò non è contraddetto dal fatto che esse costituiscono informazioni concernenti (anche) l'esaminatore.

⁶⁶ Analizza, in particolare, la rilevanza e l'impatto della sentenza in rapporto alla nozione di "dato personale", C. IRTI, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus civile*, 2020, 2, pp. 390 ss.

⁶⁷ Così CGUE, 20 dicembre 2017, II sezione, C-434/16, *Peter Nowak c. Data Protection Commissioner*, cit., punti 53-54; v. anche le conformi conclusioni dell'Avvocato Generale Juliane Kokott.

La tutela dell'interessato e, precisamente, la liceità del trattamento dei suoi dati trova riconoscimento nella possibilità per l'interessato di esercitare (anche) il diritto di accesso, prodromico all'eventuale richiesta di rettifica (o cancellazione) di dati inesatti o di cui non risulta più necessaria la conservazione. Sotto questo ultimo profilo, si deve infatti ammettere che l'interessato-candidato possa richiedere che le risposte date in sede di esame e le annotazioni dell'esaminatore alle prime riferite, vengano cancellate una volta raggiunte le finalità per le quali tali dati personali erano stati rilevati e trattati: verosimilmente una volta conclusosi il procedimento e trascorsi i termini per presentare ricorso, momento nel quale non può escludersi la maturazione da parte dell'interessato di un legittimo interesse alla cancellazione dei dati, fatti salvi eventuali obblighi di legge sulla conservazione per una maggiore durata della documentazione concorsuale.

Il caso *Nowak* rappresenta una dimostrazione di come sia fondamentale comprendere quali informazioni debbano essere considerate come dati personali sia per definire al meglio l'ambito di applicazione materiale del GDPR e, in particolare, del principio di esattezza dei dati, sia per poter assicurare una massima tutela ai soggetti i cui dati vengono trattati. Solo in questo modo, l'interessato potrà attivarsi nel caso in cui i suoi dati siano inesatti, esercitando i diritti previsti dal Regolamento, al fine di scongiurare una falsa rappresentazione della sua identità ed altri probabili pregiudizi di natura personale e patrimoniale.

3.2. Il principio di esattezza nelle pronunce del Garante

Il principio di esattezza si rinviene in una molteplicità di pronunce del Garante per la protezione dei dati personali, ma spesso viene evocato unicamente a fianco di altri principi che paiono, almeno ad una prima lettura, assumere maggior centralità. Ne deriva l'opportunità di analizzare *funditus* il ruolo che tale principio svolge nelle argomentazioni dell'autorità Garante al fine di comprenderne l'effettiva portata.

A ben vedere, le pronunce del Garante denotano una spiccata consapevolezza dei pregiudizi che possono derivare all'interessato nel caso in cui i dati trattati siano inesatti: l'autorità è infatti intervenuta⁶⁸ condannando le società che non pongono in essere adeguate misure tecniche e organizzative volte ad assicurare da un lato l'esattezza dei dati trattati, anche intesa come un costante aggiornamento degli stessi, e, dall'altro, a diminuire i rischi per i diritti e le libertà degli interessati in caso di *data breach*, permettendo una tempestiva verifica da parte dell'autorità di controllo. Una errata gestione delle c.d. *black lists* di esclusione dei soggetti dalle campagne commerciali, perpetrata anche attraverso un loro mancato aggiornamento, finisce per

⁶⁸ Cfr., a titolo di esempio, GPDP, Prov. 15 gennaio 2020, doc. *web* n. 9256486, sanzionatorio nei confronti di Tim S.p.a., in cui viene richiesto alla società di effettuare entro centottanta giorni di operare un «rafforzamento delle misure volte ad assicurare la qualità, l'esattezza e il tempestivo aggiornamento dei dati personali trattati dai diversi sistemi della Società», nonché «l'effettuazione di specifici e documentati test di regressione volti a verificare, per ogni modifica (correttiva o evolutiva) riguardante i sistemi che trattano dati personali della clientela, che l'impatto della modifica stessa non riduca la qualità dei trattamenti effettuati e l'esattezza dei dati trattati»; in senso conforma v. anche GPDP, Prov. 9 luglio 2020, doc. *web* n. 9435753 e GPDP, Prov. 17 gennaio 2020, doc. *web* n. 9244351.

impattare sui consensi *privacy* forniti in precedenza e riportati nelle schede anagrafiche della clientela, rendendo pertanto illecito il trattamento.

