PROFILI DI TUTELA DEL REGOLAMENTO (UE) 2016/679

Alessandro Tomaselli

Abstract*:* *Il Regolamento (UE) 2016/679 entrato in vigore nel maggio del 2018 reca con sé rilevanti novità in materia di tutela di dati sensibili e privacy del singolo nell'era di internet, in particolare, tra l'altro, attraverso una compiuta disciplina del c.d. diritto all'oblio, prerogativa soggettiva di recente emersione e sempre più attuale all'interno dell'odierno dibattito giuridico, nonché una serie di obblighi gravanti sui soggetti (server di posta elettronica, internet providers, motori di ricerca, aziende, enti pubblici, ecc.) la cui attività in rete implica il trattamento dei dati in questione. Specificamente, il testo normativo in questione, promulgato al fine di aggiornare la precedente disciplina di cui alla Direttiva 95/46/CE e finalizzato testualmente all'ambizioso obiettivo di elevare la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale a diritto fondamentale in prospettiva uniformante, sembra caratterizzarsi per una ratio maggiormente garantista nei confronti dei singoli cittadini europei in termini di controllo sull'utilizzo delle informazioni riguardanti la propria persona da parte degli accennati soggetti. Tuttavia, in tale sede si proverà ad offrire un approfondimento all'interno di una differente visuale critica e di analisi della norma in questione per il tramite, da un lato, del confronto del suddetto diritto all'oblio con la classica estrinsecazione del medesimo, e, dall'altro, dell'individuazione di ciò che appare l'autentico oggetto di tutela in materia, e cioè il rafforzamento e susseguente corretto funzionamento del mercato.*

Parole chiave: *Unione Europea, diritto all'oblio, mercato unico, diritti umani*

1. Premessa

Il 25 maggio 2018 ha trovato applicazione all'interno del territorio dell'UE il *Regolamento* (UE) del Parlamento europeo e del Consiglio 2016/679[1] (di seguito, anche GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la *Direttiva* 95/46/CE[2].

[1] Il testo, adottato il 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, è operativo a partire dal 25 maggio 2018, al fine di permettere agli ordinamenti degli Stati membri dell'UE di apprestare i relativi strumenti normativi di adeguamento

[2] E che insieme alla *Direttiva* (UE) 2016/280 (relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio) compone il c.d. "pacchetto protezione dei dati".

E' bene preliminarmente precisare come tale iniziativa legislativa individui la base giuridica di riferimento nell'art. 16 del Trattato sul Funzionamento dell'Unione Europea, nonché nell'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea ("Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano"), e come la medesima vada da considerarsi riflesso diretto dell'esigenza di apprestare una disciplina uniforme e maggiormente dettagliata a garanzia del singolo nei confronti delle implicazioni conseguenti ad un agire digitale sempre più esteso: è innegabile, infatti, come all'interno della società dell'informazione, contraddistinta da un utilizzo sempre più massiccio di internet con contestuale accresciuta capacità di archiviazione, uso e condivisione di ingenti quantità di dati c.d. sensibili immessi nello stesso (*big data*), agli occhi del legislatore di Bruxelles si è posta come improcrastinabile la necessità di elevare in materia gli standard di protezione a favore dell'individuo.

Segnatamente, al fine di ovviare alla "frammentazione della protezione dei dati personali nel territorio dell'Unione" e ai pregiudizi derivanti dalla "compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali", l'Unione Europea, conscia di come le criticità derivanti dal non esaustivo quadro normativo di cui alla richiamata *Direttiva* 95/46/CE si traducessero in una forte instabilità del mercato europeo, ha deciso di apprestare una nuova disciplina relativamente alla materia che ci occupa, in particolare per il tramite di alcuni istituti e principi a tutela del singolo certamente degni di menzione[3]: il c.d. *risk based approach*, principio in virtù del quale si

