SERGIO LOCORATOLO

Professore associato di Diritto commerciale – Università degli Studi di Napoli Federico II

IMPRESA DIGITALE E TUTELA DELLA PRIVACY TRA DIRITTO EUROPEO E NAZIONALE

SOMMARIO: *1. L'utilizzo di strumenti di intelligenza artificiale nell'impresa. – 2. Impresa digitale e trattamento dei dati personali. – 3. Strumenti di tutela in ipotesi di violazione della privacy. – 4. Diritto interno e orientamento giurisprudenziale europeo.*

1. – Il diritto dell'impresa reclama la riqualificazione del tessuto dispositivo e il ridisegno degli strumenti normativi, una volta riconosciuta al diritto la vocazione, che gli è propria, di guida dei processi.

Comunque sia, un percorso di modernità ha influenzato il mondo dell'impresa e le forme di *governance*, nonché restituito fiducia a investitori e consumatori improntandosi a trasparenza le operazioni economiche e finanziarie una volta preservati i profili informativi e comunicativi.

Anche i nuovi modelli organizzativi, d'altronde, non avrebbero fatto a meno dei fattori di modernità, usufruendo le articolazioni dell'impresa dell'apporto della informatizzazione e della digitalizzazione. Riequilibrare gli assetti di sistema sul metro della tutela della riservatezza, commisurando alle spinte in avanti oramai intervenute la 'rivoluzione' tecnologica, induce a reimpostare le modalità di esercizio dell'attività di impresa.

Uno sforzo congiunto. Accedere a mirate scelte tecniche, né solo tecniche; adeguare i registri giuridici economici, persino etici, ad esigenze inedite dell'impresa; sceverare all'interno del giuridico quanto risulti pregnante e adeguato, orienta al rinvenimento del punto di equilibrio tra il legittimo esercizio dell'attività di impresa e la gestione dei dati.

Processi convergenti ed il crescente apporto tecnologico e digitale, l'utilizzo di strumenti di intelligenza artificiale nell'impresa, elevano la soglia di rischio sociale con effetti potenziali di imponderabile perniciosità. Alle tradizionali incombenze afferenti agli aspetti gestionali e al ruolo rivestito dall'organo amministrativo di *corporation* digitali dovrà allora aggiungersi la modalità di governo del rischio d'impresa dovuta all'apporto dei sistemi automatizzati e degli strumenti di intelligenza artificiale. Enucleandosi, entro la cornice della responsabilità, uno specifico profilo di *Corporate Digital Responsibility*.

Comprensibili le apprensioni in materia, si è pertanto invocato l'assunto di sostenibilità, confortato dal *background* giuridico. Pertanto:

a) il '*Codice di Corporate Governance*', del gennaio 2020, approntato dal 'Comitato per la Corporate Governance' perpetra condizioni di buon governo delle società italiane quotate, assicurando la conformità

alle *best practices* internazionali, svolgendo il Comitato funzione propulsiva e, al tempo stesso, funzione di verifica e monitoraggio annuale dell'adesione delle società alle raccomandazioni impartite [1];

