X CONVEGNO ANNUALE

DNT® DIRITTO NUOVE TECNOLOGIE
CENTRO STUDI PER L'INNOVAZIONE

Trattamento dei dati personali, persona, mercato nel GDPR: gestione del rischio correlato tra responsabilizzazione e responsabilità

Prof. Avv. Emilio Tosi – Università di Milano Bicocca
Direttore Centro Studi Diritto Nuove Tecnologie®

RELAZIONE DI APERTURA DEL X CONVEGNO ANNUALE DNT®

Premessa

E' ormai passato oltre un triennio dal 25 maggio 2018 data di piena applicazione del *Regolamento Generale per la Protezione dei Dati Personali*, Regolamento UE 27 aprile 2016, n. 679, meglio conosciuto, considerata la vocazione transnazionale quale *legal benchmark* globale in tale settore, come *General Data Protection Regulation* (di seguito, per brevità, GDPR).

Un tempo adeguato per un primo bilancio applicativo e qualche riflessione.

Tra i profili maggiormente significativi si ritiene di particolare interesse approfondire le nuove regole introdotte dal GDPR sotto il profilo della responsabilizzazione *ex ante* ossia prima di iniziare l'attività di trattamento dei dati e di responsabilità ex post ossia successivamente al trattamento dei dati in caso di deviazioni rispetto al modello conformativo delineato dal GDPR.

Il tema in parola è denso di implicazioni giuridiche che oggi cercheremo di illustrare adeguatamente con il prezioso contributo del Garante per la Protezione dei Dati Personali e degli autorevoli partecipanti alla Tavola Rotonda.

Il Convegno odierno s'inserisce nel quadro dei periodici incontri scientifici annuali del **Centro Studi Diritto Nuove Tecnologie®** che, sin dall'ormai lontano 2003, è attivamente impegnato nello studio sistematico delle interferenze tra diritto, in particolare diritto privato, e nuove tecnologie digitali, come testimoniato concretamente anche dalla pubblicazione del ventitreesimo volume "***Diritto Privato delle Nuove Tecnologie Digitali***", dell'omonima Collana internazionale di studi giuridici che oggi si presenta.

Il GDPR esprime la propria innovativa forza regolatoria proprio facendo leva sul doppio livello di responsabilizzazione preventiva e responsabilità successiva correlati al trattamento dei dati personali in un contesto digitale globale in cui si registra la tensione evidente tra **persona e mercato**, tra istanze di tutela diritti fondamentali – protetti, innanzitutto, dall'art. 2 della

nostra Costituzione oltre che dal GDPR e dalla *Carta dei diritti fondamentali della UE* – e le esigenze contrapposte dei mercati digitali di sfruttamento commerciale dei dati personali.

Già dalla lettura del primo considerando, il GDPR prende chiaramente posizioni in tali termini qualificatori: "*La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale*".

Dati personali nella società digitale della sorveglianza

La tutela della persona, la protezione dei dati personali e la disciplina della responsabilità per trattamento illecito dei dati sono temi centrali nel contesto socio-economico del ***capitalismo digitale della sorveglianza*** per usare la suggestiva definizione elaborata da *Soshana* ZUBOFF.

Il fenomeno della digitalizzazione è *disruptive* — dirompente — e pervasivo, nella vita personale di tutti noi e nel mondo produttivo: si fonda, in estrema sintesi, sull'utilizzo intensivo e sistematico di dati — grandi quantità di dati i c.d. *big data* — elaborati attraverso sofisticati algoritmi e *artificial intelligence.* Non a caso una definizione ricorrente è quella di *economia della conoscenza.*

Ma si badi bene: non economia della conoscenza in genere, ***economia della conoscenza dei nostri dati personali.***

La pervasività dei trattamenti si incontra con la pericolosa concentrazione di potere economico, informativo e tecnologico nelle poche mani dei *signori della rete* noti conglomerati societari globali: *Facebook, Amazon, Google, Apple, Microsoft (c.d.* FAGAM) per citare i principali colossi digitali globali.

I *gatekeeper* sistemici che anche nella recente proposta di riforma della Commissione Europea (**Digital Services Act - DSA e Digital Markets Act - DMA**) si cerca di disciplinare per ristabilire trasparenza, correttezza ed equità nei mercati digitali tentando attraverso l'azione regolatoria di mitigare le ormai vertiginose asimmetrie di potere venutesi a creare tra persona e *big tech,* in circa un ventennio di sostanziale totale libertà di azione: diseguaglianze di potere negoziale, e non solo, accresciutesi ulteriormente dalla pandemìa globale.

