GIUSTIZIA CIVILE.com

IMPRESA DIGITALE E TUTELA DELLA PRIVACY

di **SERGIO LOCORATOLO**

Approfondimento del 04 aprile 2023

ISSN 2420-9651

Il lavoro pone a tema le vicende della moderna impresa e la progressiva rimodulazione degli assetti organizzativi quale riverbero delle nuove opportunità offerte dalla digitalizzazione. In questo scenario, l'impresa è chiamata a contemperare esigenze tra di loro confliggenti, prestando cura all'adeguato trattamento e utilizzo dei dati personali, senza tralasciare il perseguimento di finalità di profitto connesse ad esigenze di performatività.

SOMMARIO: 1. Tecnologia d'impresa e assetti regolamentativi - 2. Obblighi informativi e tutela della privacy nell'impresa digitale - 3. Tutela rimediale in ipotesi di violazione della privacy - 4. Gestione dei dati e accesso alla rete

1. Tecnologia d'impresa e assetti regolamentativi

La moderna impresa reclama nuove cure da parte del diritto posta l'incessante progressione di processi di trasformazione correlati all'utilizzo, sempre più massiccio, di strumenti offerti dalla tecnologia info-telematica. L'architettura a sostegno di un sistema, e di un modello d'impresa, si sarebbe palesata inadeguata accentuate le spinte nel verso della crescita economica e della diffusione del benessere, conducendo ad una *new age* anche per l'impresa. I processi di modernità avrebbero interessato già dall'interno l'impresa, funzionalmente ad obiettivi di crescita della produttività, riqualificando gli assetti di *management* e ridisegnando lo strumentario tecnico-operativo.

Si rileva che la performatività dell'impresa moderna attiene a indefettibili caratteri di duttilità, che qualificano questa quale primario attore economico, entro i circuiti di mercato, in aperta competizione con altri soggetti. In concreto, duttilità, maggior grado di flessibilità – richiama il Sennett – pregiano di modernità il ruolo imprenditoriale [1].

Si tratta di andamenti che misurano la contemporaneità ma, a ben vedere, ogni discorso risulterebbe immiserito, se si mancasse di dar conto dell'apporto della nuova tecnologia, della digitalizzazione, dell'intelligenza artificiale, ovverossia, di un ambito di incommensurabile portata rispetto a cui, inevitabilmente, resta tributaria ogni lettura che attenga alla modernizzazione dell'impresa.

Questo il crinale su cui svolgere l'analisi.

Si deve al recente approfondimento di autorevole dottrina se un varco viene aperto su tali scenari e si illustra lo sfondo di un fenomeno prorompente rispetto a cui il diritto è tenuto ad escogitare nuove categorie, un armamentario efficace e pertinente. Seguire i processi che interessano l'impresa moderna è cimentarsi nella lettura di fenomeni *in progress*: processi di elevata suggestione, “sagittali” e “in progressiva irradiazione”, che restituiscono l'attualità dell'impresa, effetto della utilizzazione della nuova tecnologia [2].

Le problematiche che ne discendono appaiono propedeutiche alla rimozione di un superato bagaglio tecnico-giuridico e all'introduzione di ulteriori principi in grado di assicurare *standards* di efficienza. E, stabilmente, ricorrono questioni attinenti alla buona *governance*, alla responsabilità degli organi societari, al rischio d'impresa, avvertendosi che l'intelligenza artificiale costituisce, in quanto tale, «autonomo rischio

d'impresa che deve essere adeguatamente valutato e governato dall'organo amministrativo, secondo un nuovo paradigma di Corporate Digital Responsability […] nuova e specifica sottocategoria della più ampia Corporate Social Responsability» e, difatti, la «Corporate Digital Responsability impone […] la definizione di apposite strategie di governance improntate ad una compliance socialmente orientata dei requisiti normativi attinenti allo sviluppo e all'utilizzo di tecnologie digitali, primo tra tutti quelli codificati nel Regolamento in materia di protezione dei dati personali e nel proposto Regolamento in materia di intelligenza artificiale» [3].

L'impresa è in progressivo divenire e la mutazione degli assetti d'impresa si avverte quale riverbero dell'incidenza di fenomeni endogeni ed esogeni. Si incastona, in tali processi di *renovatio*, la tecnologia innovativa in un'accezione addirittura "autoreferenziale", in quanto capace, la tecnologia innovativa di sviluppare processi di azione che conseguono al proprio apporto e non traggono forza dall'esterno [4].

Sovvengono rischi non marginali allorché le nuove scienze – nel caso specifico, la nuova tecnologia e i principi che vi attengono – si incrociano con l'economia.

Sarebbe stato Joseph Schumpeter ad avvertire «lo sfaldamento del rapporto "oggettivo" tra scienza ed economia», e il celebre economista austriaco, superata «la fragile staticità del discorso marginalista», individuava, «all'interno del processo produttivo, le forze propulsive dello scarto innovativo, che rende nuovamente competitivo e dunque dinamico il modello. Uno scarto, denso di contingenza e di rischio, che invalida i sistemi di equazione che lo volevano determinato, prevedibile, e ne fa un *novum*, che resta indeducibile dal flusso della riproduzione semplice». Conclude icasticamente Schumpeter: «C'è un nesso strutturale tra ricerca e sviluppo» [5] e fonda, su questo, l'apporto idoneo e corretto delle nuove tecnologie all'attività dell'impresa.

Aderendo a una visuale realista, è attendibile ritenere che la tecno-scienza costituisca valore, essa stessa, e non già valore aggiunto, ma stabile "valore di struttura". Il superamento di un tralaticio paradigma eleva ad archetipo di modernità un assetto dell'impresa recettivo delle varie opportunità offerte dalle tecnologie necessitando, per effetto, una ristrutturazione degli assetti interni. Affrancarsi da stereotipati *clichés* avrebbe comportato la indefettibilità di ridisegnare gli assetti organizzativi, gestionali, manageriali in ragione dell'apporto tecnologico e digitale [6]: questo il *novum* d'impresa strettamente connesso alla prerogativa di ingenerare processi di incremento produttivo, riduzione dei costi di produzione, rafforzamento delle spinte alla competitività entro

circuiti di portata globale.

La somma degli addendi – strumenti di intelligenza artificiale e processi interni all'impresa – denota l'identità della moderna impresa e la stabile allocazione entro perimetri di *new economy*. Metro di classificazione dell'avanzamento aziendale è l'accesso all'utilizzo della rete, stabilendosi una demarcazione che attiene ai criteri dell'*old* e del *new* rispetto a posizioni antitetiche: *old-old*, inesorabilmente, vengono qualificate le imprese insuscettibili ad approvvigionarsi di modalità e strumentazioni telematiche con incidenze sui processi produttivi; *new-new* sono le imprese che operano esclusivamente utilizzando la rete informatica, accolte le sfide della modernità. Il *trend* apre a una ampiezza di orizzonti che arride all'impresa ora in grado di fruire dei benefici effetti della sburocratizzazione, del rinnovamento manageriale, della confezione di nuove forme di *governance*. Tutti processi implementativi di efficienza, snellezza, dinamicità che involgono il mondo dell'impresa.

Se ne avvertono le conseguenze e come risulti complesso commisurarsi ai processi di mutamento, cogliere le torsioni funzionali, imbastire un inedito strumentario del diritto. Potente sforzo in avanti del giuridico proteso a confezionare una modellistica giuridica di fattura *multilevel*, che misuri la vocazione globale dell'impresa tecnologica e digitale. I sentori più forti e le maggiori apprensioni attengono alla materia della protezione dei dati personali, al trattamento e all'utilizzo dei dati.

Materia sensibile, effetto di esigenze confluenti ovvero, da un lato, la vicenda della tutela della riservatezza della persona; dall'altro, la vicenda della tutela della trasparenza circa l'utilizzo dei dati personali. Portato, la prima, di idealità distintive della società di stampo liberale, inneggiante alla libertà di intraprendere; la seconda, conseguenza delle idealità democratiche, che rinviene, nel carattere di trasparenza, criterio e misura della conoscenza e della comunicazione, in una prospettiva partecipativa. Ciò consente di argomentare che il principio di tutela della riservatezza si coniuga al divieto di diffusione e pubblicizzazione di notizie e di elementi di conoscenza che attengono alla sfera privata della persona. Diversamente, la tutela della trasparenza attiene alla raccolta dei dati, a prescindere dalla loro comunicazione e diffusione.