b) la proposta di '*Regolamento sull'intelligenza artificiale*' ('*Regulation on a European approach for Artificial intelligence*') [2] pubblicata dalla Commissione europea il 21 aprile 2021. Si legge nelle presentazione che il Regolamento viene emesso «con l'obiettivo di plasmare la legislazione europea sull'intelligenza artificiale (I.A.), armonizzando, quindi, la normativa applicabile e caldeggiare l'innovazione, la sicurezza e la tutela dei diritti individuali» e si aggiunge: «Risulta piuttosto visibile il ruolo coperto dall'intelligenza artificiale nella trasformazione digitale di svariati settori economici e sociali (beni, servizi, mondo del lavoro, finanza, sanità, sicurezza). Essa rappresenta il presente e il futuro della tecnologia ed "un punto centrale nel Green Deal europeo e nel rilancio dell'economia post COVID-19», altresì, preannunciando che «la recente proposta di Regolamento pone un primo quadro giuridico sull'I.A. che, con l'introduzione di nuove regole, azioni, ed affrontandone i rischi, punta a trasformare l'Europa nel polo mondiale per un'intelligenza artificiale affidabile». Volgendo alle istanze del progresso onde costruire un futuro che sia sostenibile, si argomenta che il nuovo approccio europeo è preceduto da una serie di iniziative intraprese negli ultimi anni: 1) la consultazione pubblica sul '*Libro Bianco sull'Intelligenza Artificiale*' (C.O.M. 2020) 65 final del 19 febbraio 2020; 2) le 'Linee guida etiche finali per un'intelligenza artificiale affidabile' emesse dal Gruppo ad alto livello sull'intelligenza artificiale, pubblicate in data 8 aprile 2019; 3) il '*Rapporto sulla responsabilità per l'intelligenza artificiale e altre tecnologie emergenti*' emesso dal Gruppo di esperti sulla responsabilità e nuove tecnologie, pubblicato in data 21 novembre 2019; 4) la '*Dichiarazione di cooperazione sull'intelligenza artificiale*' firmata da 25 Stati europei in data 10 aprile 2018, fondata sui risultati e sugli investimenti della comunità europea della ricerca e delle imprese nell'I.A. Infine, si è inteso chiarire che «la scelta della forma del Regolamento, quale atto legislativo vincolante da applicare nella sua interezza in tutta l'U.E., non è casuale, ma fa parte del più ampio progetto garantista e di piena tutela dell'individuo, da raggiungere con l'applicazione congiunta di altre normative vincolanti quali la proposta di Regolamento e *Privacy* (presentata il 10 febbraio 2021 dal consiglio dell'Unione Europea) e il Regolamento n. 679/2016 (G.D.P.R.).

La tematica è di sicura presa e situare al centro dei processi la tecnologia d'impresa significa attendere il presente e volgere al futuro, sebbene già intravedibile in ogni potenzialità.

Una dottrina coglie questi profili, assunto l'onere di disegnare le fisionomie modulanti l'odierna impresa ed il nuovo capitolo dell'imprenditoria aperto alla *business community*.

Al mondo dell'impresa e, in particolare, alla sfera societaria si richiede di non soggiacere all'impatto della tecnologia e, in argomento, autorevole dottrina constata che «le impetuose trasformazioni tecnologiche in atto, pur non richiedendo una riforma strutturale del sistema di corporate governance, rendono ineludibile un ripensamento del quadro regolatorio, da ridisegnare alla luce della valorizzazione delle nuove interazioni tra diritto societario e diritto dell'informazione, nella dimensione tecnica oltre che nelle sue implicazioni etiche» [3].

2. – Decisa centralità acquista odiernamente la questione dell'informazione afferente alla tecnologia d'impresa e notevole è il tradotto che ne discende: si avverte la carenza, persino la mancanza, di un'adeguata e/o

[1] Per ulteriori chiarimenti v. il sito *http://www.borsaitaliana.it/comitato-corporate-governance/homepage/homepage.htm*.

[2] Si rimanda al sito *resource.html* (europa.eu).

[3] N. Abriani, G. Schneider, *Diritto delle imprese e intelligenza artificiale. Dalla* Fintech *alla* Corptech, Bologna, 2021, 300.

di una corretta divulgazione degli obblighi informativi, fonte di guasti all'esterno tuttavia riverberanti all'interno dell'impresa. L'ontologia dell'attualità esige continua cura degli aspetti informativi e comunicativi e il macigno delle conseguenze lesive prodotte sull'impresa da una manchevole e/o non corretta informazione ricorre, senz'altro, quando sovvengano lesioni alla *privacy* e inadeguato trattamento dei dati personali.

Materia sensibile che coinvolge ragioni di etica relazionale, di etica della responsabilità, cui prestare attenzione.

Fornire, e divulgare, informazioni circa il grado di tecnologia di cui fruisce l'impresa è questione che non attiene solo al piano della prassi operativa, ma al piano deontologico, sfondo su cui si apre una finestra sui concetti di *privacy* e di trattamento dei dati personali.

Vi è generale consapevolezza del rischio dell'utilizzo telematico dei dati personali, né restano ai margini le problematiche afferenti alla sicurezza cibernetica e neanche, per vero, appaiono in tutto rassicuranti le soluzioni ancora inadatte e deboli a fronteggiare la celerità incontenibile del *web* e ad incanalare entro corretti ambiti la circolazione telematica dei dati personali e delle informazioni sottratti, oltre tutto, ad un preventivo *screening*.