La fragilità della tutela individuale della persona e della riservatezza digitale, persino del meccanismo del *consenso informato* che parte

depotenziato in tale contesto iper-asimmetrico, si disvelano così in tutta la loro evidenza di fronte all'inarrestabile dominio tecnologico dei *Big Tech*.

Occorre, dunque, scongiurare con un rigoroso quadro normativo - integrato e rafforzato - di regole protettive della persona il **progressivo *dominio dell'algoritmo opaco.*** Rischio denunciato dal giurista Frank Pasquale nel suo noto saggio **Black Box Society** del 2015*:* il controllo dei nostri dati personali elaborato dai software di gestione dei motori di ricerca, da sistemi esperti e intelligenze artificiali.

Non si possono affidare - nel contesto in cui più di ogni altro si dispiega la nostra esistenza - tutela di diritti e osservanza di obblighi esclusivamente ai ***codici informatici*** e nemmeno esclusivamente alle condizioni contrattuali asimmetriche, unilateralmente stabilite dagli Over The Top globali.

Non si tratta semplicemente di una nostalgica e anacronistica visione protettiva della persona peculiare della vecchia Europa: si tratta invero di una necessità globale anche nella prospettiva di disciplinare – illuminati da un ***nuovo umanesimo digitale*** - i prossimi incredibili salti tecnologici che certamente verranno.

Si ritiene per tale ragione corretto procedere ad esaminare il complesso fenomeno mediante una lettura assiologica costituzionalmente orientata: in tale prospettiva la tensione intrinseca tra persona e mercato che emerge in relazione al trattamento dei dati personali nella società digitale non può e non deve risolversi in danno di diritti fondamentali della persona tutelati dall'art. 2 della Cost. oltre che dagli articoli 7 e 8 della *Carta dei diritti fondamentali della UE* (*Carta UE*) e dall'art. 8 della *Convenzione Europea dei Diritti dell'Uomo* (CEDU).

Mai come oggi potremmo dire, a ragione, che la tutela della privacy e la protezione dei dati personali costituiscono una vera e propria sfida regolatoria: *Social Network, Cloud Computing, Internet of Things,*

Smartphone, Fintech, Artificial Intelligence, reti neurali e Big Data sono solo alcune delle principali "temibili" variabili socio-economiche e tecnologiche che occorre disciplinare in modo equilibrato, ora e in futuro, bilanciando contrapposti interessi.

Anche in Europa il quadro regolatorio si avvia, dunque, a un consolidamento delle molteplici fonti ma soprattutto a un rafforzamento delle tutele a protezione del soggetto debole nei rapporti asimmetrici, sempre più **diseguali** con le piattaforme digitali e più in generale della dignità della persona.

Così pare di potersi dedurre la testo delle recenti ambiziose proposte di regolamento DSA e DMA presentate dalla Commissione UE lo scorso 15 dicembre 2020.

Il nuovo principio di responsabilizzazione e la gestione del rischio correlato

L'innovativo *principio dell'accountability* (art. 5 — GDPR) — che permea, come si è detto, tutto l'impianto normativo del GDPR — è alla base dell'evoluzione della disciplina europea applicabile che ora valorizza il processo di valutazione, prevenzione e gestione del rischio da parte del Titolare del trattamento.

Si tratta forse del innovazione di maggior pregnanza nell'orditura regolatoria complessiva del GDPR considerato che richiede un drastico cambio culturale di approccio alla gestione del rischio correlato al trattamento dei dati.

La normativa europea in discussione supera la precedente logica stringente dello schema normativo *obbligatorio-non obbligatorio,* per entrare in una dimensione sfumata - più evoluta e matura - il Titolare deve preventivamente autovalutare il rischio del trattamento alla luce dei precetti del GDPR e conseguentemente differenziare adeguate misure organizzative e tecniche, caso per caso, in ragione della diversità del trattamento di dati operati e del rischio correlato.

Registrata la **fragilità del consenso**, da parte della più attenta dottrina, di fronte alla pervasività dei trattamenti digitali di dati personali, con il GDPR si realizza il progressivo passaggio della tutela dei dati personali fondata solamente sulla centralità dell'autodeterminazione informata dell'interessato, che pure permane ma in un quadro protettivo integrato, alla valorizzazione soprattutto del principio di responsabilizzazione preventiva del Titolare.

L'art. 5 del GDPR individua nel Titolare il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina in tema di trattamento dei dati personali, quali quelli di:

- liceità, correttezza e trasparenza,
- limitazione delle finalità, minimizzazione, esattezza,
- limitazione della conservazione, integrità e riservatezza.