Le ragioni del nuovo si innestano nei percorsi ermeneutici e il potente sforzo analitico induce a comporre le esigenze secondo una visuale estensiva dei diritti della personalità, in linea di coerenza col disposto dell'art. 2 Cost. evitandosi, così, sfaldamenti concettuali e derive destabilizzanti.

La polarizzazione delle esigenze intorno ad un fulcro trova amalgama con la legge 31 dicembre 1996, n. 675, a tutti gli effetti *plate-forme* stabilizzante l'esigenza del rispetto della riservatezza in materia di trattamento dei dati personali. All'art. 1 si enunciano indefettibili tutele: la salvaguardia della persona, i diritti delle persone fisiche, il richiamo delle libertà fondamentali e, quale primaria finalità, la tutela della dignità della persona con riguardo alla riservatezza e all'identità personale, inclusi i diritti delle persone giuridiche e di ogni altro ente o associazione [7].

Regime normativo confluito, in seguito, nel d.lgs. 30 giugno 2003, n. 196 ("Codice in materia di dati personali": c.d. "codice *privacy*") [8].

La *consecutio temporum* che scandiva il varo delle disposizioni normative avrebbe comportato altri interventi di riordino – nel 2011 e nel 2012 si apprestano disposizioni dirette a sciogliere nodi complessi –, e tuttavia, si perviene a una effettiva disciplina della materia una volta traslata la riflessione sul piano sovranazionale, denotando sensibilità il legislatore continentale, in particolare, per la tematica della riservatezza e del trattamento dei dati personali. A tali motivi si informava il *Regolamento generale sulla protezione dei dati* 2016/679 (*General Data Protection Regulation*, "GDPR"), del 27 aprile 2016, applicabile dal 25 maggio 2018, entrato in vigore in Italia con d.lgs. 10 agosto 2018, n. 101, a partire dal 19 settembre dello stesso anno, recante disposizioni per l'adeguamento dell'ordinamento nazionale. Nell'occasione, si provvedeva a modificare il testo del d.lgs. n. 196/2003, mediante il d.lgs. 10 agosto 2018, n. 101, e l'ordinamento nazionale avrebbe fatto propria l'esigenza di dotarsi di uno strumento di tutela del "diritto alla protezione dei dati personali", come autonomamente contemplato all'art. 8 CDFUE, insistendo su un assunto-cardine, ovverossia che il trattamento dei dati personali avvenisse "nel rispetto della dignità umana, dei diritti e delle libertà fondamentali", si enuncia all'art. 1 del citato d.lgs. n. 196/2003 in diretta connessione col disposto dell'art. 1 GDPR [9].

Il pregio della disciplina introdotta a mezzo della normativa decretale è condensare le varie questioni rientranti nella generale tutela della riservatezza, di talché, all'esito dello sforzo normativo profuso, si maturava una definizione circa il trattamento dei dati personali – ai sensi dell'art. 4 GDPR – circoscrivendo l'assunto di "dato personale" in una formula coerente [10]: «qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un

identificativo, come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economia, culturale, sociale» [11]. Agli estensori della citata definizione non sarebbe sfuggito che la liceità del trattamento dei dati personali presupponesse il "consenso" da parte dell'interessato rispetto a una o più specifiche finalità, *ex* art. 6, comma 1, GDPR, e che il titolare del trattamento dovesse essere in grado di provare che questo fosse stato prestato, *ex* art. 7, comma 1, GDPR, sempre che venisse preventivamente e adeguatamente resa allo stesso interessato la necessaria "informativa" «in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro», altresì, «per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici», come disposto dall'art. 12, comma 1, GDPR.

La *renovatio* normativa si commisurava alla "rivoluzione" tecnologica e digitale che investiva il mondo dell'impresa. E in funzione di tali andamenti una dottrina legge «le sfide che la digitalizzazione delle aziende pone al diritto delle imprese […] fenomeno già oggi immanente alle realtà imprenditoriali, alcune delle quali devono il loro successo agli algoritmi o esercitano comunque attività dagli stessi fortemente condizionate». Fenomeno tutto moderno «che ha visto in questi ultimi anni – e soprattutto è destinato a registrare in un futuro ormai prossimo – un'impetuosa accelerazione, direttamente proporzionale allo sviluppo tecnologico dei sistemi di intelligenza artificiale, alla loro capacità computazionale nel trattare una mole sempre più ampia di dati e alla conseguente maggiore attendibilità e accuratezza dei relativi output» [12].

Altresì, fenomeno che avrebbe richiesto di essere governato, di talché, ai primi di ottobre del 2017, il gruppo dei Garanti Privacy U.E. WP 29 adottava tre provvedimenti di cui, il primo, approvato in via definitiva in occasione della consultazione pubblica del 27 maggio 2017, recante il n. WP 248 rev.01, intitolato "*Guidelines on data Protection Impact Assessment and determing weheter processing is "likely result in hig risk" for the purposes of Regulation 2016/679"* (DPIA); il secondo e il terzo concernenti le *Guidelines on Personal data breache notification under Regolation 2016/679* (WP 250) e le *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251).

Se ne avvertiva la necessità stante l'irradiazione della informatizzazione inerente all'impresa e discendendone inedite situazioni di responsabilità giuridica rispetto al delicato ambito del trattamento dei dati personali: i provvedimenti varati dal gruppo dei

Garanti Privacy U.E. WP 29 illustravano punti specifici del GDPR quanto al corretto utilizzo delle tecnologie innovative, l'intelligenza artificiale, il *machine learning*, l'*internet* delle cose. L'introduzione dell'obbligo di valutazione in capo al titolare, eventualmente in capo al responsabile, dei rischi che inerissero al trattamento dei dati personali procurante compressioni dei diritti e delle libertà delle persone fisiche, costituiva aspetto da tenere in particolare conto e veniva trasfuso in due articoli specificamente tagliati in argomento: l'art. 24, che poneva l'assunto di provvedere alla previsione dei rischio ai fini della individuazione di misure tecniche e organizzative di contrasto; l'art. 35, che introduceva una valutazione "d'impatto" se i trattamenti, sussistendo le circostanze individuate nella norma, comportassero rischi elevati per gli interessati. Accedendo a un'analisi comparativa degli artt. 24 e 35, è agevole avvedersi che al gruppo dei Garanti Privacy U.E. WP 29, prima d'altro, premesse radicare termini netti di demarcazione tra la valutazione di impatto effettuata a seguito dell'analisi circa il trattamento dei dati personali e la valutazione di impatto all'esito della individuazione di specifiche misure se venissero richieste in conseguenza della valutazione effettuata.

Ma un rilievo è possibile avanzare, e attiene all'assetto regolamentativo restituito alla materia del trattamento dei dati personali dal gruppo dei Garanti Privacy U.E. WP 29: prima esigenza sarebbe stata quella di impostare una modalità di gestione del rischio, di modo che, avvertito il predetto rischio quale componente strutturale dell'attività d'impresa, sarebbe occorso confezionare idonee misure di contrasto, tese a ridurlo e/o ad eliminarlo. E rimedio rigorosamente da adottare, già nella fase iniziale del trattamento, sarebbe stato provvedere all'obbligo di valutazione del rischio afferente al trattamento stesso interessando il terreno della responsabilità del titolare della decisione, eventualmente, di altro soggetto responsabile.

La regolamentazione normativa elaborata induceva la scienza gius-commercialistica a riconsiderare paradigmi, revisionare registri, avvertire il nuovo e la imponderabilità del nuovo, specificamente, in ordine all'apporto, sempre più "esuberante", della tecnologia innovativa e della digitalizzazione coinvolte nell'attività d'impresa. Il trattamento dei dati costituiva materia viva, non immune da afferenze di varia entità, non da ultimo, afferenze coinvolgenti il piano dell'etica.