Così si assiste all'emanazione del 'Regolamento U.E. n. 679 del 27 aprile 2016, corredato con riferimenti a 173 *'Considerando'*, recepito dagli Stati membri e definitivamente applicabile in via diretta nei Paesi U.E. a partire dal 25 maggio 2018 [4].

Si prevede, al comma 2 dell'art. 5, che ricorra competenza del titolare del trattamento dei dati personali e la norma regolamentare esigendo che questi «deve essere sempre in grado di 'comprovare' il pieno rispetto di questi principi». Un nesso stringe all'altro disposto, l'art. 24, rubricato 'responsabilità del titolare del trattamento' che delinea i contorni della responsabilità in capo al titolare del trattamento, a cui si impone di «mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al presente regolamento».

La normativa europea deve ritenersi propulsiva, di indirizzo, rispetto alle regolamentazioni nazionali, inducendo a provvedere alle condizioni di applicabilità dei principi in materia di trattamento dei dati personali ed alle modalità occorrenti ad attestare alle autorità garanti, o alle autorità di controllo nazionali, il rispetto della normativa facendo ricorso a ogni modo consono. Si tratti di documentazioni da esibire, procedure da attuare, mappature, utilizzo di *software*.

Un assetto regolamentare stabile, che alloca la materia entro un assetto di organica *regulation* es attiene alle tematiche della sicurezza, alla previsione del rischio, alla valutazione dell'impatto della *privacy* ed alle rispettive declinazioni: per meglio chiarire, a principi '*privacy by design'* e '*privacy by default',* necessitando garanzie, nell'una e nell'altra circostanza di *privacy*, a beneficio degli utenti.

Disegnare una intelaiatura di tutele giuridiche rivolte specificamente a questo delicato ambito significa elevare la materia al piano costituzionale [5]. Muta la teorica sottesa alle tutele e muta l'approccio ermeneutico

---

[4] Sufficiente richiamare che la normativa europea contempla 11 Capi, taluni suddivisi in Sezioni, corredando con riferimenti a 173 '*Considerando'*: Capo I ('*Disposizioni generali'*);Capo II('*I Principi'*);Capo III ('*I Diritti dell'interessato'*);Capo IV ('*Titolare del trattamento e responsabile del trattamento'*);Capo V ('*Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali'*);Capo VI ('*Autorità di controllo indipendenti'*);Capo VII ('*Cooperazione e coerenza'*);Capo VIII ('*Mezzi di ricorso, responsabilità e sanzioni'*); Capo IX ('*Disposizioni relative a specifiche situazioni di trattamento'*);Capo X ('*Atti delegati e atti di esecuzione'*);Capo XI ('*Disposizioni finali'*).

[5] D. SCHEFOLD*, Resoconto*, a cura di A. BURATTI, E. CANITANO, della Relazione svolta nel corso dell'incontro dell'11 novembre 2003 sul tema "*La dignità umana*", in AA.VV*., I Costituzionalisti e la tutela dei diritti nelle Corti europee*, a cura di S. PANUNZIO, Padova, 2007, *passim*.

alla questione del trattamento dei dati personali, affermandosi prioritarie le esigenze di realismo giuridico: queste esigono di commisurare la sfera privata alla sfera pubblica e pongono l'accento su principi di intangibilità dei diritti e inderogabilità ai doveri.

In tal senso, occorre rimandare alla normativa regolamentare europea e si richiama l'art. 5 ('*Principi applicabili al trattamento dei dati personali*'), del Capo II ('*Principi*'), ove viene posta, assiomaticamente, la questione della tenuta del diritto alla riservatezza ed al trattamento dei dati personali: disposizione – vettore di una moderna visione improntata a rinnovati dettami di responsabilizzazione.