[3] Si rammenti come la promulgazione del testo regolamentare in oggetto sia, in realtà, da ricondurre ad un rinnovato iter intrapreso in materia nel 2012 da parte del legislatore di Bruxelles, e finalizzato all'individuazione di nuove regole comuni a tutti gli Stati membri dell'UE nell'ambito della protezione dei dati personali e del quale il GDPR medesimo, dunque, è da considerarsi l'esito finale: in particolare, è datata 25 gennaio 2012 la presentazione da parte della Commissione Europea del pacchetto completo sulla protezione dei dati personali in cui venivano presentate per la prima volta sia la proposta di Regolamento oggetto del presente saggio, sia la proposta di Direttiva concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati. A ciò ha fatto seguito l'adozione in ambito europeo di altre iniziative mosse all'obiettivo di facilitare la transizione dei singoli ordinamenti nazionali verso gli accennati nuovi orizzonti digitali, e la più rilevante delle quali è certamente costituita da quella intrapresa dalla Commissione UE nel 2016, nota come *Digitising European Industry Iniziative* e specificamente funzionale alla creazione del Mercato unico digitale (*Digital Single Market*). Tale progetto, in particolare, finalizzato a garantire che ogni impresa operante all'interno del territorio dell'UE possa usufruire dei vantaggi derivanti dall'innovazione digitale a prescindere dalle proprie dimensioni, dall'ubicazione e dal settore in cui opera, si fonda sui seguenti quattro

determina la misura di responsabilità del titolare o del responsabile del trattamento tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti; l'accresciuta applicabilità territoriale (la disciplina vincola chiunque, operatore europeo o non, a prescindere dalla sua collocazione territoriale, utilizzi dati relativi a cittadini dell'Unione); la rete di cautele previste in ordine al consenso (comunque revocabile in ogni momento), di modo che non vi sia più possibilità, per le imprese, di ricorrere a condizioni contrattuali incomprensibili; il rafforzamento del diritto di accesso, con la possibilità, per l'interessato, di ottenere la conferma del trattamento dei dati e sulle sue finalità, nonché una copia di detti dati in formato elettronico, senza oneri per il richiedente; la portabilità dei dati (diritto di trasmettere i propri dati a un altro titolare); la "*privacy by design*", concezione non certo innovativa ma che ora soltanto trova consacrazione in un testo normativo; la previsione di un nuovo ruolo, quello del c.d. DPO (*Data Protection Officer*), responsabile del trattamento dei dati (per le imprese la cui attività principale consista in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala); il diritto alla cancellazione dei dati (il c.d. diritto all'oblio)[4].

pilastri fondamentali: 1) creazione di una piattaforma europea per le iniziative nazionali in materia di digitalizzazione industriale; 2) innovazioni digitali per tutti: *digital innovation hubs*; 3) rafforzare la leadership attraverso partenariati e piattaforme industriali, 4) determinazione di un quadro normativo adatto all'era digitale; 5) preparare i cittadini al futuro digitale. Nell'ambito di tale iniziativa è stata, poi, adottata la c.d. *Direttiva* (UE) 2016/1148 del Parlamento Europeo e del Consiglio recante misure per un livello comune di sicurezza delle reti e dei sistemi informativi dell'Unione (la c.d. *Direttiva* NIS, *Network and Information Security*), e sono successivamente stati siglati vari documenti rilevanti ai fini dell'implementazione delle nuove tecnologie in relazione a vari contesti dell'agire europeo: tra gli altri, meritano menzione l'"*EU eGovernment Action Plan 2016-2020 - Accelerating the digital transformation of government*" dedicato alla digitalizzazione della pubblica amministrazione e alla creazione di servizi digitali a favore degli utenti (COM(2016) 179 *final*) e l'"*European Cloud Initiative - Building a competitive data and knowledge economy in Europe*" – finalizzata alla creazione di una economia europea basata sullo scambio dei dati e delle informazioni attraverso l'utilizzo di tecnologie come il *cloud computing*. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (COM (2016) 178 *final*).

