ROMAOSSERVATORIO

**XIV ASSEMBLEA NAZIONALE DEGLI OSSERVATORI SULLA GIUSTIZIA CIVILE**

***GIUSTIZIA E DIRITTI UMANI***

**Reggio Calabria 7, 8 e 9 giugno 2019**

**GRUPPO DATA PROTECTION**

**OSSERVATORIO PER LA GIUSTIZIA CIVILE TRIBUNALE DI ROMA**

**per**

**GRUPPO EUROPA**

# la tutela dei diritti sostanziali nell'epoca dei big data

Il lavoro del gruppo ha focalizzato tre tematiche di riflessione:

1) il trattamento dei dati personali e la possibile tutela cautelare del danno per violazione della privacy.

2) il diritto all'oblio con riferimento all'introduzione dell'art. 17 del Reg. 676/2016 ed agli sviluppi giurisprudenziali più recenti;

3) le novità normative in tema di *blockchain* e registri distribuiti anche in riferimento alla compatibilità con il diritto all'oblio.

## Premessa

Il documento conclusivo dell'ultima Assemblea Nazionale degli Osservatori, tenutasi a Reggio Emilia ( 2018 ) è stato predisposto contemporaneamente all'entrata in vigore del Regolamento UE 676/2016 ( 25.5.2018 ) ed in attesa della emanazione del decreto legislativo per l'adeguamento della normativa nazionale: il Dlgs 101/2018, entrato in vigore dal 19.9.2018, ha modificato le disposizione del Dlgs 196/2003 ( Codice della Privacy) prevedendo una disciplina transitoria per regolare i procedimenti e gli affari pendenti, riordinare le autorizzazioni generali del Garante Privacy ed orientare l'azione sanzionatoria dell'Autorità.

Tale documento – al quale il presente contributo intende riallacciarsi – conteneva la diffusa convinzione che il nuovo Regolamento UE non costituisse una vera e propria rivoluzione, ma rappresentasse soltanto una evoluzione di quanto già previsto nel nostro codice della privacy.

E, a distanza di circa un anno dall'entrata in vigore, tempo trascorso simultaneamente alla galoppante evoluzione dell'invasione tecnologica, tale convinzione non può che essere confermata in quanto gli eventi quotidiani riferibili alle incursioni che ciascuno subisce, quanto meno attraverso una non richiesta profilatura dei propri dati personali – rilevabili attraverso la raccolta di dati relativi a tutte le nostre attività quotidiane ( acquisti di qualsiasi natura, consultazione dei siti di ogni genere, viaggi, pagamenti on line, bonifici bancari etc) – consente di ritenere che le tutele previste dal Regolamento non siano sufficienti per fronteggiare il potere degli algoritmi e che, quanto meno, esse debbano essere continuamente aggiornate per una concreta difesa dall'utilizzo spregiudicato della tecnologia.

**1) Sul primo tema.**

## Il trattamento dei dati personali e la possibile tutela cautelare del danno per violazione della privacy.

- Formalmente i rischi per chi pone in essere i trattamenti di dati personali senza rispettare il regolamento sono elevati.

Innanzitutto sono previste pesanti sanzioni amministrative.

Inoltre, l'interessato i cui dati sono stati trattati in modo illecito può chiedere un risarcimento danno.

Il GDPR prevede la responsabilità solidale tra il titolare del trattamento ed il responsabile del trattamento.

Il GDPR prevede che le azioni legali per l'esercizio del diritto al risarcimento del danno devono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

Il sistema di tutela della protezione dei dati personali è fondato su un duplice binario: l'attività amministrativa delle autorità garanti, che lo esplicano attraverso il sistema di sanzioni amministrative, di sanzioni penali ed attraverso la tutela indiretta in via amministrativa dei diritti degli interessati; il sistema basato sul risarcimento del danno al privato derivante dall'art. 82.

Il reclamo in via amministrativa è attualmente il mezzo di tutela preferito, sia perchè è gratuito, sia perchè i tempi di definizione del procedimento sono

accettabili. La tutela è indiretta ed è realizzata attraverso il sistema dissuasivo delle pesanti sanzioni che il Garante può applicare.

Ma tutto ciò non realizza il ristoro del danno in capo all'interessato, per ottenere il quale non vi è che il ricorso al giudice ordinario.