Declina, poi, l'art. 5. una enumerazione di principi:

– alla lettera a) i principi di '*liceità*', '*correttezza*' e '*trasparenza*' indefettibili ai fini del trattamento dei dati personali;

– alla lettera b) il principio di '*limitazione della finalità*', ponendosi stretta corrispondenza tra la raccolta dei dati personali e finalità e obiettivi determinati ed esplicitati escludendo che si possa esorbitare da tali parametri;

– alla lettera c) il principio di '*minimizzazione dei dati*', occorrendo che i dati siano adeguati, pertinenti e commisurati alle finalità per le quali vengono trattati;

– alla lettera d) il principio di '*esattezza*', richiedendosi l'esattezza dei dati e l'aggiornamento progressivo dei dati personali. Pertanto, l'adozione di misure adatte a rettificare e/o cancellare i dati alterati rapportando alle finalità di utilizzo degli stessi;

– alla lettera e) il principio di '*limitazione della conservazione*', disponendosi che la conservazione dei dati personali sia rapportata ad un dato periodo di tempo, corrispondente al tempo occorrente a conseguire le finalità per le quali i dati vengano trattati. Corollario a tale principio, la possibilità di conservare i dati personali per più lunghi periodi a condizione che il trattamento sia inteso a fini di archiviazione nel pubblico interesse, in chiave di ricerca scientifica o storica, a fini statistici;

– alla lettera f) il principio di '*integrità e riservatezza*' dei dati personali attiene ai profili di sicurezza e di protezione attuati ricorrendo ad adeguate misure tecniche e organizzative, inoltre prevedendo misure di contrasto al trattamento dei dati che non sia autorizzato o che sia illecito, e ancora, prevedendo la perdita dei dati, la distruzione degli stessi, il danno accidentale;

– alla lettera g) il principio di '*responsabilizzazione*' rimanda alla persona del titolare dei dati a cui si richiede di comprovare gli stessi.

Novero di principi, questi, comportante ripercussioni sull'attività d'impresa e affinché i menzionati principi restino preservati e salvaguardata la preminente esigenza di riservatezza, la stessa normativa decretale si sarebbe fatta carico di individuare il rimedio idoneo prevedendo l'obbligo, anche a carico dell'impresa, di dotarsi di un apposito organo interno 'Responsabile della protezione dei dati', di fornirsi di un 'registro delle attività di trattamento' al fine di notificare le violazioni dei dati personali. Il fenomeno della *privacy*, come la questione dei dati personali, attiene a una tassonomia di motivi che rimanda al profilo tecnico-giuridico, certo, ma a cui non è avulso il profilo etico-comportamentale e valoriale che richiede cure normative e costanti premure del legislatore.

Accreditare, in linea con una logica di coerenza, i nessi di impresa e la tutela della privacy è altresì tornare a occuparsi di buona gestione e corretta amministrazione dell'impresa, prestando attenzione ai profili di salvaguardia che attengono alla questione comunicativa-informativa. E per quanto attiene alla sfera societaria, il 'dovere di informare' e il 'dovere di agire informati' ricadono nelle competenze degli amministratori,

conseguendone un fascio di diritti, e di doveri, preordinati alla cura della riservatezza e al corretto trattamento dei dati personali.

3. – La disciplina giuridica offerta dal Regolamento UE in tema di privacy usufruisce di un tangibile contributo fornito dai 'Considerando', ove molte istanze ottengono risposte. Questi ultimi fungono da proscenio alla normativa regolamentare ed il Considerando 11 assume rilievo paradigmatico ed enunciativo del principio di '*funzionalità di sistema*', restituendo afflato generale alla materia: «Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni degli Stati membri».

Per quanto riguarda le imprese di investimento, è fatto obbligo alle stesse di produrre corrette ed esaustive informazioni, secondo la previsione del Regolamento Delegato U.E. 2018/1229 della Commissione, del 25 maggio 2018 – "*che integra il Regolamento U.E. n. 909 del 23 luglio 2014 del Parlamento europeo e del Consiglio relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento UE n. 236/2012*" – che prevede, quanto al corredo informativo, che: «Le imprese di investimento dovrebbero accertarsi di disporre per tempo di tutte le informazioni di regolamento necessarie per un regolamento delle operazioni efficace ed efficiente» e le imprese di investimento che non disponessero di tutte le informazioni occorrenti hanno l'obbligo di ottenerle dai clienti per conseguire «i dati standardizzati necessari per il processo di regolamento» (Considerando 4).