Accresciuto il carico delle complessità la scienza gius-commercialistica, richiesta di dare risposte e di rinvenire soluzioni sostenibili, non si sarebbe sottratta ai propri oneri, non da meno assumendo su di sé anche questioni venate di accezioni etiche. Vero è che

l'impatto procurato sull'attività d'impresa in conseguenza del nuovo trattamento normativo sarebbe stato potente, decisamente ammodernante, necessitando sforzi aggiunti per poter rinvenire un assetto di equilibrio tra l'esercizio dell'attività di impresa e la corretta gestione dei dati: orbene, un tale sforzo diretto al rinvenimento del corretto equilibrio, per massima parte, restava commisurato al giuridico e, per altra parte, rivolto all'etico, posto che la materia si presta alla intersezione della dimensione giuridica con quella etico-valoriale. Si è sostenuto che «grazie al metodo – il *meta odos*, la strada obbligata attraverso cui si perviene ai risultati – ciascuno trova il suo cammino e il sapere le sue salde fondamenta» [13].

L'apporto tecnologico e digitale e il ricorso all'intelligenza artificiale innalzano la soglia di rischio sociale con esiti potenzialmente perniciosi per l'impresa, e alle responsabilità afferenti propriamente al ruolo gestionale del *management*, e del ruolo amministrativo, si aggiunge un rischio più imponderabile, più insidioso, declinato secondo modalità strette a paradigmi di *Corporate Digital Responsability*.

Problematica avvertita da una dottrina che avvedutamente insiste sulle interazioni di responsabilità sociale d'impresa e sulla penetrazione delle tecnologie negli assetti societari, leggendo secondo approcci angolati: innanzi tutto – si osserva –, la «prospettiva della responsabilità sociale suggerisce […] una declinazione dei requisiti normativi rilevanti nel contesto societario automatizzato» ed è approccio che consente di «concretizzare attraverso le lenti della responsabilità sociale previsioni normative quali quelle predisposte dal Regolamento generale in materia di protezione dei dati personali ovvero dal proposto Regolamento sull'intelligenza artificiale, che [….] sono affette da un'intrinseca vaghezza, lasciando molta incertezza alle imprese che si trovano ad applicarle» [14].

Assunto propedeutico al primo attiene al rilievo che «la riconsiderazione delle disposizioni normative in punto di strumenti tecnologici, tra i quali l'intelligenza artificiale, alla luce del paradigma della responsabilità sociale d'impresa vale a rafforzare le istanze di accountability da parte dei portatori di interessi rispetto alle modalità con le quali la tecnologia viene in concreto utilizzata dalle società e alle finalità che ispirano tale utilizzo» e, ancora, si constata una certa debolezza, e inconsistenza, delle normative di settore. Difatti, «Il Regolamento in materia di dati personali non prevede alcun meccanismo di supervisione delle tecnologie impiegate per lo svolgimento di trattamento dei dati personali, contemplando unicamente dei poteri di

indagine di cui agli artt. 30, 35, 36, comma 1 e 58, comma 1 lett. b) RGDP in capo alle autorità di controllo, ossia, i Garanti della Privacy. La proposta di Regolamento in materia di intelligenza artificiale introduce invece al suo art. 17 un sistema di c.d. *quality management* relativo alle tecnologie IA impiegate, comprendente l'obbligo per le imprese interessate di predisporre un adeguato framework di accountability, idoneo a identificare *ex ante* le responsabilità connesse al governo (management) delle stesse tecnologie impiegate» [15].

Le argomentazioni appaiono condivisibili e l'auspicio è che si pervenga, in tempi non remoti, ad un espresso riconoscimento della *Corporate Digital Responsability*. Si chiosa ribadendo il punto: «la prossima approvazione della direttiva in materia di dovuta diligenza e responsabilità d'impresa, ponendo le basi di un primo statuto giuridico europeo della *Corporate Social Responsability*, potrebbe infatti contribuire a rafforzare il fondamento giuridico della responsabilità digitale» [16].

Il quadro normativo si commisura a preminenti esigenze di deterrenza, delineato un paradigma di garanzie tecnico-giuridiche, ed è il taglio del *Codice di Corporate Governance delle società quotate*, varato nel gennaio 2020, rivolto alle società con azioni quotate sul Mercato Telematico Azionario (MTA), gestito da Borsa italiana e approntato dal Comitato per la Corporate Governance. Vi si illustrano le condizioni di buon governo a cui dovranno attenersi le società italiane quotate ed espleta il Codice funzioni di raccordo assicurando le conformità alle *best practices* internazionali e svolgendo sia funzione propulsiva che funzione di verifica e monitoraggio annuale in ordine all'attuazione dello stesso Codice e all'osservanza prestata dalle società alle "raccomandazioni" impartite [17]. Va appena richiamato che l'adesione delle società al Codice è da ritenersi volontaria ed esplicitata nella *Relazione sul governo societario e gli assetti proprietari* e, altresì, che le società quotate si conformano alle disposizioni codicistiche prevalentemente curando gli aspetti di "sostanza" in via prevalente rispetto agli aspetti di "forma", e che le raccomandazioni impartite si uniformano al criterio *comply or explain*, basandosi l'applicazione del Codice su criteri di flessibilità e proporzionalità.

Più recente è la proposta di *Regolamento sull'intelligenza artificiale* (*Regulation on a European approach for Artificial intelligence*) [18] pubblicata dalla Commissione europea il 21 aprile 2021. Si legge nella "presentazione" che il Regolamento attiene all'«obiettivo di plasmare la legislazione europea sull'intelligenza artificiale (IA),

armonizzando, quindi, la normativa applicabile e caldeggiare l'innovazione, la sicurezza e la tutela dei diritti individuali». 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». Un manifesto di intenti denotante l'indefettibilità dell'apporto della tecnologia innovativa, e della digitalizzazione, nei processi d'impresa e in cui si afferma che: «la recente proposta di Regolamento si 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».

I fattori di progresso supportano il futuro dell'impresa a condizione, tuttavia, che venga garantita la sostenibilità e se l'impresa si denoti adatta e capace di sostenere la performatività tecnologica coordinando l'agire al moto dei flussi economici con *souplesse* e agilità di processi.

Motivi avvertiti dal legislatore europeo provvedendo, negli ultimi anni, ad antecedere alla proposta richiamata di Regolamento sull'intelligenza artificiale un novero di iniziative coese nei fini: 1) il *Libro Bianco sull'Intelligenza Artificiale* (COM 2020) 65 final del 19 febbraio 2020; 2) le *Linee guida etiche finali per un'intelligenza artificiale affidabile* approntate 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, individuante i risultati e illustrativa degli investimenti nella IA. Iniziative finalizzate a 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 (GDPR)».

Si dipanano i meccanismi di regolamentazione all'esito di una efficace normativa di settore, e tuttavia, se vi è evidenza che la modernità d'impresa attenga all'innesto nei

processi operativi della nuova tecnologia e della digitalizzazione, non sfugge, certo, che l'apporto delle tecnologie vada adeguatamente calmierato e sicuramente governato. Dentro l'accettazione consapevole di tale assunto va circoscritto il positivo, e il sano, dell'apporto tecnologico, persino in termini valoriali, affinché le opportunità dell'oggi non si convertano nelle difficoltà del domani: la cooptazione delle tecniche nell'impresa è indefettibile che avvenga in via indolore, non stravolgendo sedimentati equilibri.

Occorre, perciò, esercitare attività di *monitoring*, verificare che il rapporto uomo-macchina irrimediabilmente non pieghi a detrimento dell'uomo. Diversamente, il rischio crescerebbe in modo esponenziale e in misura ben maggiore rispetto alla “fisiologica” rischiosità d'impresa: gli scenari futuri si colorerebbero di un grigiore cupo, foriero di ulteriori complessità e pericoli, scenari post-moderni, in assoluto non inopinabili se dovessero intervenire dinamiche che sovvertissero gli assetti primigeni a beneficio delle tecnologie iper-innovative.

Analizzare i processi, non obliterando una visuale che potrebbe sembrare al momento immaginifica, è accogliere pertinenti sollecitazioni dottrinali e tenere in conto un monito: la imprescindibilità di ingegnare una «governance dell'intelligenza artificiale», risponde a premure “oggettive” come pure “soggettive”. Operare *a parte obiecti* è prestare cura al ruolo che l'IA riveste, e viepiù assumerà, quale «strumento di governo d'impresa ed elemento costitutivo degli assetti imprenditoriali»; operare *a parte subiecti*, con riguardo alle *policy*, è ri-definirne gli assetti e garantire «un ricorso effettivamente *trustworthy* agli strumenti di intelligenza artificiale, in funzione del più generale obiettivo di sostenibilità dell'impresa nel medio e lungo periodo» [19], in linea con quanto contemplato dal *Codice di Corporate Governance.* Di talché – si argomenta pertinentemente –, «le impetuose trasformazioni tecnologiche in atto […] 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» [20].