- Ma il più delle volte la difficoltà o l'impossibilità di provare il *quantum debeatur*, i costi di accesso alla giustizia e quelli per la difesa tecnica, hanno come effetto quello di non rendere conveniente il ricorso al giudice ordinario.

Peraltro, l'art. 79, co. 2 del GDPR ha previsto che lo stato membro debba assicurare all'interessato il diritto di proporre un ricorso giurisdizionale effettivo e la previsione è stata attuata attraverso le nuove disposizioni processuali , contenute nell'art. 17 del d.lgs. 101/2018, modificativo dell'articolo 10 del decreto legislativo 1° settembre 2011 n. 150 (c.d. semplificazione dei riti), il quale prevede che: "tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo Regolamento, sono attribuite all'autorità giudiziaria ordinaria".

- Nonostante il d.lgs. 101/2018 abbia abrogato l'art. 15 d.lgs. 196/2003 in base al quale il legislatore aveva previsto che "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile", si può affermare che la responsabilità per violazione della privacy continua ad ispirarsi al modello della responsabilità per esercizio di attività pericolosa di cui all'art. 2050 cod. civ., in quanto l'art. 82 del GDPR prevede che: "chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del

trattamento. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2, se dimostra che l'evento dannoso non gli è in alcun modo imputabile".

- Per quanto riguarda il rito applicabile, sia per i ricorsi avverso i provvedimenti emessi dall'autorità garante, che per i ricorsi aventi ad oggetto le controversie in materia di privacy, è previsto che: "le controversie previste dall'articolo 152 del decreto legislativo 30 giugno 2003, n. 196, sono regolate dal rito del lavoro, ove non diversamente disposto dal presente articolo" e sono decise dal Tribunale in composizione monocratica con sentenza non appellabile, ricorribile solo per cassazione.

- La limitata portata del comma 7 dell'art. 17 cit. il quale prevede che "l'efficacia esecutiva del provvedimento impugnato può essere prevista secondo quanto previsto dall'articolo 5", non può limitare l'ambito della tutela cautelare di cui dispone il giudice civile in virtù dell'art. 700 c.p.c. e quindi ben potrà il giudice civile adottare tutti i provvedimenti ritenuti necessari all'eliminazione del fatto illecito, ivi compreso l'oscuramento, la rimozione o il blocco di qualsiasi dato personale diffuso nella rete internet, ovvero detenuto e/o trattato illecitamente.

Il comma 9 dell'art. 17 cit. prevede che anche se non sia parte in giudizio, il Garante possa presentare osservazioni nella controversia in corso ed a tal fine è previsto che: "il giudice dispone che sia data comunicazione al Garante circa la pendenza della controversia, trasmettendo copia degli atti introduttivi, al fine di consentire l'eventuale presentazione delle osservazioni".

- Inoltre, si segnala che il d.lgs. 101/2018 ha riconosciuto al Garante un proprio potere di agire e di rappresentanza in giudizio.

Invero, in base all'art. 154-ter del Codice Privacy, "il Garante è legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali".

In questi casi, il Garante è rappresentato in giudizio dall'Avvocatura dello Stato, salvo nei casi di conflitto di interesse, allorché il Garante, sentito l'Avvocato generale dello Stato, può stare in giudizio tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero

avvocati del libero foro.

- Come esempio di un sollecito e puntuale intervento del Garante si può richiamare il provvedimento n. 11 del 17.1.2019, con il quale il Garante ha ordinato la rimozione di un URL a Google riconoscendo la violazione del diritto all'oblio del richiedente.

- La tutela cautelare, rispetto alla velocità impressa alla diffusione delle notizie dalla tecnologia informatica, risulta lo strumento più adatto a fornire una risposta tempestiva che tuttavia non sempre risulta utile e, quindi, efficace.

Il provvedimento cautelare, infatti, non sempre è idoneo a fornire una adeguata protezione rispetto all'uso dei dati da parte dei social networks, alle profilazioni e geolocalizzazioni personali ai fini della sollecitazione al consumo di beni o servizi, alle attività di marketing aggressivo dei call center o, peggio ancora, alle attività degli hacker che, violando sistemi di sicurezza risibili, carpiscono e diffondono dati di terzi detenuti su piattaforme in *outsourcing* (mi riferisco al recente caso di violazione delle Pec degli avvocati).