Al Considerando 5 si formula un auspicio: «Dovrebbe essere incoraggiato il trattamento interamente automatizzato [*straight-through processing* (S.T.P.)], poiché il suo utilizzo in tutto il mercato è essenziale sia per mantenere tassi di regolamento elevati sia per assicurare il regolamento tempestivo delle negoziazioni transfrontaliere. Inoltre, i partecipanti al mercato, sia diretti che indiretti, dovrebbero poter disporre dell'apporto dell'automazione interna necessaria per avvalersi delle soluzioni S.T.P. disponibili e le imprese di investimento offrire ai loro clienti professionali la possibilità di inviare, per via elettronica, le conferme e i dettagli dell'attribuzione, utilizzando, in particolare, procedure e norme di comunicazione internazionali aperte riguardo alla messaggistica e ai dati di riferimento».

Quanto ai requisiti normativi occorrenti per i depositari centrali di titoli (C.S.D.), apporta novità il Considerando 2 che, ribadito «il carattere globale dei mercati finanziari», prevede l'opportunità di «tenere debitamente conto dei principi per le infrastrutture dei mercati finanziari, emessi nell'aprile 2012 dal '*Committee on Payment and Settlement Systems*' (Comitato sui sistemi di pagamento e regolamento – C.P.S.S.) e dall'*'International Organization of Security Commissions*'(Organizzazione internazionale delle commissioni sui titoli – I.O.S.C.O.) (principi C.P.S.S. – I.O.S.C.O.), che servono da riferimento mondiale per i requisiti normativi per i depositari centrali di titoli (C.S.D.)». E altre misure contemplate dal detto Regolamento attengono alla disciplina degli strumenti finanziari, ai tipi di attività, alla determinazione del prezzo, alla liquidità dei prodotti finanziari.

Si avverte tutta la determinazione del legislatore europeo nel perseguire effetti di omogeneità, e stabilità, che possano valere per la disciplina giuridica del trattamento dei dati personali richiamato il principio della distribuzione dell'onere della prova – nell'ordinamento interno previsto all'art. 2697 cod. civ. – ora correlato

al contrasto delle prassi di distorto utilizzo e di indebita divulgazione dei dati. L'esigenza di perimetrare in termini giuridici il fenomeno *de quo* sarebbe apparsa indefettibile e insistere su punti fermi necessario per disegnare una rete di coerenza che valesse nei tradotti nazionali.

Prova ne sia l'adozione di un comune lessico giuridico [6].

Il Regolamento europeo riempie vuoti mai prima colmati restituendo contenuti al concetto di 'trattamento dei dati personali' e indicandone la portata alquanto estesa: «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» (art. 4, § 2); altresì, specificando che 'titolare del trattamento' è la «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri» (art. 4, § 7). In materia di responsabilità il Regolamento stigmatizza e circoscrive, all'art. 24, gli aspetti di responsabilità attinenti al trattamento dei dati commisurando al piano oggettivo, del verificarsi fattuale della vicenda trasgressiva, il piano soggettivo della individuazione di un 'responsabile del trattamento' a cui imputare la vicenda stessa restituendone la 'definizione' all'art. 4, § 8: «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

La disciplina del risarcimento del danno, materiale o immateriale, viene contemplata al § 1 dell'art 82 ('*Diritto al risarcimento e responsabilità*') qui rilevando il nesso di consequenzialità, di talché, si prescrive che «Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento dal titolare del trattamento o dal responsabile del trattamento», con ciò non esitando gli estensori europei nel riconoscere ammissibile il danno non patrimoniale rinvenendo gli estremi dell'obbligazione risarcitoria e il pieno ristoro del danno. Al § 2 dell'art. 82 si illustrano i caratteri della responsabilità imputabile al titolare del trattamento e i caratteri connotanti la responsabilità asseverabile al 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». Al § 3 sovvengono le condizioni di esonero dalla responsabilità: «Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del § 2, se dimostra che l'evento dannoso non gli è in alcun modo imputabile». L'esonero dalla responsabilità del titola-