2. Obblighi informativi e tutela della privacy nell'impresa digitale

L'attività d'impresa esige cure insistite per gli ambiti dell'informazione, e della comunicazione, che rivestono una maggiore indispensabilità accentuato l'ingresso, nella vita d'impresa, delle “tecnologie dell'informazione e della comunicazione aziendale” (Ict) [21].

Il macigno delle conseguenze procurate all'esito di una manchevole e/o non corretta informazione prestata ricorre allorché si ravvisino lesioni procurate alla sfera della *privacy* e minanti il trattamento dei dati personali e soccorre il "Sistema Informativo Aziendale" (*Enterprise Information System*, o "EIS") registro delle informazioni contestuali all'esercizio dell'attività d'impresa e alla gestione delle risorse umane e tecnologiche. Il novero di informazioni raccolte attesta e ragguaglia, all'interno e all'esterno, circa le strategie dell'impresa.

Si coordinano i piani – il giuridico, l'etica relazionale, l'etica della responsabilità – ricorrendo questioni afferenti al trattamento dei dati e si pone il tema della individuazione della confacente strumentazione tecnico-giuridica di contrasto al rischio, sottolineando il positivo che risiede nella corretta gestione e nella adeguatezza, ma nella professionalità, dei soggetti-operatori che produttivamente "ingegnano" nuove forme di *governance* affinché l'impresa possa cimentarsi nei circuiti globali.

Si aprono varchi alle suggestioni e, facendo ricorso ad una suggestiva "immagine naturalistica", una dottrina immagina la normativa in tema di protezione dei dati personali come una "struttura ramificata" dipartendo dal fusto due rami vigorosi, "assi primari", «l'uno dal quale si sviluppa la disciplina delle basi giuridiche per effettuare il trattamento, l'altro relativo ai presidi organizzativi funzionali a eseguirlo correttamente. Il primo ramo a sua volta si articola in ulteriori propaggini, su ciascuna delle quali possono collocarsi le riflessioni della dottrina, per lo più giusprivatistica, sui diversi fondamenti di liceità del trattamento» [22]. Si rafforza l'immagine: «L'importanza della predisposizione di presidi organizzativi adeguati, in particolare, si comprende appieno se si pone in relazione con le diverse basi giuridiche del trattamento. Le cautele organizzative sono infatti richieste a prescindere che il trattamento si radichi sul consenso o sull'interesse legittimo, ma con una portata differente», di talché, «Nel primo caso può ritenersi infatti, semplificando, che esse integrino l'autotutela valutativa del titolare dei dati; nel secondo operano invece quali condizioni che permettono si superare la necessità del consenso» [23]. Si argomenta che l'eterotutela che informa la gestione organizzata, e procedimentalizzata, del rischio poggia su una impalcatura strutturale dell'impresa soverchiante rispetto all'autotutela che attiene al meccanismo della volontà dell'individuo e comporta un approccio alla disponibilità dei dati radicato su uno «stato di c.d. sovranità sugli stessi».

Rilievi pertinenti, e si avverte la generale consapevolezza circa il rischio dell'utilizzo

errato dei dati personali non restando ai margini le problematiche inerenti alla sicurezza cibernetica. D'altronde, è pur vero che le soluzioni avanzate non appaiono rassicuranti, anzi, alquanto deboli ad arginare l'incontenibile irradiazione del *web* e ad incanalare, entro ambiti di legittimità giuridica, la circolazione telematica incontrollata dei dati personali comunque richiesto il preventivo *screening* delle informazioni.

Il Regolamento U.E. n. 679/2016, corredato da 173 *considerando*, accolto dagli Stati membri e applicato in via diretta nei Paesi U.E., a partire dal 25 maggio 2018 [24], restituisce il quadro regolamentativo, allo stato, migliore possibile.

Si prevede, al comma 2, dell'art. 5, che ricorra competenza del titolare del trattamento dei dati personali disponendo che egli «deve essere sempre in grado di "comprovare" il pieno rispetto di questi principi». Si connette tale disposizione all'altra, in combinato disposto, dell'art. 24, rubricato "responsabilità del titolare del trattamento", delineante 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 riveste valenza propulsiva, insieme di indirizzo, rispetto alle regolamentazioni interne, sollecitando queste a delineare l'intelaiatura delle condizioni di applicabilità dei principi in materia di trattamento dei dati personali ed esortando le autorità garanti, e le autorità di controllo nazionali, a definire modalità pertinenti – documentazioni da esibire, procedure da attuare, mappature, utilizzo di *software* – a che possa delinearsi un assettoregolamentativostabile, a tutti gli effetti, una organica *regulation* della materia.

Regulation che contempla i vari aspetti – rilievo della sicurezza, previsione del rischio, valutazione dell'impatto della *privacy* con il tradotto delle relative declinazioni –, ma l'apporto di novità si rinviene nella previsione dei principi *privacy by design* e *privacy by default* che riproducono una "filosofia" del trattamento dei dati personali assolutamente nuova, imponendosi l'obbligo alle imprese di prevedere idonei strumenti a tutela dei dati personali. All'art. 25 GDPR si dispone che incombe sulle imprese l'onere di valutazione del rischio afferente all'attività esercitata (*Risk Based Approach*, principio della valutazione del rischio) e, in ragione di questa, si ha modo di quantizzare la responsabilità in capo al titolare, o in capo al responsabile, del trattamento tenendo conto di un novero di parametri, ovvero, natura, portata, contesto, finalità del

trattamento, nonché, probabilità e gravità dei rischi incidenti sui diritti e le libertà degli utenti: valutazione del rischio da effettuarsi al momento stesso della progettazione del sistema prima che il trattamento abbia inizio.

La *ratio* normativa su cui poggia l'assetto di tutela dei dati personali è "centralizzare" intorno alla figura dell'utente, obbligando il titolare del trattamento a ingegnare una effettiva tutela, non già, in punto formale, ma in punto sostanziale, denotandosi insufficiente che la sola progettazione in quanto tale, pur conforme alla normativa, consenta una effettiva tutela dell'utente.

Comunque sia, delineare una cornice di tutele giuridiche risponde ad una precisa premura del legislatore, europeo e nazionale, e perpetra esigenze di sano realismo giuridico. Il fervore interpretativo che coglie la scienza gius-commercialistica è indice di cure analitiche e il suggerimento di cantierare «una proposta di coordinamento interpretativo sistematico con i temi […] del governo delle società e delle connesse responsabilità» coglie nel segno e appunto in tale prospettiva – si argomenta – «è immediato cogliere un collegamento con la centralità che la predisposizione di assetti organizzativi adeguati è andata assumendo nella teorica della corretta gestione d'impresa». Di talché, si argomenta: «Rispetto a tale più ampio tema, l'ottica del rischio specifico per i dati induce a porre in correlazione il concetto di adeguatezza con l'obiettivo del conseguimento di un livello minimo di tutela, e ad individuare nella conseguente responsabilità una leva per mantenere un equilibrio tra diritti individuali e interessi di mercato» [25].

Tale argomentazione di sintesi spiega perché il trattamento dei dati personali attenga a una moderna attività d'impresa soverchiata da un preponderante rischio, ed è un rischio ingenerato dalla esuberante presenza della tecnologia innovativa e della digitalizzazione. Uno scenario governato da registri normativi asseverati a «logiche strettamente giuridiche di distribuzione dei poteri (di etero o di autodisciplina dell'esercizio dell'impresa) e di collocazione gerarchica degli interessi (in particolare alla sicurezza rispetto a quello del contenimento dei relativi costi in funzione di una maggiore distribuzione di utili)» [26].

L'impresa è aperta al divenire: la tecnologia sospinge e il diritto sostiene, indirizza, malleva, fende gli spazi. Il diritto applicato alla realtà dell'impresa presenta caratteri senza misura, non avverte senza limitazioni, posto che, senza misura, senza limitazioni, è l'apporto della tecnologia.

Sono suggestioni avvertite dal legislatore, e il GDPR restituisce la disciplina avanzata del trattamento dei dati personali commisurata alla figurazione delle connesse responsabilità e dei rischi.