Oltre a dover garantire il rispetto dei suddetti principi generali, il Titolare deve essere in grado di *comprovarlo:* in questo impegno ulteriore – esplicitato dal secondo comma dell'art.5 del GDPR – possiamo cogliere l'essenza del nuovo *principio di accountability*,.

Il Titolare ha l'onere di porre in essere — a seguito di consapevole e prudente preliminare ***autovalutazione*** **del rischio** correlato al trattamento da effettuare — una serie di adempimenti, a che a, titolo esemplificativo e non esaustivo, possono essere individuati nella:

— protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 GDPR);

— mappatura delle operazioni di trattamento mediante la creazione di appositi registri delle attività di trattamento (art. 30 GDPR);

— sicurezza del trattamento (art. 32 GDPR);

— valutazione di impatto sulla protezione dei dati (art. 35 GDPR);

— designazione *Data Protection Officer* (art. 37 GDPR).

Il GDPR – come si è già osservato – si fonda su un sistema protettivo integrato che valorizza, innanzitutto, la responsabilizzazione consapevole e documentata *ex ante* oltre alla responsabilità successiva.

In base alle regole di *accountability* i principi statuiti dalla nuova disciplina divengono adattabili e flessibili alle effettive esigenze concrete, emerse all'esito della doverosa **autodiagnosi preliminare**, del singolo Titolare e verificabili in concreto.

Non più meri obblighi formali, astratti e indifferenziati per tutti i destinatari ma al contrario obblighi adattabili al caso concreto, differenziati in ragione della **diversa natura, qualità, quantità del trattamento effettuato oltre che dei rischi specifici correlati**.

Il principio di *accountability* risulta, in particolare, delineato dal combinato disposto degli artt. 24, 25, 32 e 35 del GPDR: principio innovativo e al tempo stesso insidioso sotto il profilo della *compliance* in quanto flessibile, caso per caso, in relazione alla tipologia dei dati trattati, alle modalità e alla struttura organizzativa del Titolare rispetto alla parametrazione di soglie precise.

Le misure tecniche — comprese le misure di sicurezza da adottare — sono sempre, dunque, da intendersi nel GDPR come quelle **maggiormente adeguate al caso concreto,** considerato lo stato della tecnica nota e la variabile economica dei costi di implementazione che la normativa europea non ignora, anzi.

Il Regolamento europeo in materia di dati ammette espressamente che il Titolare e le altre figure soggettive, in concorso tra loro, chiamati a gestire il processo di trattamento dei dati personali possano tenere conto della **variabile economica** in sede di autovalutazione del rischio differenziato relativo al trattamento considerato.

Si pensi ai ***costi di attuazione*** che devono essere sostenibili, ragionevoli e proporzionati alla struttura organizzativa e alle risorse economiche del Titolare. Menzionano espressamente tale fattore rilevante le seguenti norme del GDPR:

- diritto all'oblio di cui all'art. 17,
- della privacy by design di cui all'art. 25 o
- del principio di sicurezza del trattamento dei dati personali di cui all'art. 32 GDPR.

Dalla violazione del principio di adeguatezza delle norme tecniche e organizzative da adottare in ragione della rischiosità del trattamento dati posto in essere discenderà l'addebito di responsabilità civile.

L'introduzione del *principio di accountability* determina l'onere di adottare un nuovo approccio *proattivo, preventivo, consapevole e responsabile* nella gestione della protezione dei dati da parte delle singole organizzazioni aziendali.

L'autovalutazione preventiva preliminare all'inizio del trattamento è strettamente correlata alla responsabilizzazione del Titolare e delle altre figure soggettive: *accountability* che si declina, in buona sostanza, non soltanto nel fare quanto richiesto dal GDPR nel caso concreto ma anche e soprattutto nel **provare di aver fatto, nel tracciare l'attività di *compliance* svolta.**

Tutela della persona e oggettivazione della responsabilità per trattamento illecito dei dati personali

Nel nuovo scenario digitale risulta evidente la necessità di rafforzare, in particolare nella società digitale, i rimedi a protezione dei diritti fondamentali della persona di fronte alla pervasività e non sempre agevole percezione dei trattamenti di dati personali operati - sino ai limiti estremi del trattamento occulto - in condizioni di conclamata asimmetria di potere informativo, tecnologico e normativo.

Il consenso informato, come si è già osservato, è fragile nel rapporto asimmetrico con i *big tech*: non è più sufficiente, da solo, a tutelare efficacemente i diritti fondamentali alla riservatezza, protezione dei dati personali e identità.