Il presidente dell'autorità ha anche avuto modo di sottolineare come il principio di esattezza, legato alla qualità dei dati trattati, sia altresì fondamentale nel contesto della lotta all'evasione fiscale⁶⁹. Solo attraverso l'utilizzo di dati personali esatti diviene infatti possibile stilare profili di rischio di evasione affidabili, fondati su solidi presupposti, scongiurando così accessi abusivi ai dati di un vastissimo numero di persone. La pretesa di protezione dei dati personali e la ancillare creazione di canali sicuri di trasmissione degli stessi non rappresentano un ostacolo, ma un contributo essenziale finalizzato ad un serio contrasto alla evasione fiscale: se i dati non sono esatti, non è infatti possibile combattere l'evasione in modo mirato e se, inoltre, non si garantisce la sicurezza della trasmissione delle informazioni, i dati espongono il fianco a violazioni e attacchi informatici⁷⁰. Per perseguire tale nobile fine è quindi imprescindibile un puntale rispetto del principio di esattezza (intesa anche come non obsolescenza) dei dati in modo da sfruttare corrette rappresentazioni di capacità patrimoniale e rischio fiscale degli interessati su cui fondare gli accertamenti⁷¹.

Un importante richiamo al principio di esattezza viene effettuato nel parere del Garante sullo schema di regolamento, predisposto dal Ministero della giustizia, volto a disciplinare il trattamento dei dati giudiziari in una pluralità di ambiti⁷². Il decreto, sul quale il Garante, seppur con alcune osservazioni, esprime un parere favorevole, nel prevedere una serie di garanzie minime, comuni a tutti i casi di trattamento previsto, già annoverava un obbligo di verifica periodica circa l'esattezza e l'aggiornamento dei dati trattati, insieme alla loro adeguatezza, pertinenza e necessità in rapporto alle finalità di volta in volta perseguite.

L'autorità Garante evidenzia, in primo luogo, come il Ministero della giustizia, facendo seguito alle indicazioni da lui fornite nelle diverse interlocuzioni, abbia introdotto specifiche garanzie indirizzate ad assicurare l'esattezza dei dati con particolare riguardo all'aggiornamento rispetto all'evoluzione della posizione giudiziaria dell'interessato, utilizzando fonti che siano affidabili e aggiornate, limitando altresì il trattamento ai soli dati indispensabili in vista delle finalità perseguite⁷³.

L'attenzione è, a più riprese, focalizzata sulle fonti e sulla loro attendibilità, come si può osservare con riguardo ai trattamenti svolti a fini di verifica della solidità, solvibilità ed affidabilità di potenziali controparti contrattuali, attività che può essere affidata solamente a soggetti muniti di licenza prefettizia⁷⁴. Considerati i notis-

⁶⁹ GPDP, Provv. 3 ottobre 2019, doc. web n. 9152641.

⁷⁰ GPDP, Provv. 15 ottobre 2019, doc. web n. 9162435.

⁷¹ GPDP, Provv. 7 luglio 2021, doc. web n. 9678216.

⁷² GPDP, Provv. 24 giugno 2021, doc. web n. 9682603 che si è espresso ai sensi dell'art. 2-*octies*, co. 2 del Codice *privacy*, così come modificato dal d.lgs. 101/2018, che demanda al Ministero della Giustizia, sentito appunto il Garante, la previsione dei casi in cui è legittimo il trattamento dei dati giudiziari (ai sensi dell'art. 10 del GDPR) nei casi in cui non sia già ammesso da norme di legge o regolamentari che prevedano garanzie appropriate per i diritti e le libertà degli interessati e che non avvenga sotto il controllo della autorità pubblica.