L'applicazione dei principi di gestione del diritto alla privacy di cui al GDPR diviene molto problematica con riferimento ai *social networks*, l'accesso ai quali, costringe gli utenti a rinunciare a questi diritti, in ragione dell'adesione ed accettazione alle condizioni di uso del sito, senza le quali non si può di fatto accedere ad esso ed impone il rilascio di tutta una serie di autorizzazioni, sia per la condivisione dei contenuti creati dall'utente, che per i dati personali immessi nel sito.

- Nessuno controlla o può cambiare questi consensi in favore dell'utente.

Parimenti non esiste un sistema efficace di controlli da parte del Garante i cui poteri sono sostanzialmente limitati ad impartire sanzioni: nel 2018, anche se in misura doppia rispetto ai dodici mesi precedenti (+115%) le ispezioni effettuate risultano limitate a 150 su scala nazionale e rivolte principalmente ai trattamenti dagli istituti di credito, da società per attività di rating sul rischio e sulla solvibilità delle imprese, dalle aziende sanitarie locali e poi trasferiti a terzi per il loro utilizzo a fini di ricerca, da società che svolgono attività di telemarketing, da quelle che offrono servizi di «money transfer», oltre ai trattamenti di dati svolti da società assicuratrici attraverso l'installazione di

«scatole nere» a bordo degli autoveicoli e da società che offrono servizi medico-sanitari tramite app; per quanto riguarda il pubblico, l'attività di verifica si è concentrata su enti svolgenti trattamenti di dati personali mediante app per smartphone e tablet, con particolare attenzione all'eventuale profilazione e geolocalizzazione degli utenti, sulle grandi banche dati, sul sistema della fiscalità, con speciale riguardo alle misure di sicurezza e al sistema degli audit, sul sistema informativo dell'Istat e sullo Spid.

Sempre da dati diffusi dal Garante sembra che lo stesso abbia fornito riscontro a oltre 5.600 quesiti, reclami e segnalazioni in materia di: marketing telefonico e cartaceo; centrali rischi; credito al consumo; videosorveglianza; concessionari di pubblico servizio; recupero crediti; settore bancario e finanziario; assicurazioni; lavoro; enti locali; sanità e servizi di assistenza sociale.

- Il numero, apparentemente elevato di riscontri, esce ridimensionato da un confronto con il numero di soggetti coinvolti nei *big data* che risultano pari alla quasi totalità degli utenti: chi non ha mai ricevuto almeno una telefonata da un call center che offriva nuove stipulazioni commerciali di servizi ?

Ma anche per la tutela dei minori sembra che si sia solo riusciti a relazionare in merito ai pericoli relativi ai possibili rischi insiti nell'uso indiscriminato dei dati personali sui social network, degli smartphone e negli smart toys.

Per il cyberbullismo il Garante ha predisposto misure ed indicazioni per la rimozione dei contenuti offensivi, così come sono stati sollecitati controlli sulle fake news, sulla geolocalizzazione personale necessaria per l'uso di alcune applicazioni (prima fra tutte Google Maps) che consente però la memorizzazione e quindi lo screening sulle abitudini delle persone al fine di propinare la fruizione di beni o servizi e sull'uso sui social.

Anche la memorizzazione delle impronte digitali dei dipendenti, fenomeno in continua crescita per evitare il falso badge, si presta a perpetrare abusi.

- Il Garante ha fornito anche indicazioni sull'uso dei droni a scopo ricreativo e su come difendersi dai software dannosi, tipo il ransomware, un programma che ha lo scopo di bloccare pc, tablet, smartphone o smart tv, ovvero di impedirne l'accesso per chiedere un riscatto.

Su tutti questi argomenti che sono stati sollevati dalla Authority, vi può essere una violazione dei diritti ed un concreto interesse ad agire in giudizio in via cautelare, anche se, nella realtà, si preferisce il ricorso amministrativo o quantomeno la denuncia al Garante per ottenere una tutela indiretta e gratuita.

- Il ricorso giurisdizionale è percepito dagli stessi operatori del diritto e dagli interessati come rischioso per gli alti costi e gli incerti risultati :la fase dell'esecuzione del cautelare o del merito merita la maggiore attenzione e presenta i maggiori rischi di "ineseguito", atteso che nella maggior parte dei casi i dati sono delocalizzati spesso all'estero, sotto giurisdizioni non trasparenti e non collaboranti.

- In definitiva, la tutela cautelare della privacy sconta le medesime problematiche degli utenti di accesso al servizio "giustizia": costi elevati (parcella degli avvocati e spese di giustizia), tempi di soluzione incerti e indeterminati, esito applicativo incerto in merito alla concreta esecuzione del provvedimento inibitorio.

