RIFLESSIONI SU NUOVE TECNOLOGIE, TUTELE E PRINCIPIO DI SOSTENIBILITÀ

REFLECTIONS ON NEW TECHNOLOGIES, PROTECTIONS AND THE PRINCIPLE OF SUSTAINABILITY

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 886-975

Luca DI NELLA

ARTICOLO CONSEGNATO: 8 de octubre de 2022
ARTICOLO APPROBATO: 5 de diciembre de 2022

ABSTRACT: Lo scritto analizza il concetto e le applicazioni della IA, degli *smart contract*, delle *DLT* e delle *blockchain* ed espone la disciplina in materia, anche nell'ottica *de iure condendo*. Su questa base vengono svolte delle considerazioni sulla *Legal Technologie* e si affronta il tema dell'impatto delle nuove tecnologie sui mercati, concentrando l'attenzione sulla economia della piattaforma, sulle negoziazioni algoritmiche nei mercati finanziari e sulla circolazione dei dati personali e non personali. Viene altresì analizzata la nozione di consumatore nell'*Ecommerce*. Infine, si propone di applicare il principio di sostenibilità quale strumento per risolvere i problemi posti dalle nuove tecnologie.

PAROLE CHIAVE: Intelligenza artificiale; *Smart Contract; Blockchain; Legal Tecnologie;* Economia della piattaforma; Mercati finanziari; Negoziazioni algoritmiche; Dati personali; Dati non personali; Circolazione; Ecommerce; Consumatore; Principio di sostenibilità.

ABSTRACT: *The paper analyzes the concept and applications of AI, Smart Contracts, DLTs and Blockchains and describes legislation in the area, including from the perspective of de iure condendo. Legal Tech is discussed on this basis and the impact of new technologies on the markets is addressed, with a focus on the platform economy, algorithmic trading in financial markets and the movement of personal and non-personal data. The role and status of the E-commerce consumer is analysed in the light of the recent ruling by the European Union Court of Justice. Finally, application of the principle of sustainability is proposed as a tool for solving the problems posed by new technologies.*

KEY WORDS: *A.I.; Smart Contract; Blockchain; Legal Tecnologie; Platform Economy; Financial Markets; Algorithmic trading; Personal Data; Non-Personal Data; Ecommerce; Consumer; Sustainability Principle.*

SOMMARIO.- I. INTRODUZIONE. - II. INTELLIGENZA ARTIFICIALE E RESPONSABILITÀ. - III. BLOCKCHAIN, SMART CONTRACT E DIRITTO DEI CONTRATTI. - IV. CONSIDERAZIONE SULLA LEGAL TECH. - V. L'IMPATTO DELLE NUOVE TECNOLOGIE SUI MERCATI: L'ECONOMIA DELLA PIATTAFORMA; I MERCATI FINANZIARI E LE NEGOZIAZIONI ALGORITMICHE. - VI. LA CIRCOLAZIONE DEI DATI PERSONALI E LE TUTELE. - VII. LA CIRCOLAZIONE DEI DATI NON PERSONALI. - VIII. L'E-COMMERCE E IL CONSUMATORE. - IX. L'EVOLUZIONE TECNOLOGICA E LE TUTELE NEL PRISMA DEL PRINCIPIO DI SOSTENIBILITÀ.

I. INTRODUZIONE.

Tra le molteplici questioni che impegnano l'esperienza giuridica contemporanea, in ragione della posta in gioco sicuramente suggestive sono quelle dell'impatto delle nuove tecnologie sulla realtà, della tutela della persona, della emersione di nuovi mercati e della circolazione dei dati personali e di quelli non sensibili. Siffatte problematiche pongono delle sfide che i legislatori italiano e unionale sono chiamati oggi ad affrontare, prestando più che mai attenzione al domani, ossia alle conseguenze sulla società e sull'ambiente che la normativa produce in una prospettiva di medio e lungo periodo[1]. Il riferimento inevitabile è quindi al principio sostenibilità, altra parola chiave della travagliata epoca contemporanea.

Le riflessioni che seguono vogliono rappresentare soltanto un primo approccio ad alcune tematiche che necessariamente andrà sviluppato in una chiave sistematica che è resa complessa dalla varietà degli argomenti trattati e dalla normativa applicabile, ma che ciò non ostante è imprescindibile per dare risposte coerenti ai problemi (presenti e futuri) da affrontare[2]. Una prima chiave di lettura non può che essere il principio di sostenibilità.

II. INTELLIGENZA ARTIFICIALE E RESPONSABILITÀ.

Tra le innovazioni sicuramente più avanzate e, nel contempo, accattivanti per tutti i risvolti connessi va annoverata l'intelligenza artificiale (IA)[3]. Le reti neuronali

1 Tra i molti scritti in materia, un attento specchio di dette questioni, e non solo di queste, si rinviene negli *Scritti in onore di Antonio Flamini*, I e II, a cura di R. Favale e L. Ruggeri, Napoli, 2020.

2 Dette riflessioni sono sviluppate nell'àmbito delle attività di ricerca svolte dal Laboratorio sul diritto del mercato e delle nuove tecnologie (DIMETECH LAB) del Dipartimento di Scienze Economiche e Aziendali dell'Università di Parma.

3 Sul tema, v. Caterini, E.: "Il «germe» dell'intelligenza artificiale", in AA. VV.: *Scritti in onore di Antonio Flamini*, I, (a cura di R. Favale e L. Ruggeri), Esi, Napoli, 2020, p. 211 ss., nonché Id.: *L'intelligenza artificiale «sostenibile» e il processo di socializzazione del diritto civile*, Napoli, 2020; tra i numerosi scritti sul tema, v., per un'analisi accurata di molti aspetti, Ruffolo, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*,

• Luca Di Nella
Professore ordinario di Diritto privato
Università degli Studi di Parma
luca.dinella@unipr.it

artificiali simulano la funzionalità della fisiologia umana, del sapere e del conoscere. Le reti imparano attraverso l'esperienza. La potenza computazionale e la capacità di autodecisione crescente della macchina orientano l'automazione verso la predizione. In alcuni casi, degli esperimenti sembrano aver dimostrato che alcune macchine non hanno soltanto potenza di calcolo, ma anche 'immaginazione': la creatività potrebbe forse essere automatizzabile. Nel 2017 il campione coreano di *Go* - gioco nel quale, fra due o quattro giocatori, vince chi riesce a piazzare per primo cinque pedine in altrettante caselle consecutive orizzontali sopra una scacchiera di quattrocento caselle - ha perso quattro volte su cinque contro *AlphaGo*, un *supercomputer* di *Deep Mind* che ha escogitato una mossa strategica mai eseguita prima da alcun giocatore, quindi non programmata.

Questo esito sembra essere dovuto al fatto che, negli ultimi anni, grazie agli algoritmi di *deep learning* si è passati da una visione dell'IA come metodo matematico - in grado di far svolgere a un computer determinate attività attraverso l'inserimento di dati - finalizzato a sostituire l'uomo in mansioni meccaniche, a una visione in cui l'IA diventa una intelligenza autonoma in grado di apprendere dai dati e fornire soluzioni creative. Si va dalla produzione di un testo alla composizione di musica, fino alla creazione di dipinti d'arte, come ad esempio nell'ambito della pittura il quadro *The Next Rembrandt* stampato con una stampante 3D e 'creato' dall'intelligenza artificiale dopo aver studiato per 18 mesi 346 dipinti del famoso pittore olandese[4].

La predittività dell'agire computazionale si manifesta in molteplici settori (dalla medicina preventiva alla mobilità urbana, dalle negoziazioni finanziarie alla giustizia predittiva) ed è connotata da un alto livello di prevedibilità, grazie anche al sempre più elevato impiego di banche dati. In conseguenza di questa evoluzione, il giurista sembra dover spostare la sua formazione dalla conoscenza del sistema a quella dei casi, salvaguardando però l'unitarietà dell'ordinamento incentrato sul sistema italo-europeo delle fonti e sulla posizione prioritaria della Costituzione. Nel settore del diritto se ne prefigura dunque l'applicazione a vari livelli, tra i quali anche l'emanazione di decisioni prospettando il c.d. "giudice macchina" (*smart judge*).

Giuffrè, Milano, 2020, nonché v., per alcuni spunti, D'Alessio, A.: "La responsabilità civile dell'intelligenza artificiale antropocentrica", *Persona e merc.*, 2022, 2, p. 243 ss.; Di Gregorio, V.: "Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie", *Danno e resp.*, 2022, 1, p. 51 ss.; Franzoni, M.: "Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale", *Juscivile*, 2021, 1, p. 4 ss.; Frattari, F.: "Robotica e responsabilità da algoritmo. Il processo di produzione dell'intelligenza artificiale", *Contr. impr.*, 2020, 1, p. 458 ss.; Finocchiaro, G.: "Intelligenza artificiale e responsabilità", *Contr. e impresa*, 2020, 2, p. 713 ss.; Ruffolo, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020; Alpa, G. (a cura di): *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020; Santosuosso, A.: *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Giuffrè, Milano, 2020.

4 Sul punto va tuttavia evidenziato che secondo altre opinioni di artisti che si avvalgono delle nuove tecnologie i risultati artistici dell'IA sono solo il riflesso dei desideri, o quanto meno della impostazione, del suo creatore (cfr., per esempio, l'intervista di un grafico italiano pubblicata in *https://www.repubblica.it/tecnologia/2022/10/21/news/intelligenza_artificiale_video_virale_evoluzione_uomo-370902133/*).

Occorre allora, in primo luogo, chiedersi con maggior precisione cosa sia l'AI. Di recente, il Consiglio di Stato ha affrontato propria la questione di quando si può parlare di intelligenza artificiale[5]. Il caso verte sulla nozione di algoritmo, che assume notevole importanza anche per le necessarie conseguenze di carattere giuridico. In particolare, tramite l'esatta perimetrazione tecnica della nozione di «algoritmo di trattamento» nell'ambito di una procedura nazionale di gara per la fornitura di *pacemaker* di alta fascia viene approfondita detta nozione, evidenziandone le differenze sostanziali rispetto alla intelligenza artificiale.

Il Consiglio ha osservato che l'«algoritmo è una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato. Tale nozione quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. Cosa diversa, invece, è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico».

Il Consiglio di Stato chiarisce quindi correttamente come la nozione comune e generale di algoritmo richiami «semplicemente una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato». La nozione, quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione, ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. Il grado e la frequenza dell'intervento umano dipendono dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare.

Cosa ben diversa, invece, è l'intelligenza artificiale. In questo caso, l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole del *software* e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, quindi in virtù di un processo di apprendimento automatico.

La distinzione non però è affatto scontata, poiché si può fare confusione fra sistemi automatici e sistemi di IA. Considerato che questi ultimi attualmente sono

5 Consiglio di Stato, Sez. III, 25 novembre 2021, n. 7891, con commento di Iaselli, M.: "Consiglio di Stato: quando si può parlare di intelligenza artificiale?", *www.altalex.com/documents/news/2021/12/10/consiglio-di-stato-quando-si-puo-parlare-di-intelligenza-artificiale*, del quale questa parte dello scritto è debitrice.

oggetto di particolare attenzione a livello nazionale ed europeo, anche nell'àmbito giuridico la chiara differenziazione diventa rilevante.

La stessa Commissione Europea nella Proposta di Regolamento per un *Artificial Intelligence Act* del 21 aprile 2021[6] chiarisce che la «nozione di sistema di IA dovrebbe essere chiaramente definita per garantire la certezza del diritto, fornendo nel contempo la flessibilità necessaria per accogliere i futuri sviluppi tecnologici. La definizione dovrebbe essere basata sulle caratteristiche funzionali chiave del *software*, in particolare la capacità, per un dato insieme di obiettivi definiti dall'uomo, di generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano l'ambiente con cui il sistema interagisce, sia in una dimensione fisica che digitale. I sistemi di intelligenza artificiale possono essere progettati per funzionare con diversi livelli di autonomia ed essere utilizzati in modo autonomo o come componente di un prodotto, indipendentemente dal fatto che il sistema sia fisicamente integrato nel prodotto (incorporato) o serva la funzionalità del prodotto senza esservi integrato (non incorporato)» (considerando n. 6). Sulla base di tali considerazioni l'art. 3 della Proposta definisce il sistema di IA come «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

Dall'analisi dei considerando e della definizione sembrerebbe che la Commissione Europea voglia accogliere una definizione piuttosto circostanziata di intelligenza artificiale, delimitandone con una certa precisione i confini. In realtà, come si ricava anche dalla *Relazione*, detta definizione intende essere *future proof*, ossia mira ad essere il più possibile neutrale dal punto di vista tecnologico e in questo senso adeguata alle esigenze future. In tal senso, il considerando n. 3 evidenzia che l'«intelligenza artificiale consiste in una famiglia di tecnologie in rapida evoluzione che può contribuire al conseguimento di un'ampia gamma di benefici a livello economico e sociale nell'intero spettro delle attività industriali e sociali». L'Allegato I, richiamato dalla definizione, fa riferimento: a) ad approcci di apprendimento automatico (tipici del *machine learning*), compreso l'apprendimento supervisionato, non supervisionato e per rinforzo, con l'utilizzo di un'ampia gamma di metodi tra cui l'apprendimento profondo (*deep learning*); b) ad approcci basati sulla logica e sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) nonché persino ad approcci statistici, stima bayesiana, e a metodi di ricerca e ottimizzazione.

6 Si tratta della *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, 21 aprile 2021, COM(2021) 206 *final*.

L'art. 4 della Proposta di Regolamento dispone che tale allegato debba essere adattato dalla Commissione in linea con i nuovi sviluppi tecnologici e di mercato. La Commissione, anche al fine di evitare problematiche interpretative, ha dunque voluto ampliare al massimo la nozione di intelligenza artificiale ricomprendendo in essa sia l'intelligenza artificiale forte, in grado di comprendere e di possedere stati cognitivi, sia l'intelligenza artificiale debole, capace di prestazioni normalmente attribuite all'intelligenza umana, pur senza assumere alcuna analogia tra le menti e i sistemi informatici.

In tal senso, il Consiglio di Stato segnala come i confini fra sistemi informatici e sistemi intelligenti rischiano di diventare molto labili. Mentre la distinzione è evidente in presenza di un algoritmo probabilistico proprio del *machine learning*, la questione diventa più complessa in presenza di un algoritmo deterministico proprio dell'intelligenza artificiale debole.

In proposito, è opportuno precisare che le attività intelligenti si basano su un impiego attivo, non rigidamente predeterminato, della conoscenza. Di qui l'esigenza di sviluppare un nuovo tipo di sistemi informatici, i c.dd. sistemi basati sulla conoscenza, mediante i quali ci si propone di usare in modo intelligente le informazioni, trasformando i dati in conoscenza.

I programmi informatici tradizionali, pur non essendo basati sulla conoscenza, ne incorporano una, ossia la descrizione della procedura (l'algoritmo) per svolgere un certo compito, e possono essere sviluppati solo tenendo conto delle caratteristiche di quel compito. Ciò posto, è possibile, su questa base, delineare delle differenze tra i sistemi informatici tradizionali e quelli basati sulla conoscenza.

Nei primi la conoscenza non è mai rappresentata esplicitamente e non è mai separata dalle procedure che la usano e che ne disciplinano l'elaborazione; è applicata in modo rigidamente predeterminato; non è possibile aggiungere nuova conoscenza senza modificare le procedure; il sistema non è in grado di esporre la conoscenza sulla quale si basa, né di spiegare perché, sulla base della stessa, sia giunto a determinati risultati[7].

Diversamente, nei sistemi basati sulla conoscenza, questa è contenuta in una determinata base, dove è rappresentata in un linguaggio ad alto livello, cioè in una forma relativamente vicina al linguaggio usato nella comunicazione umana; è possibile adottare una rappresentazione dichiarativa del compito affidato al sistema informatico, lasciando al sistema l'individuazione della procedura da seguire per svolgere quel compito; la conoscenza è usata da un motore inferenziale, ovvero da un meccanismo in grado di interpretare il contenuto della base di conoscenza ed

7 Iaselli, M.: "Consiglio di Stato: quando si può parlare di intelligenza artificiale?", cit.

effettuare deduzioni logiche in modo da risolvere il problema posto al sistema; la base di conoscenza può essere arricchita da nuove informazioni, senza intervenire sul motore inferenziale; il sistema è in grado di esporre in forma comprensibile le premesse e le inferenze che hanno condotto ad un determinato risultato, cioè di giustificare le conclusioni cui giunge[8].

La problematica della corretta distinzione tra diverse tipologie di sistemi informatici anche avanzati e sistemi di IA diventerà centrale, quando si arriverà a definire in modo compiuto le prime forme di regolamentazione dell'IA con riferimento agli aspetti legali ed etici e alle necessarie implicazioni in tema di *privacy* e responsabilità.

In proposito, l'Unione Europea ha prodotto negli ultimi anni una copiosa serie di documenti, azioni e proposte normative in materia di IA. Tra queste ultime, di grande interesse sono la proposta di regolamento per un *Artificial Intelligence Act* sulle regole armonizzate in materia di intelligenza artificiale e le due proposte di direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale 2022 e sulla responsabilità da prodotto difettoso, entrambe del 28 settembre 2022.

Con il documento COM(2021) 206 *final* del 21 aprile 2021, recante «Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione», la Commissione europea ha pubblicato una proposta volta a fissare un quadro di divieti e di requisiti per i sistemi di IA, comprensivo di un apparato sanzionatorio e istituzionale. La Proposta di *AI Act* comprende la «Bozza di Regolamento», i relativi «Allegati» la «Relazione» esplicativa[9].

La Relazione illustra le molteplici iniziative adottate dalla UE in argomento[10] e spiega che la Bozza si basa sui valori e sui diritti fondamentali della UE, prefiggendosi

8 Iaselli, M.: "Consiglio di Stato: quando si può parlare di intelligenza artificiale?", cit.

9 Sulla Proposta di Regolamento, v. Amidei, A.: "La proposta di Regolamento UE per un Artificial Intelligence Act: prime riflessioni sulle ricadute in tema di responsabilità", *Tecnologie e Diritto*, 2022, 1, p. 1 ss.; Casonato, C. e Marchetti, B.: "Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale", *Bio-Law Journal*, 2021, 3, p. 415 ss.

10 Tra le principali iniziative adottate negli ultimi anni dalle istituzioni dell'Unione europea in materia di intelligenza artificiale, per quanto riguarda il Consiglio Europeo, vengono menzionati: *European Council meeting (19 October 2017) - Conclusion EUCO 14/17*, 2017, p. 8; *Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption* 6177/19, 2019; *Special meeting of the European Council (1 and 2 October 2020) – Conclusions*, EUCO 13/20, 2020, p. 6; *Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020. Quanto al Parlamento europeo - oltre alla *Risoluzione del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, 2015/2103(INL), sulla quale v. Amidei, A.: "Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo", in Ruffolo, U. (a cura di): *Intelligenza artificiale e responsabilità*, Giuffrè, Milano, 2017, p. 77 ss., e Rodi, F.: "Gli interventi dell'Unione Europea in materia di intelligenza artificiale e robotica: problemi e prospettive", in Alpa, G. (a cura di): *Diritto e intelligenza artificiale*, Pisa, 2020, p. 188 ss. -, vengono evidenziare le risoluzioni adottate nell'ottobre

di dare alle persone e agli altri utenti la fiducia necessaria per adottare le soluzioni di IA e di incoraggiare le imprese a svilupparle. Si tratta dunque di uno strumento legislativo orizzontale fondato su un approccio equilibrato e proporzionato basato sul rischio che pone i requisiti legali per le imprese che immettono soluzioni di IA nel mercato nella misura minima necessaria per affrontare i relativi «rischi» e «problemi».

La Bozza prevede regole armonizzate sulla progettazione, sviluppo e uso di determinati sistemi di IA ad alto rischio, nonché integra la legislazione esistente sulla non discriminazione al fine di minimizzare il rischio di «discriminazione algoritmica». Secondo l'art. 6, un «sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II; b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II. 2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III»[11].

2020 sull'etica, la responsabilità civile e il *copyright* (precedute dalla pubblicazione di tre *draft report* della Commissione *JURI* dell'aprile 2020: la *European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, 2020/2012(INL): la *European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence*, 2020/2014(INL), la *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies*, 2020/2015(INI)); vi sono poi i documenti del 2021 in materia di diritto penale e in materia di educazione, cultura e settore audiovisivo: European Parliament Draft Report, *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, 2020/2016(INI); European Parliament Draft Report, *Artificial intelligence in education, culture and the audiovisual sector*, 2020/2017(INI). Quanto alla Commissione Europea, importanti sono il libro bianco sulla IA, ossia lo Commissione Europea, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 *final*, 2020, nonché il *Digital Education Action Plan 2021- 2027: Resetting education and training for the digital age, which foresees the development of ethical guidelines in AI and Data usage in education - Commission Communication* COM(2020) 624 *final*; v. anche High-Level Expert Group on AI, *Ethics Guidelines for Trustworthy Artificial Intelligence*, 8 aprile 2019.

11 I sistemi di IA ad alto rischio sono quelli elencati in uno dei settori indicati di seguito: «1. Identificazione e categorizzazione biometrica delle persone fisiche: a) i sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota "in tempo reale" e "a posteriori" delle persone fisiche. 2. Gestione e funzionamento delle infrastrutture critiche: a) i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione del traffico stradale e nella fornitura di acqua, gas, riscaldamento ed elettricità. 3. Istruzione e formazione professionale: a) i sistemi di IA destinati a essere utilizzati al fine di determinare l'accesso o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale; b) i sistemi di IA destinati a essere utilizzati per valutare gli studenti negli istituti di istruzione e formazione professionale e per valutare i partecipanti alle prove solitamente richieste per l'ammissione agli istituti di istruzione. 4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo: a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicizzare i posti vacanti, vagliare o filtrare le candidature, valutare i candidati nel corso di colloqui o prove; b) l'IA destinata a essere utilizzata per adottare decisioni in materia di promozione e cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti e per il monitoraggio e la valutazione delle prestazioni e del comportamento delle persone nell'ambito di tali rapporti di lavoro. 5. Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi: a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi; b) i sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia

Con riferimento a detti sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla legislazione del c.d. *New Legislative Framework* (*NLF*)[12], come ad esempio macchinari, dispositivi medici, giocattoli ecc., la Relazione specifica che i requisiti per i sistemi di IA previsti nella Bozza di Regolamento dovranno essere verificati nel contesto delle procedure di controllo di conformità previsti dalla

delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA messi in servizio per uso proprio da fornitori di piccole dimensioni; c) i sistemi di IA destinati a essere utilizzati per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi vigili del fuoco e assistenza medica. 6. Attività di contrasto: a) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per effettuare valutazioni individuali dei rischi delle persone fisiche al fine di determinare il rischio di reato o recidiva in relazione a una persona fisica o il rischio per vittime potenziali di reati; b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica; c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per individuare i "deep fake" di cui all'articolo 52, paragrafo 3; d) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per la valutazione dell'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati; e) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi; f) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati; g) i sistemi di IA destinati a essere utilizzati per l'analisi criminale riguardo alle persone fisiche, che consentono alle autorità di contrasto di eseguire ricerche in set di dati complessi, correlati e non correlati, resi disponibili da fonti di dati diverse o in formati diversi, al fine di individuare modelli sconosciuti o scoprire relazioni nascoste nei dati. 7. Gestione della migrazione, dell'asilo e del controllo delle frontiere: a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica; b) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti per valutare un rischio (compresi un rischio per la sicurezza, un rischio di immigrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro; c) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti per verificare l'autenticità dei documenti di viaggio e dei documenti giustificativi delle persone fisiche e per individuare i documenti non autentici mediante il controllo delle caratteristiche di sicurezza; d) i sistemi di IA destinati ad assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status. 8. Amministrazione della giustizia e processi democratici: a) i sistemi di IA destinati ad assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti».

12 Nell'Allegato II, Sezione A della Bozza di Regolamento, sono elencati i seguenti atti della legislazione *NLF*: Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la Direttiva 95/16/CE (che si prevede sarà abrogata dal nuovo regolamento sui prodotti macchina); Direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli; Direttiva 2013/53/UE del Parlamento europeo e del Consiglio, del 20 novembre 2013, relativa alle imbarcazioni da diporto e alle moto d'acqua e che abroga la Direttiva 94/25/CE; Direttiva 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori; Direttiva 2014/34/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva; Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la Direttiva 1999/5/CE; Direttiva 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione; Regolamento (UE) 2016/424 del Parlamento europeo e del Consiglio, del 9 marzo 2016, relativo agli impianti a fune e che abroga la Direttiva 2000/9/CE; Regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la Direttiva 89/686/CEE del Consiglio; Regolamento (UE) 2016/426 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sugli apparecchi che bruciano carburanti gassosi e che abroga la Direttiva 2009/142/CE; Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la Direttiva 2001/83/CE, il Regolamento (CE) n. 178/2002 e il Regolamento (CE) n. 1223/2009 e che abroga le Direttive 90/385/CEE e 93/42/CEE del Consiglio; Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medicodiagnostici in vitro e che abroga la Direttiva 98/79/CE e la Decisione 2010/227/UE della Commissione.

legislazione *NLF* di volta in volta applicabile. Per quanto riguarda la questione del coordinamento tra i vari e diversi requisiti, la Relazione precisa che mentre la Bozza di Regolamento intende occuparsi dei rischi di sicurezza tipici dei sistemi di IA attraverso la predisposizione di specifici requisiti, la legislazione *NLF* è intesa ad assicurare la sicurezza complessiva del prodotto finale e può, di conseguenza, contenere la previsione di specifici requisiti che riguardano condizioni per integrare in modo sicuro un sistema di IA in un prodotto finale[13]. Invece, per quanto riguarda i sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla legislazione del vecchio approccio[14] (ad esempio, aeromobili, autoveicoli ecc.) la Proposta di *AI Act* non si applica direttamente, ma gli essenziali requisiti *ex ante* per i sistemi di IA di alto rischio dovranno essere presi in considerazione, quando si adotteranno normative attuative o delegate della medesima legislazione[15].

La Bozza persegue i seguenti obiettivi specifici: assicurare che i sistemi di IA immessi e utilizzati nel mercato dell'Unione siano sicuri e rispettino la normativa esistente sui diritti fondamentali e i valori dell'Unione; assicurare certezza del

13 Al riguardo, la Relazione sottolinea che tale approccio è seguito dalla proposta di *Machinery Regulation*, ossia la *Proposal for a Regulation of the European Parliament and of the Council on machinery products* COM(2021) 202 (in *https://ec.europa.eu/docsroom/documents/45508*), che è stata adottata il 21 aprile 2021, quindi lo stesso giorno della Proposta di *IA Act*.

14 Ciò è ribadito nel *considerando* 29 e nell'art. 2, § 2, della Bozza di Regolamento, relativamente ai seguenti atti della *Old Approach Legislation*: Regolamento (CE) 300/2008 che istituisce norme comuni per la sicurezza dell'aviazione civile; Regolamento (UE) No 167/2013 sull'omologazione e la vigilanza del mercato dei veicoli agricoli e forestali; Regolamento (UE) No 168/2013 sull'omologazione e la vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli; Direttiva 2014/90/UE sull'equipaggiamento marittimo; Direttiva (UE) 2016/797 sull'interoperabilità del sistema ferroviari dell'Unione europea; Regolamento (UE) 2018/858 sull'omologazione e la vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli; Regolamento (UE) 2018/1139 recante norme comuni nel settore dell'aviazione civile e che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea; Regolamento (UE) 2019/2144 sui requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada. Il *considerando* n. 29 della Bozza di Regolamento sottolinea che è opportuno modificare tali atti per far sì che la Commissione, nell'adottare qualsiasi futuro provvedimento attuativo o delegato sulla base dei medesimi atti, possa tener conto dei requisiti obbligatori *ex ante* stabiliti nella Bozza di Regolamento per i sistemi di IA ad alto rischio, sulla base delle specificità tecniche e regolamentari di ciascun settore; l'art. 2, par. 2, della Bozza prevede che ai sistemi di IA ad alto rischio, che costituiscono componenti di sicurezza di prodotti o sistemi o che sono essi stessi prodotti o sistemi disciplinati dai predetti atti, si applica soltanto l'art. 84, il quale affida alla Commissione alcuni compiti in materia di revisione della normativa. L'art. 2, § 4, esclude l'applicazione del regolamento alle «autorità pubbliche di un paese terzo [e] alle organizzazioni internazionali […], laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri».