[4] Da non trascurarsi che il GDPR sancisce come il trattamento di dati personali vada supportato da una specifica base normativa, espressamente ed, in tale sede, però più dettagliatamente individuata rispetto alla precedente normativa: segnatamente, l'art. 6 del Regolamento in questione specifica sei (6) casi in cui il trattamento de quo è da considerarsi lecito, e cioè *a)* la scontata ipotesi di previo consenso dell'interessato, seguite da altre che, al contrario, prescindono da quest'ultimo, e cioè *b)* laddove l'utilizzo in questione sia finalizzato all'adempimento di obblighi contrattuali da parte dell'interessato, *c)* nell'eventualità di trattamento da ricondurre a obblighi derivanti da legge, regolamento o normativa europea cui è soggetto il titolare del medesimo, *d)* nella necessità di salvaguardare interessi vitali della persona interessata o di terzi (possibilità, quest'ultima, di carattere residuale rispetto alle altre), *e)* nell'evenienza di tutelare interessi legittimi del titolare o di terzi cui i dati vengono comunicati

Inoltre, è da rimarcare che il GDPR amplia significativamente l'elenco di operazioni che - singolarmente o nel loro insieme, nonché compiute o meno con l'ausilio di processi automatizzati - costituiscono un trattamento di dati personali: alle tradizionali attività di raccolta, registrazione, organizzazione, conservazione, elaborazione o modifica, estrazione, consultazione, impiego, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, nonché congelamento, cancellazione o distruzione, si aggiungono, infatti, la strutturazione, l'uso e la limitazione.

Infine, nuova è la definizione di "profilazione", che si riferisce a qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di essi per valutare determinati aspetti relativi ad una persona fisica (le cc.dd. analisi predittive riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti della persona interessata).

2. Diritto all'oblio e GDPR: peculiarità originali e riflessioni critiche

Al di là di quanto sommariamente esposto, e senza volere trascurare gli indiscutibili vantaggi che, perlomeno *prima facie*, sembrano derivare a favore del singolo dall'entrata in vigore del GDPR con riguardo alla tutela del trattamento dei dati personali, il testo regolamentare in esame sembra prestare il fianco a più di un rilievo critico, e ciò sia in riferimento allo specifico contenuto di alcune disposizioni che, in prospettiva più ampia, alle autentiche finalità che ne hanno ispirato la promulgazione, nonché all'inquadramento dogmatico di istituti e principi al medesimo riconducibili.

A tal ultimo riguardo, ciò che non convince appieno rimanda, innanzitutto, ad uno dei "nuovi" diritti configurabile in capo al singolo e da ricondurre al richiamato e sempre più diffuso agire digitale nell'era di Internet: il c.d. diritto all'oblio, originariamente individuato, si rammenti, al fine di tutelare l'onore e la reputazione di colui la cui condizione attuale non

e da ritenersi prevalenti rispetto al soggetto i cui dati vengono utilizzati (a condizione, tuttavia, che non prevalgano gli interessi o i diritti fondamentali dell'interessato e che richiedono la protezione dei dati personali, in particolare se lo stesso interessato è un minore) e *f)* in ipotesi di interesse pubblico o nell'esercizio di pubblici poteri.

corrisponde più a quella che è stata in passato (e che, proprio in quanto tale, deve essere dimenticato, *rectius* deindicizzato)[5], ma che all'interno del GDPR sembra assumere, invece, differente, seppure in parte, configurazione.