## B) Sul secondo tema

## Il diritto all'oblio con riferimento all'introduzione dell'art. 17 del Reg. 676/2016 [1]ed agli sviluppi giurisprudenziali più recenti.

[1] L'articolo 17 GDPR – Diritto alla cancellazione («diritto all'oblio») dispone:
1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, 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.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale 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 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;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

[2] Tali principi sono stati individuati come segue: 1) il contributo arrecato dalla diffusione dell'immagine o della notizia ad un dibattito di interesse pubblico; 2) l'interesse effettivo ed attuale alla diffusione dell'immagine o della notizia (per ragioni di giustizia, di polizia o di tutela dei diritti e delle libertà altrui, ovvero per scopi scientifici, didattici o culturali), da reputarsi mancante in caso di prevalenza di un interesse divulgativo o, peggio, meramente economico o commerciale del soggetto che diffonde la notizia o l'immagine; 3) l'elevato grado di notorietà del soggetto rappresentato, per la peculiare posizione rivestita nella vita pubblica e, segnatamente, nella realtà economica o politica del Paese; 4) le modalità impiegate per ottenere e nel dare l'informazione, che deve essere veritiera (poiché attinta da fonti affidabili, e con un diligente lavoro di ricerca), diffusa con modalità non eccedenti lo scopo informativo, nell'interesse del pubblico, e scevra da insinuazioni o considerazioni personali, sì da evidenziare un esclusivo interesse oggettivo alla nuova diffusione; 5) la preventiva informazione circa la pubblicazione o trasmissione della notizia o dell'immagine a distanza di tempo, in modo da consentire all'interessato il diritto di replica prima della sua divulgazione al grande pubblico. ( cfr. Cass. 6919/2018)

[3] La S.C. ha precisato che "se è vero che l'art. 20, comma 3, cod. amm. digitale prevede che la data e l'ora del documento informatico sono opponibili ai terzi solo «se apposte in conformità alle regole tecniche sulla validazione temporale», è anche vero che l'accreditamento e la conseguente iscrizione della società certificatrice nell'apposito elenco pubblico tenuto dal CNIPA, ai sensi dell'art. 29 cod. cit. (nel testo, qui applicabile ratione temporis, anteriore alle modifiche introdotte con il d.lgs. 26 agosto 2016, n. 179) comporta necessariamente una presunzione di conformità della sua attività a dette regole - che, ai sensi del comma 2 del predetto articolo, chi richieda l'accreditamento deve impegnarsi a rispettare - in ciò risiedendo appunto l'utilità di un accreditamento da parte della pubblica autorità. Conseguentemente, è onere di chi intenda contestare che una certificazione sia avvenuta nel rispetto delle regole tecniche, allegare e provare che il certificatore non le abbia invece rispettate"
[4] Questo sistema garantisce un'estrema trasparenza delle operazioni e l'eliminazione degli intermediari e garantisce la certezza dei dati ivi contenuti. Difatti, una volta validato il blocco e scorsa la catena, l'eventuale manipolazione del dato archiviato richiederebbe una capacità informatica inesigibile, oltre al fatto che non potrebbe incidersi su una piattaforma diffusa in cui tutti sono proprietari del dato originale.
Nella blockchain operano gli smart contract, che non sono veri e propri contratti, ma protocolli di transazione computerizzati che eseguono i termini di un contratto. Attraverso gli smart contract le parti stabiliscono che al verificarsi di un evento si verificherà la conseguenza direttamente collegata dal programma: tutto secondo l'algoritmo if-then.
Una volta lanciato il programma di esecuzione le parti non potranno più annullare l'operazione o modificarla all'interno del medesimo blocco, sicché al verificarsi del fatto if partirà la reazione then, senza alcuna ulteriore valutazione.

- Il regolamento Europeo ha legittimato, codificandolo, il diritto all'oblio, frutto di una pregressa e progressiva elaborazione dottrinaria e giurisprudenziale che va oltre la tutela della privacy (in Italia assumono rilevanza alcune decisioni della Corte di Cassazione come Cass. 9/4/1998, n. 3679; Cass., 25/6/2004, n. 11864; Cass., 05/04/2012, n. 5525; Cass. 26/06/2013, n. 16111; Cass. 24/06/2016, n. 13161) mirando a salvaguardare il riserbo imposto dal tempo ad un notizia già resa di dominio pubblico.