15 Per quanto concerne i sistemi di IA forniti o utilizzati da enti creditizi regolamentati, le autorità competenti per il controllo sulla legislazione dell'Unione in materia di servizi finanziari dovrebbero essere designate come autorità competenti per il controllo dell'osservanza dei requisiti previsti dalla Proposta di *AI Act*, al fine di assicurare un'applicazione coerente della normativa unionale in materia di servizi finanziari, là dove i sistemi di IA siano in una certa misura implicitamente regolamentati in relazione al sistema di *governance* interna degli enti creditizi. A tal proposito, l'art. 9, § 9, prevede che per gli enti creditizi disciplinati dalla Direttiva 2013/36/UE (la Direttiva sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale) le previsioni dettate dagli altri §§ del medesimo articolo in materia di gestione dei rischi si debbano osservare, includendole nelle procedure di gestione dei rischi previste dall'art. 74 di detta Direttiva. Infine, la Relazione dichiara che la Proposta di *AI Act* è coerente con la legislazione unionale applicabile ai servizi, compresi i servizi di intermediazione regolati dalla Direttiva 2000/31/CE sul commercio elettronico, e la recente proposta della Commissione per la legge sui servizi digitali (*Digital Services Act*).

diritto al fine di facilitare l'investimento e l'innovazione in IA; rafforzare l'effettiva applicazione della normativa esistente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA; facilitare lo sviluppo di un mercato unico per applicazioni di IA legittime, sicure e meritevoli di fiducia ed evitare la frammentazione di mercato.

Quanto ai contenuti della Bozza[16], il Titolo I (artt. 1-4) definisce l'oggetto del regolamento e l'àmbito di applicazione delle nuove regole concernenti l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di IA. L'art. 2, § 1, stabilisce che la Bozza di Regolamento si applica: a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un paese terzo; b) agli utenti dei sistemi di IA situati nell'Unione; c) ai fornitori e agli utenti di sistemi di IA situati in un paese terzo, là dove l'*output* prodotto dal sistema sia utilizzato nell'Unione[17]. L'art. 3 della Bozza di Regolamento stabilisce le definizioni utilizzate in tutto l'atto, tra le quali quella di AI sopra analizzata. L'art. 3 descrive anche gli "*operatori*" lungo l'intera catena del valore dell'IA, ossia il «fornitore», compreso quello «di piccole dimensioni», l'«utente», il «rappresentante autorizzato», l'«importatore» e il «distributore», considerando tanto gli operatori pubblici quanto quelli privati.

Molto interessante è il Titolo II, il quale prevede nell'art. 5 quattro «pratiche» di IA vietate. Coerentemente con l'approccio basato sul rischio, la Bozza differenzia tra gli usi dell'IA che creano un rischio inaccettabile, un rischio alto, un rischio basso o minimo: le «pratiche» vietate *ex* art. 5 sono quelle che creano un rischio inaccettabile. Le prime tre «pratiche» consistono nella «immissione sul mercato, la messa in servizio o l'uso» di un sistema di IA, mentre la quarta nel solo «uso». Le prime due pratiche (lett. *a*, *b*) riguardano sistemi di IA basati su tecniche subliminali che sono idonei a distorcere materialmente il comportamento delle persone in modo tale da procurare loro o ad altri un «danno fisico o psicologico»: sembrerebbe trattarsi di pratiche commerciali scorrette attuate con le nuove tecnologie che pongono a rischio la salute dell'utente[18]. La terza (lett. *c*) riguarda sistemi di IA di c.d. *social scoring* e il divieto si applica solo se le pratiche sono poste in essere da autorità pubbliche o per loro conto e se tali sistemi sono idonei a

16 Sul contenuto della proposta, v. la completa illustrazione di Orlando, S.: "Verso l'Artificial Intelligence Act: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale", *Persona e mercato*, 2021, 2, p. 444 ss.

17 L'art. 2, § 3, prevede che la Bozza di Regolamento non si applica ai sistemi di IA sviluppati o usati per scopi esclusivamente militari.

18 Sono proibiti *ex* art. 5, § 1, lett. *a*, *b*: «a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico; b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico».

produrre determinati «trattamenti pregiudizievoli o sfavorevoli» per determinate persone o gruppi di persone[19]. La quarta (lett. *d*) consiste invece nell'uso di sistemi di IA di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto svolte dalle autorità per la prevenzione, indagine, accertamento o perseguimento di reati o per esecuzione di sanzioni penali, fatta salva l'applicazione di talune eccezioni limitate[20].

Il Titolo III (artt. 6-51) contiene regole specifiche per i sistemi di IA che creano un «rischio alto» per la salute e la sicurezza o per i diritti fondamentali delle persone fisiche. Tali sistemi sono consentiti sul mercato europeo subordinatamente al rispetto di determinati requisiti obbligatori e a una valutazione della conformità *ex ante*. La classificazione di un sistema di IA come ad alto rischio si basa sulla sua finalità prevista, in linea con la normativa vigente dell'UE in materia di sicurezza dei prodotti: la classificazione come ad alto rischio non dipende dunque solo dalla

19 Sono proibiti *ex* art. 5, § 1, lett. *c*: «c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità».

20 È proibito *ex* art. 5, § 1, lett. *d*: «d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi: i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro». Secondo l'art. 5, § 2, l'uso dei predetti sistemi di identificazione biometrica, «a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), tiene conto dei seguenti elementi: a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema; b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze. L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, lettera d), rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali». L'art. 5, § 3, relativamente alla lett. *d* e al § 2, dispone che ogni singolo uso «è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione solo durante o dopo l'uso. L'autorità giudiziaria o amministrativa competente rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, lettera d), come indicato nella richiesta. Nel decidere in merito alla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi di cui al paragrafo 2». Infine, *ex* art. 5, § 4, uno «Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, lettera d), e ai paragrafi 2 e 3. Tale Stato membro stabilisce nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, lettera d), compresi i reati di cui al punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto».

funzione svolta dal sistema, ma anche dalle finalità e modalità specifiche di utilizzo dello stesso.

Il Capo 1 fissa le regole di classificazione e individua nell'art. 6 due categorie principali di tali sistemi di IA: quelli destinati ad essere utilizzati come componenti di sicurezza di prodotti, o che sono essi stessi prodotti, soggetti a valutazione di conformità e*x ant*e da parte di terzi, ai sensi della normativa di armonizzazione dell'Unione di cui all'Allegato II; altri sistemi c.dd. «indipendenti» che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'Allegato III[21]. Al fine di assicurare che il Regolamento possa essere adattato in futuro agli usi e alle applicazioni emergenti dell'IA, è previsto che la Commissione possa ampliare l'elenco dei sistemi ad alto rischio utilizzati all'interno di alcuni settori predefiniti, applicando una serie di criteri e una metodologia di valutazione dei rischi.

Il Capo 2 definisce i requisiti giuridici per i sistemi di IA ad alto rischio in relazione a dati e *governanc*e dei dati (art. 10), documentazione (art. 11 e Allegato IV) e conservazione delle registrazioni, trasparenza e fornitura di informazioni agli utenti, sorveglianza umana, robustezza, accuratezza e cibersicurezza.

Il Capo 3 definisce una serie di obblighi orizzontali per i fornitori di sistemi di IA ad alto rischio, i rappresentanti autorizzati e gli importatori (artt. 16 ss.). Obblighi proporzionati sono imposti anche ai distributori, importatori, utenti e altri terzi (artt. 28 ss.).

Il Capo 4 definisce il quadro normativo per le autorità e per gli organismi notificati che saranno coinvolti come terze parti indipendenti nelle procedure di valutazione della conformità, mentre il Capo 5 prevede le procedure di valutazione della conformità da seguire per ciascun tipo di sistema di IA ad alto rischio. A tali procedure si riferiscono gli Allegati V, VI, VII e VIII.

Il Titolo IV prevede all'art. 52 «Obblighi di trasparenza» per i sistemi di IA che interagiscono con gli esseri umani, sono utilizzati per rilevare emozioni o stabilire un'associazione con categorie (sociali) sulla base di dati biometrici oppure generano o manipolano contenuti (*deep fake*). Il § 1 prevede che le persone debbano essere informate quando interagiscono con un sistema di IA, ma tale obbligo non si applica quando ciò risulti dalle circostanze e dal contesto e si tratti di sistemi di

21 L'elenco di sistemi di IA ad alto rischio di cui all'Allegato III contiene una descrizione tipologica di 21 sistemi afferenti ai seguenti otto settori, dichiaratamente scelti dalla Commissione per il fatto che i relativi rischi si sono già «concretizzati» o «potrebbero concretizzarsi nel prossimo futuro»: i) identificazione e categorizzazione biometrica delle persone fisiche; ii) gestione e funzionamento delle infrastrutture critiche; iii) istruzione e formazione professionale; iv) occupazione, gestione dei lavoratori e accesso al lavoro autonomo; v) accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi; vi) attività di contrasto di reati; vii) gestione della migrazione, dell'asilo e del controllo delle frontiere; (viii) amministrazione della giustizia e processi democratici.

IA autorizzati dalla legge ad accertare, prevenire, indagare e perseguire reati. Il § 2 dispone lo stesso obbligo anche quando il riconoscimento delle emozioni o la categorizzazione biometrica delle persone avvenga attraverso mezzi automatizzati, salvo che i sistemi di categorizzazione biometrica, che siano autorizzati dalla legge per accertare, prevenire e indagare reati. Quando un sistema di IA viene utilizzato per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a contenuti autentici, il § 3, comma 1, dispone l'obbligo di rivelare che tali contenuti sono generati ricorrendo a mezzi automatizzati; il comma 2 esclude l'applicazione del primo comma se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o se è necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

Il Titolo V (artt. 53-55), intitolato «Misure di sostegno all'innovazione», prevede alcune disposizioni in materia di «spazi di sperimentazione normativa per l'IA» (*sand-boxes*)[22].

Il Titolo VI (artt. 56-59) delinea la *governance* pubblica per i sistemi di IA con l'istituzione di un Comitato europeo per l'IA (*European Artificial Intelligence Board*), costituito da rappresentanti degli Stati membri e della Commissione europea. A livello nazionale, è previsto che gli Stati membri dovranno designare una o più autorità nazionali competenti e, tra queste, l'autorità nazionale di controllo, al fine di controllare l'applicazione e l'attuazione del regolamento.

Il Titolo VII contempla la creazione e il mantenimento di una banca dati a livello dell'UE per sistemi di IA ad alto rischio «indipendenti» che presentano principalmente implicazioni in relazione ai diritti fondamentali. La banca dati è gestita dalla Commissione e alimentata con i dati messi a disposizione dai fornitori dei sistemi di IA, che saranno tenuti a registrare i propri sistemi prima di immetterli sul mercato o altrimenti metterli in servizio (art. 60).

22 Secondo l'art. 53, § 1, detti spazi, «istituiti da una o più autorità competenti degli Stati membri o dal Garante europeo della protezione dei dati forniscono un ambiente controllato che facilita lo sviluppo, le prove e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico. Ciò avviene sotto la guida e il controllo diretti delle autorità competenti al fine di garantire la conformità ai requisiti del presente regolamento e, se del caso, di altre normative dell'Unione e degli Stati membri controllate all'interno dello spazio di sperimentazione». Tra le altre disposizioni, vanno menzionate le seguenti: da un lato, gli spazi «non pregiudicano i poteri correttivi e di controllo delle autorità competenti. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi deve comportare l'adozione di immediate misure di attenuazione e, in mancanza di ciò, la sospensione del processo di sviluppo e di prova fino a che tali rischi non risultino attenuati» (art. 53, § 3); dall'altro, i «partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi della normativa applicabile dell'Unione e degli Stati membri in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione» (art. 53, § 4).

Nel Titolo VIII, «Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni, vigilanza del mercato», gli artt. 61-68 stabiliscono gli obblighi in materia di monitoraggio e segnalazione in capo ai fornitori di sistemi di IA per quanto riguarda il controllo successivo all'immissione sul mercato e la segnalazione di incidenti e malfunzionamenti correlati all'IA nonché le indagini in merito. Il Regolamento (UE) 2019/1020 sulla vigilanza dei mercati e sulla conformità dei prodotti si applicherà ai sistemi di IA disciplinati dalla Bozza in esame[23].

Il Titolo IX, recante la disciplina dei «Codici di condotta», mira a incoraggiare i fornitori di sistemi di IA non ad alto rischio ad applicare volontariamente i requisiti obbligatori previsti per i sistemi di IA ad alto rischio di cui al Titolo III, Capo 2, sulla base di specifiche tecniche e soluzioni che costituiscono mezzi adeguati per garantire la conformità a tali requisiti alla luce della finalità prevista dei sistemi (art. 69)[24].

Il Titolo X (artt. 70-73), intitolato «Riservatezza e sanzioni», contiene alcune importanti disposizioni. L'art. 70 prevede che le autorità nazionali competenti e gli organismi notificati che partecipano all'applicazione del regolamento debbano rispettare la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, *inter alia*, i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, salva l'applicazione dell'art. 5 della Direttiva 2016/943 sulla protezione del *know-how* riservato e delle informazioni commerciali riservate (segreti commerciali). L'art. 71 infligge sanzioni amministrative pecuniarie per la violazione del divieto di cui all'art. 5 (pratiche vietate) e la mancata osservanza dei requisiti di conformità di cui all'art. 10 (dati e *governance* dei dati) nella misura di un importo fino a 30 milioni di euro o, in caso di società, di un importo fino al 6% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Sanzioni amministrative pecuniarie con tetti massimi inferiori sono previste per l'inosservanza di altre disposizioni, diverse da quelle contenute negli artt. 5 e 10.

I Titoli XI e XII contengono le regole per l'esercizio della delega e delle competenze di esecuzione e alcune disposizioni finali, tra cui la previsione

23 L'art. 63 statuisce che, «ai fini dell'efficace applicazione del presente regolamento: a) ogni riferimento a un operatore economico a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti gli operatori di cui al titolo III, capo 3, del presente regolamento; b) ogni riferimento a un prodotto a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti i sistemi di IA che rientrano nell'ambito di applicazione del presente regolamento».

24 In particolare, «la Commissione e il Comitato incoraggiano e agevolano l'elaborazione di codici di condotta intesi a promuovere l'applicazione volontaria ai sistemi di IA dei requisiti relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità per le persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo dei sistemi di IA e alla diversità dei gruppi che si occupano dello sviluppo sulla base di obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi (art. 69 , § 2)».

dell'esclusione di applicazione del regolamento ai sistemi di IA che sono componenti di «sistemi IT su larga scala» come istituiti dagli atti giuridici elencati nell'Allegato IX, che siano stati immessi sul mercato o messi in servizio in un periodo antecedente alla futura entrata in vigore del regolamento[25].

Oltre alla predisposizione della proposta di *AI* Act, è stata elaborata da parte del Parlamento europeo anche la Risoluzione del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), contenente una serie di raccomandazioni e indicazioni finalizzate ad indirizzare la futura disciplina della responsabilità civile applicabile al funzionamento dei sistemi di intelligenza artificiale e una proposta di regolamento[26]. Da parte sua, la Commissione europea ha pubblicato il 28 settembre 2022 due proposte di direttiva che si collocano all'interno di un pacchetto di misure atte a sostenere gli obiettivi di «eccellenza e fiducia» relativi all'IA come già delineati nei precedenti documenti istituzionali dell'Unione: una riguarda la nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE (*Product Liability Directive*)[27], l'altra l'armonizzazione delle regole di responsabilità civile adeguate alle caratteristiche dei moderni sistemi di IA (*AI Liability Directive*)[28].

La proposta di *AI Liability Directive* è volta ad armonizzare alcuni profili probatori inerenti ai regimi di responsabilità civile esistenti negli Stati membri e fondati sul criterio della colpa, in modo da garantire che i soggetti danneggiati da un sistema di IA c.d. «ad alto rischio» godano di un livello di protezione equivalente a quello di cui godrebbero se i danni in questione fossero stati causati senza il coinvolgimento di un sistema di IA (*considerando* n. 7). A tal fine, si prevedono in favore del danneggiato meccanismi di semplificazione probatoria potenzialmente in grado di supplire alle difficoltà generate dalle peculiarità dei sistemi di IA, caratterizzati da funzioni di c.d. auto-apprendimento, nonché da scarsa comprensibilità da parte del soggetto danneggiato chiamato a provare in giudizio la condotta colposa del responsabile e il nesso di causalità tra questa e il danno.

25 L'Allegato IX elenca la legislazione dell'Unione nei seguenti sette settori: Sistema di informazione Schengen; Sistema di informazione visti; Eurodac; Sistema di ingressi/uscite; Sistema europeo di informazione e autorizzazione ai viaggi; Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi; Interoperabilità.

26 Sulla proposta del Parlamento Europeo, v. D'Alessio, A.: "La responsabilità civile dell'intelligenza artificiale antropocentrica", *Persona e mercato*, 2022, 2, p. 243 ss.

27 De Mari Casareto Dal Verme, T.: "Verso la nuova Product Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE", *Persona e mercato*, 2022, 1, p. 502 ss.

28 De Mari Casareto Dal Verme, T.: "Verso la AI Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale", cit., p. 500 ss.

L'art. 1 circoscrive oggetto e scopo chiarendo che la direttiva pone regole armonizzate in tema di «divulgazione di elementi di prova relativi a sistemi di intelligenza artificiale (IA) ad alto rischio» per consentire all'attore in un'azione civile di responsabilità extracontrattuale per colpa di motivare adeguatamente la domanda di risarcimento del danno nonché di onere della prova nei casi di richieste di risarcimento danni proposte davanti ai giudici nazionali a titolo di responsabilità extracontrattuale fondate sul criterio di imputazione della colpa. Allo stesso tempo, precisa la Commissione, la direttiva non incide: sulle norme del diritto dell'Unione che disciplinano le condizioni di responsabilità nel settore dei trasporti, sui diritti da chiunque azionabili in virtù delle norme nazionali di recepimento della Direttiva 85/374/CEE sulla responsabilità del produttore, sulle norme nazionali che regolano l'onere della prova, il grado di certezza richiesto in ordine alla stessa, ovvero il modo in cui viene definita la colpa, al di fuori di quanto previsto dagli articoli 3 e 4. Il *considerando* n. 11 precisa che agli Stati membri è consentito adottare o mantenere norme nazionali più favorevoli per i danneggiati, purché compatibili con il diritto dell'Unione, dunque anche regimi di responsabilità oggettiva fondati su elementi diversi dal difetto del prodotto.

Dalle definizioni di cui all'art. 2 emerge il coordinamento tra la proposta in esame e la proposta di *AI Act*, il cui contenuto viene richiamato *per relationem* con riguardo alle nozioni di «sistema di IA» (n. 1), «sistema di IA ad alto rischio» (n. 2), «fornitore» (n. 3) e «utente» (n. 4). Inoltre, viene precisato il significato di alcune locuzioni, tra cui quella di «domanda di risarcimento del danno» (n. 5), che viene circoscritta al danno causato da un *output* prodotto da un sistema di IA o dall'omissione di tale sistema nel produrre un *output* che avrebbe dovuto essere prodotto[29]. Infine, l'«obbligo di diligenza» è definito come «il livello di condotta richiesto, stabilito dal diritto nazionale o dell'Unione, al fine di evitare danni agli interessi giuridici riconosciuti dal diritto nazionale o dell'Unione, tra cui la vita, l'integrità fisica, la proprietà e la tutela dei diritti fondamentali» (n. 9).

Gli artt. 3 e 4 introducono dei sistemi di semplificazione probatoria in favore del danneggiato. L'art. 3 prevede un meccanismo di c.d. «divulgazione» degli elementi di prova (*disclosure* nella versione inglese), cui consegue eventualmente una presunzione di colpa del fornitore o di un soggetto ad esso equiparato ovvero dell'utente del sistema di IA. Il giudice nazionale ha il potere di ordinare a tali soggetti di produrre prove relative a specifici sistemi di IA ad alto rischio sospettati di aver causato un danno, purché la relativa richiesta sia necessaria e proporzionata. Non è specificato in cosa debbano consistere tali prove, prevedendosi soltanto che per stabilire se una richiesta di prove sia proporzionata il giudice deve prendere in

29 Questa la definizione proposta dall'art. 2, n. 5: «domanda nel quadro di un'azione civile di responsabilità extracontrattuale per colpa volta a ottenere il risarcimento del danno causato dall'output di un sistema di IA o dalla mancata produzione di un output che avrebbe invece dovuto essere prodotto da tale sistema».

considerazione i segreti commerciali nel significato di cui all'art. 2, § 1, Direttiva n. 2016/943 e le informazioni confidenziali, quali quelle relative alla sicurezza pubblica o nazionale. Tale potere è esercitabile dal giudice in due casi: in via anticipatoria, qualora venga proposta istanza da un «attore potenziale» (la persona fisica o giuridica che non ha ancora proposto domanda giudiziale, art. 2, n. 7), il quale abbia previamente richiesto con «ogni sforzo proporzionato» tale esibizione ai suddetti soggetti senza ottenere riscontro, purché fornisca elementi sufficienti a sostenere la plausibilità della domanda risarcitoria; nel corso di un giudizio già avviato su richiesta dell'attore. In questo modo si consente al danneggiato di ottenere informazioni che devono essere conservate a norma dell'*AI Act*, il quale tuttavia non prevede il corrispondente diritto del danneggiato di accedervi (*considerando* 16)[30]. Il giudice può anche ordinare la conservazione della prova nei modi che ritenga più consoni.

Qualora il convenuto non ottemperi all'ordine di esibizione o conservazione della prova, scatta la presunzione di «non conformità a un pertinente obbligo di diligenza da parte del convenuto, che gli elementi di prova richiesti erano intesi a dimostrare ai fini della domanda di risarcimento del danno». In sostanza, si presume l'inosservanza da parte del convenuto dei doveri diligenza relativi al sistema di IA per cui era stato pronunciato l'ordine, rilevanti a livello nazionale ed europeo, con particolare riferimento ai requisiti posti dall'*AI Act*. Detta presunzione ha carattere relativo, in quanto è superabile dal convenuto fornendo prova contraria (*considerando* n. 21, art. 3, § 5). L'art. 3 delinea, dunque, un regime di responsabilità per colpa di fornitori e utenti per la mancata ottemperanza agli standard posti dall'*AI Act*, la cui prova gravante sul danneggiato viene alleggerita tramite un meccanismo di divulgazione posto a carico del convenuto e una eventuale sua presunzione di colpa, che interviene nel caso di sua mancata ottemperanza all'ordine di divulgazione. Esso contempla solo quei danni che siano la manifestazione di un rischio specificamente contemplato dalla normativa di sicurezza *ex ante* (*considerando* n. 22 e 25)[31].

30 «L'accesso alle informazioni su specifici sistemi di IA ad alto rischio sospettati di aver causato danni è un fattore importante per decidere se chiedere un risarcimento e motivarne la richiesta. Inoltre, per i sistemi di IA ad alto rischio, [la legge sull'IA] stabilisce requisiti specifici in materia di documentazione, informazioni e registrazione, ma non riconosce al danneggiato il diritto di accesso a tali informazioni. È pertanto opportuno stabilire, ai fini dell'accertamento della responsabilità, norme sulla divulgazione degli elementi di prova pertinenti da parte di coloro che ne hanno la disponibilità. Ciò dovrebbe rappresentare anche un ulteriore incentivo a rispettare l'obbligo di documentare o registrare le pertinenti informazioni previsto dalla [legge sull'IA]»

31 Secondo il *considerando* n. 22, «Per porre rimedio alla difficoltà di dimostrare che un determinato input, di cui è responsabile la persona potenzialmente tenuta a rispondere del danno, ha provocato un determinato output del sistema di IA, che a sua volta ha causato il danno in questione, è opportuno prevedere, a determinate condizioni, una presunzione di causalità. Anche se in un'azione per colpa l'attore deve solitamente dimostrare il danno, l'azione o l'omissione umana che costituisce un comportamento colposo del convenuto e il nesso di causalità che li unisce, la presente direttiva non armonizza i criteri in base ai quali gli organi giurisdizionali nazionali accertano l'esistenza della colpa. Tali criteri rimangono disciplinati dal diritto nazionale e, ove siano armonizzati, dal diritto dell'Unione applicabile. Allo stesso modo, la presente direttiva non armonizza i criteri relativi al danno, ad esempio i tipi di danno risarcibile, che rimangono anch'essi disciplinati dal diritto nazionale e dell'Unione applicabile. Affinché si possa applicare

Il secondo strumento presuntivo, fissato dall'art. 4 concerne il nesso di causalità tra la condotta colposa del convenuto e l'*output* prodotto dal sistema di IA, oppure, secondo il caso, tra la condotta colposa del convenuto e la mancata produzione da parte del sistema di IA dell'*output* che detto sistema avrebbe dovuto produrre. Tale presunzione opera, ed è rilevante, subordinatamente all'avverarsi di tutte le seguenti condizioni: a) l'attore ha provato, o il giudice ha presunto *ex* art. 3, la colpa del convenuto, consistente nella violazione di uno degli obblighi di diligenza rilevanti a livello nazionale ed europeo, diretti a prevenire la tipologia di danno occorso; b) si può ritenere ragionevolmente probabile, in base alle circostanze del caso, che la colpa del convenuto abbia influenzato l'*output* generato dal sistema, ovvero la sua mancata produzione; c) l'attore ha provato il nesso di causalità tra il danno subito e l'*output* o la sua mancata produzione da parte del sistema di IA. L'art. 4, §2, specifica che la condizione di cui alla lett. *a* dovrebbe ritenersi integrata unicamente qualora l'attore abbia dimostrato che il fornitore o l'utente non si sono conformati ai requisiti stabiliti dai Capi 2 e 3 del Titolo III dell'*AI Act*. In particolare, si fa riferimento alla inosservanza degli obblighi: a) di cui all'art. 10, §§ 2-4 dell'*AI Act*, in caso di mancato sviluppo del sistema tramite fasi di addestramento, convalida e test di set di dati che soddisfano i criteri di qualità ivi contenuti; b) di trasparenza (art. 13 *AI Act*); c) di supervisione umana (art. 14 *AI Act*); d) di accuratezza, robustezza e cybersicurezza (artt. 15 e 16 *AI Act*). La disposizione considera, poi, specificamente i profili di colpa dell'utente, facendo riferimento alla violazione degli obblighi previsti dall'art. 29 dell'*AI Act* (obbligo di utilizzare il sistema secondo le istruzioni per l'uso, obbligo di interrompere l'uso quando necessario, qualora abbia

la presunzione di causalità prevista dalla presente direttiva, è opportuno che la colpa del convenuto accertata consista in un comportamento umano attivo od omissivo non conforme a un obbligo di diligenza, stabilito dal diritto dell'Unione o nazionale, direttamente inteso a proteggere dal danno verificatosi. Tale presunzione può pertanto trovare applicazione, ad esempio, nelle domande di risarcimento del danno per lesioni fisiche se l'organo giurisdizionale accerta che la colpa del convenuto consiste nell'inosservanza delle istruzioni per l'uso intese a prevenire danni alle persone fisiche. Il mancato rispetto di obblighi di diligenza non direttamente intesi a proteggere dal danno verificatosi, ad esempio la mancata presentazione della documentazione richiesta alle autorità competenti da parte del fornitore, non comporta l'applicazione della presunzione nelle domande di risarcimento del danno per lesioni fisiche. Dovrebbe inoltre essere previsto che si possa ritenere ragionevolmente probabile, sulla base delle circostanze del caso, che il comportamento colposo abbia influito sull'output prodotto dal sistema di IA o sulla mancata produzione di un output da parte di tale sistema. Infine l'attore dovrebbe essere comunque tenuto a dimostrare che l'output o la mancata produzione di un output ha causato il danno». Per il *considerando* n. 25, «Anche qualora sia accertato un comportamento colposo consistente nella non conformità a un obbligo di diligenza direttamente inteso a proteggere dal danno verificatosi, non tutte le fattispecie di colpa dovrebbero comportare l'applicazione della presunzione relativa che stabilisce il nesso tra la colpa e l'output del sistema di IA. Tale presunzione dovrebbe applicarsi solo se si può ritenere ragionevolmente probabile, in base alle circostanze in cui si è verificato il danno, che il comportamento colposo abbia influito sull'output prodotto dal sistema di IA o sulla mancata produzione di un output da parte di tale sistema, che a sua volta ha causato il danno. Si può ad esempio ritenere ragionevolmente probabile che il comportamento colposo abbia influito sull'output o sulla mancata produzione di un output se la colpa risiede nella violazione di un obbligo di diligenza consistente nel definire l'ambito di funzionamento del sistema di IA e il danno si è verificato al di fuori di tale ambito di funzionamento. Al contrario una violazione dell'obbligo di presentare determinati documenti o di registrarsi presso un'autorità, anche se tale obbligo è previsto per una data attività o addirittura specificamente applicabile al funzionamento di un sistema di IA, non può essere ritenuta ragionevolmente idonea a influire sull'output di un sistema di IA o sulla mancata produzione di un output da parte di tale sistema». Il *considerando* n. 24 precisa che «Nei settori non armonizzati dal diritto dell'Unione continua ad applicarsi il diritto nazionale e la colpa deve essere accertata in base al diritto nazionale applicabile».

esposto il sistema a *input* rientranti nel suo controllo) e precisando che, qualora si tratti di utente non professionale, la presunzione opera solo se dimostrato che questo abbia concretamente interferito con il funzionamento del sistema. Anche la presunzione di causalità di cui all'art. 4 è superabile dal convenuto, dimostrando, ad esempio, che la sua condotta non può aver cagionato il danno (*considerando* n. 30, art. 4, § 7)[32]. Inoltre, la presunzione è preclusa *ab origine* all'attore, qualora il convenuto dimostri che la prova di cui è stata ordinata la divulgazione era facilmente accessibile al danneggiato (art. 4, § 4). Occorre rilevare, infine, che la medesima disposizione contempla l'ipotesi di danni cagionati da sistemi di IA non ad alto rischio (non soggetti ai requisiti obbligatori di cui all'*AI Act*), prevedendo che la presunzione di causalità debba applicarsi tutte le volte in cui il giudice ritenga eccessivamente complesso per il danneggiato fornire la relativa prova (art. 4, § 5).