[6] Preme precisare che all'art. 4 ('*Definizioni'*) del G.D.P.R. si illustrano con cura meticolosa gli idiomi '*dato personale*' (al punto 1), '*trattamento*' (al punto 2), '*limitazione ditrattamento*' (al punto 3), '*profilazione*' (al punto 4), '*pseudonimizzazione*' (al punto 5), '*archivio*' (al punto 6), '*destinatario*' (al punto 9), *'terzo*' (al punto 10), '*consenso dell'interessato*' (al punto 11), '*violazione dei dati personali*' (al punto 12), '*dati genetici*' (al punto 13), '*dati biometrici*' (al punto 14), '*dati relativi alla salute*' (al punto 15),*'stabilimento principale*' (al punto 16), '*rappresentante*' (al punto 17), '*impresa*' (al punto 18), '*gruppo imprenditoriale*' (al punto 19), '*norme vincolanti d'impresa*' (al punto 20), '*autorità di controllo*' (al punto 21), '*autorità di controllointeressata*' (al punto 22), '*trattamento transfrontaliero*' (al punto 23), '*obiezione pertinente emotivata'* (al punto 24), '*servizio della società dell'informazione*' (al punto 25), '*organizzazione internazionale*' (al punto 26). E si riportano, ancora, le espressioni '*titolare del trattamento*' (al punto 7), e l'altra, '*responsabile del trattamento*' (al punto 8) a indicare la differenza dei rispettivi ruoli e funzioni.

re del trattamento, come del responsabile del trattamento, ricorre al § 3 e qui si contempla l'inversione dell'onere della prova, prevedendosi una deroga alla regola generale: il resistente è tenuto ad accollarsi l'onere di prestare la prova in luogo del ricorrente, né è sufficiente restituire esclusivamente la prova del fatto dalla parte non obbligata, ma occorrerà che appaia inequivoca la volontà dell'offerente di rinunciare ai vantaggi che gli deriverebbero dall'applicazione del principio dell'onere della prova, dunque, che appaia inequivoca la volontà di assumere gli svantaggi dell'eventuale insuccesso in conseguenza della prova avanzata.

L'inversione dell'onere della prova attesta che il trattamento non corretto dei dati venga avvertito alla stregua di attività 'pericolosa' intervenendo la normativa codicistica, di talché, recita l'art. 2050 cod. civ. (*'Responsabilità per l'esercizio di attività pericolose'*) che «Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa per sua natura o per la natura dei mezzi adoperati è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno», per effetto, si ammette l'inversione dell'onere della prova quale rimedio funzionale alla compensazione del rischio incombendo obblighi a carico delle società tenute a garantire la sicurezza dei trattamenti. Nel pretendere il risarcimento, il titolare dei dati non può sottrarsi dal fornire prova del danno subito all'esito dell'altrui condotta difforme ai dettami della normativa sulla tutela dei dati personali, altresì, dall'accertarsi che sussista il nesso causale, dall'individuare il titolare del trattamento e/o il responsabile del trattamento, dal confutare l'assunto che l'evento dannoso sia imputabile a proprie mancanze.

Indicare la linea, avvertita *in nuce* il rischio dell'estendersi in modo difforme delle regolamentazioni nazionali, è sicuro merito del legislatore europeo: la confusione, anche normativa, va contrastata con la certezza degli assunti, e senz'altro vale il principio per la regolamentazione del trattamento dei dati personali. Materia sensibile, a maggior ragione, nelle differenti prospettazioni, e procurante ricadute sull'attività d'impresa, coinvolta nei processi di *technical* e *digital transformation,* dischiudendosi inedite forme di responsabilità.

Materia che si faticherebbe a non connettere all'altra, la tutela della *privacy*, entrambe collegate nella considerazione che ha loro prestato il legislatore europeo come, d'altronde, dai legislatori nazionali – l'aggiornamento del 'Codice della *privacy*' rimanda alle modifiche apportate alla precedente regolamentazione dal D.L. 14 giugno 2019, n. 53, dal D.M. 15 marzo 2019 e dal d.lgs. 10 agosto 2018, n. 101 *('Decreto di adeguamento al G.D.P.R.'*), quest'ultimo emanato in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (l. 25 ottobre 2017, n. 163), in vigore in tutti i paesi dell'Unione dal 25 maggio 2018, teso ad armonizzare il Codice della *privacy* alla normativa europea –, e ben si intendono le finalità calmieranti, occorrendo sovente arginare fenomeni incontrollati di concessione di libertà in modo sempre più ampio e persino lesivo della sfera dei diritti personali. Motivi sottesi al 'Codice della *privacy*' sebbene il disposto dell'art. 15 *('Danni cagionati per effetto del trattamento'*) sia stato abrogato nella versione originaria né, per vero, il Decreto di adeguamento al G.D.P.R. comporti l'obbligo di prestare il consenso al trattamento dei dati personali.