Come fondamento normativo del diritto all'oblio, il Codice della Privacy prevedeva l'illegittimità del trattamento qualora i dati fossero conservati in una forma tale da consentire l'identificazione dell'interessato per un periodo di tempo superiore a quello necessario agli scopi per i quali sono stati raccolti o

---

In sostanza, una volta lanciato il programma non vi sarà più possibilità di intervenire sull'operazione demandata.
I vantaggi sono evidenti: oltre alla potenziale riduzione delle frodi on line, data l'immutabilità dello smart contract una volta lanciato, anche la necessaria chiarezza del testo contrattuale elettronico e la impossibilità di violazione delle obbligazioni assunte potrebbe rendere superflua la normativa sulla patologia del contratto quali quella sulle clausole penali.
Uno dei limiti degli smart contract viene individuato nella loro struttura rigida ed immodificabile, per cui, una volta lanciati, non possono essere più arrestati con evidenti conseguenze in tema di inadempimento e di autotutela contrattuale.

[5] Un discorso analogo deve essere svolto in merito al principio sotteso alla "privacy by design". L'articolo 25 del GDPR 2018, introduce il principio Privacy by Design e by Default, e cioè "la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita". Si tratta di un obbligo generale e prescrive: "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso*" il Titolare del trattamento dei dati "*mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*".
Nell'ambito del Privacy by Design e by Default, dunque, il titolare del trattamento deve assicurarsi di mettere in atto "*misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento*". In tal senso "*tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità*. Ciò significa che tali "*misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*". In questo ambito, il testo prevede infine un meccanismo di certificazione che "*può essere utilizzato come elemento per dimostrare la conformità ai requisiti*" sopra citati.

trattati (art. 11 d.lgs. n. 196/2003).
Era previsto che lo stesso interessato avesse il diritto di conoscere in ogni momento chi possedeva i suoi dati personali, le modalità di utilizzo, con facoltà di opporsi al trattamento dei medesimi, ancorché pertinenti allo scopo della raccolta, ovvero di ingerirsi al riguardo, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione (art. 7 d.lgs. n. 196/2003).
- Il diritto all'oblio si colloca, quindi, nel quadro dei diritti della personalità come una particolare forma di garanzia connaturata al diritto alla riservatezza e si distingue dal diritto all'identità personale che può essere definito come l'interesse di ogni persona a non vedere travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, professionale causa dell'attribuzione di idee, opinioni, o comportamenti differenti da quelli che l'interessato ritenga propri e abbia manifestato nella vita di relazione.
- Il diritto all'identità personale è relativo alla tutela dell'immagine pubblica della persona, o comunque dell'immagine di sé che il soggetto intende proiettare nel mercato delle relazioni sociali (intendendo immagine in senso metaforico), mentre il diritto all'oblio attiene alla protezione di una sfera intangibile di intimità e riservatezza dell'individuo, da mettere al riparo da intrusioni altrui. Quest'ultimo è stato invocato da parte di soggetti che, dopo aver conosciuto momenti di sovraesposizione mediatica, essendo stati protagonisti – talvolta loro malgrado – di fatti eclatanti, episodi di cronaca nera, e così via, sono stati successivamente "riscoperti" dai media (inchieste giornalistiche, documentari, film-verità, ecc.) e riportati così all'attenzione del pubblico.
- Si tratta quindi del diritto dell'individuo a non veder "risuscitare", e proiettare agli occhi del pubblico, una propria identità ormai appartenente al passato, e che magari si è cercato faticosamente di emendare.
Nonostante la stretta contiguità tra riservatezza e oblio, i due concetti però non coincidono.
Il diritto all'oblio può essere considerato in qualche misura speculare rispetto al diritto alla riservatezza, dal momento che il primo si pone relativamente a

situazioni che, per loro natura, nel momento in cui si sono verificate, non rientravano nell'ambito della tutela della riservatezza.

- Il tempo è in ogni caso il fattore che consente di distinguere i due concetti. Richiamandosi al diritto all'oblio s'intende, infatti, impedire che la notizia già pubblicizzata, resa nota, sfuggita alla sfera privata del soggetto, venga pubblicizzata nuovamente a distanza di un considerevole lasso di tempo.