Ai sensi dell'art. 5, la Direttiva sarà sottoposta a revisione dopo cinque anni dalla sua entrata in vigore al fine di valutare l'eventuale opportunità di introdurre forme di responsabilità oggettiva e di assicurazione obbligatoria.

Le suddette proposte consentono di svolgere alcune osservazioni. La Bozza di Regolamento mira ad allestire una strumentazione di *public enforcement* che si affianca a quella di *private enforcement* la quale è imperniata sulla disciplina della responsabilità civile per i danni causati da sistemi di IA[33]: il modello del doppio *enforcement* ripete *mutatis mutandis* quello già adottato in altri settori, come l'*antitrust*. La *AI Liability Directive* si propone infatti di completare il quadro di tutele approntate dall'*AI Act*, che prevede l'imposizione di taluni obblighi gravanti *ex ante* su fornitori e utenti di sistemi di IA «ad alto rischio» nella fase di immissione del *software* sul mercato. La proposta di Direttiva vuole contribuire a rendere effettivi i suddetti requisiti, poiché la non conformità del sistema di IA agli standard previsti dall'*AI Act* è in grado di attivare *ex post* i meccanismi di alleggerimento probatorio in caso di verificazione di eventi dannosi causalmente riconducibili al sistema stesso.

La normativa sul risarcimento del danno ha formato oggetto di specifica e separata considerazione da parte del Parlamento europeo in studi e progetti normativi culminati nella Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), contenente una serie di raccomandazioni e indicazioni finalizzate ad indirizzare la futura disciplina della responsabilità civile applicabile al funzionamento dei sistemi di intelligenza

32 Il *considerando* n. 30 lapidariamente afferma che, «Poiché la presente direttiva introduce una presunzione relativa, il convenuto dovrebbe poter confutarla, in particolare dimostrando che il danno non può essere conseguenza di una sua colpa».

33 Così, Orlando, S.: "Verso l'Artificial Intelligence Act: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale", cit., p. 449.

artificiale e una proposta di regolamento[34]. Alla Risoluzione è seguita la proposta di Direttiva sull'armonizzazione di alcuni profili probatori inerenti ai regimi di responsabilità civile esistenti negli Stati membri e fondati sul criterio della colpa[35], in modo da garantire che i soggetti danneggiati da un sistema di IA c.d. «ad alto rischio» godano di un livello di protezione equivalente a quello di cui godrebbero se i danni in questione fossero stati causati senza il coinvolgimento di un sistema di IA (*considerando* n. 7). A tal fine, come già illustrato, sono previsti in favore del danneggiato meccanismi di semplificazione probatoria potenzialmente in grado di supplire alle difficoltà generate dalle peculiarità dei sistemi di IA, caratterizzati da funzioni di c.d. autoapprendimento, nonché da scarsa comprensibilità da parte del soggetto danneggiato chiamato a provare in giudizio la condotta colposa del responsabile e il nesso di causalità tra questa e il danno. La proposta di Direttiva non ha molto in comune con la suddetta proposta di Regolamento del Parlamento europeo. A parte la differente scelta dello strumento normativo, la *AI Liability Directive* introduce una forma di armonizzazione dei regimi di responsabilità civile esistenti tra gli Stati membri, mentre la Risoluzione del 2020 elaborava in capo agli operatori di sistemi di IA nuove forme di responsabilità *ad hoc*, non limitative di altri regimi di responsabilità, introducendo le nozioni di operatore di *back-end* e di *front-end*. Da ultimo, mentre la proposta di Regolamento prevedeva un regime di responsabilità oggettiva di detti operatori fondata sul rischio e sul grado di controllo su di esso esercitato da ciascuno, la Commissione ha scelto di armonizzare unicamente i regimi di responsabilità per colpa esistenti a livello nazionale, demandando alla futura revisione della direttiva la valutazione dell'opportunità di introdurre regimi di responsabilità oggettiva e di forme di assicurazione obbligatoria.

III. *BLOCKCHAIN, SMART CONTRACT* E DIRITTO DEI CONTRATTI.

Quanto finora scritto si intreccia a perfezione con le tematiche degli *smart contract*, già esistenti da molti anni[36], e della *blockchain,* presentata nel 2008[37]

34 Sulla proposta del Parlamento Europeo, v. D'Alessio, A.: "La responsabilità civile dell'intelligenza artificiale antropocentrica", *Persona e mercato*, 2022, 2, p. 243 ss.

35 De Mari Casareto Dal Verme, T.: "Verso la AI Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una direttiva sull'adattamento delle regole di responsabilità civile all'Intelligenza Artificiale", *Persona e mercato*, 2022, 1, p. 500 ss.

36 Il concetto di *smart contract* è stato elaborato da Nick Szabo (N. Szabo, *Smart contracts: building block for digital markets,* in *Phonetic Sciences Amsterdam* 1996 (*http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html*); Id., *Formalizing and Securing Relationships on Public Networks*, in *First Monday*, 1997, 2, n. 9 - 1 September 1997 (*http://firstmonday.org/ojs/index.php/fm/article/view/548/469*); in argomento, v. Perugini, M.L.: *Distributed Ledger e sistemi di blockchain. Digital currency, smart contract e altre applicazioni*, Vicalvi, 2018 (e-book), p. 29 ss., spec. 33 ss.

37 Satoshi Nakamoto, *Bitcoin: a Peer-to-Peer Electronic Cash Sistem*, del 2008, in *https://bitcoin.org/-bitcoin.pdf*, e nella versione italiana Id., *Bitcoin: un sistema di moneta elettronica peer-to-peer*, in *https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf*. Nel novembre del 2008 Satoshi Nakamoto (pseudonimo dell'inventore di cui non si conosce l'identità) pubblicò il protocollo Bitcoin su *The Cryptography Mailing list* sul sito *metzdowd.com*. Nel 2009 ha distribuito la prima versione del software client e successivamente ha contribuito al

che è sempre più spesso utilizzata, tra l'altro, per l'implementazione dei primi in ragione dell'autonomia e immodificabilità dei processi in esso programmati. Si tratta di nuove tecnologie che stanno cambiando la realtà[38]. Il dibattito civilistico in argomento è oramai avviato in Italia[39], nel quadro della ricchezza dei contributi sul tema dei contratti informatici[40], e in altre esperienze[41].

progetto in via anonima insieme ad altri sviluppatori, per ritirarsi dalla comunità di Bitcoin nel 2010 (v. in proposito, v. Perugini, M.L.: *Distributed Ledger e sistemi di blockchain*, cit., p. 36 ss.).

38 A tal riguardo, il Parlamento Europeo ha pubblicato nel il *paper* EPRS - P. Boucher, *Come la tecnologia blockchain può cambiarci la vita. Analisi approfondita*, Bruxelles, febbraio 2017, in *http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_IT.pdf*, riconoscendo che «le blockchain rappresentano una modalità particolarmente trasparente e decentralizzata per la registrazione di elenchi di transazioni» ed analizzando quali possano essere gli utilizzi concreti oltre la registrazione di criptovalute, quali quelli nel settore dei brevetti, della gestione dei diritti dei contenuti digitali, del voto elettronico, degli *smart contract*, delle catene di approvvigionamento, dei servizi pubblici e delle organizzazioni autonome decentralizzate.

39 In letteratura, tra gli altri, v. Maugeri, M.: Smart contracts *e disciplina dei contratti*, Bologna, 2021, p. 19 ss.; Federico, A.: "Equilibrio contrattuale e contrattazione algoritmica", e Benedetti, A.M.: "Contrattazione, algoritmi e diritto civile transnazionale: cinque questioni e due scenari", entrambi in *Rapporti civilistici* e *intelligenze artificiali*, Atti Convegno SISDIC, Napoli, 2021, rispettivamente p. 85 ss. e p. 69 ss.; Di Sabato, D.: "Autonomia negoziale e distibuted ladger technology", in Valentino, D. (a cura di): *Nuovi contratti della* digital economy, *Singoli contratti. Leggi collegate,* II, Commentario UTET, Torino, 2 ed., 2020, p. 245 ss.; Di Giovanni, F.: "Sui contratti delle macchine intelligenti", in Ruffolo, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 251 ss.; Finocchiaro, G. e Bomprezzi, C.: "A legal analysis of the use of blockchain technology for the formation of smart legal contracts", *Riv. dir. media*, 2020, 2, (*http://www.medialaws.eu/rivista/a-legal-analysis-of-the-use-of-blockchain-technology-for-the-formation-of-smart-legal-contracts/*), p. 1 ss.; Pernice, C.: "Distributed ledger technology, blockchain e smart contracts: prime regolazioni", *Tecn. dir.*, 2020, 2, p. 490 ss.; Bellomia, V.: "Il contratto intelligente: questioni di diritto civile", *www.judicium.it/contratto-intelligente-questioni-diritto-civile/*, 2020; Remotti, G.: "Blockchain smart contract: primo inquadramento e prospettive di indagine (commento all'art. 8 ter D.L. 14 dicembre 2018, n. 135)", *ODCC*, 2020, p. 189 ss.; Giaccaglia, M.: "Gli Smart Contracts. Vecchi e nuovi(?) paradigmi nella prospettiva della protezione dei consumatori", www.dimt.it/wp-content/uploads/2020/08/Giaccaglia-SmartContracts-completo.pdf; Id.: "Considerazioni su Blockchain e smart contracts (oltre le criprovalute)", *Contr. impr.*, 2019, p. 944 ss.; Perugini, M.L.: "Distributed Ledger e sistemi di blockchain", cit., p. 29 ss.; Battaglini, R. e Giordano, M.T. (a cura di): Blockchain e smart contract. *Funzionamento, profili giuridici* e *internazionali, applicazioni pratiche*, Giuffrè, Milano, 2019; Pardolesi, R. e Davola, A.: "«Smart contract»: lusinghe ed equivoci dell'innovazione purchessia", *Foro it.*, 2019, V, p. 195 ss.; Di Sabato, D.: "Gli Smart contracts: robot che gestiscono il rischio contrattuale", *Contr. impr.*, 2017, p. 378 ss.; v. anche Rundo, F. e Conoci, S.: "Tecnologia "blockchain": dagli smart contracts allo smart driving", *SeG_III_MMXVII* (*www.sicurezzaegiustizia.com, 2017, III*); sia consentito rinviare anche a Di Nella, L.: "Smart Contract, Blockchain e interpretazione dei contratti", *Rass. dir. civ.*, 2022, p. 48 ss.

40 In letteratura, per tutti, v. AA. VV.: *Diritto dell'informatica*, (a cura di F. Delfini e G. Finocchiario), 2014, Torino; Clarizia, R. (a cura di): *I contratti informatici*, in *Trattato dei contratti* diretto da P. Rescigno e E. Gabrielli, Torino, 2007; Follieri, L.: *Il contratto concluso in* Internet, Esi, Napoli, 2005; Pennalisico, M.: "La conclusione dei contratti on-line tra continuità e innovazione", *Dir. inf.*, 2004, p. 810 ss.; Tosi, E.: "La conclusione dei contratti on-line", in Id. (a cura di): *I problemi giuridici di Internet (dall'E-Commerce all'E-Business*), Giuffrè, Milano, 2003, p. 101 ss.; Delfini, F.: *Contratto telematico* e *commercio elettronico*, Giuffrè, Milano, 2002; Ricciuto, V. e Zorzi, N. (a cura di): *Il contratto telematico*, in *Tratt. di dir. comm. e dir. pubbl. econ.* diretto da F. Galgano, XXVII, Padova, 2002; Giova, S.: *La conclusione del contratto via* Internet, Esi, Napoli, 2000; Delfini, F.: "Il commercio elettronico", in Vaccà, C. (a cura di): *Il commercio elettronico*, Giuffrè, Milano, 1999, p. 27 ss.; Finocchiaro, G.: *I contratti informatici*, in *Tratt. Dir. comm. e dir. pubbl. econ.* diretto da F. Galgano, XXII, Padova, 1997; Giannantonio, E.: *Diritto dell'informatica*, Giuffrè, Milano, 1997; Id.: *Manuale di diritto dell'informatica*, Cedam, Padova, 1994; Borruso, R.: *Computer e diritto*, II, *Problemi giuridici dell□informatica*, Giuffrè, Milano, 1988; Parisi, F.: *Il contratto concluso mediante computer*, Cedam, Padova, 1987; Clarizia, R.: *Informatica e conclusione del contratto*, Giuffrè, Milano, 1985.

41 Senza pretese di completezza, nella letteratura di lingua tedesca, v. Brägelmann, T. e Kaulartz, M. (a cura di): *Rechtshandbuch Smart Contracts*, München, 2019; Fries, M.e Paal, B.P. (a cura di): *Smart Contracts*, Tübingen, 2019, p. 1 ss.; Schuhmacher, E. e Fatalin, M.: "Compliance-Anforderungen an Hersteller autonomer Software-Agenten. Fünf Grundprinzipien für gesetzliche Instrumente", *Computer und Recht (CR)*, 2019, p. 200 ss.; Vorpeil, K.: „Digitalisierung der Außenhandelfinanzierung - Neue ICC-Richtlinien zur elektronischen Vorlage von Dokumenten bei Akkreditiven und Imkassi - Teil I", *Zeitschrift für Wirtschafts- und Bankrecht*, 2019, 32, p. 1469 ss.; Weiss, S.: *Potenziale und Risiken der Blockchain Technologie im Bankenbereich*, München, 2018; Zimmermann, A.S.: *Blockchain-Netzwerke und Internationales Privatrecht*

Non ostante il nome con cui sono diffusamente chiamati, gli *smart contract* non sono contratti, bensì programmi informatici che automaticamente agevolano, controllano o fanno rispettare la negoziazione o l'esecuzione di un contratto; di solito, hanno anche una interfaccia utente e spesso simulano la logica delle clausole contrattuali[42]. Il carattere *smart* è rappresentato dal fatto che le parti raggiungono un accordo sulle clausole contrattuali e sui tempi sfruttando la logica *If This - Then That* (*IFTTT*), per la quale se si verifica un presupposto (*this*) allora consegue un

oder: der Sitz dezentraler Rechtverhältnisse, in *Praxis des Internationalen Privat- und Verfahrensrechts*, 2018, 6, p. 566 ss.; Spindler, G.: *Gesellschaftsrecht und Digitalisierung*, in *Zeitschrift für Gesellschaftsrecht*, 2018, p. 17 ss.; Heckelmann, M.: *Zulässigkeit und Handhabung von Smart Contracts*, in *NJW*, 2018, p. 504 ss.; Linardatos, D.: *Smart Contracts – einige klarstellende Bemerkungen*, in *Kommunikation & Recht*, 2018, p. 85 ss.; Söbbing, T.: *Smart Contracts und Blockchain-Technologie. Definition, Arbeitswiese, Rechtsfragen*, in *ITRB*, 2018, p. 43 ss.; Paulus, D. e Matzke, R.: *Smart Contracts und das BGB. Viel Lärm um nichts?*, in *ZfPW*, 2018, p. 431 ss.; Idd.: *Digitalierung und private Rechtsdurchsetzung. Relativierung der Zwangsvollstreckung durch smarte IT-Lösungen?*, in *Computer und Recht (CR)*, 2017, p. 769 ss.; Sattler, A.: *Der Einfluss der Digitalisierung auf das Gesellschaftsrecht*, in Betriebsberater, 2018, p. 2243 ss.; Müller, M.: *Bitcoin, Blockchain und Smart Contracts. Technische Grundlagen und mögliche Anwendungsbereiche in der Immobilienwirtschaft*, in Zeitschrift für *Immobilienrecht*, 2017, p. 600 ss.; Schrey, J. e Thalhofer, T.: *Rechtliche Aspekte der Blockchain*, in *NJW*, 2017, p. 1431 ss.; Börding, A., Jülicher, T., Röttgen, C. e von Schönfeld, M.: *Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht: Praxis und Rechtsdogmatik*, in *Computer und Recht*, 2017, p. 134-140; Buchleitner, C. e Rabl, T.: *Blockchain und Smart Contracts*, in *ecolex*, 2017, p. 4-14; Djazayeri, A.: *Rechtliche Herausforderungen durch Smart Contracts*, in *jurisPR-BKR*, 2016, 12, no. 1; Jacobs, C. e Lange-Hausstein, C.: *Blockchain und Smart Contracts: zivil- und aufsichtsrechtliche Bedingungen*, in *IT-Rechts-Berater (ITBR)*, 2017, p. 10-15; Jünemann, M. e Kast, A.: *Rechtsfragen beim Einsatz der Blockchain*, in *Kreditwesen*, 2017, p. 531-536; Mann, M.: *Die Decentralized Autonomous Organization - Ein neuer Gesellschaftstyp? Gesellschaftrechtliche und kollisionsrechtliche Implikationen*, in *Neue Zeitschrift für Gesellschaftsrecht*, 2017, p 1014 ss.; Kaulartz, M. e Heckmann, J.: *Smart Contracts - Anwendung der Blockchain-Technologie*, in *Computer und Recht (CR)*, 2016, p. 618-624; Kaulartz, M.: *Herausforderungen bei der Gestaltung von Smart Contracts*, in *Zeitschrift zum Innovations- und Technikrecht (InTeR)*, 2016, p. 201-206; Id.: *Die Blockchain-Technologie: Hintergründe zur Distributed Ledger Technology und zu Blockchain*, in *Computer und Recht (CR)*, 2016, p. 474 ss.; Gless, S. e Seelmann, K. (a cura di): *Intelligente Agenten und das Recht*, Baden-Baden, 2016; Treiber, K.: *Aus der Praxis: Schuldscheindarlehen als Smart Contracts*, in *REthinking Law*, 2018, 1, p. 10 ss. Nella letteratura di lingua inglese, v. Finck, M.: *Blockchain Regulation and Governance in Europe*, Cambridge, 2019, p. 161 ss.; Durovic, M. e Janssen, A.: *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, *European Review of Private Law* (ERPL), p. ss., e Idd.: *The Formation of Smart Contracts and Beyond: Shaking the Fundamentals of Contract Law?*, in *https://www.researchgate.net/publication/327732779_The_Formation_of_Smart_Contracts_and_Beyond_Shaking_the_Fundamentals_of_Contract_Law*, versione ampliata del primo lavoro; Bourque, S. e Fung Ling Tsui, S.: *A Lawyer's Introduction to Smart Contracts*, in *Lask: Scientia Nobilitat*, 2014, p. 4-23; Casey, A.J. e Niblett, A.: *Self-Driving Contracts*, in 43 *Journal of Corporation Law*, 2017, p. 1-33; Catchlove, P.: *Smart Contracts: A New Era of Contract Use*, ssrn.com/abstract=3090226; Finck, M.: *Blockchains: Regulating the Unknown*, in *German Law Journal*, 2018, 19, p. 665-691; Guggenheim, N.: *The Potentional of Blockchain for the Conclusion of Contracts*, in Schulze, R., Staudenmeyer, D. e Lohse, S. (a cura di): *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps*, Baden-Baden, 2017, p. 83-97; De Filippi, P. e Wright, A.: *Blockchain and the Law: The Role of the Code*, Harvard University Press 2018; I-H Hsiao, J.: *Smart Contract on the Blockchain-Paradigm Shift for Contract Law*, in *US-China Law Review*, 2017, 14, p. 685-694; Mik, E.: *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, in 10 *Journal of Law, Innovation and Technology (JLIT)*, 2017, p. 269-300; O'Shields, R.: *Smart Contracts: Legal Agreements for the Blockchain*, in 21 *North Carolina Banking Institute*, 2017, p. 177-194; Paech, P.: *The Governance of Blockchain Financial Networks*, in 80 *Modern Law Review*, 2017, p. 1072-1100; Raskin, M.: *The Law and Legality of Smart Contracts*, in 1 *Georgetown Technology Review*, 2017, p. 305-341; Reyes, C.L.: *Conceptualizing Cryptolaw*, in 96 *Nebraska Law Review*, 2017, p. 384-445; Ryan, P.: *Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain*, in 7 *Technology Innovation Management Review*, 2017, p. 10-17; Savelyev, A.: *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law*, ssrn.com/abstract=2885241; Scholz, L.H.: *Algorithmic Contracts*, in 20 *Stanford Technology Law Review*, 2017, p. 101-147; Sklaroff, J.M.: *Smart Contracts and the Cost of Inflexibility*, in 166 *University Pennsylvania Law Review*, 2017, p. 263-303; Werbach, K. e Cornell, N.: *Contracts Ex Machina*, in 67 *Duke Law Journal*, 2017, p. 313-382. Nella letteratura di lingua olandese, Tjong Tjin Tai, T.F.E.: *Juridische aspecten van blockchain en smart contracts*, in 54 *Tijdschrift voor Privaatrecht*, 2017, p. 563-608; Id.: *Smart contracts en het recht*, in 93 *Nederlands Juristenblad*, 2017, p. 176-182.

42 Cfr., Paulus, D. e Matzke, R.: *Smart Contracts und das BGB*, cit., p. 433 s.; Brägelmann, T.: *Incomplete Contracts: Eine Sisyphusaufgabe für Legal Tech-Fans*, in *REthinking Law*, 2018, 1, p. 34 ss.; Kaulartz, M. e Heckmann, J.: *Smart Contracts - Anwendung der Blockchain-Technologie*, cit., p. 618.

risultato (*that*). Per il resto, lo *smart contract* ha la capacità di far rispettare le proprie clausole ed entrare in esecuzione senza il supporto di una parte esterna. Pertanto, gli *smart contracts* possono svolgere diverse funzionalità nell'intera vicenda contrattuale.

In generale, detti programmi possono rappresentare un contratto concluso secondo le regole generali e/o porre in essere automaticamente, secondo determinati dati, processi giuridicamente rilevanti di esecuzione del contratto (ad es., pagamenti, accesso ad un bene, spedizione di merci ecc.), evitando così in via preventiva anche inadempimenti contrattuali[43].

Uno *smart contract* può essere anche programmato in modo da reagire a violazioni del contratto digitalmente accertabili, ad esempio tramite ripetizione parziale del pagamento in caso di ritardo nell'esecuzione della prestazione o di esecuzione parzialmente scorretta, oppure tramite lo spegnimento di apparecchi messi a disposizione della controparte o la limitazione dell'accesso o dell'utilizzo di beni (c.d. *smart lock*) in caso di ritardo del pagamento o di scadenza del termine contrattuale.

Inoltre, gli *smart contract* possono essere strumenti per rendere dichiarazioni di volontà negoziali o per porre in essere comportamenti concludenti e atti reali o materiali[44].

Infine, gli *smart contract* possono anche concludere dei contratti, così come accade per i distributori automatici: anche in tal caso, non sarebbero dei negozi giuridici, dovendosi piuttosto discorre di *software*-agenti automatici[45].

43 Secondo Szabo, N.: *Formalizing and Securing Relationships on Public Networks*, cit., «The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas». Pertanto, la *vending machine* (distributore automatico) sarebbe il prototipo primitivo degli *smart contracts* e il fenomeno della 'automatizzazione' dei contratti non sarebbe quindi nuovo.

44 In tal senso, cfr. Paulus, D. e Matzke, R.: *Smart Contracts und das BGB*, cit., p. 434.

45 V., Heckelmann, M.: *Zulässigkeit und Handhabung von Smart Contracts*, cit., p 505 s.; D. Linardatos, *Smart Contracts - einige klarstellende Bemerkungen*, cit., p. 88 s.; Sartor, G.: "Gli agenti software: nuovi soggetti del ciberdiritto?", *Contr. impr.*, 2002, II, p. 465 ss., definiva detti programmi (detti anche agenti digitali, elettronici, o informatici) come programmi informatici capaci di azione autonoma in ambienti complessi, caratterizzati da alcune attitudini tipiche, che concorrono, in misura variabile e in diverse combinazioni, a costituire la loro capacità di azione: la reattività al proprio ambiente (adeguano il proprio comportamento agli stimoli forniti dal contesto nel quale operano), la pro-attività (assumono iniziative per realizzare i propri obiettivi), la persistenza (la loro esecuzione si protrae nel tempo) la capacità d'interazione comunicativa e strategica (inviano e ricevono messaggi, e adeguano il proprio comportamento a quello dei partner), l'intelligenza (sono in grado di acquisire ed elaborare conoscenze, e di apprendere dall'esperienza), la flessibilità (sono

L'importanza degli *smart contract* sta attualmente crescendo a seguito della diffusione dei processi di digitalizzazione e di messa in rete di attività e di beni nel pubblico e nel privato: ad esempio, per le imprese la negoziazione di titoli, gli ordinativi di merce ecc., per i privati gli acquisti o le locazioni di immobili, auto o altri mezzi per brevi periodi effettuati tramite delle applicazioni, oppure il collegamento alla rete di determinate cose, come le serrature di appartamenti o stanze di albergo e i 'lucchetti' di mezzi di trasporto - c.dd. *smart lock* -, di frigoriferi per ordinare generi alimentari o richiedere interventi tecnici, discorrendosi in tali ultimi casi del noto fenomeno dell'*internet* delle cose (*Internet of Things*).