In particolare, l'art. 17 del GDPR al riguardo prevede espressamente il "diritto alla cancellazione" da identificarsi con il richiamato diritto all'oblio, sovrapposizione concetto-lessicale che non pare potersi condividere, soprattutto perché quanto indicato non sembra affatto condurre ad un effettivo risultato in termini di *delisting*: segnatamente, laddove l'articolo richiamato[6] disciplina le ipotesi in cui al singolo è riconosciuta la possibilità di vedere rimosse informazioni personali che lo riguardano (e cioè, chiedere che i propri dati personali siano cancellati e non più sottoposti a trattamento ove non più necessari per le finalità per le quali sono stati precedentemente raccolti o qualora egli intenda revocare il consenso in assenza di altri motivi che prestino fondamento al trattamento stesso, oppure opporvisi, a maggior ragione qualora i dati siano stati trattati in modo illecito), non pare in realtà ricondurre a specifiche esemplificazioni di oblio, al contrario espressamente disciplinando semplicemente ipotesi di cancellazione di dati personali racchiudenti elementi di oblio, ma con quest'ultimo non pienamente coincidente.

---

[5] Al riguardo v. VALVO, *Diritti umani e realtà virtuale,* Padova, 2013, p. 170 ss..

[6] A cui fa da "naturale" compendio quanto sancito dal Considerando n. 65 del GDPR medesimo e che espressamente sancisce che "Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il «diritto all'oblio» se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria".

Assumere, cioè, a fondamento teorico della singola architettura legislativa *de qua* l'equazione cancellazione – oblio è opzione non condivisibile[7], come d'altra parte evidenziato da autorevole dottrina: "Analizzando l'art. 17 del GDPR viene naturale domandarsi che cosa vi sia di diritto all'oblio o di diritto alla deindicizzazione o, per meglio dire, che cosa possa essere utilizzato, all'interno della norma, per giustificare la "dimenticanza" forzosa di un dato personale o la sua deindicizzazione. Questo accade perché, preso nella sua interezza, l'art. 17 ricorda da vicino, e sia pure in chiave assai dilatata, il diritto alla cancellazione dei dati personali (…) di deindicizzazione, per meglio della sua finalità di (tentativo di) rendere meno agevole il recupero della informazione dalla memoria pubblica, non si fa parola (…) I presupposti che attivano la pretesa alla cancellazione si prestano a coprire aneliti di oblio; ma non vi si identificano necessariamente (…) Si obietterà che il più contiene il meno; che la cancellazione è misura più radicale del *delisting* e può comodamente assorbirla. Solo parzialmente vero, ma il senso di distacco rimane e alimenta l'impressione che si sia attuata una giustapposizione neppur troppo meditata, in cui la *new entry* normativa trascolora, senza particolari elaborazioni, nelle pieghe dei risvolti rimediali".[8]

Ancora, sembra lasciare spazio a più di una critica il Considerando n. 66 del GDPR, anch'esso relativo al diritto in questione, laddove, al fine precipuo di "rafforzare il 'diritto all'oblio' nell'ambiente online", e conseguentemente "che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali", resta tuttavia avvolto dal mistero il corrispondente onere di natura tecnologica gravante sul titolare del trattamento dei dati, in tal direzione obbligato non solo a cancellare questi ultimi (qualora in precedenza resi pubblici), ma vieppiù ad intraprendere non meglio specificate "misure ragionevoli" per informare i titolari del trattamento, che stanno trattando i dati personali, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

---

[7] *A fortiori* se riconducibile all'operato del legislatore europeo in regime di sostanziale indifferenza della decisione "pilota" in materia, e cioè quella pronunciata dalla Corte di Giustizia in relazione al caso *Consteja* (C-131/12), al contrario incentrata sulla deindicizzazione come presupposto necessario per l'oblio.

[8] Così BONAVITA – PARDOLESI, *GDPR e diritto alla cancellazione (oblio),* in *Danno e responsabilità,* 3/2018, Ipsoa.

Tali ultime disposizioni richiamate sembrano prestare il fianco ad ulteriori rilievi critici se, oltretutto, ricondotte all'attualità della sempre crescente pratica costituita dalla c.d. *big data analysis,* contraddistinta dalla capacità di raccolta e relativo studio di enormi masse di dati personali, con ciò rendendo di fatto ancora più impervio (se non financo del tutto non percorribile) l'iter teoricamente finalizzato a conseguire la totale scomparsa dal *web* di un soggetto.