⁷³ GPDP, Provv. 24 giugno 2021, doc. web n. 9682603, cit.

⁷⁴ *Ibidem*.

simi problemi inerenti alla tutela dei dati personali indicizzati (senza aggiornamenti) dai motori di ricerca, il Garante, criticando il ricorso a fonti c.d. aperte che non sono sempre in grado di garantire affidabilità ed esattezza, suggerisce il solo utilizzo, quali legittime fonti di raccolta, di siti istituzionali, di ordini professionali e di associazioni di categoria⁷⁵. A questo aggiunge l'opportunità di escludere la possibilità di modificare il contenuto delle informazioni eventualmente acquisite da fonti aperte, salvo il loro puntuale aggiornamento, nonché di utilizzarle con finalità di elaborazione di informazioni valutative⁷⁶.

Il principio di esattezza viene poi richiamato in alcuni provvedimenti del Garante che hanno ad oggetto i trattamenti effettuati in relazione alla certificazione verde (c.d. *green pass*), in base al d.l. 22 aprile 2021, n. 52. L'autorità Garante⁷⁷, nel sottolineare come tale d.l. non rappresenti un'ideale base giuridica per legittimare i trattamenti, mancando in particolare un'indicazione esplicita e tassativa delle finalità perseguite con le certificazioni verdi, afferma che tale fonte normativa viola il principio di esattezza, «essenziale nella valutazione della proporzionalità della limitazione e della idoneità della misura di contenimento e contrasto dell'emergenza epidemiologica da Covid-19»⁷⁸. Il contrasto con il principio di esattezza si palesava dal momento che il sistema transitoriamente posto in essere (nelle more dell'adozione di un decreto attuativo che istituiva la piattaforma nazionale *Digital Green Certificate*, DGC) non consentiva una verifica dell'attualità delle condizioni attestate, non potendo tener conto di eventuali modifiche dello stato di salute dell'interessato, sopraggiunte in un momento successivo al rilascio della certificazione, a causa della mancanza di una piattaforma. Erano, quindi, chiari i rischi per i diritti e le libertà degli interessati da un lato e la potenziale inefficacia della misura in rapporto alla finalità di contenimento della diffusione del virus Sars-Cov-2.

Il Garante ha successivamente avuto modo di esprimersi⁷⁹ sulla bozza di decreto del Presidente del Consiglio dei Ministri, da adottare ai sensi dell'art. 9, co. 10, del d.l. 52/2021, trasmessa all'autorità unitamente alla valutazione di impatto sui dati personali con riferimento ai trattamenti disciplinati dal DPCM ed in particolare a quelli effettuati attraverso la piattaforma DGC. Il parere (favorevole seppur con alcune condizioni) del Garante si sofferma sulle criticità già espresse in merito alla mancata indicazione delle finalità di trattamento, sottolineando la necessaria introduzione di una riserva di legge statale che individui puntualmente le finalità per le quali possano essere utilizzate le certificazioni verdi – attestanti l'avvenuta vaccinazione di un soggetto o la sua guarigione da Covid-19 o, ancora, l'esito negativo al virus Sars-Cov-2 in seguito ad un test antigenico rapido o molecolare – così da eliminare *ex ante* la possibilità di incorrere in interpretazioni discrezionali particolarmente estensive. L'obbligo di presentare il *green pass* per accedere a luoghi o servizi rappresenta del resto, come argomenta il Garante, una limitazione della libertà

⁷⁵ *Ibidem*.

⁷⁶ *Ibidem*.

⁷⁷ GPDP, Provv. 23 aprile 2021, doc. *web* n. 9578184.

⁷⁸ *Ibidem*. Espressamente, nel Provv. cit., il Garante ha affermato che «il decreto legge del 22 aprile 2021, 52, si ritiene violi anche il principio di esattezza».