In ragione di siffatta rapida evoluzione e del crescente bisogno di automazione, agli *smart contract* è potenzialmente aperto un gran numero di possibili impieghi digitali rispetto a valori patrimoniali che sono oggetto della prestazione o della controprestazione di un contratto o di prestazioni risarcitorie o compensative in caso di inadempimento[46]. In particolare, è incrementata la loro applicazione insieme alla *distributed ledger technology* (tecnologie basate su registri distribuiti, ossia le strutture di banche dati diffuse che pubblicamente e decentralmente registrano la sequenza delle transazioni, abbreviate in *DLT*), quindi anche con l'ambiente operativo di una *blockchain*[47]. Nel novero degli ambiti di applicazione delle *DLT*, anche sulla scorta di quanto riconosciuto in uno studio del *Financial Stability Board*[48], lo stesso Parlamento Europeo ha in più occasioni evidenziato come uno degli ambiti di maggior impatto dell'utilizzo delle tecnologie *DLT* possa essere rappresentato proprio dagli *smart contract*. Sia nel *paper* del febbraio 2017, sia nella risoluzione del 3 ottobre 2018, il Parlamento Europeo ha riconosciuto che «i contratti intelligenti sono un elemento importante abilitato dalle *DLT* e possono fungere da fattori chiave delle applicazioni decentralizzate».

È alle *DLT* che va quindi rivolta l'attenzione. La locuzione *distributed ledger technologies* (tecnologie a registri distribuiti), indica un insieme di protocolli che permettono a una rete composta da nodi di attori di pari entità (*peer nodes*) di gestire un registro, o *ledger*, sincronizzato tra i partecipanti grazie all'utilizzo della crittografia e senza necessità di un unico nodo centrale che si occupi della gestione e del controllo del registro.

Le *DLT* abilitano la possibilità di gestire un registro in cui le evoluzioni dei dati custoditi siano condivise e controllate da più attori contemporaneamente. Un

in grado di affrontare situazioni complesse ed imprevedibili), la mobilità (possono spostarsi nell'ambiente, al fine di individuare le risorse di cui abbisognano e i partner con cui collaborare).

46 Paulus, D. e Matzke, R.: *Smart Contracts und das BGB*, cit., p. 435, riportano un esempio di uso degli *smart contracts* nella *sharing economy* e uno nell'*e-commerce*.

47 V., in proposito, Spindler, G.: *Gesellschaftsrecht und Digitalisierung*, in *Zeitschrift für Gesellschaftsrecht*, cit., p. 44; De Filippi, P. e Wright, A.: *Blockchain and the Law: The Role of the Code*, cit., p. 13 ss.

48 Financial Stability Board, *Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that merit Authorities' attention*, 27 June 2017.

sottoinsieme di tali protocolli, indicato con il termine di *blockchain*, individua quelli in cui l'evoluzione dei dati del registro è governata attraverso strutture a blocchi crittograficamente concatenati l'uno all'altro. In generale, e in via semplificata, una *blockchain* è una banca dati particolarmente sicura che effettua registrazioni di diversi dati e si differenzia da altre banche dati essenzialmente per l'utilizzo di diversi procedimenti criptografici e per la sua fondamentale autonomia e immodificabilità[49]. Siffatte caratteristiche trovano applicazione nell'ambiente *peer-*

49 Cfr. la definizione di *blockchain,* riferito alla criptovalute, elaborata dalla CONSOB: «Un *distributed ledger* o *blockchain* (quest'ultimo nome è in genere accomunato all'utilizzo del bitcoin e in italiano si traduce letteralmente in 'catena di blocchi') è un registro aperto e distribuito che può memorizzare le transazioni tra due parti in modo sicuro, verificabile e permanente. I partecipanti al sistema vengono definiti 'nodi' e sono connessi tra di loro in maniera distribuita. Nella sostanza è una lista in continua crescita di record, chiamati *block*, che sono collegati tra loro e resi sicuri mediante l'uso della crittografia. I dati in un blocco sono per loro natura immutabili (non possono essere retroattivamente alterati senza che vengano modificati tutti i blocchi successivi ad esso; per fare ciò, dati la natura del protocollo e lo schema di validazione, servirebbe il consenso della maggioranza della rete). La natura distribuita e il modello cooperativo rendono particolarmente sicuro e stabile il processo di validazione, pur dovendo ricorrere a tempi e costi non trascurabili, in gran parte riferibili al prezzo dell'energia elettrica necessaria per effettuare la validazione dei blocchi (questo nel caso della Blockchain del bitcoin) e alla capacità computazionale necessaria per risolvere complessi calcoli algoritmici (attività che viene comunemente definita come 'mining'). L'autenticazione avviene tramite la collaborazione di massa ed è alimentata da interessi della comunità. La Blockchain è un registro pubblico delle transazioni Bitcoin in ordine cronologico. È utilizzata per memorizzare in modo permanente le transazioni Bitcoin e per prevenire il fenomeno del cosiddetto 'double spending' (per evitare che possa spendere i bitcoin più di una volta nello stesso momento). Come già osservato, la Blockchain è un insieme di blocchi fra loro concatenati: ogni blocco è identificato da un codice, contiene le informazioni di una serie di transazione, e contiene il codice del blocco precedente, così che sia possibile ripercorrere la catena all'indietro, fino al blocco originale (una sorta di DNA delle transazioni Bitcoin). Tutti i nodi della rete memorizzano tutti i blocchi e quindi tutta la Blockchain», in *http://www.consob.it/web/investor-education/criptovalute*. Cfr. anche la definizione del *Bundesanstalt für Finanzdienstleistungsaufsich* (abbreviato in *BaFin*, autorità federale pubblica e indipendente per la supervisione del settore finanziario, soggetta alla stretta vigilanza tecnica e legale del Ministero Federale della Finanza tedesco): «Blockchains sind fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert, nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind. Mit der Blockchain-Technologie lassen sich Eigentumsverhältnisse direkter und effizienter als bislang sichern und regeln, da eine lückenlose und unveränderliche Datenaufzeichnung hierfür die Grundlage schafft», in *https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html*. Rundo, F. e Conoci, S.: "Tecnologia "blockchain": dagli smarts contracts allo smart driving", *SeG_III_MMXVII* (*https://www.sicurezzaegiustizia.com*, 2017) forniscono questa descrizione della blockchain: «L'infrastruttura blockchain può essere descritta semplicemente come una rete globale di dispositivi interconnessi (nodi) e nella quale è opportunamente memorizzato un registro digitale pubblico condiviso (denominato in gergo "Global Distributed Ledger") il quale è riprodotto opportunamente su ciascuno dei dispositivi-nodi. Pertanto, all'interno della rete blockchain è memorizzato un notevole quantitativo di dati distribuito opportunamente tra i vari records informativi presenti su ciascun dispositivo-nodo. Tali records sono in continua evoluzione sia in relazione al loro numero che in relazione all'informazione in essi contenuta. L'elevata sicurezza dei dati memorizzati nella blockchain è garantita dal meccanismo di funzionamento, di fatto estremamente innovativo. Elemento chiave del funzionamento della blockchain è la tecnica di memorizzazione dei dati: una copia dell'intero registro della blockchain (ledger) è memorizzata su ciascun dispositivo-nodo partecipante. Ogni record informativo del ledger memorizzato su un dispositivo-nodo è composto dalle seguenti due parti: - transazioni: includono i dati in un formato prestabilito; blocchi: questi dettagliano il flusso di operazioni sulle transazioni, in opportuno ordine temporale. Ogni blocco include un codice hash di sicurezza. Le transazioni sono generate dai partecipanti alla rete blockchain in relazione all'utilizzo applicativo che intendono perseguire (smart contracts, accesso dati, comunicazione tra nodi remoti, trasmissione o invio dati o altro, etc..), mentre i blocchi sono generati da partecipanti speciali, i cosiddetti miners (letteralmente "minatori"), che utilizzano software, hardware specializzato e potenti algoritmi matematici per validare le transazioni e creare i blocchi. Quando una transazione digitale viene completata, viene inclusa in un raggruppamento di transazioni (blocco) opportunamente criptato (di solito vengono raggruppati più blocchi ad intervalli di tempo regolari, tipicamente 10 minuti) e diffusa nell'intera blockchain dove sarà validata dai miners, mediante opportuni algoritmi matematici alquanto complessi. Ad ogni blocco validato dai miners viene assegnata (sempre mediante un algoritmo complesso) una c.d. marca temporale (Timestamp). Ogni blocco validato con marca temporale, sarà aggregato agli altri blocchi in una catena lineare, cronologicamente ordinata e sempre aggiornata, dunque, sarà inviato a tutta la blockchain: in tal modo ogni dispositivo-nodo della blockchain conterrà una copia di questi blocchi in un registro

to-peer, ossia nel collegamento e comunicazione tra nodi paritari (*peer*) in una rete aperta o chiusa priva di una unità centrale di controllo o di archiviazione dei dati. Si possono configurare le più diverse tipologie di *blockchain* tra loro anche molto differenti, non esistendone quindi una unica[50].

La principale caratteristica delle *blockchain*, rispetto alle *DLT*, è proprio che in ciascun nodo della rete vi è una copia completa del registro contenente tutte le transazioni effettuate da tutti gli attori. Le *DLT* che non rientrano in questa definizione di *blockchain*, invece, non sono basate su una struttura a blocchi e permettono quindi di creare sottogruppi di *data disclosure* dove ciascun nodo detiene solo una parte del registro delle transazioni, ovvero quelle in cui il nodo stesso è originatore o ricevente, per garantire maggiore *privacy* tra i partecipanti.

Si può quindi affermare che mentre nelle *DLT*, diversamente dai registri centralizzati (i classici *database*), il controllo dell'evoluzione dei dati è condiviso tra alcuni partecipanti della rete, nelle *blockchain*, sottoinsieme delle *DLT*, il controllo dell'evoluzione dei dati tracciati nel registro è condiviso tra tutti i partecipanti della rete.

Una transazione è l'elemento chiave di una *blockchain*: è il modo con cui un generico attore (nodo) può richiedere una modifica al registro andandone ad alterare il contenuto. Il registro non sarà altro che il risultato di tutte le transazioni fatte da tutti i nodi dal momento esatto in cui è nata la *blockchain* fino al momento attuale in cui la si osserva.

In una *blockchain*, infatti, ciascun nodo ha una propria copia completa del registro delle transazioni. Il protocollo prevede che solo un nodo della rete per volta (e mai lo stesso) possa aggregare tutte le transazioni fatte dai nodi in un intervallo di tempo definito (a seconda della rete) in una struttura dati chiamata 'blocco'. Questo blocco viene legato crittograficamente a quello precedente, includendo al suo interno l'impronta digitale (*hash*) dell'ultimo blocco disponibile sulla rete, e successivamente viene inviato a tutti i partecipanti.

Ciascun nodo (o partecipante) andrà ad aggiornare il proprio registro locale sulla base delle transazioni presenti nel blocco ricevuto. In questo modo si ha

distribuito (ledger). In tal modo la struttura della blockchain sarà decentralizzata e priva di un arbitro o di un server centrale di aribitraggio oltre che protetta da potenti algoritmi di crittografia. Queste caratteristiche rendono le transazioni della blockchain "autonome" nel senso che queste avvengano automaticamente senza l'intervento di intermediari. Se un hacker volesse violare un blocco della blockchain, dovrebbe violare tutti i blocchi costituenti la catena associata a quel blocco eseguendo delle azioni non autorizzate su ciascuno dei ledgers associati ad ogni dispositivo-nodo, il cui numero è di fatto sconosciuto a priori e può, ben essere, elevato rendendo praticamente e materialmente impossibile eseguire un cyber-attacco o un qualsivoglia tentativo di corruzione dati».

50 Così, Paulus, D. e Matzke, R.: *Smart Contracts und das BGB*, cit., p. 434; *contra*, Wilsch, H.: „Die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts", *Deutsche Notar-Zeitschrift*, 2017, p. 761, sembra prendere le mosse da un concetto unitario.

la ragionevole certezza che tutti i nodi della rete abbiano, in locale, un registro perfettamente identico a quello degli altri partecipanti.

Questa tecnologia ha dei risvolti interessanti: non esiste una copia centrale da alterare, qualora si voglia modificare un'informazione inclusa nel registro attraverso una transazione passata. Un ipotetico nodo malevolo dovrebbe cambiare tutti i registri di tutti i nodi della rete. Inoltre, cambiare l'informazione equivale a modificare il blocco passato, ma questa operazione ne cambia anche la sua impronta digitale, richiedendo la modifica (o il ricalcolo) anche del blocco successivo e di tutti gli altri blocchi della catena fino a quello attuale.

Questa riscrittura dell'intera catena può avvenire solo in alcuni tipi di *blockchain* e solo se tutti i nodi (o almeno la maggioranza) sono concordi nell'effettuarla. In alcuni casi questa operazione è improbabile: ad esempio nelle *blockchain* c.dd. *permissionless* (sia per lo pseudonimato dei partecipanti, sia per i disincentivi dovuti al *proof-of-work*) la probabilità di riuscire a riscrivere i blocchi è prossima allo zero. In alcune *blockchain* c.dd. *permissioned*, invece, gli attori sono tutti noti, ma se il numero è sufficientemente elevato e la *governance* della rete tiene conto di alcuni aspetti, anche in questo caso la probabilità di effettuare una riscrittura potrebbe in teoria essere ridotta al minimo.

Per questo motivo alcune *blockchain*, ma non tutte, hanno una caratteristica (anche giuridicamente) molto interessante: le informazioni al loro interno sono immutabili e riconducibili a un particolare istante nel tempo.

La diffusione di queste tecnologie rende oramai necessario intervenire per predisporre una regolamentazione. Qualche Paese ha già emanato provvedimenti in tal senso. Il Parlamento Europeo, nella *Risoluzione del Parlamento europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione (2017/2772(RSP))* proprio in merito agli *smart contract* ha sottolineato la necessità che la Commissione effettui una valutazione approfondita delle potenzialità e delle implicazioni giuridiche, ad esempio i rischi relativi alla giurisdizione e la necessità di dare certezza alla validità di una firma digitale crittografata quale passo fondamentale per favorire gli *smart contract*. Allo stesso tempo, ha invitato la Commissione a promuovere l'elaborazione di norme tecniche a livello delle pertinenti organizzazioni internazionali, quali ISO, UIT e CEN-CELENEC ed a condurre un'analisi del quadro giuridico esistente nei vari Stati membri in relazione all'applicabilità degli *smart contract*, cercando anche di rafforzare la loro validità attraverso il coordinamento giuridico o il riconoscimento reciproco tra gli Stati membri.

Il Parlamento Europeo ha individuato due macroambiti di interesse che richiederebbero ulteriori approfondimenti e una definizione certa del quadro

giuridico, al fine di garantire la certezza necessaria agli operatori per poter applicare quanto ipotizzato:

l'inquadramento degli *smart contract* nell'ambito degli ordinamenti giuridici nazionali, superando il contrasto che si verrebbe a creare tra una tecnologia fondata sulla immutabilità di termini e condizioni e ordinamenti giuridici fondati, almeno in parte, sull'autonomia delle parti che potrebbero decidere di modificare determinate condizioni in corso di validità del contratto;

il riconoscimento della validità di una firma digitale crittografata, anche attraverso l'elaborazione di norme tecniche da parte delle organizzazioni internazionali competenti.

A tal fine, il Parlamento Europeo ha espressamente incaricato la Commissione Europea di promuovere l'introduzione di tali tecniche, nonché il superamento di potenziali ostacoli all'utilizzo di tali contratti nel c.d. mercato digitale unico (*digital single market*).

In Italia le *DLT* e gli *smart contract* sono disciplinati dall'art. 8-*ter* d.l. n. 135 del 2018, convertito con modifiche in l. n. 12 del 2019. Il comma 1 descrive le «tecnologie basate su registri distribuiti», di cui le *blockchain* sono sottoinsiemi, come «le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili»[51]. Il comma 3 ne regola gli effetti quale mezzo di prova in procedimenti giudiziali: la «memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014»[52]. Ai sensi del comma 4, «Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le

51 La Bank for International Settlements - Committee on Payments and Market Infrastructures, *Distributed ledger technology in payment, clearing and settlement*, February 2017, ha definito le tecnologie basate su registri distribuiti come «processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes», evidenziando come la natura di tali tecnologie sia insita nell'utilizzo delle c.dd. reti di nodi, che collegati gli uni agli altri rendono possibile lo scambio di dati tra un utente ed un altro.

52 Questo il testo dell'art. 41 reg. UE 910/2014 «Effetti giuridici della validazione temporale elettronica. 1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata. 2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate. 3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri».

tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3».

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

Queste disposizioni inducono a svolgere alcune riflessioni. La disciplina fissa gli effetti delle tecnologie basate su registri distribuiti quali mezzi di prova in procedimenti giudiziali, al ricorso di determinate condizioni fissate dall'AGID: la «memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti» produce gli effetti giuridici della «validazione temporale elettronica». Queste prescrizioni fanno sorgere alcuni dubbi. In base a siffatta definizione, un registro distribuito erogato da un singolo attore utilizzando tre *server* di un servizio *cloud* dovrebbe poter beneficiare degli effetti giuridici della validazione temporale elettronica: in questo caso però un qualsiasi esperto (ad esempio, in caso di contestazione della validità di tale tecnologia in sede giurisdizionale) potrebbe dimostrate la semplice alterabilità del contenuto da parte dell'attore e quindi farne decadere gli effetti giuridici. È importante, dunque, fissare con precisione i requisiti tecnici entro i quali ricade un registro distribuito o una *blockchain* per poter essere considerata immutabile e conseguentemente beneficiare degli effetti giuridici definiti dalla normativa.

Allo stesso modo, è fondamentale delineare tecnicamente i concetti di «distribuito, condiviso e replicabile»: mentre alcune *blockchain* prevedono una copia completa del registro su tutti i nodi della rete, altre tecnologie innovative di registri distribuiti contemplano una distribuzione, condivisione e replicazione dei dati solo tra i nodi interessati alla transazione (*on a need to know basis*). È importante quindi porre attenzione alla definizione, se si vuole evitare di lasciare questo ultimo tipo di registri distribuiti al di fuori dell'ambito di applicazione della normativa.

Lo *smart contract* è definito nell'art. 8-*ter* come un programma per elaboratore che opera su tecnologie basate su registri distribuiti la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Secondo siffatta disposizione uno *smart contract*, per essere considerato tale, deve possedere congiuntamente le seguenti caratteristiche: essere un programma per elaboratore; operare su tecnologie basate su registri distribuiti; l'esecuzione vincola automaticamente due o più parti; gli effetti sono predefiniti dalle stesse.

Mentre i primi due requisiti sono comuni a tutte le tipologie di *smart contract* e non sembrano creare particolari questioni, gli altri due pongono dei problemi.

Molto spesso in rete una delle parti offre un prodotto o un servizio predisponendo unilateralmente il regolamento negoziale, ciò che accade anche per l'acquisto di *token* contro criptovalute. Tale fattispecie è riconducibile all'offerta al pubblico *ex* art. 1336 c.c. e si configura come una proposta, spesso irrevocabile, i cui termini sono unilateralmente predeterminati dal proponente. È quest'ultimo, infatti, che decide il quantitativo di *token* che trasferirà in cambio della criptovalute e che può stabilire altri vincoli accessori in capo a colui che accetta la proposta, come, tra gli altri, limiti temporali alla libera negoziabilità dei *token* trasferiti. In tale contesto gli effetti del contratto non sono «predefiniti» dalle parti, ma vengono unilateralmente determinati da una di esse ed eventualmente accettati da coloro ai quali l'offerta è diretta[53]. In base al tenore letterale della disposizione, una tale fattispecie contrattuale rimarrebbe irragionevolmente esclusa dall'applicazione della norma, mancando la congiunta predeterminazione degli effetti tra le parti. Una possibile interpretazione che potrebbe superare questa infelice previsione è quella per la quale con il termine «predefiniti dalle stesse» si intende discorrere di effetti predisposti da entrambe le parti, oltre che soltanto da una di esse come solitamente accade. In tal modo, si ricomprendono nel perimetro della definizione anche i casi in cui gli *smart contract* attuano un regolamento di interessi che è il frutto delle classiche trattative prenegoziali intercorse tra i contraenti. Infine, va altresì ricordato che, in ogni caso, gli effetti non sono soltanto quelli previsti dal predisponente o dai contraenti, bensì anche quelli fissati dalla legge ai sensi dell'art. 1374 c.c.: in tal senso, peraltro, sarebbe più corretto discorrere di effetti "individuati" dalle parti.

Anche il requisito secondo il quale uno *smart contract* vincola automaticamente le parti in conseguenza della sua esecuzione pone dei dubbi. Il termine "esecuzione" potrebbe essere riferito sia al fatto che lo *smart contract*, essendo un programma per elaboratore, viene eseguito (nel senso dell'elaborazione da parte della macchina delle istruzioni in esso contenute), sia all'esecuzione delle obbligazioni e prestazioni in senso stretto. Si osserva in proposito che si tratta di due momenti distinti che in concreto potrebbero non coincidere: l'esecuzione in senso informatico di uno *smart contract* non necessariamente comporta l'esecuzione delle prestazioni contrattuali, qualora, ad esempio, non si avverino le condizioni nello stesso previste, oppure riguardi soltanto una parte di esse,

53 V., Rampone, F.: "Linee guida AGID e il paradosso della forma scritta", *https://associazioneblockchain.it/wp-content/uploads/2020/02/20.02.14-Le-Linee-Guida-dellAgID-su-smart-contract.pdf*, p. 2, il quale afferma quanto segue: «poiché gli utenti, in genere, non partecipano alla stesura di uno smart contract prima di eseguirlo, né comprendono il significato del codice laddove potessero leggerlo, la "predefinizione degli effetti" deve essere intesa in senso restrittivo, come mera selezione delle variabili dello smart contract per indirizzare la sua esecuzione, proprio come la selezione sul pannello di un distributore automatico fa sì che questo eroghi il prodotto scelto».

ad esempio il pagamento tramite criptovalute, presupponendo un contratto già formato. Inoltre, far dipendere il sorgere del vincolo dall'esecuzione del contratto intesa quale esecuzione della prestazione, sembra richiamare l'art. 1327 c.c. relativo alla conclusione del contratto mediante inizio dell'esecuzione e in alcune ipotesi sembra persino far ricadere gli *smart contract* nell'ambito dei contratti reali che si perfezionano al momento della consegna materiale della cosa. In tale ottica, fin quando non sono eseguite le prestazioni, uno *smart contract* non vincolerebbe le parti in quanto non ancora concluso. Siffatta interpretazione comporta dunque dei problemi di diversa natura. Si ipotizzi che due parti decidano di regolare tra loro un determinato rapporto prevedendo, per la fase esecutiva, il ricorso ad uno *smart contract* che a scadenze determinate provveda a trasferire una criptovaluta quale corrispettivo di una prestazione, magari da svolgere *off-chain*. L'oblato di detta prestazione la esegue confidando nello *smart contract*, mentre la parte debitrice della controprestazione, per sfuggire alla stessa, non provvede al deposito sull'indirizzo dello *smart contract* della criptovaluta corrispondente. In questo caso, il contratto non andrebbe in esecuzione in quanto non viene attuato alcun trasferimento e secondo la norma non sarebbe suscettibile di tutela, proprio perché ancora non perfezionato. Oltre a questo aspetto critico sul piano fattuale, va altresì rilevato che gli *smart contract* possono svolgere nel contesto della operazione contrattuale diverse funzioni, generando ad esempio le manifestazioni di volontà dei contraenti, dando esecuzione alle stesse, oppure attuando alcuni aspetti del rapporto o determinando la cessazione delle prestazioni allo scadere del termine finale. È evidente, dunque, che la caratteristica in esame non può essere intesa come riferita a un modo di formazione tipico e necessario dei contratti in cui si fa ricorso a uno *smart contract*. Piuttosto, sembrerebbe potersi ritenere che i negozi in cui è utilizzato uno *smart contract* abbiano piena rilevanza giuridica, a prescindere dalla modalità consensuale o reale con cui si formano, dal tipo di effetti obbligatori e/o reali che producono e dalle modalità di esecuzione. Interpretata in tal senso, la previsione in esame sembrerebbe allora non porre un requisito, ma dare pieno riconoscimento al ruolo svolto dall'esecuzione degli *smart contract*, ossia dei programmi, nella vicenda contrattuale e di conseguenza al relativo contratto. Detto riconoscimento è anche automatico, non essendo richiesto a tal fine alcun altro elemento, come ad esempio un consenso specifico all'uso dello *smart contract* o una dichiarazione di consapevolezza dell'intervento degli stessi emessa da una o da entrambe le parti. Ai fini della individuazione della disciplina applicabile, occorrerà di volta in volta individuare quale operatività hanno detti programmi per comprenderne la funzione (di manifestazione di volontà, di trattativa, di determinazione del contenuto, di esecuzione totale o parziale del rapporto ecc.) nella complessiva vicenda contrattuale.

La seconda parte della disposizione statuisce che lo *smart contract* soddisfa il requisito della forma scritta nel caso di previa identificazione informatica delle

parti interessate, tramite un processo i cui requisiti devono essere fissati da AGID. Pertanto, uno *smart contract* sembra poter soddisfare il requisito della forma scritta. In proposito, va osservato innanzi tutto che tale forma è un *vestimentum* di un contratto ai sensi dell'art. 1325 c.c. per gli atti indicati dall'art. 1350 c.c., non di un programma per elaboratore, il quale può svolgere una serie di funzioni anche soltanto esecutive del programma contrattuale alle quali non è estendibile la forma scritta[54]. Oltre a questi rilievi già decisivi sulla portata della disposizione, si deve considerare che, essendo un programma per elaboratore, in assenza di un'espressa previsione potrebbero sorgere dubbi sulla conformità di uno *smart contract* al requisito dell'immodificabilità di cui all'art. 3, comma 2, del DPCM 13 novembre 2014 e a quanto previsto dall'art. 4, comma 3 del DPCM 22 febbraio 2013 secondo cui non può considerarsi immodificabile un documento informatico che contiene macroistruzioni o codici eseguibili (questi ultimi contenuti, per definizione, in uno *smart contract*). In assenza di una previsione espressa lo *smart contract*, pertanto, potrebbe non essere in grado di rientrare nell'ambito della categoria di documento informatico immodificabile, con la conseguenza che ne verrebbe meno la validità da questo punto di vista.

Tale seconda disposizione sembra inoltre richiamare l'art. 20, comma 1 *bis*, d.lgs. n. 82 del 2005, che stabilisce i presupposti per cui un documento informatico è idoneo a soddisfare il requisito della forma scritta. Detto art. 20, inoltre, individua anche gli strumenti di attribuzione della paternità del documento informatico (firma elettronica qualificata, firma elettronica avanzata, firma "identificata", nonché firme elettroniche "semplici" a seguito della valutazione del giudice) che consentono di conferirgli tale efficacia.