Sarà opportuno evocare la normativa regolamentare europea e richiamare il disposto dell'art. 5 (*Principi applicabili al trattamento dei dati personali*), del Capo II (*Principi*) che pone a tema la tenuta del diritto alla riservatezza e il trattamento dei dati personali che funge da norma-vettore. Declina un "catalogo" di principi:

- alla lett. *a*) i principi di *liceità*, *correttezza* e *trasparenza* indefettibili ai fini del trattamento dei dati personali;
- alla lett. *b*) il principio di *limitazione della finalità* ponendosi stretta corrispondenza tra la raccolta dei dati personali e le finalità e gli obiettivi esplicitati escludendo che si possa esorbitare da questi;
- alla lett. *c*) il principio di *minimizzazione dei dati* occorrendo che i dati siano adeguati, pertinenti e commisurati alle finalità per le quali vengono trattati;
- alla lett. *d*) il principio di *esattezza* richiedendosi l'esattezza dei dati e il loro aggiornamento progressivo, pertanto, si impone l'adozione di misure adatte a rettificare, e/o cancellare, i dati alterati;
- alla lett. *e*) il principio di *limitazione della conservazione* disponendosi che la conservazione dei dati personali si rapporti strettamente a un dato periodo di tempo corrispondente al tempo occorrente a conseguire le finalità per le quali i dati vengono trattati. Viene altresì consentito di conservare i dati personali per periodi più lunghi a condizione che il trattamento sia effettuato a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica, a fini statistici;
- alla lett. *f*) il principio di *integrità e riservatezza* dei dati personali attiene ai profili di sicurezza e protezione degli stessi mediante l'utilizzo di adeguate misure tecniche e organizzative. Altresì, si prevedono misure di contrasto al trattamento dei dati quando non autorizzato, o manifestamente illecito; ancora, si regolamenta il fenomeno della perdita dei dati, la distruzione degli stessi, il danno accidentale;
- alla lett. *g*) il principio di *responsabilizzazione* rimanda alla persona del titolare dei dati a cui si richiede di comprovarne l'attendibilità.

L'art. 5 funge da baricentro della disposizione europea e affinché venga preservata la riservatezza dei dati personali, il GDPR prevede la sussistenza di un organo interno all'impresa ed è il Responsabile della protezione dei dati; impone un "registro delle

attività di trattamento"; predispone modalità tecniche per notificare le violazioni dei dati personali.

Disciplina della *privacy* e trattamento dei dati personali rimandano, di talché, a una tassonomia di motivi e ragioni che attengono ai profili tecnico-giuridici, non da meno, che si raccordano a valenze etiche, assunti valoriali, ammantandosi tale materia di utilità e interessi che involgono la sfera del privato come la sfera del pubblico. Si è rilevato pertinentemente che «l'evoluzione tecnologica sospinga verso modelli di co-regolazione tra pubblico e privato che, oltre a preservare sul piano giuridico il libero esercizio dell'impresa, sono funzionali a garantire alla tecnologia quel contesto flessibile e in continua evoluzione che la può agevolare e al contempo guidare senza diventare obsoleto. Il deterrente utilizzato è la responsabilità, la cui connessione con l'adeguamento a standard è esplicitata dallo stesso GDPR, che premia l'adesione a codici di condotta, ovvero la sottoposizione di attività o prodotti a certificazioni di sicurezza, con un'agevolazione nella prova della *compliance* ai requisiti normativi» [27].

Si avanza un rilievo, in ultimo: se è certo che la buona gestione e la corretta amministrazione dell'impresa attengono ai profili di modernità dell'impresa, ripensati a seguito dell'apporto delle tecnologie, sarà necessario che ve ne sia fruizione esterna e rileva, oltre modo essenziale, il piano comunicativo-informativo. Il "dovere di informare" si interfaccia al "dovere di agire informati" e rimandano, insieme, ad un fascio di diritti, e doveri, protesi alla cura della riservatezza e al corretto trattamento dei dati personali [28].

3. Tutela rimediale in ipotesi di violazione della privacy

La disciplina giuridica introdotta dal Regolamento UE in materia di *privacy* e trattamento dei dati personali utilizza il contributo fornito dai *considerando*, sede di risposte a molte istanze sollevate, e questi fungono da proscenio alla disposizione regolamentare. Il *considerando* 11 ha rilievo paradigmatico, stigmatizzato il 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».

Alle imprese di investimento viene fatto obbligo di veicolare corrette ed esaustive informazioni secondo i dettami 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*" – e, indulgendo sul corredo comunicativo-informativo, viene disposto che: «Le imprese di investimento dovrebbero accertarsi di disporre per tempo di tutte le informazioni 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).

Un auspicio viene formulato al *considerando* 5: «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 con l'aumentare dei volumi 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 richiesti per i depositari centrali di titoli (C.S.D.) apporta novità il *considerando* 2 che, preliminarmente ribadito «il carattere globale dei mercati finanziari», invita a «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 Organitation of Security Commissions* (Organizzazione internazionale delle commissioni sui titoli – I.O.S.C.O.) (principi C.P.S.S. – I.O.S.C.O.)» ovvero, di attenersi ai "catalizzatori", requisiti normativi richiesti per i depositari centrali di titoli (C.S.D.). Altre misure contemplate attengono alla disciplina degli strumenti finanziari, i tipi di attività, la determinazione del prezzo, la liquidità dei prodotti finanziari.

Si avverte la determinazione del legislatore europeo motivato ad approntare stabili assetti e si richiama il principio di "distribuzione dell'onere della prova" – nell'ordinamento interno regolato all'art. 2697 c.c. – correlandolo al distorto utilizzo e all'indebita divulgazione dei dati: l'esigenza di perimetrare la materia entro confini certi sarebbe stata preminente e centrale sarebbe stato insistere su aspetti tali da intelaiare un tessuto di coerenze che valesse nei tradotti nazionali.

Ne costituisce prova l'utilizzo di un lessico giuridico omogeneo [29].

Il Regolamento europeo riempie vuoti e nel delineare la disciplina del trattamento dei dati personali inclina per una regolamentazione 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) – tenendo a specificare che il "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», di talché, «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 illustra, all'art. 24, l'entità della responsabilità commisurando al piano oggettivo, al verificarsi della vicenda trasgressiva, e, quanto al piano soggettivo, alla individuazione del "responsabile del trattamento" a cui imputare la vicenda di responsabilità restituendone, distinguendo dalla figura del "titolare del trattamento", 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") ove rileva il nesso di consequenzialità: «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», di tal guisa, valutando

ammissibile il danno non patrimoniale e consentendo l'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 quelli 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 titolare del trattamento, analogamente del responsabile del trattamento, ricorre al § 3 e quivi si contempla l'inversione dell'onere della prova prevista una deroga alla regola generale: il resistente è tenuto ad accollarsi l'onere di prestare la prova in luogo del ricorrente, né sufficiente è 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. Infine, occorre che risulti inequivoca la volontà di assumere gli svantaggi dell'eventuale insuccesso all'esito della prova addotta.

L'inversione dell'onere della prova attesta che il trattamento non corretto dei dati si avverta alla stregua di attività “pericolosa" e recita l'art. 2050 c.c. (“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», di talché, si prevede l'inversione dell'onere della prova come rimedio funzionale alla compensazione del rischio incombendo l'obbligo 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 in conseguenza dell'altrui condotta difforme ai dettami della normativa sulla tutela dei dati personali; tanto meno, sottrarsi dall'accertare la sussistenza del nesso causale; dall'individuare la persona del titolare del trattamento e/o del responsabile del trattamento; dal confutare l'assunto che

l'evento dannoso sia imputabile a proprie mancanze.

L'omogeneità procurata latitudinalmente, raccordante le regolamentazioni nazionali in materia di trattamento dei dati personali, e l'utilizzo nella traduzione operativa dell'attività d'impresa, premia l'avvedutezza del legislatore europeo e il disegno continentale di confezionare discipline coerenti, di ingegnare modalità attuative che restituiscano certezza e contrastino la confusione normativa. Conformare a principi comuni il trattamento giuridico della materia avrebbe significato, infine, corrispondere al genuino spirito europeo e corrispondere alla consapevolezza, generale e condivisa, che la tecnologia costituisce la vera misura della modernità d'impresa, rafforzata dai processi di *technical* e *digital transformation*, se mai da calmierare – si diceva –, giammai da ostacolare.