3. Oggetto di tutela del GDPR: il cittadino europeo come funzione di mercato

Con ogni probabilità, le accennate criticità di cui al *Regolamento* in questione andrebbero riconsiderate all'interno di una rinnovata prospettiva, maggiormente concreta, cruda perfino, ma forse capace, in quanto rivelatrice degli autentici presupposti e finalità alla base della sua promulgazione, di svelarne la matrice essenziale.

E per far ciò, sembra senz'altro necessario rifarsi al nuovo percorso inaugurato nel 2012 dalle Istituzioni europee in materia di trattamento dei dati personali al fine specifico della creazione di un mercato unico digitale; di conseguenza, anche il GDPR, sebbene contraddistinto almeno in apparenza da una matrice umanistica in quanto contenente una disciplina relativa all'utilizzo di informazioni afferenti il singolo, deve necessariamente calarsi all'interno dell'accennata prospettiva mercantilistica, ove *naturaliter* il soggetto, ahimè, *non* ricopre (né potrebbe anche volendo) centralità alcuna.

Conferme in tal senso sembrano riscontrabili all'interno dello stesso GDPR tramite l'individuazione nell'"importanza di creare un clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno", nonché la precisazione in forza della quale "E' opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche" (Considerando n. 7).

Ulteriori conferme nell'indicata prospettiva, inoltre, sembrano potersi evincere dai Considerando n. 9, 13 e 42 del *Regolamento* in questione: il primo, riguardante le ragioni alla

base di una disciplina uniforme che ponesse fine alla frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'UE, specifica come le differenze tra diversi livelli di protezione dei diritti e delle libertà delle persone fisiche possano costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione; il secondo, individua espressamente nel buon funzionamento del mercato interno l'obiettivo alla base dell'esigenza di non limitare o vietare la libera circolazione dei dati personali all'interno dell'Unione per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali; il terzo, infine, nel richiamare in via analogica la disciplina predisposta dalla *Direttiva* 93/13/CEE[9] a favore del consumatore con riguardo alle clausole abusive dei contratti c.d. per adesione sembra avallare l'opzione ermeneutica suggerita.

Alla luce di quanto appena esposto, le reali finalità sottese all'emanazione del *Regolamento* in esame non sembrano, quindi, identificarsi con l'esigenza di assicurare un livello di protezione più elevato in favore del soggetto in sé considerato, sempre più presente nel web e a prescindere dalla sua capacità di consumo, bensì pare siano in realtà da ricondurre solo alle ipotesi in cui chi agisce *on line* pone in essere un'attività che in qualche modo possieda una valenza economica.

Conseguentemente, l'obiettivo ultimo ed autentico alla base dell'intervento normativo del legislatore europeo sembra, ancora una volta, rappresentato dalla tutela e dal rafforzamento del mercato, e dunque dalla relativa individuazione di criteri, regole e principi atti a disciplinarne il corretto e sicuro andamento, nel caso specifico per il tramite del progressivo consolidamento di un sicuro ambiente virtuale ove il soggetto possa operare senza paura.

In tale ottica, la protezione del singolo, per quanto oggetto immediato di protezione, assume una rilevanza comunque funzionale al raggiungimento dell'obiettivo testé indicato, in ultima analisi assumendo rilevanza per l'ordinamento UE le potenzialità di consumo ascrivibili all'individuo, che dunque non rileva in *re ipsa*.