Ad ogni modo, la definizione di *smart contract* necessita di un approfondimento importante da parte di AGID e forse anche di una rimodulazione. Nella sostanza uno *smart contract* non è altro che una logica di *business* applicata a una transazione effettuata su un registro distribuito, essendo quindi non riconducibile al classico concetto di "contratto" anche da questo punto di vista[55]. L'aspetto più delicato

54 In tal senso, v. Rampone, F.: "Linee guida AGID e il paradosso della forma scritta", cit., p. 2 e 5, ove osserva che «lo smart contract non può avere forma scritta in quanto non è un atto o un contratto, ma solo un ingranaggio digitale. Al contrario, forma scritta può averla la manifestazione di volontà delle parti in ordine alla determinazione degli effetti («effetti predefiniti dalle stesse», art. 8-ter, comma 2, primo periodo). Solo in questa fase di "riempimento" di contenuti specifici dello smart contract può intervenire un protocollo che conferisca forma scritta (art. 2702 c.c.) alla manifestazione di volontà dell'utente (o delle parti). Se dobbiamo infatti riconoscere - come effettivamente è - che l'utente ha di fronte una vending machine virtuale e che la sua manifestazione di volontà è limitata al più alle sole variabili da lui selezionate nello smart contract, dobbiamo allora riconoscere che l'art. 8-ter nella sua attuale formulazione estende la forma scritta anche ad elementi che non sono manifestazioni di volontà. Si finisce infatti per attribuire il requisito della forma scritta a cose (la vending machine, *aka* smart contract) o a fatti e comportamenti (la mera esecuzione di un programma per elaboratore)».

55 Secondo Rampone, F.: "Linee guida AGID e il paradosso della forma scritta", cit., p. 2, il sillogismo espresso dalla norma sulla forma degli *smart contract* [«A. tutti gli smart contract sono programmi per elaboratore; B. gli smart contract (a certe condizioni) soddisfano la forma scritta; C. la forma scritta è attributo di atti e contratti; quindi: D. i programmi per elaboratore sono atti e contratti, sono cioè atti umani o

è proprio dovuto al fatto che il vero vantaggio di uno *smart contract* rispetto ad un generico *software* è la possibilità di poter automaticamente dare esecuzione delle logiche codificate rispetto ad *asset* tracciati sul registro distribuito. Per meglio chiarire questo concetto si pensi ad esempio a un registro distribuito che tracci *asset* puramente digitali e quindi esistenti unicamente sullo stesso registro (ad esempio, voti, euro, *bitcoin* o altre *cryptocurrencies*). In questo caso, uno *smart contract* è in grado, da solo, di dare esecuzione alle regole di *business* in esso codificate: "permetti l'assegnazione di un voto solo se il chiamante non ha già effettuato altre transazioni in passato". Lo *smart contract* è autonomo nel decidere se la transazione è lecita e non necessita di intervento da parte di soggetti esterni. Le potenzialità degli *smart contract* al di fuori dell'*enforcement* automatico di regole di *business* codificate sono marginali: l'identificazione certa, la non ripudiabilità, la codifica informatizzata ecc., sono caratteristiche offerte da molte tecnologie preesistenti come la crittografia PKI, la *digital identity* o le funzioni di *hashing*.

Detto vantaggio, però, lo si può sfruttare solo in contesti in cui lo *smart contract* agisce su *asset* tracciati dal registro distribuito: nel caso in cui l'*asset* sia presente nel mondo reale, ma solo rappresentato in formato digitale su una *blockchain*, allora lo *smart contract* ha bisogno di supporto dal mondo esterno. Ad esempio, un registro distribuito che traccia proprietà fisiche (come beni immobili o auto), avrà al suo interno *asset* univoci che fanno riferimento al mondo reale. In questi casi, tuttavia, uno *smart contract* non è in grado di effettuare *enforcing* delle logiche di *business*: è possibile verificare attraverso uno *smart contract* il passaggio da un proprietario (ad esempio, lo scrivente) ad un altro (ad esempio, il lettore), tuttavia quello sarà solo un passaggio della rappresentazione digitale. Nel mondo reale lo scrivente potrebbe rifiutarsi di cedere la proprietà dell'oggetto al lettore.

Qui entra in gioco la regolamentazione e, dunque, le specifiche tecniche dell'AGID: definire come e quando è possibile creare una relazione tra ciò che appartiene al mondo fisico/reale ed il relativo *digital twin* tracciato nel registro distribuito, in modo che uno scambio effettuato sul registro (*on-chain*) da uno *smart contract* sia legale (ed *enforceable*) anche per il suo corrispondente nel mondo reale.

Inoltre, sia per quanto riguarda il caso di *asset* puramente digitale sia quello di *digital twin*, il lavoro di AGID è molto delicato: dando piena efficacia a uno

manifestazioni di volontà che assumono rilevanza per l›ordinamento giuridico»] è «paradossale. Tanto più se consideriamo un elemento niente affatto secondario, e cioè che il contenuto di uno smart contract non è quasi mai intellegibile alle parti e non può quindi costituire espressione della loro volontà: non può cioè essere nemmeno un *atto umano*, trattandosi semmai di un fatto, ovvero un elemento esterno che preesiste rispetto alla volontà e coscienza delle parti (è lontanamente paragonabile ad un modulo o formulario *ex* art. 1342 c.c. scritto in una lingua incomprensibile all'aderente). Come ho sottolineato molte volte, uno smart contract è un'istruzione rivolta ad una macchina e non un *medium* del dialogo tra esseri umani che invece si svolge sul differente piano del linguaggio naturale» (i corsivi sono nel testo).

smart contract, sembrerebbe confermarsi quell'aspetto che è stato definito *code-is-law*[56]. A prescindere dal fatto che il codice non è la legge del contratto, ma soltanto - appunto - un codice di programma, l'esperienza insegna che gli *smart contract* possono essere soggetti a malfunzionamenti e *bug* che possono essere sfruttati da attori malevoli per far eseguire a detti programmi istruzioni non espressamente volute dall'utilizzatore o dall'autore. In questi casi, occorre fare attenzione: se valesse la logica del *code-is-law*, allora anche le azioni non volute (potenzialmente fraudolente) sarebbero considerabili come 'legali' e quindi fonte di pretese tutelabili. Diversamente, invece, si dovrebbe valutare caso per caso cosa è accaduto in concreto in relazione ai parametri normativi per concedere o negare tutela secondo la conformità di quanto previsto dal codice alla normativa. Un possibile accorgimento da adottare da un punto di vista tecnico potrebbe essere quello di prevedere la necessità per ciascuno *smart contract* di includere l'*hash* di un contratto tradizionale che descriva a parole quello che è stato codificato nello *smart contract*. Alcune tecnologie (cfr. Corda) hanno introdotto questo concetto di *Legal Prose*: se un attore malevolo dovesse sfruttare un *bug* del codice per eseguire delle operazioni non previste dalla *Legal Prose*, allora la transazione potrebbe essere ritenuta invalida e l'attore malevolo sarebbe costretto ad effettuare la transazione contraria (nel caso di *asset* reali non ci sarebbe tutela). Ad ogni modo, sarà necessario uno studio attento dei possibili risvolti delle specifiche proposte da AGID.

Nel complesso, comunque, l'approccio seguito dal legislatore italiano sembra inserirsi nel dibattito internazionale sugli *smart contract* e sulle *blockchain*. Va però evidenziato che queste tecnologie sono deputate a essere applicate in tutta l'Unione Europea, oltre che nel mondo. Questo pone dei problemi dal punto di vista normativo sia per i profili evidenziati nella citata Risoluzione UE (giurisdizione, certezza della validità delle firme elettroniche utilizzate), sia per i possibili conflitti che potrebbero sorgere tra i diversi principi e istituti giuridici applicati nei Paesi membri. Più opportunamente forse si dovrebbe tener conto di tali aspetti, non cercando di regolare nel dettaglio requisiti e validità degli *smart contract*, ma ponendo quelle regole necessarie ad incentivarne l'utilizzo eliminando le incertezze degli operatori, senza creare conflitti interpretativi e normativi.

56 Sul tema, v gli scritti di Lessing, L.: *Code: And Other Laws of Cyberspace. Version 2.0,* New York, 2006, e Id.: *Code,* nonché Id.: "Code Is Law. On Liberty in Cyberspace", *Harvard Magazine*, 1.1.2000 (*https://www.harvardmagazine.com/2000/01/code-is-law-html*). In argomento, v. anche Hassan, S. e De Filippi, P.: "The Expansion of Algorithmic Governance: From Code is Law to Law is Code", *Field Actions Science Reports The journal of field actions*, *Special Issue* 17|2017, *Artificial Intelligence and Robotics in the City,* scaricabile alla *URL: https://journals.openedition.org/factsreports/4518*; De Filippi, P. e Wright, A.: *Blockchain and the Law. The Rule of Code*, Harvard, 2018.

IV. CONSIDERAZIONE SULLA *LEGAL TECH*.

Sulla base di quanto esposto a proposito della *AI*, della *blockchain* e degli *smart contract* sinteticamente si possono svolgere le seguenti considerazioni di portata generale che riguardano la c.d. *Legal Tech*.

Sicuramente non può essere stigmatizzato il ricorso a *blockchain* e *smart contract* in sede di negoziazione e di esecuzione del contratto. I vantaggi sono sotto gli occhi di tutti: grande agevolazione nel trovare ciò che serve in rete con incremento quindi di opportunità per clienti e offerenti, facilitazione nell'acquisto di beni e servizi a distanza, riduzione dei costi di produzione e transazione e conseguente abbassamento dei prezzi.

Del pari, sono però evidenti anche gli svantaggi legati al ricorso dei suddetti strumenti digitali: negazione di diritti di autotutela ai clienti, eccessiva rigidità nei processi di formazione ed esecuzione del contratto, in ultima analisi possibilità di lesione anche dei diritti fondamentali delle persone.

A tutto questo è possibile porre rimedio con adeguati e mirati interventi legislativi, là dove lo si ritenga necessario. Ma il presidio più importante resta in ogni caso questo: l'interpretazione del contratto e della legge deve essere considerata un'attività esclusivamente umana, che pertanto non può essere affidata ad un programma, algoritmo o intelligenza artificiale che sia. Come è stato autorevolmente affermato, l'interprete opera non soltanto come giurista, ma anche come psicologo, sociologo, esperto di linguistica, esperto del settore ecc. che valuta dei fatti collocati nella realtà unitaria per coglierne il valore e attuare la Costituzione nella individuazione della normativa da applicare al caso concreto[57]. Il giurista interviene dunque nel processo ermeneutico sia come tecnico caratterizzato da una propria cultura giuridica e non solo, sia come persona che ha una propria sensibilità ed un vissuto fatto di esperienze di vita e di relazioni umane. Tutto questo non può essere replicato da un programma e

57 Rizzo, V.: *Interpretazione dei contratti e relatività delle sue regole*, Esi, Camerino-Napoli, 1985, p. 11 ss.

semmai soltanto con grandi difficoltà da una intelligenza artificiale[58], almeno allo stato attuale dell'evoluzione tecnologica[59].

Ne consegue allora che anche l'elaborazione di sentenze e decisioni analoghe, come i lodi arbitrali, è un'attività umana non delegabile a programmi, algoritmi o all'intelligenza artificiale[60]. Da parte di alcuni si ventila invece l'opportunità di affidare funzioni giudicanti a tali sistemi[61]. Sul punto, nell'economia di questo scritto si ritiene sufficiente muovere, tra le altre, quattro critiche a questa tendenza[62].

La prima è quella di metodo. Come verrebbero prodotte queste decisioni? Nella letteratura tedesca si discorre in proposito di algoritmi di sussunzione e di ricostruzione dogmatica delle decisioni di futuri programmi in base agli elementi legali della fattispecie[63]. Ma se si ritorna alla sussunzione, si rischia di negare rilievo alle circostanze del caso concreto e alla valutazione del fatto e dei valori da esso espressi. In generale, allora questo sembra configurarsi come un ritorno al formalismo insito nella dialettica fatto-norma, negando quella fatto-valore e affermando così un metodo formalistico digitale simile a quello degli inizi del

58 Sull'intelligenza artificiale, v. il libro bianco realizzato dall'AGID, *L'intelligenza artificiale al servizio del cittadino*, versione 1.0, marzo 2020, in *https://ia.italia.it/assets/librobianco.pdf*, ove se ne prospettano le diverse possibili applicazioni: «L'Intelligenza Artificiale, oggi, può guidare al posto nostro, prendersi cura delle persone anziane o malate, svolgere lavori pericolosi o usuranti, aiutarci a prendere decisioni ponderate, basate sulla gestione razionale di grandi moli di dati. Ci può permettere di comunicare in lingue che non conosciamo, può seguirci nello studio e aumentare le esperienze culturali o di intrattenimento a nostra disposizione. Nella Pubblica amministrazione può essere utilizzata con profitto nel sistema sanitario, scolastico, giudiziario, nel pubblico impiego, nella sicurezza e, più in generale, nella gestione delle relazioni coi cittadini, che possono venire semplificate e rese allo stesso tempo più efficaci, veloci ed efficienti». Sui complessi rapporti tra intelligenza artificiale e diritto, tra gli altri, v. Ruffolo, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit.; *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, cit.; Santosuosso, A.: *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Giuffrè, Milano, 2020; Ashley, K.D.: *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambrigde University Press, 2014; Sartor, G.: *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996; in argomento, v. anche la sezione monografica del fasc. 7/2019 della rivista *Giur. it*., dedicato al tema «Intelligenza Artificiale e diritto», a cura di E. Gabrielli e U. Ruffolo.

59 V., AGID, *L'intelligenza artificiale al servizio del cittadino*, cit., p. 10: «l'Intelligenza Artificiale non è ancora in grado di riprodurre il funzionamento complesso della mente umana, ma solo alcune sue capacità circoscritte. Uno degli obiettivi è dunque quello di rendere queste tecnologie un po' più simili al nostro modo di relazionarci col mondo, pur essendo qualcosa ancora da costruire».

60 In tal senso, Gambino, A.: "I sette vizi capitali dei giudici-robot (tra blockchain e AI)", ù*www.agendadigitale.eu/cultura-digitale/i-sette-vizi-capitali-dei-giudici-robot-tra-blockchain-e-ai*, 11 dicembre 2018; Kaissis, A.: "Recourse to Courts in times of Alternative Dispute Resolution and Disruptive Technologies", in Apalagaki, C. e Pipsou, L.-M. (a cura di): *Dikaio Choris Synora - Liber Amicorum Athanassios Kaissis*, Atene-Salonicco, 2018., p. 301 ss. (la traduzione del titolo dal greco all'inglese è del Prof. Kaissis).

61 Cfr., ad esempio, Fries, M.: "PayPal Law and Legal Tech - Was macht die Digitalisierung mit dem Privatrecht?", *Neue Juristische Wochenschrift*, 2016, p. 2862 ss. e 2684 ss., il quale discorre di «Digitalisierung der Justiz»; Heckelmann, M.: *Zulässigkeit und Handhabung von Smart Contracts*, cit., p. 509 s., il quale parla di «Smart Judge» e si chiede «Warum soll Software nicht imstande sein, eines Tages auch die Rolle eines Richters zu übernehmen?».

62 Cfr., in argomento, Messinetti, R.: "La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata", *Contr. impr.*, 2019, p. 861 ss.

63 Cfr., Fries, M.: *PayPal Law and Legal Tech - Was macht die Digitalisierung mit dem Privatrecht?*, cit., p. 2862 ss. e 2684 ss., ove utilizza il termine «Subsumtionsautomat», e p. 2865.

ventesimo secolo che l'attuale teoria dell'interpretazione ha superato in molti paesi, dando così piena attuazione al dettato costituzionale[64].

La seconda è quella della controllabilità delle sentenze. La correttezza della decisione adottata da un algoritmo può essere soltanto limitata alla corrispondenza tra i precedenti e la decisione concreta? Se così è, per un verso, la motivazione non avrebbe più alcun ruolo e con essa il procedimento argomentativo assiologico che porta ad adottare la sentenza e a consentirne il controllo di conformità al sistema complessivo; per l'altro, si pone il problema dei fatti nuovi mai decisi prima e, soprattutto, dell'evoluzione dell'ordinamento e della interpretazione che genera nuovi orientamenti in superamento di quelli precedenti anche in ragione del mutato contesto socio economico di riferimento, che una macchina non è per definizione in grado di conoscere e considerare.

La terza critica è quella relativa alla tutela della persona. Un algoritmo che operi in base alla fattispecie e alle precedenti decisioni applicative di una norma rischia in molti casi di negare protezione alla personalità umana. In proposito, è paradigmatico un famoso caso deciso dal *BVerfG* in materia di fideiussione bancaria sottoscritta dal figlio a favore dei genitori: pur se la fideiussione era in sé e per sé inoppugnabile, i Giudici costituzionali tedeschi l'hanno dichiarata nulla in quanto negava i diritti fondamentali del figlio, costretto per tutta la sua esistenza per tentare di restituire un mutuo che lo avrebbe schiacciato e gli avrebbe negato il diritto a perseguire una vita felice[65]. Come avrebbe deciso un algoritmo?

Quarta critica è quella dell'accettazione sociale di un programma che giudica, quindi di uno *smart judge*. Come reagirebbe un cittadino di fronte alla decisione emessa da un programma che gli dà torto, magari nei confronti di una impresa? La questione non è certamente di stretto diritto, ma impatta pienamente sulla visione della giustizia nella collettività. Mettendola seriamente in discussione. La conseguenza è che ci potrebbe essere una reazione di rifiuto del "giudice macchina" che porterebbe anche a porne in dubbio la sua imparzialità, posto che si tratta di sistemi programmati da imprese che peraltro sono tanto difficilmente

64 Per tutti, v. Perlingieri, P.: *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, II, *Fonti e interpretazione*, 4 ed., Esi, Napoli, 2020, p. 278 ss.

65 *BVerfG*, 19 ottobre 1993, in *Neue jur. Wochenschr.*, 1994, p. 36 ss.: «Die Zivilgerichte müssen – insbesondere bei der Konkretisierung und Anwendung von Generalklausel wie § 138 und 242 BGB – die grundrechtliche Gewährleistung der Privatautonomie in Art. 2 I GG beachten. Daraus ergibt sich ihre Pflicht zur Inhaltskontrolle von Verträgen, die einen der beiden Vertragspartner ungewöhnlich stark belasten und das Ergebnis strukturell ungleicher Verhandlungsstärke sind»; tra gli altri, sulla decisione v., oltre al commento di Adomeit, K.: *Die gestörte Vertragsparität - ein Trugbild, ivi*, p. 2467 ss. e alla critica (di portata piú generale) di Medicus, D.: *Abschied von der Privatautonomie im Schuldrecht? Erscheinungsformen, Gefahren, Abhilfen*, Köln, 1994, p. 7 ss., la nota di Barenghi, A.: "Una pura formalità. A proposito di limiti e di garanzie dell'autonomia privata in diritto tedesco", *Nuova giur. civ. comm.*, 1995, I, p. 202 ss., e Id.: "Il dibattito tedesco sulla fideiussione bancaria: a proposito di un recente saggio", *Banca borsa tit. cred.*, 1995, p. 101 ss.; in argomento v. Di Nella, L.: "La tutela del garante nell'esperienza tedesca e negli ordinamenti europeo e italiano: la Mithaftung von Nahbereichpersonen", *Rassegna di diritto civile*, 2012, 4, p. 1191 ss.

controllabili anche da tecnici esperti, quanto facilmente manipolabili e indirizzabili verso certi esiti da chi abbia i mezzi e la possibilità di farlo.

In conclusione, si ritiene fondato il timore di chi paventa che le nuove tecnologie del ventunesimo secolo possano annullare la rivoluzione umanistica, qualora l'uomo si spogli della prerogativa di giudicare e lo affidi ad algoritmi[66]. Con questo non si vuol escludere l'evoluzione tecnologica dall'àmbito del diritto[67]: la *Legal Tech* deve supportare in modo sostenibile le attività degli operatori, non sostituirsi ad essi disumanizzando l'esperienza giuridica. La complessità e imprevedibilità dei sistemi aperti come quelli dei rapporti umani non è infatti paragonabile alla complessità di sistemi chiusi come quelli riferiti, ad esempio, a macchine, cose, fenomeni fisici, gioco degli scacchi o quant'altro.

V. L'IMPATTO DELLE NUOVE TECNOLOGIE SUI MERCATI: L'ECONOMIA DELLA PIATTAFORMA; I MERCATI FINANZIARI E LE NEGOZIAZIONI ALGORITMICHE.

La potenza computazionale dei nuovi strumenti modifica anche il paradigma di funzionamento di alcuni mercati.

L'economia della piattaforma è incentrata sulla integrazione delle risorse: tutti gli attori sono beneficiari di un servizio scambiato e sono coinvolti nel generare un valore che diviene dunque sistemico e co-generato.

L'esempio di *Airbnb* aiuta a comprendere la nuova realtà. Si tratta di un portale *online* che mette in contatto persone in cerca di un alloggio o di una camera per brevi periodi, con persone, generalmente privati, che dispongono di uno spazio extra di qualsiasi tipo da affittare. *Airbnb* mette a disposizione la risorsa della piattaforma. A sua volta, chi dispone di uno spazio, integra la propria risorsa (ad esempio, la casa) per attivare il servizio creando una inserzione di offerta. Il prodotto della piattaforma è il servizio o esperienza di locazione che viene creato mettendo insieme le risorse degli attori dell'ecosistema. Chi usa la stanza, integra la propria risorsa cognitiva (tempo di ricerca nella piattaforma, capacità di muoversi, *social rating*).

66 Questo l'ammonimento di Harari, Y.N.: *Homo Deus. Eine Geschichte von Morgen*, traduzione dall'inglese di A. Wirthensohn, 2017, München, p. 465.

67 In Italia, il Consiglio di Stato (Cons. Stato, 8 aprile 2019, n. 2270, sulla quale v. Prosperetti, E.: "Obbligo di motivazione e procedimenti in cui non è nota a priori la logica dell'algoritmo", *www.dirittomercatotecnologia.it.*), seguendo la dottrina maggioritaria, ha deciso che il ricorso a *software* di produzione automatica di provvedimenti amministrativi sia ammissibile solo riguardo all'attività vincolata della p.a. in cui vi è, per definizione, corrispondenza univoca tra dati da esaminare, regole da applicare e risultato del procedimento, senza spazi di elasticità, in perfetta consonanza con la logica deterministica che è propria dell'elaborazione elettronica: in argomento, con ampi riferimenti di letteratura, v. di Martino, A.: "Intelligenza artificiale e decisione amministrativa automatizzata", *Tecn. dir.*, 2020, 1, p. 83 ss.

In questo tipo di mercato, dunque, il valore si crea con l'uso, in rete e tramite lo scambio. Il consumatore assume un ulteriore ruolo di co-creatore. Qualcuno, forse non del tutto correttamente, asserisce che il consumatore non è più al centro del sistema: l'affermazione non è corretta, poiché il problema delle asimmetrie informative e della posizione di forza della controparte permangono comunque. A prescindere da questo aspetto, sicuramente si può dire che il valore è ecosistemico.

La nuova tecnologia incide radicalmente anche sul funzionamento di mercati tradizionali. Tra gli altri, questo è il caso dei mercati finanziari e delle negoziazioni algoritmiche ad altra frequenza, regolate dalla Direttiva 2014/65/UE (MifID II).

La tecnologia della negoziazione ha subito una profonda evoluzione nell'ultimo decennio. Attualmente numerosi partecipanti al mercato utilizzano la negoziazione algoritmica. Questa è definita in maniera ampia, al fine di ricomprendere qualsiasi modalità di negoziazione in cui un algoritmo calcolato tramite computer determina automaticamente parametri individuali di ordini (ossia momento di immissione dell'ordine, tempi di esecuzione, prezzo o quantità dell'ordine) senza alcun intervento umano, pur se limitato (art. 4, § 1, n. 39 dir.)[68]. Questa definizione ricomprende inevitabilmente un numero elevato di sistemi elettronici.

I rischi derivanti dal ricorso a siffatta tecnologia sono ora oggetto di regolamentazione. Innanzi tutto, la negoziazione algoritmica viene intesa in un modo specifico in relazione alla disciplina in esame e al suo scopo: la sua definizione è pertanto indipendente da definizioni quali quella di «attività di supporto agli scambi (*market making*)» di cui al Regolamento n. 236/2012[69]. Le imprese di investimento che effettuano negoziazioni algoritmiche perseguendo una strategia di *market making* sono tenute ad attivare controlli e sistemi adeguati per siffatta attività. Esse devono svolgere la stessa in modo continuo in una fascia specifica dell'orario di contrattazione della sede di negoziazione, garantendo che detta fascia sia rilevante rispetto all'orario di contrattazione totale, tenuto conto della liquidità, delle dimensioni nonché della natura del mercato specifico e delle caratteristiche degli strumenti finanziari negoziati[70].

68 V. in proposito il *considerando* 59 dir.: tale è quella svolta con un algoritmo informatizzato che determina automaticamente taluni aspetti di un ordine con intervento umano minimo o nullo; secondo lo stesso considerando, «l'utilizzo di algoritmi nel trattamento post-negoziazione delle operazioni eseguite non costituisce una negoziazione algoritmica».

69 Regolamento (UE) n. 236/2012 del Parlamento europeo e del Consiglio, del 14 marzo 2012, relativo alle vendite allo scoperto e a taluni aspetti dei contratti derivati aventi ad oggetto la copertura del rischio di inadempimento dell'emittente (*credit default swap*), in GUUE L 86 del 24.3.2012, pag. 1; in argomento v. il *considerando* n. 60: «Le imprese di investimento che effettuano negoziazioni algoritmiche perseguendo una strategia di "market making" dovrebbero porre in essere controlli e sistemi adeguati per tale attività. Tale attività dovrebbe essere intesa in un modo specifico in relazione al suo contesto e al suo scopo. La definizione di tale attività è pertanto indipendente da definizioni quali quella di "attività di supporto agli scambi (market making)" di cui al regolamento (UE) n. 236/2012 del Parlamento europeo e del Consiglio».

70 Così il *considerando* n. 59 dir.

Un tipo specifico è costituito dalla «negoziazione algoritmica ad alta frequenza» (art. 17, § 2, comma 5, dir.), per la quale «un sistema di negoziazione analizza dati o segnali del mercato a velocità elevata per poi inviare o aggiornare un gran numero di ordini entro un tempo brevissimo in risposta all'analisi»[71]. Tale tecnica è caratterizzata da: «a) infrastrutture volte a ridurre al minimo le latenze di rete e di altro genere, compresa almeno una delle strutture per l'inserimento algoritmico dell'ordine: co-ubicazione, *hosting* di prossimità o accesso elettronico diretto a velocità elevata; b) determinazione da parte del sistema dell'inizializzazione, generazione, trasmissione o esecuzione dell'ordine senza intervento umano per il singolo ordine o negoziazione, e c) elevato traffico infragiornaliero di messaggi consistenti in ordini, quotazioni o cancellazioni» (art. 4, § 1, n. 40 dir.). Siffatta negoziazione contiene dunque requisiti quali l'inizializzazione, la generazione, la trasmissione e l'esecuzione dell'ordine che sono determinati dal sistema senza intervento umano per ciascun singolo ordine o negoziazione, un tempo breve per la creazione e la liquidazione delle posizioni, un elevato indice giornaliero di rotazione del portafoglio, un elevato rapporto infragiornaliero ordini/operazioni e la chiusura del giorno di negoziazione in una posizione *flat*, o prossima a essa. Nel «determinare che cosa costituisce un traffico infragiornaliero elevato di messaggi, si dovrebbe tenere conto dell'identità del cliente al quale è riconducibile l'attività in ultima analisi, della lunghezza del periodo di osservazione, della comparazione con l'attività complessiva del mercato durante tale periodo e della concentrazione o frammentazione relativa di attività»[72].

La negoziazione algoritmica ad alta frequenza è generalmente utilizzata dagli operatori che impegnano capitale proprio per la negoziazione e, anziché essere una strategia in sé, consiste piuttosto nell'uso di tecnologie sofisticate per attuare strategie di negoziazione più tradizionali, come le attività di supporto agli scambi (*market making*) o l'arbitraggio.