⁷⁹ GPDP, Provv. 9 giugno 2021, doc. *web* n. 9668064.

personale che, in quanto tale, può essere ammessa solo se prevista da una norma di legge di rango primario.

Il parere in questione rileva anche, ai fini della presente trattazione, proprio per l'attenzione da esso riservata al principio di esattezza e, segnatamente, al superamento delle criticità precedentemente espresse sul contrasto con detto principio. La bozza di DPCM infatti – come, ovviamente, poi il DPCM stesso del 17 giugno 2021⁸⁰ – istituisce la piattaforma DCG e permette all'interessato di esercitare il diritto di rettifica con una modalità semplificata, ossia rivolgendosi ad un servizio messo a disposizione dal Ministero della salute, tramite un numero di pubblica utilità e ricevendo un riscontro in un termine congruo rispetto alla certificazione rilasciata. Viene in tal modo assicurato un doppio controllo, a monte dal titolare e poi dall'interessato, sull'esattezza e sull'aggiornamento dei dati così da scongiurare, almeno in linea di massima, i gravissimi pregiudizi che potrebbero derivare in capo all'interessato a causa di un inesatto trattamento di suoi dati sensibili e all'intera collettività per un utilizzo non congruo (soprattutto in termini di esattezza dei dati trattati) delle certificazioni verdi nella contingente situazione pandemica.

Da ultimo, pare opportuno sottolineare che l'attenzione del Garante per il principio di esattezza è dimostrato dai numerosi richiami che ne vengono effettuati in una pletera di provvedimenti che interessano i temi più diversi, ma nei quali tale principio assurge sempre a strumento fondamentale per guidare la *compliance* del trattamento posto in essere con la normativa *privacy*⁸¹. Proprio dal numero dei prov-

⁸⁰ Al DPCM di attuazione del d.l. 52/2021, ha fatto seguito una nota del Presidente del Garante per la protezione dei dati personali (GPDP, 21 giugno 2021, doc. *web* n. 9681670) in cui evidenzia come il DPCM tenga conto delle osservazioni formulate dal Garante nel parere del 9 giugno *supra cit.*, sottolineando però la «necessità di soprassedere dall'adottare o dal dare attuazione a disposizioni adottate a livello locale che: – introducono fattispecie diverse da quelle allo stato previste dalla normativa di livello nazionale in cui possa essere richiesta l'esibizione dei certificati (...); – prevedono modalità di emissione, gestione e controllo delle predette certificazioni difformi da quelle disciplinate nel predetto decreto del Presidente del Consiglio dei Ministri».

⁸¹ Cfr. a titolo di esempio, tra i più recenti, GPDP, Provv. 9 marzo 2023, doc. *web* n. 9868836 relativo all'approvazione di un codice di condotta per le attività di *telemarketing* e *teleselling*; GPDP, Provv. 21 dicembre 2022, doc. *web* n. 9856315 in merito ad un parere, richiesto al Garante dall'Organismo agenti e mediatori, con riguardo alle specifiche tecniche relative alla procedura di registrazione degli operatori in valute virtuali alla sezione speciale del Registro dei Cambiavalute; GPDP, Provv. 24 novembre 2022, doc. *web* n. 9842737 con riguardo all'esattezza dei dati usati per finalità di ricerca medica; GPDP, Provv. 15 settembre 2022, doc. *web* n. 9815094 riguardante un parere sullo schema di decreto del Ministero dell'Interno, recante «modalità di aggiornamento della piattaforma di funzionamento dell'Anagrafe Nazionale della Popolazione residente per l'erogazione dei servizi resi disponibili ai comuni per l'utilizzo dell'Archivio Nazionale informatizzato dei registri dello Stato Civile»; GPDP, Provv. 16 dicembre 2021, doc. *web* n. 9738899 sulla «necessità di assicurare il rispetto del principio di esattezza dei dati relativi ai consumi energetici che potrebbero risultare non correttamente associabili agli interessati»; GPDP, Provv. 13 dicembre 2021, doc. *web* n. 9727220 in merito alla «necessità di garantire l'esattezza e l'aggiornamento dei dati in base ai quali è generata la certificazione verde»; GPDP, Provv. 23 aprile 2021, doc. *web* n. 9582723 che lamenta come, nel caso concreto, la comunicazione o diffusione dei dati potrebbe «porsi in contrasto con il principio generale di "esattezza dei dati"»; GPDP, Provv. 21 aprile 2021, doc. *web* n. 9676101 in cui si rileva che «il trattamento (...) tramite il motore di ricerca risulta pertanto in contrasto con i principi di esattezza ed aggiornamento dei dati»; GPDP, Provv. 25 febbraio 2021, doc. *web* n. 9556958 che sottolinea: «in