Un patrimonio di idee presiede allo sforzo di forgiare uno strumentario giuridico adeguato ed efficace e ne costituisce prova, nel tradotto interno, l'aggiornamento offerto dal Codice della *privacy*, che introduce modifiche alla precedente regolamentazione ascendente al D.L. 14 giugno 2019, n. 53, dal d.m. 15 marzo 2019, e al d.lgs. 10 agosto 2018, n. 101 (“Decreto di adeguamento al G.D.P.R.”), quest'ultimo, varato in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (l. 25 ottobre 2017, n. 163), in vigore nei paesi dell'Unione dal 25 maggio 2018 e diretto ad armonizzare il Codice della *privacy*alla normativa europea.

Avvertiva il legislatore l'entità dei rischi prodotti a cagione di un indebito, esuberante e non adeguatamente controllato utilizzo dei dati personali e all'anomala propensione a tracimare i limiti della tolleranza. Condotte che avrebbero richiesto un intervento di argine all'indiscriminata libertà di utilizzo dei dati afferente ad una malsana idea di indiscriminata e assoluta libertà, da esercitarsi comunque, anche se causa lesioni alla sfera dei diritti personali. A tali motivi corrisponde il Codice della *privacy* che eleva il livello di tutela della persona in materia di trattamento dei dati personali, correlando al “principio di necessità” (art. 3, d.lgs. n. 196/2003) che dispone la limitazione dell'utilizzo dei dati personali da parte dei sistemi informativi favorendo l'utilizzo di dati anonimi.

Questione che si espande su un terreno adiacente intricato e di non agevole regolamentazione normativa, relativo al risarcimento dei danni procurati dal titolare del trattamento, o dal responsabile del trattamento, e ripreso dal GDPR al *considerando* 146. Presenta, questo, una singolarità riscontrabile già sul piano della illustrazione del

principio utilizzando il legislatore 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» – segno che la disciplina ha tenore di suggerimento più che di disposizione stentorea e di imperativo normativo.

Il *considerando* 146 "fende" l'altra questione connessa, ovvero, della imputazione della responsabilità a seguito del danno 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». E si puntualizza: «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 dannocagionato dal trattamento, a condizioneche 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 il *considerando* 146 col garantire il pieno ristoro economico all'interessato leso nei suoi diritti 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 costituisca materia a cui prestare cure accentuate è provato dal rilievo che riveste l'aspetto della risarcibilità del danno e dell'individuazione dei criteri di imputabilità della responsabilità.

Il baricentro della responsabilità si sposta dall'autore del fatto dannoso alla vittima del danno e il presupposto da accertare viene posto in funzione di parametri: se la

responsabilità consegua a colpa; se l'autore materiale del danno corrisponda al soggetto a cui imputare la colpa; in quale misura la vittima del danno debba essere risarcita. Non poche suggestioni conseguono all'interprete dall'esegesi del *considerando* 146 e si avverte tutta la difficoltà di restituire una configurazione coerente della responsabilità, e del danno, ponderata ogni circostanza.

Un rilievo si ritiene utile avanzare ancora e attiene ai *considerando* – questione appena lambita in precedenza – che in modo conciso motivano le norme essenziali dell'articolato, pur non riproducendone e/o parafrasandone il dettato. La mancanza di una enunciazione a carattere normativo fa dubitare dell'afferenza al piano giuridico.

Si onera della questione la recente ordinanza emessa dalla Cass., sez. V, 7 marzo 2022, n. 7280 – analogo chiarimento si legge nella "Guida pratica comune" del Parlamento europeo e del Consiglio, e della Commissione approntata per la redazione dei testi legislativi dell'Unione europea del 2015 – che chiarisce, in linea generale, la portata da attribuire al "diritto unionale" e argomenta che i *considerando* assumono valenza esplicativa delle ragioni sottese all'intervento normativo, integrano le disposizioni con "concisa motivazione", sebbene non corrispondano a enunciazioni di portata normativa.

Su questa *raison* poggia la pronuncia della Suprema Corte: a corredo degli atti normativi dell'Unione europea i *considerando* presentano, al più, portata enunciativa, né – sostiene il giudice di legittimità – «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, c.p.c.» [30].

4. Gestione dei dati e accesso alla rete

Insistere sul concetto di equilibrio costituisce una costante dell'apporto ermeneutico ed il concetto di equilibrio normalmente viene evocato come antidoto al rischio.

Vale tale rilievo traslando all'impresa, e alle trasformazioni che interessano l'impresa, la prefigurazione di inediti scenari di responsabilità, la morfologia del rischio in tempi di tecnologie innovative e di digitalizzazione.

I riverberi della modernità si irradiano lungo percorsi inopinabili e il crescente impegno della gius-commercialistica è proteso a rinvenire una sintesi che riassuma le varie esigenze centrate nel punto di equilibrio. Effetto da scongiurare è la "liquefazione" dell'equilibrio, dunque, di non poter dispiegare le innovazioni introdotte lungo il "secolo *biotech*".

Rispetto a tempi iniziali, l'equilibrio intorno al fulcro costituito dall'impresa avrebbe supposto una intelaiatura di assetti garantistici e una strumentazione di tipo deterrente e rimediale, richiesta al diritto e dal diritto fornita. Correndo gli anni Novanta dello scorso secolo sarebbe di seguito lievitata una sensibilità ulteriore in materia di *privacy* e di trattamento dei dati, così, evolvendo una normativa di settore interattiva dei piani interno ed esterno dell'impresa.

Fatte proprie molte e decisive consapevolezze, maturate in ambito continentale, il legislatore interno si premuniva ad apprestare il varo della l. 31 dicembre 1996, n. 675 (*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*), normativa confluita nel d.lgs. 30 giugno 2003, n. 196 (*Codice in materia dei dati personali*) – ovvero, il *Codice della privacy*, attualmente coordinato ed aggiornato, da ultimo, con le modifiche apportate dal d.l. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla l. 3 dicembre 2021, n. 205 e il cui Titolo originario ("Codice in materia dei dati personali") era dismesso e sostituito dall'art. 1, comma 1, del d.lgs. 10 agosto 2018, n. 101, con quello di "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE". Insistiti ed espliciti riferimenti al rispetto dei diritti e delle libertà fondamentali, nonché al valore di dignità della persona, "elevano" la nuova normativa e ne pregiano i tradotti, restando valorizzati i principi di riservatezza e idoneità personale, imbastite coerenze col dettato dell'art. 8 della Carta dei diritti fondamentali U.E.

Ne sarebbe discesa la necessità di pervenire ad un equilibrio dei piani normativi, sovranazionale e nazionale, e di modulare gli strumenti, e i meccanismi, utili ad assicurare una coerente correlazione: sarebbe stato merito dell'apporto dottrinale, e della *interpretatio* giurisprudenziale, offrire le opportune delucidazioni, verificato il grado di conformità ai dettami europei della normativa interna in materia di *privacy* e di trattamento dei dati, ma estendendo alla responsabilità imputabile ai motori di ricerca. Affiora, in primo piano, la cosiddetta "ragnatela intorno al mondo" – all'uopo utilizzata, in modo convenzionale nella latitudine globale, la sigla *world wide web* (w.w.w.) – attinente alla generale condivisione di documenti ipertestuali multimediali frutto di assemblaggio di elementi testuali, visuali, auditivi, veicolati sulla infrastruttura di

Internet.

Le attività di selezione dei dati, indicizzazione, memorizzazione, messa a disposizione degli utenti di connessioni, orbene, tutta questa materia avrebbe costituito oggetto di disamina e approfondimento da parte della Corte di giustizia dell'Unione europea e questo giudice si sarebbe espresso con una pronuncia, di importante tenore, delineando la cornice in cui inscrivere la disciplina. Trattasi della decisione emanata all'esito della nota vicenda giudiziale C-311/18, *Data Protection Commissioner v/s Facebook Ireland Ltd e Maximillian Schrems* (Schrems II), e la Corte, sollecitata riguardo alla possibilità di trasferire i dati personali secondo i dettami posti dalle norme vincolanti d'impresa, rimarcava che la protezione dei dati personali avrebbe dovuto transitare, all'interno dello spazio economico continentale (S.E.E.), contestualmente al transito dei dati stessi, ovunque fossero trasferiti, in quanto il trasferimento transfrontaliero dei dati personali non avrebbe né minato, né indebolito, le tutele predisposte nello S.E.E.