Non è da trascurarsi, poi, che la raccolta di dati personali assuma rilevanza economica in sé considerata, oltre ed a prescindere, dunque, da una configurazione del soggetto come *medium*

[9] Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, (GU L 95 del 21.4.1993, pag. 29).

del mercato; ed è proprio questo il passaggio meritevole a parere di chi scrive, di attenzione specifica: l'accresciuta capacità di conservazione di dati da parte degli attuali *databases* in capo a chi esercita in Internet un'attività commerciale costituisce una fonte di nuova ricchezza, benché allo stato potenziale priva di apposita disciplina. Le competenze in materia di analisi dei suddetti dati, infatti, è innegabile come ormai rappresentino indicatori di tale rilevanza al fine di intercettare le mutevoli tendenze di mercato da assurgere ad attività autonomamente dotata di enormi capacità di profitto.

Come è stato al riguardo giustamente specificato, in sostanza, "Il dato, grazie alle modalità di trattamento ora possibili, ha aumentato esponenzialmente il proprio valore economico. Appare possibile così affermare un valore economico intrinseco del dato in quanto tale, e un valore economico relativo alle informazioni che questo dato è portatore nel momento in cui esso si palesa verso terzi, generando potenzialmente la percezione della identità di un determinato soggetto e della relativa reputazione".[10]

Si è così, dunque, in grado di individuare una nuova forma di economia, la c.d. economia della reputazione, che trova nel dato e nella relativa analisi la propria specifica ragion d'essere, ed inscindibilmente legato al diritto all'oblio, considerato che quest'ultimo "diviene così un problema legato alla percezione, all'analisi, alla persistenza e alla amplificazione di dati, posto che questi dati hanno iniziato ad acquisire un valore economico - afferente sia ai dati stessi, sia relativo alle informazioni delle quali sono portatrici – che, a detta di molti, può essere quantificato. Una questione di *data governance*, dunque, che si estrinseca nella pretesa dell'ordinamento di garantire a titolari di diritti un preciso ed efficiente controllo dei dati all'interno di sistemi di memorizzazione, un controllo tale da definire ogni sfumatura di singola operazione di trattamento".[11]

[10] Così BONAVITA, *Le ragioni dell'oblio,* in *Cyberspazio e diritto*, vol. 18, n. 57 (I-2017), pp. 94 – 95.
[11] Ancora BONAVITA, *Le ragioni dell'oblio, cit.,* p. 99.

4. Conclusioni

In conclusione, le perplessità riconducibili al *Regolamento* 2016/679 non sembrano di poco conto, soprattutto relativamente alle imprevedibili potenzialità deflagranti derivanti dall'utilizzo, dall'analisi e dalla conservazione di sconfinate quantità di dati sensibili all'interno dell'indefinito spazio virtuale costituito da Internet[12], nonché all'autentico oggetto di tutela di cui allo stesso.

Al riguardo, si aggiunga che anche il c.d. *risk based approach,* uno dei principi fondativi del GDPR, non convince appieno, perché delega di fatto all'azienda la valutazione del rischio, rendendo più difficili le contestazioni in caso di violazioni, e pone maggiore attenzione al trattamento di un grande insieme di dati, laddove è pacifico che anche il trattamento di esigue quantità di dati può comportare un danno per i singoli.

In secondo luogo, non è dato cogliere appieno l'esigenza di apprestare un'apposita disciplina normativa al fine attribuire alla protezione dei dati personali il crisma di "diritto fondamentale", considerato, intanto, che tale prerogativa di natura soggettiva possiede già tale carattere in quanto ricompresa all'interno dell'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea; inoltre, lascia alquanto perplessi quanto sancito dal Considerando n. 4 del *Regolamento* che, proprio in riferimento al diritto umano in questione, sembra capace, a quanto pare, di dare vita ad una sorta di aberrante giano bifronte giuridico di natura assoluta, ma, al tempo stesso, relativa: "Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità"[13].

Al riguardo si evidenzia che, se è innegabile come anche in tema di diritti dell'uomo sia ammissibile la ricerca di strumenti atti a conciliarne il relativo dispiegamento, d'altro canto è anche vero, però, che all'esito finale di tale operazione non può conseguire l'effetto di degradare

[12] Fenomeno cui il GDPR contrappone l'irrealistico obiettivo della minimizzazione dei dati.