Il ricorso della tecnica ad alta frequenza è facilitato dalla co-ubicazione degli impianti dei partecipanti al mercato in stretta vicinanza fisica al motore di confronto di una sede di negoziazione. Al fine di garantire condizioni di ordinato e corretto svolgimento delle negoziazioni, è indispensabile richiedere alle sedi di negoziazione di fornire tali servizi di co-ubicazione su base non discriminatoria, equa e trasparente (art. 48, § 8, dir.)[73].

Siffatta nuova tecnica reca con sé ovviamente vantaggi e svantaggi. Quanto ai vantaggi, essa ha aumentato la velocità, la capacità e la complessità delle modalità di negoziazione degli investitori; ha consentito agli operatori dei mercati di facilitare

71 V. il *considerando* n. 61 dir.

72 Così il *considerando* n. 61 dir.

73 V. il *considerando* n. 62 dir.

l'accesso elettronico diretto agli stessi per i loro clienti mediante l'utilizzo dei loro sistemi di negoziazione oppure tramite l'accesso diretto ai mercati o l'accesso sponsorizzato[74]. In generale, dunque questa tipologia di negoziazione ha apportato vantaggi sia al mercato, sia ai partecipanti, quali l'opportunità di una più ampia partecipazione agli scambi, un aumento di liquidità, dei differenziali più ridotti, una minore volatilità a breve termine e i mezzi per ottenere una migliore esecuzione degli ordini per i clienti.

Quanto agli svantaggi, tale tecnica è anche fonte di una serie di problemi, quali un aumento del rischio di sovraccarico dei sistemi nelle sedi di negoziazione a causa del gran numero di ordini, i rischi che vengano generati ordini erronei o doppi o che comunque i sistemi non funzionino correttamente e generino così disordine nel mercato. Esiste inoltre il rischio che i sistemi di negoziazione algoritmica reagiscano in modo eccessivo ad alcuni eventi, esacerbando così la volatilità, qualora preesista un problema di mercato. Infine, come ogni altra tradizionale forma, anche la negoziazione algoritmica e quella ad alta frequenza, se non utilizzate correttamente, possono prestarsi a talune forme abusive di comportamento, vietate dalla normativa sugli abusi di mercato[75]. Considerati i vantaggi in termini di informazione forniti a chi la pratica, la negoziazione ad alta frequenza può anche indurre gli investitori a scegliere di effettuare gli scambi nelle sedi dove possono evitare contatti con gli operatori che effettuano siffatte negoziazioni.

Molto importante è l'introduzione di norme per l'utilizzo di algoritmi per lo svolgimento delle negoziazioni (art. 17 dir.). In particolare, è opportuno sottoporre le tecniche ad alta frequenza che rispondono a determinate caratteristiche a uno speciale controllo regolamentare. Sebbene si tratti prevalentemente di tecniche basate sulla negoziazione per conto proprio, il controllo regolamentare deve riguardare anche i casi in cui l'esecuzione della tecnica è strutturata in modo tale da evitare che si svolga per conto proprio. Per mitigare tali rischi potenziali derivanti da un maggior ricorso alla tecnologia, la nuova disciplina ha approntato una combinazione di misure e controlli specifici del rischio diretti alle imprese

74 Secondo l'art. 4, § 1, n. 41: l'«accesso elettronico diretto» è «un accordo in base al quale un membro di una sede di negoziazione o un suo partecipante o cliente consente a una persona di utilizzare il proprio codice di negoziazione in modo da trasmettere per via elettronica ordini relativi a uno strumento finanziario direttamente alla sede di negoziazione e comprende gli accordi che implicano l'utilizzo da parte della persona dell'infrastruttura del membro, del partecipante o del cliente, o di qualsiasi sistema di collegamento fornito dal membro, partecipante o cliente per trasmettere gli ordini (accesso diretto al mercato) e gli accordi che non prevedono l'uso di una siffatta infrastruttura da parte di tale persona (accesso sponsorizzato)».

75 L'art. 12, comma 2, lett. *c*, reg. n. 396/2014 ha esteso la definizione di manipolazione del mercato anche agli ordini di negoziazione effettuati attraverso mezzi elettronici, come le strategie di negoziazione algoritmiche e ad alta frequenza. In proposito, v. il considerando n. 68 dir.: «Al fine di garantire il mantenimento dell'integrità del mercato in seguito agli sviluppi tecnologici nei mercati finanziari, l'ESMA dovrebbe periodicamente avvalersi dei contributi degli esperti nazionali sugli sviluppi relativi alla tecnologia di negoziazione, compresa la negoziazione ad alta frequenza e le nuove pratiche suscettibili di costituire abusi di mercato, per identificare e promuovere strategie efficaci di prevenzione e trattamento di tali abusi».

che effettuano negoziazioni algoritmiche o adottano tecniche di negoziazione algoritmica ad alta frequenza e che forniscono un accesso elettronico diretto, e di altre misure dirette ai gestori delle sedi di negoziazione a cui tali imprese hanno accesso[76]. Gli interventi si diramano così in due direzioni.

Per un verso, al fine di potenziare la "resistenza"[77] dei mercati agli sviluppi tecnologici, le misure e i controlli devono rispecchiare gli orientamenti tecnici adottati dall'Autorità europea degli strumenti finanziari e dei mercati ESMA[78], emanati nel febbraio 2012 ed intitolati «Sistemi e controlli in un ambiente di negoziazione automatizzato per piattaforme di negoziazione, imprese di investimento e autorità competenti»[79]. È importante poi che tutte le imprese che effettuano negoziazioni algoritmiche ad alta frequenza siano autorizzate (artt. 44, 48 dir.). Tale autorizzazione deve garantire che siano soggette ai requisiti di organizzazione previsti dalla MiFID II e ad un'adeguata vigilanza. Tuttavia, gli enti che sono autorizzati e controllati a norma del diritto europeo sul settore finanziario ed esenti dall'applicazione della disciplina in materia, ma che effettuano negoziazioni algoritmiche, devono essere soggetti alle misure e ai controlli volti a contrastare il rischio specifico derivante da tali tipi di negoziazione. In tal senso, l'ESMA è chiamata a svolgere un importante ruolo di coordinamento, definendo le idonee dimensioni dello scostamento di prezzo, così da assicurare l'ordinato funzionamento dei mercati dell'Unione[80]. Proprio al fine di assicurare una vigilanza efficace e di consentire alle autorità competenti di adottare misure adeguate e tempestive contro le strategie algoritmiche difettose o scorrette, è necessario segnalare tutti gli ordini generati mediante negoziazione algoritmica. Attraverso la segnalazione, le autorità competenti sono in grado di identificare e distinguere gli ordini provenienti da algoritmi differenti e di ricostruire e valutare efficacemente le strategie utilizzate dagli operatori che adottano siffatte negoziazioni. Ciò dovrebbe attenuare il rischio che gli ordini non siano assegnati inequivocabilmente a una strategia algoritmica o a un operatore. La segnalazione consente alle autorità competenti di reagire in modo efficiente ed efficace contro le strategie di negoziazione algoritmica che costituiscono un comportamento vietato o creano rischi per il corretto funzionamento del mercato[81].

76 Cfr. il *considerando* n. 63 dir.

77 L'art. 48 dir. discorre di «Resilienza dei sistemi» e di «interruttori di circuito», mentre nella versione tedesca della MiFID II sono utilizzate le espressioni «Belastbarkeit der Systeme» e «Notfallsicherungen („circuit breakers")», ossia di capacità di resistenza dei sistemi e di interruttori di sicurezza.

78 V., Mezzacapo, S.: *La regolamentazione dell'*algorithmic trading *nell'UE*, in Troiano, V. e Motrone, R. (a cura di), *La MiFID II. Rapporti con la clientela - regole di* governance *- mercati*, cit., p. 341 ss.

79 «Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities» - ESMA/2012/122, febbraio 2012.

80 V. il considerando n. 63 dir.

81 Così, il *considerando* n. 67 dir.

Per l'altro, sia le imprese di investimento, sia le sedi di negoziazione devono provvedere affinché siano messe in atto solide misure per assicurare che le tecniche di negoziazione algoritmica o di negoziazione algoritmica ad alta frequenza non creino un mercato disordinato e non possano essere utilizzate per porre in essere comportamenti abusivi o vietati dalle sedi di negoziazione ad esse collegate. Le sedi di negoziazione devono inoltre garantire che i loro sistemi di negoziazione siano resistenti e adeguatamente testati per far fronte ad un aumento del flusso degli ordini o a condizioni critiche dei mercati e che presso le sedi di negoziazione siano in funzione degli interruttori per arrestare temporaneamente o vincolare le negoziazioni se si verificano all'improvviso movimenti di prezzo inattesi (art. 17, § 1, dir.)[82].

Oltre alle predette misure, la nuova disciplina vieta alle imprese di investimento di fornire ai clienti un accesso elettronico diretto ai mercati, se tale accesso non è soggetto a sistemi e controlli adeguati. Indipendentemente dalla forma di accesso elettronico diretto fornito, le imprese devono valutare e riesaminare l'idoneità dei clienti che utilizzano tale servizio e provvedere affinché siano imposti controlli del rischio connesso all'utilizzo del servizio: senza tali controlli, è vietato l'accesso elettronico diretto. Esse sono anche responsabili per le negoziazioni effettuate dai loro clienti mediante l'uso dei loro sistemi o l'utilizzo dei loro codici di negoziazione (art. 17, § 5, commi 1 e 2, dir.). Requisiti di organizzazione dettagliati concernenti tali nuove forme di negoziazione devono essere prescritti in modo più circostanziato nelle norme tecniche di regolamentazione. In tal modo si assicura che i requisiti possano essere modificati in funzione della necessità di tener conto tempestivamente di ulteriori innovazioni e sviluppi in tale settore[83].

VI. LA CIRCOLAZIONE DEI DATI PERSONALI E LE TUTELE.

Le nuove tecnologie hanno contribuito anche alla creazione del mercato dei dati personali, divenuto oramai una realtà economica molto significativa che porta a discorrere di una nuova economia *data driven*[84]. In estrema sintesi, in questo mercato molti servizi (ad esempio, *social network*) vengono offerti in rete ai consumatori ai quali viene chiesto di prestare il consenso al trattamento dei propri dati personali per finalità ulteriori da quelle legate alla mera prestazione del servizio, senza che ciò costituisca una condizione necessaria per l'erogazione.

82 V. il *considerando* 64 dir.

83 Cfr. il *considerando* n. 66 dir.

84 In argomento, v. Ricciuto, V.: "La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno", *Dir. inf.*, 2018, p. 689 ss.; Resta, G.: "I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale* (a cura di V. Ricciuto e C. Solinas), Milano, 2022, p. 53, ove si evidenzia che i dati personali, come i dati *tout court*, possiedono oggi un rilevante valore economico: l'«intero sistema dell'industria 4.0, che è tipicamente *data driven*, non può essere compreso prescindendo da tale assunto».

Il senso e il valore economico di questa operazione si colgono nel fatto che l'operatore che chiede, e magari ottiene, i dati personali, li utilizza esso stesso per rielaborarli oppure li cede a terzi, questa volta dietro il pagamento di un "classico" corrispettivo, affinché li si possa utilizzare per varie finalità quali ad esempio indagini di mercato, analisi dell'andamento degli orientamenti culturali, politici e sociali ecc.[85]. Il tema della circolazione dei dati personali nel mercato "digitale" si pone dunque con forza all'attenzione del giurista.

Un importante caso in materia è stato deciso con il provvedimento n. 27432 del 2018 dell'Autorità *antitrust* che ha riconosciuto l'esistenza di una pratica commerciale scorretta e ha sanzionato *Facebook Ireland Ltd.* e la sua controllante *Facebook Inc.*[86]. L'Autorità ha accertato che *Facebook*, in violazione degli artt. 21 e 22 c. cons., ha indotto ingannevolmente gli utenti consumatori a registrarsi nella sua piattaforma, non informandoli adeguatamente e immediatamente, in fase di attivazione dell'*account*, dell'attività di raccolta con fini commerciali dei dati da loro forniti, e più in generale delle finalità remunerative che sottendono la fornitura del servizio di *social network*, enfatizzandone solo la gratuità. In tal modo, i consumatori hanno assunto una decisione di natura commerciale che non avrebbero altrimenti preso (registrazione al *social network* e permanenza nel medesimo). Le informazioni fornite risultano generiche e incomplete senza adeguatamente distinguere tra l'utilizzo dei dati necessario per la personalizzazione del servizio (con l'obiettivo di facilitare la socializzazione con altri consumatori) e l'utilizzo dei dati per realizzare campagne pubblicitarie mirate. L'Autorità ha altresì accertato che *Facebook*, in violazione degli artt. 24 e 25 c. cons., attua una pratica aggressiva in quanto esercita un indebito condizionamento nei confronti dei consumatori registrati, i quali subiscono senza espresso e preventivo consenso la trasmissione per finalità commerciali dei propri dati da *Facebook* a siti *web/app* di terzi e viceversa. L'indebito condizionamento deriva dall'applicazione di un meccanismo di preselezione del più ampio consenso alla condivisione di dati. La decisione dell'utente di limitare il proprio consenso comporta, infatti, la prospettazione di rilevanti limitazioni alla fruibilità del *social network* e dei siti *web/app* di terzi. Questo condiziona gli utenti a mantenere la scelta preimpostata da *Facebook*. Successivamente sono intervenuti il TAR Lazio (n. 260/2020)[87] e il Consiglio di Stato (n. 2631/2021)[88] che hanno confermato la decisione dell'AGCM.

85 Per la descrizione del funzionamento di questi mercati, detti *two-sided* e *multisided* secomdo la loro conformazione, delle operazioni economiche sottostanti e dell'inquadramento di queste attività nell'impresa, v. C. Solinas, *La circolazione dei dati personali nell'ottica dello scambio tra diritti*, in *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, cit., p. 109 ss.

86 AGCM, PS1112 - FACEBOOK-CONDIVISIONE DATI CON TERZI, provv. n. 27432, in *Bollettino*, 2018, n. 46, p. 22 ss. (in *https://www.agcm.it/dotcmsdoc/bollettini/2018/46-18.pdf*).

87 TAR Lazio, 10 gennaio 2020, n. 260, in *Giur. it.*, 2021, II, p. 320 ss., con nota di C. Solinas, *Trattamento dei dati personali e pratiche commerciali scorrette*.

88 Cons. Stato, 29 marzo 2021, n. 2631, in *Foro it.*, 2021, VI, p. 325 ss., con nota di Davola, A. e Pardolesi, R.: "Protezione dei dati personali, tutela della concorrenza e del consumatore (alla prese con i 'dark pattern'):

Sulla scorta di questo precedente, l'AGCM con i provvedimenti n. 29888 e n. 29890 del 2021 ha sanzionato anche *Apple Distribution International Ltd.* e *Google Ireland Ltd.*[89]. L'Autorità ha riscontrato da parte di ciascuna delle società due violazioni del Codice del Consumo, consistenti in carenze informative e in pratiche aggressive collegate all'acquisizione e all'utilizzo dei dati dei consumatori a fini commerciali[90]. Quanto alla prima violazione degli artt. 21 e 22 c. cons., *Google* sia nella fase di creazione dell'account, indispensabile per l'utilizzo di tutti i servizi offerti, sia durante l'utilizzo dei servizi stessi, omette informazioni rilevanti di cui il consumatore ha bisogno per decidere consapevolmente se accettare che la società raccolga e usi a fini commerciali le proprie informazioni personali; *Apple* sia nella fase di creazione dell'*ID Apple*, sia in occasione dell'accesso agli *Store* (*App Store*, *iTunes Store* e *Apple Books*), non fornisce all'utente in maniera immediata ed esplicita alcuna indicazione sulla raccolta e sull'utilizzo dei suoi dati a fini commerciali, enfatizzando solo che la raccolta dei dati è necessaria per migliorare l'esperienza del consumatore e la fruizione dei servizi. Riguardo alla seconda violazione, è stato dimostrato che le due società hanno attuato una pratica aggressiva ai sensi degli artt. 24 e 25 c. cons. Nella fase di creazione dell'*account*, *Google* preimposta l'accettazione dell'utente al trasferimento e/o all'utilizzo dei propri dati per fini commerciali; questa preattivazione consente il trasferimento e l'uso dei dati da parte di *Google*, una volta che questi vengano generati, senza la necessità di altri passaggi in cui l'utente possa di volta in volta confermare o modificare la scelta preimpostata dall'azienda. Nel caso di *Apple*, invece, l'attività promozionale è basata su una modalità di acquisizione del consenso all'uso dei dati degli utenti a fini commerciali senza prevedere per il consumatore la possibilità di scelta preventiva ed espressa sulla condivisione degli stessi; siffatta architettura di acquisizione predisposta da *Apple* non rende possibile l'esercizio della propria volontà sull'utilizzo a fini commerciali dei propri dati, venendo il consumatore condizionato nella scelta di consumo e subendo pertanto la cessione delle informazioni personali, di cui *Apple* può disporre per le proprie finalità promozionali effettuate in modalità diverse.

parallele convergenti?"; *Giorn. dir. amm.*, 2021, VI, p. 609 ss., con nota di Midiri, F.: "Proteggere i dati personali con le tutele del consumatore"; *Nuova giur. civ. comm.*, 2021, V, p. 1079 ss., con nota di D'Alberti, D.: "Tutele "multilivello" e l'effettività dei rimedi per gli utenti online".

89 AGCM PS11150 – ICLOUD, provv. n. 29888, e AGCM PS11147 - GOOGLE DRIVE-SWEEP 2017, provv. n. 29890, pubblicati in *Bollettino*, 2021, n. 47, p. 153 ss. e p. 196 ss. (in *https://www.agcm.it/dotcmsdoc/bollettini/2021/47-21.pdf*).

90 Dal punto di vista del modello di *business* queste sono le differenze individuate dall'AGCM tra le due società. *Apple* raccoglie, profila e utilizza a fini commerciali i dati degli utenti attraverso l'utilizzo dei suoi dispositivi e dei suoi servizi. Quindi, pur senza procedere ad alcuna cessione di dati a terzi, *Apple* ne sfrutta direttamente il valore economico attraverso un'attività promozionale per aumentare la vendita dei propri prodotti e/o di quelli di terzi attraverso le proprie piattaforme commerciali *App Store*, *iTunes Store* e *Apple Books*. *Google* invece fonda la propria attività economica sull'offerta di un'ampia gamma di prodotti e di servizi connessi a *internet*, che comprendono tecnologie per la pubblicità *online*, strumenti di ricerca, *cloud computing*, *software* e *hardware*, basata anche sulla profilazione degli utenti ed effettuata grazie ai loro dati.

Vi è dunque il decisivo riconoscimento della rilevanza giuridica del mercato dei dati[91], sussistendo un rapporto di consumo tra gli utenti e gli operatori, pur in assenza di esborso monetario, la cui "controprestazione" sembra essere rappresentata dai dati che i consumatori cedono utilizzando i servizi offerti dai professionisti. Tale questione ha ovviamente suscitato un acceso dibattito tra chi è favorevole alla configurazione dello scambio dei dati contro l'erogazione di un servizio digitale e chi si oppone vivamente in nome della non mercificazione della persona per il tramite dei suoi dati. In proposito, per quanto qui interessa, occorre in primo luogo analizzare sinteticamente tre aspetti dal punto di vista normativo: il dato, il trattamento e la libera circolazione dei dati personali.

Il «dato personale» è definito dall'art. 4, n. 1, GDPR come «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, economica, culturale o sociale». Alcuni *considerando* aiutano a delineare il concetto di dato anche attraverso il suo riferimento soggettivo alle persone fisiche, indipendentemente dalla loro nazionalità e dalla residenza[92]; non sono invece destinatarie della tutela predisposta dal GDPR le persone giuridiche e le persone decedute, salvo diversa scelta del legislatore interno[93]. Ciò posto dal punto di

91 Sulle vicende esaminate e sulle pronunce intervenute, oltre agli scritti menzionati nelle precedenti note, v. Matera, D.M.: "Patrimonializzazione dei dati e pratiche commerciali scorrette", *Tecnologie e Diritto*, 2022, 1, p. 155 ss.; Ricciuto, V. e Solinas, C.: "Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto", *Giust. civ.*, 2021, p. 3 ss.; Giannone Codiglione, G.: "I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy", *Dir. inf.*, 2017, p. 418 ss.; Scorza, G.: "Facebook non è gratis? Nota a Consiglio di Stato, sentenza 29 marzo 2021, n. 2631", *Dir. internet*, 2021, III, p. 561 ss.

92 V. il *considerando* n. 2: «I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale ("dati personali") dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza», e il *considerando* n. 14 «È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali».

93 Per le persone giuridiche, v. il *considerando* n. 14 («Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto»), per le persone decedute il *considerando* n. 27 («Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute»). [«(26) È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici»]. Qualora il dato risulti anonimo, raccolto anche per scopi di ricerca scientifica o statistici, non è sottoposto alla disciplina del GDPR [«(26) I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica

vista soggettivo, la portata del concetto di dato sembra essere descritta in modo molto ampio, per garantire una tutela effettiva alla persona fisica identificata o anche soltanto identificabile. Qualora il dato risulti anonimo, raccolto ad esempio anche per scopi di ricerca scientifica o statistici, non è sottoposto alla disciplina del GDPR: tale è l'informazione non riferibile a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato[94].

Per «trattamento» il n. 2 del medesimo articolo intende «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»[95]. Il considerando n. 4 chiarisce il fine normativo del trattamento, osservando che «dovrebbe essere al servizio dell'uomo», e il suo rapporto con diritto alla protezione dei dati di carattere personale che «non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»[96].

Una particolare attenzione è dedicata alla pseudonomizzazione, ossia a quel trattamento «tale che i dati personali non possano più essere attribuiti a

identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca»]. Infine, il *considerando* n. 30 precisa che «Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (*cookies*) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

94 V. ancora il *considerando* n. 26: «I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca»].

95 Il *considerando* n. 10 chiarisce che, per «quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE, gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito».

96 Il considerando n. 4 assicura che il GDPR rispetta «tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile» (art. 4, n. 5, GDPR). Detto trattamento è considerato quale strumento di tutela della persona e pertanto incentivato[97] in quanto contribuisce a ridurre i rischi per gli interessati e, nel contempo, ad aiutare i titolari e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati, non essendo intesa a precludere altre misure di tutela[98]. I dati personali sottoposti alla pseudonomizzazione, che possono essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, sono considerati informazioni su una persona identificabile[99].

Il *considerando* n. 30 chiarisce che le «persone fisiche possono essere associate a identificativi *online* prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (*cookies*) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

Quanto alla libera circolazione, il *considerando* n. 12 sottolinea che l'«articolo 16, paragrafo 2, TFUE conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati». Il *considerando* n. 13 precisa che per «il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla

97 V. il considerando n. 29: «Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale nell'ambito dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento in questione, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate nell'ambito dello stesso titolare del trattamento».

98 Così il considerando n. 28: «L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della "pseudonimizzazione" nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati».

99 V. il *considerando* n. 26: «È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici».

protezione delle persone fisiche con riguardo al trattamento dei dati personali», e che «Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un controllo coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri»[100].

Ciò posto dal punto di vista normativo, occorre partire da una riflessione di fondo sulla disciplina di tutela della riservatezza. La normativa è correttamente rivolta a tutelare il singolo contro il trattamento algoritmico dei suoi dati. Questo lo si fa giustamente per proteggere l'individuo contro l'uso illecito dei propri dati e il bilanciamento di interessi è tarato nell'ottica della relazione titolare di dati-titolare del trattamento. Vi sono però delle situazioni in cui la raccolta e l'elaborazione dei dati è utile per la collettività e persegue degli scopi meritevoli di tutela: anche in tali casi si manifesta con forza l'applicazione della tutela di portata individuale e si afferma l'illegittimità della raccolta dei dati.

In letteratura vi è però anche un altro approccio. Dopo aver inquadrato il nuovo fenomeno e le questioni della sua regolazione, che va anche oltre il GDPR approdando al diritto *antitrust* e a quello contrattuale, consumeristico e dei servizi digitali, viene disegnato il passaggio dei dati dalla dimensione schiettamente personale a quella patrimoniale, con le conseguenze che reca la loro circolazione anche dalla prospettiva della tutela dei diritti fondamentali, sottolineando la piena dimensione normativa del trasferimento delle posizioni giuridiche dei dati anche in assenza di un corrispettivo[101]. Siffatta lettura del fenomeno del trattamento dei dati anche in termini contrattuali discende dall'affermazione normativa della centralità del principio di libera circolazione dei dati personali sancito dall'art. I GDPR e dalla costatazione che questi costituiscono la nuova forma di ricchezza che alimenta l'economia digitale e non solo[102].

100 V. anche il *considerando* n.10: «Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri».

101 Ricciuto, V.: "Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale, in Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale", cit., p. 7 ss.

102 V. ancora Ricciuto, V.: "Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale", cit., p. 25 ss.

Vanno allora individuate nel dettaglio anche alcune problematiche centrali che si pongono in questo acceso dibattito.

In primo luogo, vi è la questione del dato personale, oggetto del contratto e manifestazione della personalità del titolare, e della sua patrimonializzazione e sfruttamento commerciale da parte del cessionario in sede di circolazione dello stesso[103]. L'opinione di parte della dottrina e della giurisprudenza, elaborata dal punto di vista ontologico-ricostruttivo, secondo la quale il dato personale è un bene e*xtra commercium* in ragione della sua natura di diritto fondamentale di cui non si può disporre, sembra oggi essere non del tutto corretta. Nel momento stesso in cui per legge è possibile autorizzare il trattamento dei dati, allora di questi si può logicamente disporre. L'art. 9 GDPR stabilisce con nettezza che una delle modalità (individuate nel § 2) per poter trattare i dati particolari elencati nel § 1, ossia i dati sensibili, è proprio quella dell'autorizzazione al trattamento e il *considerando* n. 4 del GDPR discorre del dato personale in una dimensione di utilizzabilità in ragione della sua funzione sociale: pertanto, il GDPR afferma che il dato personale e la sua tutela dovrebbero essere al servizio dell'individuo[104]. La normativa europea e interna prende quindi atto dell'attuale evoluzione digitale delle società contemporanee e positivizza il fatto che il dato personale sarà la vera ricchezza della persona fisica e costituirà un bene giuridicamente percepibile con una vocazione innegabilmente economica, con la conseguenza che la sua patrimonializzazione non dovrebbe essere demonizzata[105]. A questo punto, per evitare eventuali pregiudizi al soggetto cui pertengono i dati, diviene necessario che venga assicurata una puntuale regolazione del fenomeno che tipizzi la loro patrimonializzazione e le forme contrattuali per il loro utilizzo: diversamente, l'atipicità dello utilizzo contrattuale rischia di esporre l'interessato a possibili sfruttamenti indebiti del dato stesso. Tra l'altro, la tutela dovrebbe garantire la dettagliata informazione del consumatore sul destino dei suoi dati e su chi li sfrutterà realmente in ambito finale[106].

103 Toschei, S.: "Dalla dimensione personale del dato alla sua tutela patrimoniale", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, cit., p. 29 ss., spec. 40 s.