Tanto deciso dalla Corte di giustizia UE, pure, la decisione non avrebbe necessariamente comportato l'obbligo di predisporre *ubique* identiche e altrettante garanzie, all'interno dei confini continentali, piuttosto, impresso uno sforzo plurale così da radicare un denominatore comune che ponesse equivalenze quanto alle garanzie da prestare e le clausole contrattuali-tipo da utilizzare, ovvero, le modalità di trasferimento fruibili in via generale e in grado di garantire, rispetto al piano contrattuale, una protezione che non risultasse difforme, entro i confini europei, in materia di tutela dei dati personali.

I riverberi nel diritto interno sarebbero stati coerenti, conformi allo spirito dei tempi, e ne costituisce prova la "Dichiarazione dei diritti in Internet" – nuovo testo redatto in 14 articoli presentato alla Camera dei deputati in data 14 luglio 2015 – ove viene ripreso il rispetto dell'equilibrio, ora, tra una esigenza di futuro, tradotta nella forza propulsiva della rete, e la garanzia giuridica prestata a tutela della *privacy* e del corretto trattamento dei dati personali. Si legge nel Preambolo, con misurata enfasi, 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», 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».

Un segmento temporale non ampio separa la vigente disposizione regolamentare dall'altra, di poco precedente, il Regolamento U.E. n. 2120, datato 25 novembre 2015, disciplinante l'accesso alla rete, inclusivo di riferimenti al circuito "internet aperta" – c.d. *net neutrality* (N.N.), o *Internet neutrality* –, fortemente inteso dal legislatore europeo al fine di correlare stabilmente il principio di neutralità al principio di non discriminazione e connettere, entro un assetto di omogenea regolamentazione, i circuiti di gestione e di utilizzo dei dati. La forza perlocutiva dell'enunciazione è 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 è posto il principio assiomatico, ovvero, il principio di "neutralità della rete" legittimante un agire informato a imparzialità, correttezza, ragionevolezza confliggente derive miserevoli e un utilizzo mercenario della rete.

Riferimenti bibliografici

[1] La tesi di sicura suggestione, esposta dal Sennett, attiene al motivo centrale del "capitalismo flessibile" (R. SENNETT, *L'uomo flessibile. Le conseguenze del nuovo capitalismo sulla vita personale*, tr. it. Milano, 2007, *passim* e si insiste su una questione che assume forza preponderante e che rimanda al ruolo del diritto, scienza sociale, trainante ai fini di indirizzo e gestione dei processi trasformativi. In tema, rilievi pertinenti vengono dalla lettura offerta da Sandro Luce il quale osserva che «In un mercato sempre più globale e deterritorializzato sorgono seri dubbi tanto sulle modalità, quanto sui soggetti politico-giuridici legittimati ad elaborare un complesso di regole valide e vincolanti i diversi attori-agenti, e dotati della forza necessaria a farle rispettare. Ci troviamo innanzi a due dispositivi che mostrano oggi una sostanziale dissonanza: da un lato, il mercato, estremamente variabile, che non conosce confini ed è in grado di espandersi illimitatamente; dall'altro la legge che, nei termini tradizionali di prescrizione, è rigida, certa e si applica su uno specifico territorio». Di talché, argomenta l'a., «Da questa incongruenza nasce la cosiddetta terza via, quella del contrattualismo, da cui prende le mosse l'odierno capitalismo finanziario e da cui nascono le nuove, ma sotto certi aspetti già vecchie. Rivendicazioni di regolazione giuridica» (S. LUCE. *Keynes e i nipotini in crisi: la svolta bioeconomica*, in L. BAZZICALUPO, A. TUCCI (a cura di), *Il grande crollo. È possibile un governo della crisi economica?*, Milano-Udine, 2010, 64, e l'a. richiama, a proposito dell'ultima opzione concettuale, la "terza via" da cui germina il "capitalismo finanziario", lo studio di G. ROSSI, *Il gioco delle regole*, Milano, 2006, *passim*). In realtà, una quarta via, che "si incastona" adeguatamente nei processi di modernizzazione attiene proprio alla nuove sfide a cui viene chiamata modernamente l'impresa a condizione che questa proceda a strategiche innovazioni, strutturali e funzionali, ripensate le forme di *management*, rivisitata l'attività gestoria e amministrativa, provveduto al confezionamento di uno strumentario adeguato, oramai, cambiati, addirittura sovvertiti, i modi di produzione, i processi di valorizzazione e gli assetti di cooperazione.

[2] Osservano Abriani e Schneider che, all'indomani dell'ingresso della tecnologia innovativa, della digitalizzazione, dell'intelligenza artificiale nell'impresa, si schiude una nuova stagione foriera di innovazione e di sviluppo.

[3] N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021, 291 s., che richiamano il *Regolamento*

generale sulla protezione dei dati (RGPD) – *General Data Protection Regulation* (GDPR) –, ossia, Regolamento UE n. 2016/679 avvertita, l'Unione Europea, l'impellenza di provvedere alla tutela dei dati personali e della *privacy* dei cittadini del vecchio continente e dei residenti in Europa, all'interno e all'esterno dei confini, e rendendo omogenea la normazione di settore entro i *limina* europei.

[4] Una teorica dai notevoli decisivi risvolti sociologici messa a punto da H. FREYER, *Theorie des gegenwartigen Zeitalters*, Stuttgart, 1956, *passim*.

[5] L. BAZZICALUPO, *Il governo delle vite. Biopolitica ed economia*, pref. di R. Esposito, Roma-Bari, 2006, 97, ove si richiama il celebre saggio di J. SCHUMPETER, *Teoria dello sviluppo economico* [München 1912, Berlin, 1934], tr. it. Firenze, 1971, *passim*. Si legga altresì, dello stesso a., *Business cycles. A theoretical historical and statistical analysis of the capitalistic process* [New York-London, 1939], tr. It. parz., *Il processo capitalistico. Cicli economici*, Torino, 1977, *passim*.

[6] Si consenta un rilievo, in questo stadio dell'analisi, e attiene alla capacità della moderna impresa di costruire ricchezza e perseguire gli obiettivi di produzione prefissati. Orbene, si ritiene di non esondare dai confini dell'analisi nel fare riferimento a un aspetto che, modernamente, si pone come effettiva chiave di volta della trasformazione delle categorie economiche, ed è il nuovo concetto di consumo. Adam Smith asseriva che il consumo è il solo fine di ogni produzione (A. SMITH, *Indagine sulla natura e le cause della ricchezza delle nazioni*, tr. it. Milano, 1973, 301) e il favore che, attualmente, il consumatore presta al prodotto d'impresa, infine, è restituire, in termini di consapevolezze e di gradimento, il favore per l'azienda produttrice accreditandone l'operato e l'attitudine a competere sui mercati. Orbene, non cade dubbio che l'accoglimento, e la soddisfazione, della platea dei consumatori accresce quando il prodotto pervenga a uno stadio di qualità superiore ed è altrettanto indubitabile che il miglior prodotto consegue all'ingresso delle nuove tecnologie nell'impresa. Orbene, la complessità del moderno comporta che anche il consumo si presti a trasformazioni corrispondendo a logiche eterogenee, non omologabili, così, progressivamente, ma inesorabilmente, restringendosi la distanza tra produttore e consumatore, tanto, che sarebbe venuto in uso il temine *prosumer* di inedita forgia, crasi di *producer* e *consumer* – (introduceva il neologismo A. TOFFLER, *La terza ondata*, tr. it. Milano, 1987, *passim*) –, esemplare di un processo di confluenza di simbiotiche esigenze e accorciamento delle distanze.