Il diritto all'oblio tuttavia non è rivolto a cancellare il passato, ma a proteggere il presente, a preservare il riserbo e la pace che il soggetto abbia ritrovato: è il diritto di un soggetto a vedersi "dimenticato" dalle banche dati, dai mezzi di informazione, dai motori di ricerca che detengono i suoi dati in relazione ad un'attività di trattamento che sono autorizzati a compiere dal diretto interessato o dalla legge; postula, sempre, nei casi affrontati, un bilanciamento fra il diritto alla riservatezza del singolo ed diritto all'informazione della collettività, attraverso il diritto di cronaca di coloro che diffondono la notizia.

- Il casi più noti affrontati dalla giurisprudenza della Corte di Cassazione prima dell'entrata in vigore dell'art. 17 GDPR ( Cass. 1611/2013, caso di un affiliato di un'organizzazione terroristica contro una testa giornalistica; Cass. 19761/2017 caso di un amministratore di società fallita contro la Camera di Commercio; Cass. 6919/2018 caso di un noto cantautore italiano contro la RAI) si sono misurati con il problema del bilanciamento degli interessi facendo prevalere quello individuale su quello collettivo a seconda della rilevanza del valore da proteggere.

- Assume particolare rilievo, al riguardo, il principio pronunciato a seguito di rimessione della questione alla Corte di giustizia (CdG C-398/2015 sentenza del 9.3.2017) che ha valorizzato, nel caso concreto, l'interesse pubblico posto a base della pubblicazione delle informazioni riguardanti la figura del ricorrente come amministratore di una società fallita, ritenendo che "alla stregua del quadro normativo e dei compiti istituzionali perseguiti dalle Camere di Commercio con la tenuta del registro delle imprese, è legittima, rispondendo ad un obbligo legale, l'iscrizione e la conservazione nel registro stesso delle informazioni relative alla carica di amministratore e di liquidatore, ricoperta da un soggetto di una società ove pure in séguito questa sia stata dapprima

dichiarata fallita e, poi, cancellata dal registro delle imprese, prevalendo le esigenze della pubblicità commerciale sull'interesse del privato ad impedirla, in funzione delle ragioni di certezza nelle relazioni commerciali che l'istituzione del registro delle imprese soddisfa" ( Cass. 19721/2017) .

- Inoltre Cass. 6919/2018 contiene una indicazione esemplificativa dei principi da seguire per il bilanciamento degli interessi[2] - affermando che in assenza di tali presupposti, la pubblicazione di una informazione concernente una persona determinata, a distanza di tempo da fatti ed avvenimenti che la riguardano, non può che integrare la violazione del fondamentale diritto all'oblio, come configurato dalle disposizioni normative e dai principi giurisprudenziali suesposti – indicazione alla quale si è riferita anche la recentissima ordinanza di rimessione alle sezioni unite ( Cass. 28084/2018 ) che ha posto la specifica questione concernente la possibile alternatività o la necessaria concorrenza di tali presupposti.

- L'udienza delle Sezioni Unite al momento della stesura di questo documento non è ancora stata celebrata ma certamente la risposta meriterà attenzione soprattutto da parte dei giudici di merito che hanno il compito di valutare il bilanciamento dei valori in gioco.

- Ma, tanto premesso, l'esame della fattispecie "prima del Regolamento UE" non può essere conclusa senza un cenno alla più famosa pronuncia della Corte di Giustizia che riguarda il caso Costeja vs Google Spain, Google Inc e La Vanguardia ( CdG 13.5.2014, C -131/12 ) ,che si è misurata con la questione del bilanciamento degli interessi nell'era della *Big Data.*

E' stato infatti affermato dalla Corte di Giustizia, rispetto alla richiesta di cancellazione dei dati di un soggetto a suo tempo esecutato, contenuti nel motore di ricerca del gruppo Google (Google Search), utilizzati da un quotidiano spagnolo sul quale figurava un annuncio, menzionante il suo nome, per una vendita all'asta di immobili connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali, che "gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione

in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato.

- Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi."

- Tale pronuncia ha avuto un grande impatto sul mondo giuridico soprattutto in relazione alla dematerializzazione delle informazioni ed alla possibilità che, al di fuori di meri enunciati, possa effettivamente realizzarsi una tutela efficace della riservatezza.