La questione relativa al risarcimento dei danni procurati dal titolare del trattamento, o dal responsabile del trattamento, ripresa dal G.D.P.R. al 'Considerando' 146, presenta una singolarità che si riscontra nella illustrazione del principio utilizzando il verbo al condizionale – «Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforma al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile» – a far intendere, attendibilmente, da parte dell'estensore europeo, che tale disciplina abbia tenore di suggerimento anziché disposizione stentorea, ovvero, imperativo normativo. E il 'Considerando' 146 'fende' l'altra questione, strettamente connessa alla imputazione della responsabilità, del dan-

no procurato dal titolare del trattamento o dal responsabile del trattamento: «Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del seguente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno». Si puntualizza ancora: «Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento». Si chiude, infine, il 'Considerando' 146 garantendo il pieno ristoro economico all'interessato leso nei suoi diritti e consentendo il diritto di rivalsa al titolare del trattamento, o al responsabile del trattamento, di talché, «pagato l'intero risarcimento del danno [di poter] successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento».

Che il trattamento dei dati personali, come la tutela della *privacy*, costituisca materia sensibile è provato dalla pregnanza che assumono il fenomeno della risarcibilità del danno ed i criteri di imputabilità della responsabilità. Il baricentro della responsabilità si sposta dall'autore del fatto dannoso alla vittima del danno, e prioritario è accertare se la responsabilità consegua a colpa, se l'autore materiale del danno effettivamente sia il soggetto a cui imputare la colpa, in quale misura la vittima del danno vada risarcita.

Non poche suggestioni conseguono all'esegesi del 'Considerando' 146 e si avverte tutta la complessità di restituire una figurazione concettuale coerente della responsabilità, e del danno, che richieda adeguata ponderazione di ogni circostanza rilevante. In punto di chiarimento, una notazione di ordine preliminare attiene specificamente alla precisazione della natura giuridica dei 'Considerando' riportati in un Regolamento U.E. e a seguire la recente ordinanza emessa dalla V sezione della Cass., 7 marzo 2022, n. 7280 – analogo chiarimento è già nella Guida pratica comune del Parlamento europeo e del Consiglio e della Commissione per la redazione dei testi legislativi dell'Unione europea del 2015 –, illustrativa della portata da attribuire al diritto unionale, i 'Considerando' assumono valenza esplicativa circa le ragioni sottese all'intervento normativo, integrandone la 'concisa motivazione', sebbene non corrispondano a enunciazioni di portata normativa. Su questa *raison* poggia la pronuncia della Suprema Corte: i 'Considerando' a corredo degli atti normativi dell'Unione europea presentano, appunto, portata enunciativa né «assurgono a parametro rilevante ai fini della configurabilità di un *error in iudicando* denunciabile mediante ricorso per cassazione ai sensi dell'art. 360, comma primo, n. 3, cod. proc. civ.» [7].

4. – Fugare i rischi indotti da una errata e perturbante lettura dei processi della modernità – si pensi alle violazioni della sicurezza d'impresa in materia di tutela della *privacy* e di corretto trattamento dei dati – è scongiurare la liquefazione di quell'equilibrio consentendo che si dispieghino le innovazioni introdotte lungo

[7] V. SICILIANO, *Diritto tributario e funzione dei "Considerando" riportati in un Regolamento UE*, in *Judicium. Il processo civile in Italia e in Europa*, *http:/www.judicium.it*.

il 'secolo *biotech*'. Rispetto ai primi stadi, gli anni '90 dello scorso secolo quando andavano profilandosi le prime cure e le prime tutele a fini di deterrenza, si avvertono oggi suggestioni potenti, prestandosi particolare specifica attenzione alla tematica della sicurezza d'impresa.

Tematiche che il legislatore nazionale recepisce rimarcando in termini di inscindibile endiadi, come si desume dalla lettura dell'art. 1 della legge 31.12.1996, n. 675 inerente al trattamento dei dati personali, normativa confluita nel d.lgs. 30 giugno 2003, n. 196 ('*Codice in materia dei dati personali*'). All'art. 2, primo comma, si enunciavano le ragioni informanti la normativa decretale, statuendosi «che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'idoneità personale, al diritto alla protezione dei dati personali» secondo coerenza al dettato dell'art. 8 della Carta dei diritti fondamentali U.E.