vedimenti che lo richiamano a fondamento della decisione, e dalla sua rilevanza, sottolineata dal Garante stesso, emerge l'importanza del principio in esame e la sua assoluta centralità per l'impianto normativo volto a disciplinare la protezione dei dati personali.

Ad esempio, il Garante⁸² ha evidenziato l'importanza del principio di esattezza, inteso come aggiornamento delle informazioni, ed il pregiudizio derivante alla reputazione personale e professionale di un soggetto dalla perdurante reperibilità in rete di articoli contenenti informazioni risalenti, relative a misure disposte nei suoi confronti successivamente revocate: in detti articoli (così come in altri reperibili) non si dava atto del decreto di archiviazione pronunciato nei suoi riguardi «determinando con ciò la circolazione di informazioni sul conto dell'interessato divenute ormai inesatte le quali, essendo collegate a gravi fattispecie di reato, risultano peraltro particolarmente pregiudizievoli per i diritti del medesimo»⁸³. Simili considerazioni sono state svolte nel caso in cui i fatti collegati al soggetto e reperibili in rete, anche a distanza di un ampio lasso temporale, erano riferiti a vicende alle quali non era seguita alcuna condanna per l'interessato⁸⁴.

Divenuto celebre è invece il provvedimento⁸⁵ che contiene una (pesante) sanzione per l'impiego di un sistema di supervisione (*proctoring*), utilizzato durante le prove scritte d'esame, in modalità "a distanza", al fine di identificare e controllare gli studenti universitari nello svolgimento della prova.

A prescindere dalle considerazioni, ampiamente esaminate dal Garante, in tema di liceità, correttezza e trasparenza del trattamento, nonché di minimizzazione e conservazione dei dati, preme, ai fini del discorso che si intende sviluppare in questa sede, evidenziare come nel provvedimento in questione si sottolinei l'importanza di «un'adeguata valutazione in merito all'effettiva affidabilità dello strumento di supervisione, con riguardo sia alle funzioni di riconoscimento facciale (...) sia ai meccanismi con i quali vengono definiti gli indici di rischio, non essendo state, pertanto, valutate le possibili ripercussioni per gli interessati in caso di errori o falsi positivi/negativi»⁸⁶. Quando si utilizzano strumenti di identificazione biometrica, è centrale l'affidabilità degli algoritmi utilizzati dal sistema e l'esattezza dei dati inseriti nel si-

assenza di dati esatti, la qualità del controllo effettuato (...) potrebbe risultare compromessa; il raffronto effettuato potrebbe infatti, da un lato, condurre all'individuazione di un soggetto sbagliato e, dall'altro, non consentire invece di identificare soggetti non aventi diritto»; GPDP, Provv. 10 dicembre 2020, doc. *web* n. 9575055 che rileva come il titolare del trattamento, nel caso di specie, abbia operato l'aggiornamento di determinate informazioni, necessario per conformare «il trattamento ai principi di esattezza».

⁸² GPDP, Provv. 25 novembre 2021, doc. *web* n. 9731941.