Infatti, tenuto conto della indefinita dislocazione degli archivi informatici di Google, ci si chiede se la cancellazione dei dati rilevanti dagli archivi di Google Spain ( Agenzia spagnola di Google Search ) consenta di ritenere che essi siano stati definitivamente eliminati anche dai registri statunitensi di Google Inc., anche in ragione della non vincolatività della regolamentazione europea negli altri continenti.

Ciò induce a ritenere che la dematerializzazione delle informazioni e degli archivi renda illusoria una effettiva tutela del diritto all'oblio, nonostante la sua codificazione nel Regolamento Europeo.

**C) Sul terzo tema: le novità normative in tema di blockchain e registri distribuiti anche in riferimento alla compatibilità con il diritto all'oblio.**

- Dal 13.2.2019 è entrato in vigore l'art. 8-ter d.l. 135/2018 come convertito che dispone:

*1. Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili.*

*2. Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.*

*3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014del Parlamento europeo e del Consiglio, del 23 luglio 2014.*

*4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3*.

- L'Italia, in Europa, è il primo Paese a disciplinare le "Tecnologie basate su registri distribuiti e smart contract" in coerenza con l'ordinamento comunitario.

L'art. 8 ter sopra riportato riconosce gli effetti della validazione temporale elettronica di cui all'art. 41 del regolamento eIDAS (Regolamento (UE) n. 910/2014) ai documenti informatici memorizzati sulla block chain.

L'art. 41 del Regolamento del 23/07/2014 - N. 910 (Gazzetta Uff. 28/08/2014 n. 257) dispone:

*1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.*

*2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.*

*3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.*

- Questo significa ottenere una "certificazione" della data ed ora di esistenza di un'evidenza informatica in un dato momento.

La validazione temporanea elettronica svolge la funzione tipica dei registri, che appunto consentono di documentare un determinato fatto in un certo istante di tempo: per esempio, il pubblico registro automobilistico, i registri catastali, il registro delle imprese.

Con riferimento alla data certa elettronica associata ad un documento informatico mediante marca temporale emessa da un certificatore accreditato, la Cassazione ha affermato il principio di **presunzione della conformità** della marca temporale, in quanto emessa per l'appunto da un certificatore che ha ottenuto l'accreditamento.

- E' stato ribadito anche il **principio di diritto secondo cui** "***è onere della parte interessata a negare la certezza della data*** *– e dunque, nel giudizio di opposizione a stato passivo, è onere del curatore fallimentare –* ***allegare e provare la violazione delle regole tecniche sulla validazione temporale"*** (Cass. 12939/17 [3]).

La fattispecie riguardava una domanda di ammissione allo stato passivo di un fallimento avente ad oggetto il credito derivante da contratto di leasing digitalizzato. La scrittura privata era stata formata in modalità digitale (**contratto di leasing digitalizzato**) ed il requisito della data certa risultava

dalla **marca temporale** apposta in sede di digitalizzazione ed emessa da un **certificatore accreditato** presso l'Agenzia per l'Italia Digitale.

- La *blockchain* è una tecnologia che consente ad ogni cittadino di poter soddisfare in maniera semplice e rapida l'esigenza di provare i propri diritti: si pensi al diritto d'autore, che sorge nel momento della creazione di un'opera, e la cui registrazione presso gli enti ha il solo scopo di dimostrare l'anteriorità della creazione; in tale ipotesi la memorizzazione dell'opera sulla DLT (Distributed Ledger Technology) ha proprio l'effetto di rendere opponibile a terzi la data ed ora di creazione dell'opera stessa, così tutelando l'autore.
- Si pensi anche a tutti i documenti che normalmente vengono creati, che potranno essere registrati su una blockchain e la loro data ed ora di esistenza potrà così essere opposta a chiunque.
- La blockchain è una piattaforma decentralizzata per l'archiviazione dei dati, che elimina la necessità di intermediari per la conclusione dei rapporti di scambio.

Ogni operazione di archiviazione o di scambio forma un blocco della catena, su cui si innestano i blocchi di tutti gli altri operatori che accedono alla piattaforma.

Secondaria, per ciò che qui interessa, la questione relativa alla valuta virtuale prevista per le transazioni ( *bitcoin*), appare invece di fondamentale rilievo che le operazioni sono validate dagli stessi soggetti che accedono al registro condiviso e che , una volta validati, i blocchi sono archiviati nella blockchain e superati dai successivi blocchi della catena, che rendono impossibile annullare o modificare quelli precedenti.