Il quadro regolatorio delineato dal GDPR, soddisfa tale necessità protettiva operando un significativo cambio di prospettiva evidenziato dall'orditura normativa di un sistema integrato di rimedi protettivi della persona.

Tale rafforzamento passa – oltre che attraverso il presidio di responsabilizzazione preventiva e di adeguato apparato sanzionatorio – anche attraverso l'oggettivazione della responsabilità per trattamento illecito dei dati e la facilitazione delle domande risarcitorie correlate oltre che del danno risarcibile.

Senza trascurare progressive virtuose convergenze e intersezioni protettive tra normativa in materia di dati personali e normativa consumeristica.

Nella prospettiva di tutela unitaria dei diritti della personalità, come noto, è stata riconosciuta al trattamento di dati personali una valenza plurioffensiva, idonea a ledere plurimi diritti fondamentali e interessi della persona meritevoli di tutala: diritto alla riservatezza, identità personale, protezione dei dati personali, immagine e oblio.

Il GDPR per facilitare tale tutela delinea opportunamente un modello speciale di responsabilità da illecito trattamento di dati personali che — a fronte del significativo *rischio d'impresa* correlato all'attività massiva di trattamento dei dati personali — rafforza la protezione dell'interessato dal trattamento nel solco normativo tracciato dalla normativa interna previgente delineata dall'art. 15 del *vecchio* Codice *Privacy*.

Referente normativo esclusivo della responsabilità civile in materia di trattamento illecito dei dati personali è, allo stato, costituito esclusivamente dall'art. 82 del GDPR, che, al comma 1, statuisce quanto segue

« *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* ».

E ancora: "*Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento*".

Infine: "Il Titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile".

L'art. 82 GDPR, per assicurare massima protezione alla persona fisica interessata dal trattamento, richiama a fondamento del rimedio risarcitorio la contrarietà della condotta del titolare del trattamento a **qualunque precetto conformativo tipizzato dal GDPR**, come pure di atti delegati, anche degli ordinamenti interni.

La lesione di un diritto fondamentale della persona — come quelli alla riservatezza e alla protezione dei dati personali — è da considerarsi **sempre rilevante – mai bagatellare -** alla luce di una lettura assiologica costituzionalmente orientata: per rafforzarne la protezione, il risarcimento del danno è ***in re ipsa*** in quanto conseguenza automatica della *condotta antigiuridica*, ossia non ottemperante ai precetti conformativi protettivi del GDPR

D'altra parte l'art. 82 del GDPR proprio al fine di rafforzare la tutela della persona danneggiata — così come in precedenza l'art. 15 del Codice *Privacy* — omette di richiamare la clausola ulteriore dell'*ingiustizia del danno:* dal mancato richiamo espresso della clausola generale della responsabilità civile comune di cui all'art. 2043 c.c. discende la sottrazione *ipso iure* di tale profilo all'accertamento giudiziale.

Si registra così, in base ad autorevole orientamento dottrinale, condivisa anche da chi vi parla, **l'*oggettivazione della responsabilità*** in forza della quale la struttura della responsabilità muta da regola comune a regola speciale: rileva non più la valutazione del danno in quanto effetto di condotta lesiva ma semplicemente la condotta antigiuridica *in se e per sé considerata.*

Tale oggettivazione segna, si ribadisce, il passaggio dal *paradigma di responsabilità comune*, che si regge sulla valutazione del danno quale conseguenza della condotta lesiva di cui all'art. 2043 c.c., al *paradigma di responsabilità speciale* per trattamento illecito dei dati personali, in cui il danno si identifica *tout court* con la condotta antigiuridica: *ergo* provata la violazione della regola di condotta risulta provato il danno, almeno nell'*an debeatur.*

Il profilo della *gravità della lesione* rileverà, quindi, esclusivamente sotto il profilo del *quantum debeatur.*

L'impostazione più tradizionale rigidamente ancorata alle *regole aquiliane comuni* non pare, si ribadisce, convincente nella misura in cui tende a minimizzare la specialità del sottosistema di responsabilità civile delineato in materia di protezione dei dati personali e conseguentemente depotenziare la ***funzione deterrente e protettiva*** dell'interessato dal trattamento dei dati, contrariamente ai segnali, anche giurisprudenziali (si pensi alle nuove sentenze gemelle di San Martino 2019 della Corte di Cassazione), di ***rinascita del danno morale soggettivo.***

A maggior ragione ora in cui lo scopo del GDPR è, semmai, proprio il contrario, ossia di armonizzare livello comunitario il regime di responsabilità europeo per fatto illecito in tale settore strategico attenuando le peculiarità e tradizioni giuridiche dei rispettivi ordinamenti degli Stati membri.