104 Toschei, S.: *Dalla dimensione personale del dato alla sua tutela patrimoniale*, cit., p. 35 s.

105 Tra i vari studi che approfondiscono il tema dello scambio e del valore dei dati personali, oltre quelli in seguito citati, v., tra gli altri, Langhanke, C. e Schmidt-Kessel, M.: "Consumer data as consideration", *Journal of European Consumer and Market Law*, 2015, p. 218 ss.; De Franceschi, A.: *La circolazione dei dati personali tra privacy e contratto*, Esi, Napoli, 2017, p. 67 ss.; Thobani, S.: *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Giuffrè, Milano, 2018; Zorzi Galgano, N. (a cura di): *Persona e mercato dei dati. Riflessioni sul GDPR*, Giuffrè, Milano, 2019; Irti, C.: *Consenso «negoziato» e circolazione dei dati personali*, Torino, 2021; Perlingieri, C.: *Profili civilistici dei social networks*, Esi, Napoli, 2014. Anche la Commissione Europea, *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*, COM(2016) 320 *final*, Bruxelles, 25.5.2016, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016SC0163&from=IT*, ha costatato che «i dati personali, le preferenze dei consumatori, e altri contenuti generati dagli utenti hanno un valore economico *de facto* e vengono venduti a terzi» (punto 3.4.1) e che «il valore economico delle informazioni relative alle preferenze dei consumatori, dei dati personali e di altri contenuti generati dagli utenti è sempre più riconosciuto» (punto 1.4.10).

106 Toschei, S.: *Dalla dimensione personale del dato alla sua tutela patrimoniale*, cit., p. 40 s. e 42.

Dalla prospettiva della circolazione, si precisa che non circola il dato ma la posizione giuridica cui lo stesso si riferisce e si evidenzia che il modello di *business* è insito nell'aggregazione dei dati della «folla» di utenti dei servizi digitali[107]. Si osserva che se, da un lato, il *gap* informativo di chi ne autorizza l'utilizzo e il meccanismo dell'*opt-out* sono oggi gli strumenti abilitanti del trasferimento, dall'altro, il GDPR esige invece l'*opt-in* e che vi sia la piena consapevolezza del cedente, il suo consenso informato all'utilizzo da parte di terzi. L'inquadramento giuridico della fase di accesso alle piattaforme *web* in un rapporto negoziale a titolo gratuito - con l'operatore che si impegna a offrire «gratis» l'accesso al servizio e l'utente che consegna elementi utili al *business* delle società di *marketing* - mostra la reale dimensione economica del fenomeno, rilevandone la prospettiva «massiva» di relazioni singole che assumono «compiuta rilevanza giuridica» solo nella fase successiva della cessione a terzi dei dati raccolti: la trasmissione dei dati del singolo alla piattaforma *web* è quindi un atto negoziale «fuori mercato», sottoposto al vaglio dell'*Antitrust* per tutelare la libertà di scelta del consumatore, la quale non ha un contenuto soltanto economico[108]. Secondo questa impostazione, dunque, l'accesso alle piattaforme *web* non può avvenire soltanto con un accordo non idoneo ad avere come oggetto un bene che per natura e scelta di sistema non è suscettibile di essere trattato come patrimonio economico. È invece necessario il consenso del titolare ad aprire le porte della propria sfera personale, dovendosi quindi considerare soltanto la prospettiva prenegoziale soggettivo-informativa dell'utente-persona-consumatore. Il consenso esplica quindi la propria efficacia tanto nell'àmbito *antitrust* delle pratiche scorrette, quanto in quello del trattamento dei dati personali e nel contesto del rapporto strettamente negoziale, soddisfacendo le prescrizioni di tutte queste discipline[109].

In parziale adesione alla ricostruzione sopra illustrata, per un verso, si ritiene che la «de-patrimonializzazione» dei dati non è una strategia che il diritto può realisticamente perseguire, essendo impossibile invertire processi sociali, economici e tecnologici oramai fortemente radicati a livello globale: a questa affermazione non osta il *considerando* n. 24 della Direttiva n. 2019/770, ove si «riconosce appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce», in quanto ciò non implica necessariamente l'impossibilità di ricorrere «a schemi di remunerazione del consenso, com'è tipico, appunto, dei modelli servizi contro dati», che è regolato dalla predetta Direttiva proprio al fine di concedere a questo tipo di negoziazione

107 Gambino, A.M.: "La circolazione dei dati personali, la configurabilità di un mercato e i diritti fondamentali", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, cit., p. 45 ss.

108 Gambino, A.M.: *La circolazione dei dati personali, la configurabilità di un mercato e i diritti fondamentali*, cit., p. 48.

109 Gambino, A.M.: *La circolazione dei dati personali, la configurabilità di un mercato e i diritti fondamentali*, cit., p. 49.

un livello di tutela parificabile a quello con cui i servizi vengono acquistati dietro il pagamento del classico corrispettivo in denaro[110]. Per l'altro, si osserva che il *considerando* n. 38 di detta Direttiva precisa che il trattamento dei dati personali relativo ai contratti ivi disciplinati deve comunque rispettare il GDPR e che il consenso fornito a tal fine deve essere conforme agli artt. 4, n. 11, 6, § 1, lett. *a*, e 7, comma 4, reg. n. 2017/679, ossia deve consistere in una manifestazione di volontà informata, specifica e «libera», nel senso di non influenzata da pressione psicologica derivata da situazioni di vulnerabilità o da strutturali asimmetrie di potere (cfr. *considerando* n. 43) e non condizionante l'esecuzione del contratto nei casi in cui non sia strettamente necessario all'adempimento della prestazione da parte del professionista (c.d. *Kopplungsverbot*, art. 7). Tali requisiti del consenso non sono di ostacolo alla configurazione della liceità dei modelli «servizi contro dati», tra l'altro, per il fatto che il consenso è qui necessario per il perfezionamento dello stesso contratto e che l'art. 7 introduce non un divieto, ma uno dei parametri di valutazione della libertà di quest'ultimo, che deve rappresentare una «effettiva espressione dell'autodeterminazione informativa» della persona[111].

La struttura contrattuale risente della natura peculiare del consenso ora illustrata. Pur se l'operazione economica è unitaria, si configura una ricostruzione giuridica secondo la quale il consenso al trattamento dei dati e il contratto di accesso al servizio sono due atti distinti sottoposti a una diversa disciplina. Il consenso è un atto unilaterale che attua l'esercizio del diritto alla autodeterminazione informativa, la cui validità dipende dalla libertà, dall'informazione e dalla specificità, mentre il contratto di fornitura di servizi e contenuti digitali opera "a valle" rispetto all'atto che ne costituisce "a monte" il presupposto indispensabile per il lecito trattamento dei dati personali, con la duplice conseguenza che il consenso non è elemento costitutivo del sinallagma contrattuale e che i due negozi sono collegati, con tutte le conseguenze che discendono dal collegamento[112].

Segue la conseguente tematica della qualificazione del relativo contratto in termini di corrispettività o gratuità, prospettandosi la dazione del dato quale presupposto del servizio e una terza tipologia contrattuale di contratti atipici a titolo gratuito ai quali resta estraneo l'interesse economico perseguito dal fruitore del servizio, la quale si collocherebbe tra i contratti a prestazioni corrispettive e

110 Resta, G.: "I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, cit., p. 81 ss.

111 Resta, G.: "I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679", cit., p. 70 s. Esprime il medesimo principio Cass., 2 luglio 2018, n. 17278, in *Giur. it.*, 2019, p. 530 ss., con nota di Thobani, S.: "Operazioni di tying e libertà del consenso"; in argomento, v. Id.: "La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità", *Europa e dir. priv.,* 2016, 2, p. 513 ss.

112 Resta, G.: "I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679", cit., pp. 74 ss., 78 ss.

gli atti di liberalità[113]. Non si rinvengono comunque ostacoli normativi insuperabili alla qualificazione trattamento dei dati personali come corrispettivo di un servizio, al ricorrere di alcune condizioni[114]; in tal senso, depone la differenza profonda che esiste tra la titolarità di un diritto fondamentale, quindi indisponibile, e il suo esercizio che è invece disponibile, purché ciò non si traduca nel trasferimento del diritto e si assicuri un adeguato bilanciamento tra le ragioni del mercato e la tutela della persona[115].

Importante è allora la precisa descrizione dell'operazione economica di circolazione dei dati, nel prisma della loro "irriducibilità" a merce, alla luce, tra l'altro, del loro valore economico e dei modelli di circolazione "a più stadi", nel quadro di quanto ha affermato già a suo tempo la Commissione europea[116]. In

113 Scorza, G.: "Il dato personale: manifestazione della personalità vs. forma di ricchezza", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, cit., pp. 85 ss. e 100, il quale osserva che nel caso *Facebook* non si può parlare di corrispettività del contratto, poiché «la prestazione del consenso» al trattamento dei dati «è solo eventuale e il servizio è destinato a essere fornito anche laddove l'utente non presti tale consenso. Di più. È circostanza incontestabile quella secondo la quale tale consenso è sempre revocabile ma tale eventuale revoca non ha un riflesso sull'obbligo del fornitore del servizio di continuare a adempiere alle proprie obbligazioni» (p. 95).

114 Scorza, G.: "Il dato personale: manifestazione della personalità vs. forma di ricchezza", cit., p. 103 ss., il quale elenca una serie di condizioni a favore degli interessati-utenti, suscettibile di approfondimenti e modifiche, affinché il trattamento dei dati personali possa rappresentare l'oggetto del contratto: a) l'oggetto deve essere rigorosamente determinato o determinabile; b) in ipotesi di dubbio, l'oggetto deve essere interpretato restrittivamente; c) il regolamento contrattuale non può privare l'interessato dei diritti riconosciutigli dal GDPR e non può subordinare il loro libero esercizio al preventivo adempimento di qualsivoglia obbligazione contrattuale; d) la disciplina contrattuale deve essere compatibile con il GDPR (in particolare, con riferimento non esclusivo alla proporzionalità, alla minimizzazione del trattamento, alla *privacy by design*, alla *privacy by default*); e) l'eventuale scambio economico diretto (sconto, riconoscimento di altra utilità in denaro o equivalente) riconosciuto all'interessato non può essere tale da indurlo a concedere più dati e/o diritti per conseguire un vantaggio maggiore; f) il contratto non può riguardare i dati particolari alla luce del GDPR; g) il contratto non può avere durata ultra annuale, né prevedere clausole di rinnovo tacito alla scadenza; h) il contratto deve essere redatto nella lingua dell'interessato e prevedere che questi possa far valere i propri diritti dinanzi al giudice competente del Paese di residenza anche nelle forme dell'art. 80 GDPR; i) non può essere prevista la facoltà di modifica unilaterale del contratto e/o della informativa relativa al trattamento dei dati: le eventuali modificazioni devono essere oggetto di nuova esplicita approvazione da parte dell'interessato; j) deve essere esclusa la possibilità di cessione a terzi o di successione nel diritto al trattamento, salvo l'ipotesi di cessione di azienda o di un suo ramo; k) divieto di comunicare i dati personali a soggetti diversi da quelli espressamente individuati nel contratto e divieto di diffonderli; l) in caso di interessato minorenne, il contratto deve essere perfezionato con i soggetti esercenti la responsabilità genitoriale.

115 Scorza, G.: "Il dato personale: manifestazione della personalità vs. forma di ricchezza", cit., p. 101 ss. In tal senso, Thobani, S.: "Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali", cit., p. 62 ss., osserva che l'indisponibilità dei diritti della personalità costituisce retaggio della concezione proprietaria degli stessi che ha condotto a ritenere che il contratto abbia la funzione di «"disporre" del (nel senso di trasferire il) proprio diritto della personalità», mentre in questo «ambito oggetto del contratto non è necessariamente il trasferimento del diritto della personalità, ma ben può essere l'assunzione di una obbligazione avente ad oggetto una determinata prestazione».

116 La Commissione Europea, *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*, COM(2016) 320 *final*, cit., ha affermato che nella commercializzazione di servizi *online* il consumatore è, a volte, «tenuto a fornire» i dati che «vengono venduti a terzi» dal professionista (punto 3.4.1). Anche il Garante Europeo dei dati personali ha riconosciuto il valore economico assunto di fatto dai dati personali già nel documento EDPS, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection*, marzo 2014, in *https://edps.europa.eu/sites/default/files/publication/14-03-26_competitition_law_big_data_en.pdf* (v. punto 2.2: «Consumers provides richly detailed information about their preferences through their online activities wich permits individuals, not groups, to be targeted with far greater precision than ever before. For consumers, therefore, personal information operates as a currency, and sometimes the sole currency, in the exchange of online services»), nonché nei pareri resi in occasione del procedimento di adozione della Direttiva UE

alcuni casi si può in effetti pervenire a configurare lo scambio servizi/dati, inteso più correttamente come scambio del diritto al trattamento contro il diritto al servizio[117]: in particolare, là dove il consumatore è tenuto a fornirli per godere della controprestazione offerta dal professionista, il quale a sua volta li trasferisce a terzi non dovendoli utilizzare soltanto ai fini della erogazione del servizio[118]. Va precisato che la portata del diritto acquisito dall'impresa è circoscritta dagli specifici fini del trattamento che devono essere indicati e accettati dal consumatore[119]: si può quindi configurare l'acquisto di un numero di siffatti diritti corrispondente alle finalità perseguite con il trattamento dei dati che quindi conformano le predette situazioni giuridiche variandone il contenuto[120]. In questi contratti, dunque, in assenza di previsioni in tal senso nel GDPR, il diritto contrattuale consente di cogliere la giustificazione funzionale dell'accordo nella reciproca attribuzione dell'interessato del diritto al trattamento dei dati per finalità patrimoniali esterne al negozio e dell'impresa del diritto ad avvalersi della erogazione del servizio offerto. A ciò non osta, come già considerato *supra*, l'art. 7, § 4, GDPR, il quale si limita a garantire la libertà del consenso del consumatore contro eventuali «costrizioni», tali da far degradare la scelta in una imposizione senza alternative, ma non dichiara illegittimo di per sé lo scambio tra consenso al trattamento e accesso al servizio[121].

La riflessione sulla Direttiva sui contratti di fornitura di contenuti e servizi digitali ha evidenziato le criticità dei negozi di acquisto dei servizi digitali e di

2019/770 (EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 marzo 2017, in *https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf*) e della Direttiva UE 2019/2161 (EDPS, *Opinion 8/2018 on the legislative package "A New Deal for Consumers"*, 5 ottobre 2018, in *https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf*), ma ha altresì sostenuto che tali pratiche non dovrebbero ottenere alcun tipo di riconoscimento o approvazione in un atto legislativo della UE (EDPS, *Opinion 8/2018 on the legislative package "A New Deal for Consumers"*, cit., punto 27).

117 Solinas, C.: "La circolazione dei dati personali nell'ottica dello scambio tra diritti", cit., pp. 114 ss., 120; per un'altra lettura del fenomeno, v. Quarta, A.: *Mercati senza scambi. La metamorfosi del contratto nel capitalismo*, Esi, Napoli, 2020.

118 Sul punto, v. Solinas, C.: "La circolazione dei dati personali nell'ottica dello scambio tra diritti", cit., p. 119, la quale precisa che «in tutte quelle ipotesi in cui il dato personale richiesto dal professionista non sia meramente necessario per l'esecuzione di una prestazione da lui contrattualmente assunta e laddove non ricorrano le altre ipotesi che per l'ordinamento giustificano il trattamento dei dati personali (art. 6 GDPR), la condivisione con il professionista del dato personale da parte dell'utente deve necessariamente trovare titolo nella volontà, nel consenso, di quest'ultimo»; pertanto, in tale caso «il trattamento *per dette finalità* [commerciali ulteriori riferibili al professionista] è lecito solo se è fondato sull'apposito consenso (*per* quel tipo di trattamento) da parte dell'utente interessato (art, 6, lett. a, GDPR)» (corsivo nel testo). Sulla base di considerazioni fondate sulla natura di diritto fondamentale del diritto alla protezione dei dati personali e della sua indisponibilità e sulla irriducibilità dei dati personali a merce o moneta, affermano la non possibile rilevanza giuridica del dato personale come corrispettivo Bravo, F.: *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018; Messinetti, R.: "Circolazione dei dati personali e autonomia privata", in Zorzi Galgano, N.: *Persona e mercato dei dati*, cit., p. 140 e 160 ss.

119 L'art. 6, § 1, lett. *a*, GDPR dispone che il consenso al trattamento è sempre espresso «per una o più specifiche finalità».

120 Ai sensi dell'art. 5, § 1, lett. *b*, GDPR, infatti, i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità».

121 In tal senso, v. Solinas, C.: "La circolazione dei dati personali nell'ottica dello scambio tra diritti", cit., p. 133 ss., per la quale «la libertà o meno del consenso va dunque concretamente valutata con riferimento al contesto, alle possibili alternative di accesso al bene (ivi comprese quelle connesse alla struttura del mercato)».

quelli in cui vi è la fornitura dei dati personali del consumatore al professionista-operatore economico che pongono la questione dell'unità o pluralità delle strutture contrattuali lasciata aperta dal legislatore unionale.

Resta sullo sfondo la necessità di sciogliere la contraddizione insita nello scambio servizi/dati dalla prospettiva del GDPR e da quella del diritto consumeristico, che ne fonderebbero, nel contempo, la illiceità e la liceità. Questa discrasia può essere risolta garantendo la libera circolazione, purché non determini il verificarsi dei rischi derivanti dal trattamento[122].

L'attento esame dei profili contrattuali deve partire dalla costatazione che elemento costitutivo di questa specifica dinamica negoziale è il consenso del consumatore. Vi è poi la questione dei riflessi sulla validità ed efficacia del contratto prodotti dalla violazione delle norme sul trattamento dei dati, con particolare attenzione al difetto di conformità, alla nullità di protezione e alla risoluzione.

L'indagine va poi spostata sul dato personale usato nella *blockchain* come fattore di sviluppo economico, alla quale si applica il GDPR in ragione della natura di sistema "pseudonimo" di quest'ultima con le problematiche che ciò comporta in termini di compatibilità con i principi di tutela dei dati personali.

Infine, è necessario disegnare il quadro normativo del mercato dei dati, analizzando il profilo della corretta informazione sul valore economico dei dati come pratica commerciale e quello più generale del diritto del mercato e della concorrenza, traendo indicazioni dall'esperienza tedesca.

Il tema delle tutele offerte in caso di violazione dei dati personali è a dir poco centrale in questo àmbito[123]. L'art. 82, § 1, reg. 2016/679/UE, il GDPR, pone la regola generale sul «Diritto al risarcimento e responsabilità» nel settore del trattamento dei dati personali, disponendo che «chiunque subisca un danno materiale o immateriale (*rectie*, patrimoniale o non patrimoniale) causato da una violazione del regolamento ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento».

La disciplina vuole quindi garantire al danneggiato pieno ed effettivo risarcimento[124] per il pregiudizio subito dall'illecito trattamento dei dati personali, come impone l'inerenza di tale attività ai diritti e alle libertà fondamentali della persona, ritenuti insopprimibili in una società ispirata al sempre più intenso garantismo in chiave solidaristica e personalistica.

122 Solinas, C.: "La circolazione dei dati personali nell'ottica dello scambio tra diritti", cit., p. 110 ss.

123 In argomento v. Gambini, M.: "Il danno (patrimoniale e non patrimoniale) da trattamento illecito di dati personali", in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), I, cit., p. 529 ss.

124 V. il *considerando* n. 146 del GDPR.

Il legislatore europeo riconosce la generale risarcibilità del danno patrimoniale e non patrimoniale in tutti i casi in cui risulti generato dalla violazione del GPDR o, secondo il *considerando* n. 146, degli atti delegati, degli atti di esecuzione adottati in conformità del regolamento e delle disposizioni del diritto degli Stati membri che specifichino le disposizioni de GDPR. Inoltre, il *considerando* n. 146 precisa che il concetto di danno deve essere interpretato in senso ampio, alla luce della giurisprudenza della CGUE.

Occorre indagare il ruolo del rimedio risarcitorio nel più vasto ambito della tutela della persona, indissolubilmente intrecciato con quello della protezione dei danni personali. In proposito, si accoglie l'orientamento elaborato delle Sezioni Unite del 2008 in materia di risarcimento del danno che individua un sistema bipolare che vede l'art. 2043 c.c. riferirsi ai danni patrimoniali l'art. 2059 c.c. ai danni non patrimoniali e conferma il superamento della distinzione tra danno-evento (lesione in sé e per sé della situazione soggettiva) e danno-conseguenza (conseguenze concrete pregiudizievoli oggettivamente apprezzabili derivate dalla lesione della situazione), già deciso dalla Cassazione del 2003. Secondo le Sezioni Unite, l'obbligo di risarcire il danno non patrimoniale sorge solo casi previsti dalla legge: tali non sono soltanto quelli prodotti da reati, ma anche quelli arrecati da una condotta che ha leso in modo significativo interessi della persona aventi il rango e la dignità di situazioni protette dalla Costituzione in base ad una interpretazione costituzionalmente orientata dell'art. 2059 c.c. Le Sezioni Unite hanno anche formulato quale strumento selettivo del pregiudizio risarcibile il duplice criterio della gravità della lesione e della serietà di pregiudizio. In tal modo si è posto un freno alla proliferazione ingiustificata della categoria del danno non patrimoniale risarcibile e delle pretese risarcitorie futili. È inaugurata così una nozione omnicomprensiva del danno non patrimoniale, posto a presidio degli interessi areddituali della persona, rispetto al quale i singoli aspetti del pregiudizio subito assumono una funzione meramente descrittiva, escludendosi dunque un'autonoma liquidazione di plurime voci di danno non patrimoniale. È così superata la distinzione di tale danno in sottocategorie tipizzate (danno morale, danno biologico, danno esistenziale) in quanto ciò che rileva ai fini del risarcimento è l'effettiva sussistenza ed entità del pregiudizio, stante l'obbligo del giudice di tener conto in sede di liquidazione unitaria del danno di tutte le conseguenze pregiudizievoli causate dall'illecito nel caso concreto in ossequio del principio dell'integralità del risarcimento. Inoltre, è ammessa la personalizzazione del risarcimento del danno non patrimoniale in presenza di circostanze specifiche ed eccezionali, allegate dal danneggiato, che rendano il danno più grave e che valgano a superare le conseguenze ordinarie liquidate in via forfettaria dalle previsioni tabellari.

La recente giurisprudenza della Cassazione ha applicato al danno non patrimoniale da violazione della *privacy* i suddetti principi, compreso il duplice

criterio della gravità della lesione, concernente il diritto fondamentale alla protezione dei dati personali, e della serietà del danno, intesa quale perdita di natura personale effettivamente patita. Anche in tale ambito opera il principio di solidarietà dell'art. 2 cost. di cui il principio di tolleranza della lesione minima è intrinseco precipitato.

La Suprema Corte di recente ha chiarito a proposito del danno, patrimoniale e non, da illecito trattamento dei dati personali l'articolazione dell'onere probatorio, specie con riferimento alla prova del danno e alla sua quantificazione. Si richiede quindi che del danno sia dia prova specifica secondo la teoria del danno-conseguenza: il richiedente il risarcimento deve provare la sussistenza di un effettivo pregiudizio oggettivamente apprezzabile da lui patito derivante dalla lesione dell'interesse protetto, anche non patrimoniale.

A conferma della scelta del risarcimento del danno conseguenza milita anche il GDPR. L'art. 82 discorre di risarcimento di danno causato o cagionato dal trattamento illecito, mostrando che il danno non coincide con il trattamento in sé. Il *considerando* n. 75, a proposito dei rischi per i diritti e le libertà delle persone fisiche che possono derivare dal trattamento di dati personali, utilizza l'espressione «suscettibili di cagionare un danno fisico, materiale o immateriale […] o qualsiasi altro danno economico o sociale significativo». Ancora, il *considerando* n. 85 sottolinea che la violazione dei dati personali «può […] provocare danni fisici, materiali o immateriali alle persone fisiche». Peraltro, l'aggettivazione come fisico, materiale, immateriale, economico e sociale riferita al danno prodotto dal trattamento illecito, induce a ritenere che essa presupponga necessariamente una valutazione concreta in merito alla natura e all'entità del danno.

Il danneggiato ha quindi l'onere di provare l'ingiustizia del danno e il pregiudizio concreto subito con riguardo al *quantum* da risarcire. L'onere della prova può essere assolto anche con meccanismi presuntivi per provare l'esistenza del danno. Il ricorso alla presunzione è giustificato dalla difficoltà di provare il danno non patrimoniale come conseguenza del fatto lesivo: il danneggiato avrà dunque l'onere di indicare tutti gli elementi necessari per ricostruire la serie concatenata dei fatti noti che permettano al giudice di risalire presuntivamente al fanno ignoto.

La quantificazione del danno non patrimoniale prodotto dalla violazione della normativa in materia di dati personali è operazione complessa, di norma rimessa al prudente apprezzamento del giudice di merito che procede secondo equità, stante l'impossibilità o l'estrema difficoltà per il danneggiato di provare il suo ammontare, operazione che sfugge ad una valutazione economica oggettiva.

Nella individuazione dei criteri che possano guidare l'equità nella liquidazione del danno non patrimoniale è avvertita l'esigenza di definire un nucleo probatorio

forte costituito da criteri costanti, oggettivamente affidabili e non manipolabili, dai quali inferire le ricadute negative di tipo esistenziale ed emotivo sul danneggiato, al fine di favorire una qualche uniformità e prevedibilità delle soluzioni adottate. Da tempo, è avvertita però anche la necessità di impiegare criteri elastici e flessibili nella quantificazione del danno non patrimoniale da trattamento illecito dei dati personali, che consentano di adeguare la liquidazione alla sofferenza effettivamente patita dal danneggiato e a tutte le circostanze del caso concreto in quanto è la regola stessa dell'equità che impone di trattare in maniere diversa fatti differenti. In giurisprudenza si rinvengono entrambi gli orientamenti, ciascuno dei quali mostra i suoi limiti che vanno dall'applicazione di parametri rigidamente fissati in astratto a decisioni ondivaghe che a volte riconoscono risarcimenti simbolici, a volte superiori ai precedenti in materia.

La rilevanza riconosciuta alle circostanze concrete induce a riflettere sulla funzione del risarcimento del danno non patrimoniale da violazione della *privacy*, che risulta difficilmente conciliabile con la tradizionale finalità reintegrativa dell'istituto. Si discute così della complessa questione dei limiti di operatività del rimedio risarcitorio nell'ambito della tutela dei dati personali, ciò che ha portato parte della dottrina a contestare l'importanza della regola della responsabilità civile in questa materia. Detti limiti discendono dal carattere non omogeneo del ristoro riconosciuto e del pregiudizio subito dal danneggiato che, considerata la natura del bene protetto (diritti e libertà fondamentali della persona) sfugge per definizione a una valutazione economica oggettiva, potendo essere misurato in denaro con grande fatica ed elevato grado di arbitrarietà. Ne consegue che il valore persona, una volta leso, non può più essere ricostituito e che il risarcimento del danno non patrimoniale nell'àmbito della protezione dei dati personali assolve (non la funzione reintegrativa tradizionale, ma) la funzione solidaristico satisfattiva, potendosi soddisfare la vittima per la perdita patita soltanto tramite la corresponsione di una somma di denaro che rappresenta una consolazione per il male subito, tesa a consentirle una migliore qualità della vita a garanzia della solidarietà sociale.

VII. LA CIRCOLAZIONE DEI DATI NON PERSONALI.

Oltre ai dati sensibili vi sono i «dati non personali», oggetto della disciplina di cui al Regolamento UE n. 2018/1807, il cui àmbito di applicazione è quello dell'attività di trattamento dei dati elettronici «diversi dai dati personali»[125]. Anche

125 Secondo l'art. 3, n. 1, tali sono «i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679». La classificazione della informazione in una o nell'altra categoria dipende anche dalla qualità del soggetto che la raccoglie (Agenzia delle Entrate, Polizia, Ministero della Salute, Registro delle imprese, OMS ecc.): alcune raccolte di dati sono infatti lecite esclusivamente se attuate da determinati enti e per scopi definiti. Il tema è affrontato da Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza

in questo settore l'UE favorisce lo scambio tra Stati dei dati non personali[126], la cui circolazione è considerata indispensabile per lo sviluppo dell'economia nel suo complesso, quindi non soltanto di quella digitale[127]. Sono dati di questo tipo le informazioni relative a fatti, cose, mondo vegetale e animale, ambiente ecc. che possono essere liberamente raccolte ed elaborate[128]; come già esposto, possono essere considerate neutre anche le informazioni relative a persone, ma gestite in forma anonima: quando il soggetto non è riconoscibile, non si configurano rischi di lesioni ai suoi diritti. Pur se l'ordinamento preserva la sfera personale dell'individuo, non vi sarebbe in effetti possibilità di ingerenza in condizioni di effettivo anonimato.