[7] Opportuno notare che la citata l. n. 675/1996 prevede la tutela dei dati personali a prescindere dalla loro comunicazione e diffusione. Oggetto della norma, pertanto, deve intendersi ogni attività che attenga ai dati personali e ne restituisce contezza la seconda parte dell'art. 1 ove si parla, in modo circoscritto, di raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, cancellazione, distruzione di dati ed è, questa, elencazione meramente indicativa. Argomenta, conseguentemente, una dottrina che «L'oggetto primariamente tutelato dalla l. n. 675/1996 è dunque la trasparenza e non la riservatezza; devono indurci a questo tipo di lettura non soltanto ragioni di carattere storico e di diritto comparato, ma soprattutto il fatto che la legge prevede una serie di istituti sorti per disciplinare le raccolte dei dati; e l'applicazione di tali istituti alla semplice comunicazione o diffusione di dati, anche singoli e non strutturati, amplia l'ambito di applicabilità della legge in misura abnorme e probabilmente incostituzionale». E ancora si argomenta che proprio «Per tutelare la trasparenza delle raccolte dei dati la legge realizza un processo di "oggettivazione" del dato personale. Questo viene tutelato non soltanto come aspetto dell'individuo, ma in sé, come oggettivamente identificabile e indipendente sia da chi lo ha creato, sia da colui al quale si riferisce come oggetto di un diritto assoluto, esperibile cioè nei confronti di chiunque. Esso è diretto, infatti, non ad attribuire a un soggetto la capacità esclusiva di utilizzazione di un'entità economica, ma a tutelare la personalità dell'individuo rispetto al potere informatico». Si è al cuore della questione e si chiosa: «Di conseguenza il diritto sui dati personali deve essere considerato come un vero e proprio diritto della personalità. La difesa dell'individuo nei confronti del potere informatico, l'*habeat corpus* della moderna era cibernetica» (E. GIANNANTONIO, s.v. *Dati personali (tutela dei)*», in *Enc. dir.*, *Aggiornamento* III, Milano, 1999, 485).

[8] Da menzionare la previsione dell'art. 2-*decies*, d.lgs. n. 196/2003 mediante cui si dispone che «i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati» (con eventuali eccezioni) nell'ambito di procedimenti giudiziari, secondo le «pertinenti disposizioni processuali» (art. 160-*bis*).

[9] Taluni "Principi generali concernenti il trattamento dei dati personali" vengono assunti dal GDPR e attengono alle modalità di utilizzo dei dati secondo principi fermi e inderogabili. Tali sono il principio di "liceità, correttezza e trasparenza" da esercitarsi

nei confronti dell'interessato. Altresì, il principio della "limitazione della finalità" nel senso che i dati devono raccogliersi «per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità». Ancora, si richiama il principio della "minimizzazione dei dati" nel senso che, gli stessi, devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattai». In ragione del principio di "esattezza" i dati devono risultare «esatti e, se necessario, aggiornati e occorre che vengano «adottate tutte le misure ragionevoli per cancellare o rettificate tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati». Vige, altresì, il principio di "limitazione della conservazione" in quanto i dati raccolti vanno «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati» e il principio di "integrità e riservatezza" dovendosi trattare i dati raccolti «in maniera tale da garantire un'adeguata sicurezza […] compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale». Non da ultimo, va menzionato il principio di "responsabilizzazione" precisandosi che «il titolare del trattamento è competente per il rispetto de principi accennati».

[10] Il legislatore avrebbe avuto sentore che una specifica particolare categoria di dati esorbitava, comunque, da questo assetto e si sarebbe trattato dei dati c.d. sensibili, di talché, si premurava di prevedere, per essi, apposite regole di cautela (art. 9, comma 2 e 4, GDPR; e artt. 2-*sexies* e 2-*septies* d.lgs. n. 196/2003) trattandosi, si enuncia *ex professo*, di «dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale», nonché, di «dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (art. 9, comma 1, GDPR), nonché, di «dati personali relativi alle condanne penali e ai reati» (art. 10 GDPR e art. 2-*octies* d.lgs. n. 196/2003).

[11] Su questa impostazione, nello specifico sull'aspetto della identificazione in via diretta o indiretta della persona, si sarebbe pronunciata la Cass. 5 luglio 2018, n. 17665 rimarcando il giudice di legittimità la necessità dell'informativa e del consenso dell'interessato ai fini della relativa utilizzazione.

[12] N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale*, cit., 290.

[13] N. ABRIANI, G. SCHNEIDER, *op. cit.*, 302.

[14] N. ABRIANI, G, SCHNEIDER, *op. cit.*, 280.

[15] N. ABRIANI, G. SCHNEIDER, *op. cit.*, 281.

[16] N. ABRIANI, G, SCHNEIDER, *op. cit.*, 283.

[17] Per ulteriori chiarimenti v. borsaitaliana.it/comitato-corporate-governance.

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

[19] N. ABRIANI, G. SCHNEIDER, *op. cit.*, 291.

[20] N. ABRIANI, G. SCHNEIDER, *op. cit.*, 300.

[21] L'essenzialità della dimensione simbolico – comunicativa veniva colta da una dottrina già a partire dagli anni '70 e '80 dello scorso secolo. Si rimanda, per tutti, al saggio-pilota di P. BOURDIEU, *Le sense pratique*, Paris, 1980, *passim*.

[22] L. MIOTTO, *Organizzazione di impresa e gestione dei dati personali. Il rischio di non* compliance *nelle catene di fornitura*, Torino, 2022, 1. Afferiscono alla dialettica gius-privatistica le questioni inerenti alle condizioni di validità del consenso del titolare dei dati e, quanto all'interesse legittimo, la legittimità di procedere al trattamento dei dati anche in mancanza dell'acquisizione della volontà autorizzatoria. Ancora, le discussioni in ordine alle fattispecie rispetto alle quali i dati vengano trattati ottemperando ad obblighi contrattuali e obblighi legali, ovvero, a fini di tutela di interessi vitali della persona interessata o di terzi, ovvero, nell'esercizio di poteri pubblici.

[23] L. MIOTTO, *Organizzazione di impresa e gestione dei dati personali*, cit., 2.

[24] 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*).

[25] L. MIOTTO, *op. cit.*, 7 s. Il ragionamento è portato sino a un limite ermeneutico e l'a. chiarisce il concetto-assioma su cui fonda la costruzione analitica, in punto di idoneità/inidoneità, in punto di omogeneità/disomogeneità operativa dei meccanismi di

salvaguardia: «È peraltro evidente il pericolo di inidoneità e soprattutto di disomogeneità applicativa di un meccanismo per la salvaguardia di interessi esterni indisponibili che si basi su autovalutazioni degli stessi soggetti coinvolti. In questa chiave critica i effetti si leggeranno i plurimi interventi che, dispiegati su tutti livelli delle fonti giuridiche, hanno in vario modo delimitato la nozione di adeguatezza organizzativa nella materia della sicurezza dei dati, per lo più stabilendo schemi procedimentali standard da seguire, talvolta giungendo a individuare possibili misure tecniche da implementare».

[26] L. MIOTTO, *op. cit.*, 7.

[27] L. MIOTTO, *op. cit.*, 8.

[28] Si deve al contributo molto recente di una dottrina gius-privatistica la sistemazione concettuale dei principi afferenti alla informazione in linea con i parametri di trasparenza e conoscenza, quanto altresì comporta correttezza nelle movenze e nell'agire. Si è sostenuto, con profondità analitica, che nelle moderne società complesse e tecnologiche l'informazione si connota come "bene giuridico" in sé, altresì, come fattore di efficienza economica e di trasparenza del mercato: «L'agire leale e corretto è comportamento che immediatamente tutela i soggetti del rapporto, ma mediatamente si risolve a vantaggio del funzionamento del mercato in quanto consente di selezionare le imprese virtuose efficienti attraverso un corretto gioco della concorrenza». E ancora: «Nell'attuale esperienza di produzione di massa e globalizzata, la scelta non è tra prodotti ma tra rappresentazione di prodotti, sicché l'informazione, determinando trasparenza e conoscenza, diventa leva essenziale di un mercato non solo efficiente ma anche equo» (F. BOCCHINI, *Il contratto*, Torino, 2023, 50 s., da F. BOCCHINI, E. QUADRI, *Diritto privato*, Torino, 2022, IX ed.).

[29] 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 di trattamento* (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 controllo interessata* (al punto 22),

trattamento transfrontaliero (al punto 23), *obiezione pertinente e motivata* (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.

[30] In tema, cfr. V. SICILIANO, *Diritto tributario e funzione dei "Considerando" riportati in un Regolamento UE*, in *Judicium. Il processo civile in Italia e in Europa*, in *judicium.it.*