- In ciascun blocco può accedere esclusivamente il titolare (o il titolato ) dei dati in esso inseriti e successivamente criptati, attraverso una impronta ( hash ) personale.[4]

## ***Blockchain*** **e diritto alla cancellazione dei dati.**

- La caratteristica di "immutabilità" di una *blockchain* può inoltre far ritenere che tale tecnologia non consentirebbe di esercitare il "diritto alla cancellazione

dei dati" riconosciuto nel GDPR a tutti gli interessati.

- È necessario ricordare che il "diritto alla cancellazione dei dati" di cui all'art. 17 GDPR prevede due differenti prerogative:

a. il diritto alla cancellazione dei dati da parte del titolare del trattamento;

b. il diritto all'oblio vero e proprio, ossia il diritto dell'interessato ad ottenere la cancellazione dei dati che lo riguardano ove "i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati" lettera (a).

- Ciò detto, bisognerebbe innanzitutto chiarire se effettivamente l'interessato che abbia utilizzato un servizio basato su *blockchain* possa esercitare il diritto alla cancellazione sulla base di uno dei motivi indicati dalle lettere da a) ad f) del primo comma dell'art. 17. Ogni dato inserito in una *blockchain* è in verità necessario per mantenere la "catena" di transazioni relative alla medesima "informazione digitale", funzione che caratterizza la *blockchain* rispetto alle altre tecnologie.

- Nella *blockchain* è evidente che il titolare richiesto della cancellazione dei dati (poniamo un *exchange*) non potrà sicuramente informare tutti gli altri titolari registrando la richiesta di cancellazione dell'interessato sulla medesima *blockchain* (unico modo per essere certi che l'informazione sia diffusa verso tutti coloro che la utilizzano), altrimenti si avrebbe il paradossale effetto di registrare (in maniera immutabile) un'informazione che invece deve essere cancellata. Neanche si può ritenere, proprio in considerazione della tecnologia disponibile e dei costi di attuazione, che la comunicazione dell'esercizio del diritto all'oblio venga diffusa, con altri mezzi, a soggetti che il titolare neanche conosce, né che possa darne comunicazione con altre forme "di pubblicità".[5]

- Si pone dunque il problema del rapporto fra blockchain e GDPR e le tutele che possono apprestarsi in relazione all'anonimato.

Alcune soluzioni sono state ideate proprio al fine di assicurare una maggiore protezione dei dati personali (rispetto l'originaria *blockchain* Bitcoin) in modo da rendere non identificabile il soggetto che effettua la transazione.

Alcune di queste prescindono dall'implementazione di nuove funzionalità, e si

basano su semplici strategie quali l'utilizzo di "*one-time accounts*", ossia l'utilizzo di una diversa coppia di chiavi per ciascuna transazione da parte del medesimo soggetto.

- Un sistema del genere, insieme alla *zero-knowledge proof*, è stata implementata nella blockchain di Zcash, che mira a garantire il completo anonimato delle transazioni.

Altri progetti si basano su sistemi più complessi, come ad esempio quello previsto dal sistema Enigma per cui le transazioni sono validate tramite un meccanismo di *multi-party computation* (che richiede che un dato insieme di risorse collaborino tra loro per poter rendere imputabile una transazione rendendola, quindi, non più imputabile ad una singola risorsa) o soluzioni quali le *ring signatures*, con cui viene dimostrato che il firmatario detiene la chiave privata corrispondente ad un determinato set di chiavi pubbliche, senza però indicarne una specifica (così rendendola non più identificabile).

## Conclusioni

In conclusione, l'ambito applicativo delle nuove tecnologie, che sono espressione dell'intelligenza artificiale, è in costante evoluzione e, di conseguenza, rimane tutt'ora aperta la questione relativa all'effettività della tutela del diritto alla privacy dei soggetti che accedono ai servizi fondati su registri distribuiti, ai limiti della responsabilità del titolare e del responsabile del trattamento nonché ai nuovi ambiti della giurisdizione.

**OSSERVATORIO PER LA GIUSTIZIA CIVILE TRIBUNALE DI ROMA**
**GRUPPO DATA PROTECTION**

Contributo a cura del coordinatore Cons. Antonella Di Florio, con riferimento ai documenti predisposti dalla dott.ssa Simona Sansa e dall'avv.to Fernando Tota ed ai contributi dei componenti del gruppo avv.to Doriana Chianese, avv.to Agostino Clemente ed Avv.to Alessandro Graziani.