⁸³ *Ibidem*, in cui si aggiunge che «il perdurante trattamento di tali dati in associazione al nominativo dell'interessato appare dunque in contrasto con i principi di esattezza ed aggiornamento previsti dal Regolamento (cfr. art. 5, par. 1, lett. d)»; in senso conforme GPDP, Provv. 25 novembre 2021, doc. *web* n. 9732385; GPDP, 25 novembre 2021, doc. *web* n. 9732368; GPDP, Provv. 10 febbraio 2022, doc. *web* n. 9750669; GPDP, Provv. 13 febbraio 2020, doc. *web* n. 9308726; GPDP, Provv. 21 luglio 2022, doc. *web* n. 9812455.

⁸⁴ GPDP, Provv. 10 febbraio 2022, doc. *web* n. 9750669.

⁸⁵ GPDP, Provv. 16 settembre 2021, doc. *web* n. 9703988.

⁸⁶ *Ibidem*.

stema per evitare distorsioni sull'identità dell'interessato, limitazioni dei suoi diritti e per un corretto e proficuo perseguimento delle finalità del trattamento.

Ancora, l'esattezza dei dati deve essere rispettata al fine di evitare l'accesso di dati personali a soggetti non legittimati, i cui risvolti negativi si acquisiscono nel caso di categorie particolari dei dati personali come quelli sanitari. Si richiama sul punto il caso di una signora che, a causa di un errore dell'operatore nell'inserire i dati nel Fascicolo Sanitario Elettronico (FSE), aveva la possibilità di visualizzare, attraverso la sua utenza, il FSE di una minore sulla quale, in realtà, non vantava la responsabilità genitoriale⁸⁷.

Un rigoroso rispetto del principio di esattezza deve quindi essere considerato (e così pare essere nei provvedimenti del Garante) un'esigenza primaria ai fini di una piena tutela dei diritti e delle libertà del *data subject* e, altresì, per garantire uno sfruttamento anche in chiave economica dei dati personali la cui protezione non è una prerogativa assoluta (*considerando* n. 4 GDPR).

Il Garante per la protezione dei dati personali dimostra, pertanto, di essere profondamente consapevole dei danni che possono derivare all'interessato in caso di trattamento di dati inesatti: danni che, si è detto, potrebbero investire sia l'ambito personale sia quello patrimoniale. Nonostante la lente del Garante per indagare il principio di esattezza sia maggiormente quella della tutela dell'interessato, non devono essere tralasciati gli interessi che il titolare potrebbe avere nel trattare dati esatti. Come si è precedentemente accennato, infatti, dato che si ammette, sempre più ampiamente, uno sfruttamento economico dei dati da parte dei titolari, solo laddove i dati trattati siano esatti, le politiche di *marketing* possono essere mirate e quindi maggiormente efficaci.

Il principio di esattezza deve quindi essere considerato sotto la doppia luce della tutela dei diritti e delle libertà dell'interessato, da un lato, e del riconoscimento e della garanzia degli interessi del titolare dall'altro: solo un suo puntuale rispetto permette, infatti, di soddisfare le esigenze dei soggetti del trattamento e di garantire stabilità all'architettura dell'intero sistema *privacy*.

⁸⁷ GPDP, Prov. 24 giugno 2021, doc. *web* n. 9709119 in cui, però, si sottolinea che, nel caso di specie, il Garante si è limitato ad una mera ammonizione per il titolare del trattamento data la sua buona fede, il suo impegno immediato indirizzato alla correzione delle inesattezze dei dati e atteso che «ha attuato misure volte a ripristinare una corretta alimentazione dei Fascicoli sanitari elettronici dei soggetti interessati dalla vicenda oggetto della segnalazione, nonché previsto misure tecniche e organizzative volte a scongiurare che episodi come quello in esame posano ripetersi».

Finito di stampare anno 2023
presso le Industrie Grafiche della Pacini Editore S.r.l.
Via A. Gherardesca • 56121 Pisa
Tel. 050 313011 • Fax 050 3130300
www.pacineditore.it





€ 70,00