[13] Per non tacer dell'incipit del medesimo Considerando n. 4 in forza del quale "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo", ma, come si è cercato di dimostrare, clamorosamente sconfessato dal contenuto di altre disposizioni del GDPR, nonché dalla propria essenziale *ratio* ispiratrice d'ispirazione mercantilistica, e dunque pienamente antitetica all'abbrivio di cui sopra, e sulla cui natura politica sembrano sussistere ben pochi dubbi.

un diritto *de quo* a diritto relativo (così come invece sembra suggerire l'infelice formulazione legislativa in esame): la natura del medesimo resta assoluta, soffrendo però al contempo di una provvisoria compressione nella propria applicabilità in forza dell'eventuale prevaricazione nel caso concreto di altro diritto fondamentale.

Oltretutto, sembra rappresentare un inestricabile paradosso individuare, perlomeno in astratto, nell'elevazione del diritto alla protezione dei dati personali delle persone fisiche la principale *ratio* ispiratrice del *Regolamento* in questione laddove è lo stesso GDPR, invece, a sancirne, proprio in forza della disposizione preliminare testé richiamata, la non assolutezza![14]

Ancora una volta, dunque, il richiamo ai diritti dell'uomo sembra più rappresentare il prodotto di un maldestro utilizzo politico degli stessi, e strumentale all'individuazione di appigli di carattere assoluto volti a legittimare l'operato del legislatore europeo, garantendo al tempo stesso il perseguimento dei reali obiettivi sottesi alle proprie iniziative.

Last but not least, neanche la tanto decantata applicazione extraterritoriale di cui si pregia il GDPR sembra in realtà andare esente da rilievi critici, non foss'altro per concretizzarsi in una sostanziale indebita violazione della discrezionalità del singolo legislatore extraeuropeo, e dunque del supremo istituto della sovranità statale: segnatamente, per quanto tale passaggio del *Regolamento* in esame, da un lato, vada a rafforzare la posizione del cittadino europeo con riguardo a transazioni commerciali concluse con soggetti aventi sede fuori dai confini dell'UE, è anche vero che tale risultato, naturalmente esclusa ogni possibilità di imposizione coercitiva, risulta però inevitabilmente condizionato all'accettazione da parte di questi ultimi, eventualità niente affatto scontata. In estrema sintesi, a tal ultimo riguardo sembra, dunque, potersi imputare al *Regolamento* in questione un ulteriore *vulnus*, nel caso specifico traducibile in un vero e proprio deficit di consenso[15].

---

[14] Perlopiù, sembra il caso di aggiungere, per il tramite di un'incongrua e goffa ridefinizione palesemente mutuata dall'ordinamento giuridico italiano: si rammenti, infatti, come l'art. 42 della nostra Costituzione espressamente investa di una funzione sociale il diritto di proprietà, scardinandone per tal via la natura essenzialmente proprietaria sancita all'interno del codice civile, ma non arrivando a negarne la peculiarità (di matrice puramente giuridica, e non anche confusamente politica come accade per la categoria dei diritti umani) dell'assolutezza come tradizionalmente intesa (e cioè, opponibilità *erga omnes*), ma solo statuendone la subordinazione rispetto a rinnovati interessi di natura pubblicistica.

[15] Ed al riguardo, in senso niente affatto casuale, è recente il parere espresso dall'Avvocato Generale della Corte di Giustizia UE Maciej Szpunar che, in sede di rinvio pregiudiziale in riferimento al caso *Google c. CNIL* (C-507/17), ha suggerito ai giudici lussemburghesi di decidere che quando Google deindicizza un contenuto in

accoglimento di una richiesta di oblio, il contenuto in questione deve divenire inaccessibile, via Google, dall'Europa ma non anche dal resto del mondo (per tal via, tra l'altro, rendendosi artefice della titanica impresa di imporre al più attuale (e controverso) diritto di origine virtuale un limite di matrice fisica).