Conferme vengono dalla *interpretatio* giurisprudenziale diretta a stabilire le coerenze dei piani normativi, continentale e nazionale, e a verificare il grado di conformità della normativa di settore in materia di *privacy* e di trattamento dei dati, specificamente, quanto all'estensione della responsabilità afferente ai motori di ricerca. Viene così in considerazione la cosiddetta 'ragnatela intorno al mondo' – globalmente intesa con la sigla convenzionale '*world wide web'* = w.w.w. – che attiene alla generale fruizione, e condivisione, di documenti ipertestuali multimediali confezionati mediante l'assemblaggio di elementi testuali, visuali, auditivi e fondata sulla infrastruttura di Internet.

Orbene, l'attività di selezione dei dati, di indicizzazione, di memorizzazione, di messa a disposizione degli utenti di connessioni costituisce materia di approfondimento da parte della Corte di giustizia dell'Unione europea, espressasi con una pronuncia che avrebbe segnato le linee tendenziali di disciplina della complessa materia. Trattasi della nota vicenda giudiziale C-311/18 '*Data Protection Commissioner v/s FacebookIreland Ltd e Maximillian Schrems*' (Schrems II): sollecitato in ordine alla possibilità di trasferire i dati personali conformemente ai dettami previsti dalle norme vincolanti d'impresa, rimarcava il giudice europeo che la protezione dei dati personali all'interno dello spazio economico continentale (S.E.E.) sarebbe dovuta transitare contestualmente al transito stesso dei dati, ovunque questi venissero trasferiti, posto che il trasferimento transfrontaliero dei dati personali non avrebbe minimamente minato e/o indebolito le tutele predisposte nello S.E.E. Tanto deciso non avrebbe significato, certo, l'obbligo di predisporre *ubique* identiche e medesime garanzie all'interno dei confini continentali, piuttosto, sforzo plurale di porre un denominatore comune che sottendesse equivalenze quanto alle garanzie da prestare e, allo stesso modo, equivalenze delle clausole contrattuali-tipo quali modalità di trasferimento assunte in via generale tali da garantire, rispetto al piano contrattuale, un grado di protezione non difforme a tutela dei dati che fossero trasferiti oltre i confini europei.

I riverberi nel diritto interno prodotti da tale orientamento giurisprudenziale europeo sarebbero stati oltre modo significativi e conformi allo spirito dei tempi, come consegue dalla lettura della 'Dichiarazione dei diritti in Internet'– nuovo testo redatto in 14 articoli e presentato alla Camera dei deputati in data 14 luglio 2015 – mediante cui ci si prefiggeva di rispettare l'equilibrio tra un'esigenza di futuro, convertita in principi di propulsione impressi dalla rete, e la garanzia prestata alla *privacy* e al corretto trattamento dei dati. Si legge con misurata enfasi nel 'Preambolo', avvertita contezza altresì del rilievo economico della rete, che «L'Unione europea è oggi la regione del mondo dove è più elevata la tutela costituzionale dei dati personali, esplicitamente riconosciuta dall'articolo 8 della Carta dei diritti fondamentali, che costituisce il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di Internet, anche in una prospettiva globale», ribadito e formalizzato che «Internet deve essere considerata come una risorsa globale e che risponde al criterio della universalità», e inoltre, che «I principi riguardanti Internet tengono conto del suo

configurarsi come uno spazio economico che rende possibili innovazione, corretta competizione e crescita in un contesto democratico».

Il citato Regolamento avrebbe di poco preceduto il varo del Regolamento U.E. n. 2120 datato 25.11.2015 regolante l'accesso alla rete inclusivo di riferimenti al circuito 'Internet aperta', c.d. '*net neutrality*' (N.N.), o '*Internet neutrality*', pertanto, diretto a statuire i principi di neutralità e non discriminazione circa il contenuto dei dati. La forza perlocutiva dell'enunciazione giuridica viene esaustivamente restituita dalla regola enunciata all'art. 2 «l'accesso a Internet è diritto fondamentale della persona e condizione per il suo sviluppo individuale e sociale», e all'art. 4 viene asserito il principio di 'neutralità della rete' legittimante l'agire informato a imparzialità e contrasto alle derive cagionate da un utilizzo mercenario della rete.