Ricordiamo che l'interessato dal trattamento - in quanto soggetto debole nel *rapporto asimmetrico* con il Titolare - deve godere di protezione rafforzata e non depotenziata.

Non si possono, quindi, sottostimare i tratti distintivi autonomi della disciplina europea della responsabilità civile per trattamento illecito dei dati personali rispetto alle regole comuni della responsabilità civile per fatto illecito *rectius* evidenziarne la natura speciale e oggettiva.

Lettura interpretativa operata, con metodo assiologico costituzionalmente orientato, attraverso il prisma del nuovo *principio di responsabilizzazione* posto dal GDPR a fondamento della *ratio* complessiva di prevenzione e gestione del rischio d'impresa correlato all'attività di trattamento dei dati personali.

Si possono applicare, in questo specifico contesto, anche i generali **principi di prevenzione e precauzione della responsabilità civile** sino a ricomprendere il rischio d'impresa *tipico imprevedibile* ma socialmente, economicamente e giuridicamente accettabile e sostenibile, tenuto conto dello stato dell'arte della tecnica e dei costi di attuazione, escluso solo il limitato *rischio atipico* inaccettabile e insostenibile in quanto *irragionevole e sproporzionato* e quindi non rientrante nel pur amplissimo dovere precauzionale.

In estrema sintesi si registra l'emersione dei seguenti tratti distintivi caratterizzanti tale speciale sottosistema di responsabilità civile per trattamento illecito dei dati personali che paiono potersi utilmente ravvisare nei seguenti profili:

(i) **facilitazione dell'accesso dell'interessato al rimedio risarcitorio:** il risarcimento discende dal trattamento illecito, *rectius* dalla ***mera condotta antigiuridica*** consistente nella violazione di un precetto del GDPR, con conseguente ammissibilità del **danno *in re ipsa***;

(ii) **ampliamento del danno risarcibile – patrimoniale e non patrimoniale – da trattamento illecito dei dati** in particolare superamento in relazione ai danni da trattamento illecito dei dati

personali del doppio filtro giurisprudenziale della gravità e serietà della lesione di San Martino 2008: la lesione dei diritti fondamentali non deve considerarsi mai bagatellare rilevando la gravità e serietà solo sulla quantificazione del danno e non anche sulla sua ammissibilità;

(iii) **rilettura della bipolarità danno patrimoniale e non patrimoniale** con conseguente valorizzazione, e riscoperta, dell'originaria **funzione deterrente-sanzionatoria** e autonomia del ***danno morale soggettivo*** sub art. 2059 c.c.

CONCLUSIONI

Mi sia consentito concludere il mio intervento richiamando l'ammonizione, quanto mai attuale, di Marshall Mc Luhan circa il rischio di essere dominati dagli strumenti tecnologici ideati dall'uomo: "*We shape our tools and thereafter our tools shape us*".

Occorre scongiurare tale rischio e riprendere il controllo delle tecnologie digitali – in particolare governare sapientemente le interazioni uomo-macchina contrastando il *capitalismo della sorveglianza* **estrattiva e predittiva** – prima che sia troppo tardi.

Tutelare i dati personali significa in ultima istanza tutelare la dignità della persona e la libertà di pensiero dalla stretta gabbia artificiale e artificiosa della *filter bubble* – per utilizzare l'efficace metafora di Eli PARISIER - ossia del pensiero unico artificialmente e artificiosamente preconfezionato e cristallizzato in base ai nostri orientamenti personali espressi, più o meno consapevolemnte, nel mondo digitale.

Constatato il fallimento dell'originario mito *naif* della sola autoregolazione che ha cessato di essere incisiva nel momento in cui si è conclamato il fenomeno della progressiva commercializzazione della rete Internet*,* occorre sviluppare un'efficace eteroregolazione per proteggere i diritti fondamentali della persona in generale — non solo il consumatore, non solo i dati personali — e in ultima istanza assicurare correttezza, trasparenza, equità e concorrenza effettiva ai mercati digitali.

Con l'auspicio che tale visione distopica della realtà, distorta dall'uso pervasivo e invadente, delle nuove tecnologie digitali, non si avveri e che quindi - anche grazie alla protezione giuridica offerta dal nuovo GDPR non si pervenga, in un prossimo futuro, all'erroneo convincimento che *la privacy è inutile sovrastruttura del passato* ma al contrario si possa affermare a livello globale – senza eccezioni – che la *privacy è un valore irrinunciabile*, un diritto fondamentale della persona che merita di essere pienamente tutelato, per noi e per le generazioni future.