Il trattamento dei dati è sicuramente uno strumento molto positivo che serve imprescindibilmente, ad esempio, ai fini dell'accrescimento e della diffusione della conoscenza, dello sviluppo scientifico, della gestione della cosa pubblica nonché, in ultima analisi, del miglioramento della qualità della vita dell'uomo. La raccolta dati è evidentemente anche utile per il perseguimento di scopi lucrativi: si pensi, ad esempio, alle nuove tecniche di *marketing* e alla possibilità di studiare le preferenze dei consumatori per stimolarli selettivamente all'acquisto. Tuttavia, le nuove tecnologie recano con sé anche, tra l'altro, il rischio che, superando l'anonimato oramai sempre più precario[129], le informazioni raccolte consentano di conoscere i comportamenti, le opinioni e le scelte dei cittadini, quindi di schedarli, per condizionarne l'esercizio dei diritti democratici, minando alla base il funzionamento

pubblica necessaria!, in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), I, cit., p. 407 ss.

126 Così recita l'art. 1: «Il presente regolamento mira a garantire la libera circolazione dei dati diversi dai dati personali all'interno dell'Unione stabilendo disposizioni relative agli obblighi di localizzazione dei dati, alla messa a disposizione dei dati alle autorità competenti e alla portabilità dei dati per gli utenti professionali». In tal senso, tra l'altro, v. anche il *considerando* n. 11: «Per istituire un quadro applicabile alla libera circolazione dei dati non personali nell'Unione e creare il fondamento per lo sviluppo dell'economia dei dati e il rafforzamento della competitività dell'industria dell'Unione, è necessario stabilire regole giuridiche chiare, complete e prevedibili per il trattamento di dati diversi dai dati personali nel mercato interno».

127 V. il *considerando* n. 1: «L'economia si sta velocemente digitalizzando. Le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni. I dati elettronici sono al centro di tali sistemi e, quando sono analizzati o utilizzati in associazione a servizi e prodotti, possono generare un ingente valore».

128 V. il *considerando* n. 9: «L'espansione dell'Internet degli oggetti, l'intelligenza artificiale e l'apprendimento automatico rappresentano fonti importanti di dati non personali, ad esempio a seguito del loro utilizzo in processi automatizzati di produzione industriale. Fra gli esempi specifici di dati non personali figurano gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati, i dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua, o i dati sulle esigenze di manutenzione delle macchine industriali».

129 In proposito d'Avack, L.: "La rivoluzione tecnologica e la nuova era digitale: problemi etici", in Ruffolo, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 23, osserva che la «enorme quantità di dati raccolti e profilati rende evanescente la riservatezza, perché è sempre possibile da alcune informazioni incrociate risalire all'identità, rendendo più difficile l'anonimizzazione totale e definitiva. Pertanto, è anche necessario dare attuazione a un riconoscimento effettivo del 'diritto all'oblio', stabilendo con procedure chiare e trasparenti la possibilità per il soggetto di richiedere la cancellazione dei dati personali, di modo che questi non siano più accessibili al pubblico sotto qualsiasi forma (copie o riproduzione)».

delle democrazie. In questa ipotesi torna ad applicarsi la disciplina a tutela della *privacy* recata dal GDPR[130].

Come già visto, però, il GDPR è rivolto a proteggere l'individuo contro l'elaborazione illecita dei suoi dati, rappresentata ad esempio dalla raccolta di informazioni vietate e/o non rese anonime oppure dalla deviazione dello scopo per cui è consentita: a tal fine, il bilanciamento di interessi è tarato nell'ottica del rapporto sorto tra il titolare di dati e il titolare del trattamento. Si osserva che il Regolamento non sembra per questo motivo offrire tecniche di intervento sufficienti a combattere i suddetti rischi: il consenso del titolare non basta, da solo, a tal fine, potendo anzi trasformarsi in una sorta di «patente indiscriminata di liceità»[131]. È pertanto necessario individuare degli strumenti efficaci di tutela attivabili in caso di un siffatto uso illecito. Si ritiene che detti pericoli debbano essere fronteggiati con le tecniche di controllo sociale, che le schedature realizzate per scopi illeciti siano da considerare proibite pur se consentite dall'interessato e aventi ad oggetto dati non sensibili, che debbano essere vietate l'utilizzazione dei dati per finalità diverse da quelle che hanno fondato la raccolta lecita e la cessione dei dati a terzi per il perseguimento di scopi diversi[132].

L'approccio proposto analizza la natura dei dati e il regime giuridico cui dovrebbero essere sottoposti. Considerato che i dati non personali sono beni diversi da quelli sensibili e idonei a produrre utilità differenti da questi ultimi, l'evoluzione dottrinale e giurisprudenziale consente di annoverarli tra i beni immateriali in grado di essere oggetto di diritti. Viene così proposta una ricostruzione nel quadro di una nozione di bene che valorizza le utilità che lo stesso è in grado di produrre e che contempla la possibilità che esse siano sfruttate attraverso un accesso plurimo. I dati aggregati sono dunque dei beni in senso giuridico, frutto della elaborazione delle informazioni grezze riferibili a una massa di persone e oggetto di diritti e di atti di disposizione. L'attività di elaborazione tramite gli algoritmi fonda la titolarità di chi lavora ai dati, in applicazione della regola dominicale della specificazione quale modo di acquisto della proprietà imperniato sulla trasformazione della materia. Il titolare del dato è il "proprietario" della materia, l'elaboratore è chi la lavora con il trattamento algoritmico[133].

130 V. il *considerando* n. 9: «Se i progressi tecnologici consentono di trasformare dati anonimizzati in dati personali, tali dati sono trattati come dati personali e si applica di conseguenza il regolamento (UE) 2016/679».

131 Così, Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 411, la quale nella nota n. 6 richiama lo scritto di Rodotà, S.: *Elaboratori elettronici e controllo sociale*, Torino, 1973, p. 51.

132 Così, Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 412.

133 Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 413 ss., ove si richiama la letteratura che configura un diverso concetto di bene che va oltre il tradizionale legame, oramai considerato superato, tra la proprietà e la soddisfazione del bisogno, e che riconosce l'accesso al bene per il tempo nella misura sufficiente alla soddisfazione del bisogno, svincolandosi dallo *jus escludendi* la cui ricorrenza nel diritto dominicale dipende dalla natura del bene: si sposta così l'attenzione dal valore di scambio al valore di uso dei beni.

Al titolare del dato reso anonimo non spetta alcuna pretesa sui dati aggregati e nessuna quota degli ingenti profitti derivanti dalla loro circolazione. A questo risultato si giunge anche applicando la regola della specificazione, se si considera l'inconsistenza dell'indennizzo a fronte dei costi del trattamento algoritmico, a prescindere dalla probabile rinuncia collegata al consenso al trattamento. Inoltre, il titolare dei dati sensibili non subisce interferenze nella propria sfera giuridica dalla elaborazione e dall'utilizzo dei dati aggregati[134].

La soluzione al problema rappresentato dalla possibilità di risalire dal dato aggregato al dato sensibile non sembra essere quella della sua incommerciabilità, essendo peraltro prevista la sua portabilità dall'art. 20 GDPR, dal quale si desume il riconoscimento di un valore suscettibile di circolazione. Quale strumento di tutela preventiva non sembra efficace neanche il ricorso al consenso informato, dovendosi osservare che forse non è tale un consenso reso in assenza di consapevolezza del valore di ciò che si sta cedendo. Puntare sul consenso avrebbe come unico effetto quello di appesantire l'informazione preliminare fornita al cedente[135].

Ad esiti differenti si giunge invece considerando che oggetto della lavorazione algoritmica non è il singolo dato, bensì una massa di dati non sensibili riferibili ad una collettività di individui che ha un valore che trascende quello risultante dalla sommatoria dei dati singolarmente considerati. I dati aggregati sono in grado di fornire utilità diverse e indefinite, tra le quali anche la possibilità di essere sfruttati per lo svolgimento dell'attività di elaborazione. Questa massa di dati costituisce quindi un bene in grado di recare utilità e di soddisfare bisogni attraverso un accesso plurimo e non dovrebbe essere oggetto di godimento esclusivo, ma essere lasciata nella disponibilità di tutti: a questo bene si ritiene addire la definizione di bene comune individuata nella proposta di legge elaborata dalla Commissione Rodotà nel 2007[136]. I beni comuni sono quelli funzionali al libero sviluppo della persona e all'esercizio dei diritti fondamentali, tra i quali rientra il diritto alla conoscenza e al progresso culturale. Detti beni dovrebbero essere soggetti al regime di libero accesso e a essi dovrebbe essere assegnato un valore almeno equivalente a quello del lavoro necessario alla creazione del nuovo bene costituito

134 Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 416.

135 Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 417; cfr., sulla questione se il consenso si ritenga informato in assenza della consapevolezza del valore di ciò che si sta cedendo, Resta, G.: "Diritti fondamentali e diritti privato nell'era digitale", in Caggia, F. e Resta, G.: *I diritti fondamentali in Europa e il diritto privato*, Roma, 2019, p. 219 ss.

136 Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 417 ss. La proposta di legge della Commissione Rodotà nel 2007 ha enucleato una nuova definizione di bene di cui all'art. 810 c.c. (che ricomprende i beni immateriali) e le categorie dei beni comuni a titolarità diffusa e beni pubblici distinti a loro volta in beni ad appartenenza pubblica necessaria, beni sociali e beni fruttiferi. Dei beni ad appartenenza pubblica necessaria lo Stato non può in alcun caso disfarsi e sono lo zoccolo della proprietà pubblica: sono beni che producono utilità indispensabili per l'esercizio del potere statuale, senza i quali lo Stato non è Stato e non è in grado di esercitare le proprie prerogative. Sono dunque beni funzionali alla sovranità di cui lo Stato non può perdere il controllo. Oggetto di riserva allo Stato non sono i beni, bensì le utilità che questi producono.

dall'informazione dinamica. Pertanto, si formula l'ipotesi che il dato aggregato prodotto dell'elaborazione algoritmica non possa essere oggetto di un diritto esclusivo, così come non possa esserlo la massa di dati oggetto di elaborazione: sono beni della conoscenza di cui tutti devono poter godere[137].

Si evidenzia che l'argomento ricorrente per contrastare siffatta proposta è l'esigenza di compensare il creatore dei *big data* per i costi sopportati e l'attività svolta e di incoraggiarlo a ulteriori investimenti che saranno ulteriormente ripagati. Attualmente si discute se i *big data* possano essere assimilati alle banche dati e ricevere la tutela a queste riservata o se possano assurgere a segreti industriali ed essere assoggettati alla relativa disciplina. In tal senso, il legislatore riconosce con una certa generosità diritti di sfruttamento esclusivo sui nuovi beni prodotti dal progresso tecnologico. Si critica questa scelta politica e si osserva che per i *big data* sarebbe inappropriata. Peraltro, un diritto esclusivo sui *big data* sarebbe difficilmente attuabile e la stessa conformazione di questi beni suggerisce il ridimensionamento della esclusiva a favore del libero accesso alle utilità che sono in grado di offrire: l'economia dei dati è molto dinamica e le informazioni trattate suscettibili di ulteriori elaborazioni. I *big data* sono quindi estremamente volatili e difficilmente attribuibili a un soggetto determinato. Il profitto ricavato dal trattamento algoritmico è anch'esso volatile, pertanto i *big data* non dovrebbero produrre rendite come quelle ricavabili dalle invenzioni: all'autore dovrebbe spettare una ricompensa per l'attività svolta e il risultato della stessa dovrebbe essere soggetto a un regime di godimento plurimo e di libero accesso. Si ritiene così essere compito dei giuristi impedire che la posizione di monopolio raggiunta dalle *big company* si rafforzi con il riconoscimento di un diritto di esclusiva e che si attivi il processo di «giuridificazione» dei *big data* tramite il riconoscimento del risarcimento per le utilizzazioni non concesse dal titolare. Si ritiene che gli sforzi tecnologici compiuti per la raccolta e l'elaborazione dei *big data* siano ampiamente compensati dal regime di monopolio in cui l'attività è svolta[138]

Il regime di accesso diffuso ai dati non sensibili non è una soluzione sempre valida, dovendosi considerare quei dati, sensibili e non, destinati a produrre utilità il cui perseguimento rientra nelle prerogative degli stati: dette raccolte, lecite in virtù delle finalità perseguite, non sono sottoponibili al libero accesso. In tal caso, si prospetta una soluzione che potrebbe essere attuata in presenza di una disciplina della proprietà pubblica riformata. Sulla base di quanto elaborato dalla proposta Rodotà, relativamente ai beni ad appartenenza pubblica necessaria, si evidenzia che l'esercizio dei poteri sovrani dello Stato nell'epoca attuale si basa inevitabilmente sul controllo del traffico dei dati che è funzionale non soltanto alla difesa nazionale da possibili aggressioni, ma anche alla tutela dell'identità nazionale,

137 Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 418 ss.

138 Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 416.

al funzionamento corretto delle strutture democratiche e alla tutela della salute pubblica. Si ritiene fondamentale assicurare alla UE e agli Stati membri il controllo su quella mole di dati essenziale per l'esercizio delle proprie prerogative, senza lasciarli alla libera appropriazione da parte dei poteri economici. Siffatti «dati sensibili» dello Stato devono essere trattati in considerazione delle utilità che sono in grado di produrre ed essere sottoposti a un regime equivalente a quello dei dati sensibili della persona. In tale ottica si propone di leggere il Regolamento n. 2018/1807, interpretando in modo ampio il riferimento alla sicurezza pubblica e considerando quindi consentiti tutti quegli obblighi di localizzazione dei dati che siano funzionali alla tutela delle prerogative proprie degli Stati. D'altra parte, l'art. 2, comma 3, dispone la non applicazione del Regolamento alle attività estranee al diritto unionale: in questi settori lo Stato può dunque sottrarre al regime di libero accesso i dati utili all'esercizio delle sue funzioni e gestirli esso stesso nell'esercizio dei poteri sovrani nonché può anche porre obblighi di localizzazione[139].

La proposta, pur se interessante in sé, non sembra essere però praticabile. Innanzi tutto, la ricostruzione dei dati aggregati non è convincente e comunque sarebbe in contrasto con la normativa europea che ne consente la libera circolazione. In proposito bisogna partire da una considerazione di fondo. Da una parte, è vero che i *big data* sono oggi nelle mani di pochi colossi stranieri che hanno creato quindi una situazione di oligopolio, essendo partiti per primi e da anni con l'esercizio di questa attività. Ma, dall'altra, questo oligopolio è contrastabile, poiché possono essere costituiti altri soggetti che elaborano masse di informazioni creando dati aggregati. Questo è reso possibile dal fatto che il dato, bene immateriale, è per sua natura cedibile un numero elevato di volte a soggetti diversi, non essendo possibile attuare una limitazione al loro trasferimento: si pensi a tutte le volte che una persona ha dato il consenso al trattamento dei suoi dati a soggetti differenti e tra loro magari anche in concorrenza (*social media*, grande distribuzione, commercio *online*, assicurazioni, banche ecc.). Questa è una parte della soluzione del problema complessivo e sembra essere la via percorsa dalla UE che sta cercando di creare nell'Unione dei centri di elaborazione di *big data* e ha assegnato a Bologna un ruolo importante in tal senso[140]. Se ci saranno nel mercato

139 Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria", cit., p. 420 ss.

140 Il riferimento è al progetto del CINECA di realizzazione del supercomputer Leonardo che verrà collocato all'interno del Tecnopolo di Bologna (per una prima informazione v. il sito della *International Foundation Big Data and Artificial Intelligence for Human Development - IFAB -, https://www.ifabfoundation.org/it/tecnopolo-di-bologna/*, e quello della Regione Emilia Romagna, *https://www.regione.emilia-romagna.it/datavalley/big-data-technopole*), il quale è stato scelto come progetto italiano da *EuroHPC Joint Undertaking*, l'impresa comune europea che acquisirà, creerà e implementerà in tutta Europa un'infrastruttura di calcolo ad alte prestazioni (*HPC*) all'avanguardia e sosterrà anche un programma di ricerca e innovazione per sviluppare le tecnologie e le macchine (*hardware*), nonché le applicazioni (*software*) destinate ai supercomputer. Leonardo è dunque uno degli otto supercomputer *pre-exascale* che formeranno la rete di calcolo europea ad alte prestazioni *EuroHPC* (così, si discorre di Emilia Romagna come *Data Valley* europea, che è destinata a divenire sempre più piattaforma e *hub* internazionale per lo studio e le applicazioni su *big data* e intelligenza artificiale). Il supercomputer Leonardo troverà impiego in diversi settori strategici: grazie a una potenza di calcolo di 270 *petaflops*, sarà in grado di elaborare i dati prodotti dai più importanti progetti internazionali ai quali partecipano l'Istituto Nazionale di Fisica Nucleare e l'Istituto Nazionale di Astrofisica, come LHC,

più soggetti europei che raccolgono ed elaborano masse di informazioni creando dati aggregati, si sarà ridotto il potere degli oligopolisti che non saranno più tali e si sarà reso più democratico il funzionamento del sistema economico e non solo. Ci saranno anche più *big data* disponibili, frutto di differenti elaborazioni quindi con informazioni differenti e con prezzi di accesso anche più bassi.

Altro aspetto critico è che l'argomento dei costi di elaborazione non è in realtà superato dalle considerazioni sopra illustrate, ed è invece centrale in quanto la creazione dei dati aggregati e dei *big data* richiede ingenti e continui investimenti per la gestione e il costante sviluppo delle tecnologie necessarie a tal fine, che devono essere in qualche modo coperti. Nella proposta si dice che il soggetto che li elabora va retribuito, ma non è chiarito come e, soprattutto, da chi. Non sembra facilmente concepibile un intervento pubblico in tal senso, poiché significherebbe acquistare con risorse statali i *big data* per metterli a disposizione di tutti, comprese le imprese private. Questa ipotesi configurerebbe, peraltro, un aiuto di stato contrario al diritto della UE.

Altro problema è che i dati aggregati, così acquistati e resi liberamente accessibili in quanto considerati come un bene comune, a chi vanno affidati? Restano a chi li ha creati oppure vanno consegnati a un soggetto pubblico che li renda disponibili a chi ne faccia richiesta? La prima ipotesi sarebbe singolare in quanto si acquisterebbe un bene per lasciarlo nella disponibilità del venditore che potrebbe anche rielaborarlo e venderlo di nuovo al medesimo (unico) acquirente, se non a terzi. L'ipotesi di un soggetto pubblico quale "custode" dei dati è molto rischiosa per i possibili abusi, di ogni genere, di cui anche questo potrebbe macchiarsi per perseguire "scopi" di pubblica utilità. Lo Stato e le varie amministrazioni sono già in possesso di una serie rilevante di informazioni: mettergli a disposizione anche quelli attinente prettamente alla vita privata dei cittadini sarebbe oltremodo pericoloso in quanto l'eventuale "schedatura" della persona sarebbe pressoché totale, a differenza di quelle che potrebbe predisporre un ente privato. Le vicende italiane degli ultimi anni hanno purtroppo conosciuto casi del genere. Peraltro, proprio perché di natura pubblica, è anche tecnicamente più difficile predisporre adeguati ed efficaci strumenti giuridici di tutela contro gli eventuali usi illegittimi dei dati ad opera di un soggetto pubblico, anche considerato che la P.A. è normalmente dominata da una politica che è oggi alla costante ricerca del consenso e della prevaricazione dell'avversario. Inoltre, va altresì menzionato il fatto che funzionamento degli enti pubblici, in Italia, non è certo caratterizzato dall'efficienza, quanto piuttosto - come minimo - da una soffocante quanto bizantina burocrazia che genera spesso lungaggini e disservizi: dalla prospettiva del servizio a favore della collettività

SKA e VIRGO, ma anche dal consorzio Cineca, che ospiterà e gestirà il supercomputer, per consentire studi nell'ambito dell'intelligenza artificiale, della robotica, della farmacologia, dei nuovi materiali ecc. La macchina potrà essere messa a disposizione degli istituti di ricerca, delle università, ma anche delle aziende per le loro necessità.

non si vede dunque quale senso avrebbe pubblicizzare il "custode" del dato. Infine, occorrerebbe creare un ente di dimensioni notevoli e molto costoso per conservare in modo tecnologicamente adeguato e sicuro tutti i dati liberamente disponibili: questo comporterebbe un ulteriore aumento strutturale del debito pubblico, magari a scapito delle voci di bilancio che si è solito sacrificare per prime - vedi università e scuola - in caso di ricerca di fondi pubblici.

Piuttosto, un intervento che potrebbe essere concepito è l'implementazione del sistema dei controlli pubblici, introducendo ad esempio l'obbligo di registrazione delle imprese che elaborano e cedono i dati, e magari anche l'obbligo di comunicazione delle cessioni degli stessi, al fine di controllare chi opera nel settore, le finalità che persegue e a chi vengono ceduti i dati. Peraltro, questo permetterebbe anche di verificare l'uso effettivo degli stessi e di intervenire sugli usi difformi da quelli dichiarati, prevedendo una serie di sanzioni che potrebbero andare dal blocco dell'attività, alla nullità dei contratti di cessione e al sequestro, con relativa distruzione, dei dati aggregati illecitamente elaborati. Questo sistema è già operante nel settore dei mercati finanziari in forza della MiFID II per gli intermediari che utilizzano algoritmi per le negoziazioni. L'autorizzazione deve garantire che siano soggette ai requisiti di organizzazione previsti dalla MiFID II e ad un'adeguata vigilanza. Anche gli enti che sono autorizzati e controllati a norma del diritto europeo sul settore finanziario ed esenti dall'applicazione della disciplina in materia, ma che effettuano negoziazioni algoritmiche, devono essere soggetti alle misure e ai controlli volti a contrastare il rischio specifico derivante da tali tipi di negoziazione. In tal senso, l'ESMA è chiamata a svolgere un importante ruolo di coordinamento, definendo le idonee dimensioni dello scostamento di prezzo, così da assicurare l'ordinato funzionamento dei mercati dell'Unione[141]. Proprio al fine di assicurare una vigilanza efficace e di consentire alle autorità competenti di adottare misure adeguate e tempestive contro le strategie algoritmiche difettose o scorrette, è anche necessario segnalare tutti gli ordini generati mediante negoziazione algoritmica. Attraverso la segnalazione, le autorità competenti sono in grado di identificare e distinguere gli ordini provenienti da algoritmi differenti e di ricostruire e valutare efficacemente le strategie utilizzate dagli operatori che adottano siffatte tecniche di negoziazioni.

VIII. L'*E-COMMERCE* E IL CONSUMATORE.

Quanto in precedenza osservato invita conseguenzialmente a spostare l'attenzione sull'*E-Commerce*[142]. Nell'àmbito degli scambi telematici il tema

141 V. il *considerando* n. 63 MIDIF II.

142 Il tema è affrontato da Lazzarelli, F.: "E-commerce e contraente debole (non consumatore). Considerazioni sistematiche a margine dei recenti interventi del legislatore UE e della Corte di Giustizia", in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), I, cit., p. 667 ss.

dell'equilibrio contrattuale è rinvigorito da profili nuovi, scaturiti dall'uso delle nuove tecnologie, che alimentano anche il dibattito sul contraente debole identificato nel consumatore (*cyber*consumatore) protetto dalla relativa disciplina.

Il *cyber*consumatore è, a volte, vittima di condotte abusive e a causa dell'incertezza sull'*an* e sul *quomodo* rinuncia spesso a far valere le proprie ragioni. Nella prospettiva di incentivare l'attività economica di piccole e medie imprese e la relativa concorrenza nel mercato digitale, la UE ha rilasciato un pacchetto di misure, tra le quali va segnalata la Direttiva 770/2019/UE, relativa ad alcuni aspetti dei contratti di fornitura di contenuto digitale e dei servizi digitale, e la Direttiva 771/2019/UE, relativa a determinati aspetti dei contratti di vendita dei beni. La disciplina è sicuramente tale da garantire una effettiva tutela al consumatore. Ma si intravede un problema nella solita circoscrizione dell'àmbito di applicazione al solo consumatore, con esclusione dunque dei non consumatori, ossia le imprese, specie piccole e medie, e i professionisti che si trovino nelle transazioni *online* in una posizione di debolezza contrattuale.

Si osserva che detta posizione del legislatore sembra trovare una battuta di arresto nella decisione Costea della CGUE che ha elaborato linee interpretative nuove, utili per estendere le tutele consumeristiche oltre le rigide maglie della definizione legislativa[143]. Si auspica dunque di applicare la normativa di tutela anche ai non consumatori che, in concreto, si trovino in una posizione di debolezza.

In proposito, si osserva che la Corte di Giustizia in realtà non ha innovato la definizione di consumatore. Il concetto europeo di consumatore è strumentalizzato e funzionalizzato, essendogli assegnato un ruolo attivo nella realizzazione del mercato interno[144]. Siffatti ruolo e funzione possono però essere svolti e adempiuti

143 CGUE, 3 settembre 2015, Causa C-110/14, Costea c. SC Volksbank România SA, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62014CJ0110&from=IT,* la quale ha deciso quanto segue: «L'articolo 2, lettera b), della direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori, deve essere interpretato nel senso che una persona fisica che eserciti la professione di avvocato e stipuli con una banca un contratto di credito nel quale lo scopo del credito non sia specificato può essere considerata un "consumatore", ai sensi di tale disposizione, qualora un simile contratto non sia legato all'attività professionale di detto avvocato. La circostanza che il credito sorto dal medesimo contratto sia garantito da un'ipoteca concessa da tale persona in qualità di rappresentante del suo studio legale e gravante su beni destinati all'esercizio della sua attività professionale, quale un immobile appartenente a detto studio legale, non è in proposito rilevante».

144 Micklitz, H.-W.: *Vorbemerkung Vor §§ 13, 14,* in *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, vol. I, *Allgemeiner Teil*, 4 ed., München, 2001, p. 369 s., individua due fasi nella concezione europea del consumatore, quella prima del 1986, ispirata al modello sociale di protezione contraente debole e racchiusa nel «Verbraucher*schutz*recht» (corsivo dell'a.), e quella successiva, fondata sul moderno concetto funzionale di consumatore che «wird instrumentalisiert und funktionalisiert» ed espressa nel «Verbraucherrecht» inteso come «Marktverhaltensrecht» (cfr., in proposito, Reich, N. e Micklitz, H.-W.: *Europäisches Verbraucherrecht*, 4 ed., Baden-Baden, 2003, p. 281 ss.). Cosí anche Heiss, H.: *Verbraucherschutz im Binnenmarkt: Art. 129a EGV und die wirtschaftlichen Verbraucherinteressen*, in *ZEuP*, 1996, p. 641 ss., il quale discorre di «Nachfragefreiheit des Verbrauchers» e della «Wichtigkeit des grenzüberschreitenden Agierens des Verbrauchers für das reibungslose Funktionieren des Binnenmarktes» e rileva che la piú recente politica europea dei consumatori «betont immer mehr die Rolle des Verbrauchers im Rahmen der Verwirklichung des Binnenmarktes»; Joerges, C. e Brüggemeier, G.: „Europäisierung des Vertragsrechts und Haftungsrechts", in Müller-Graff, P.-C.: *Gemeinsames Privatrecht in der Europäischen Gemeinschaft*, 2

efficacemente soltanto se il consumatore sia consapevole di ciò e normativamente fornito di quelle competenze e di quei poteri in concreto specificamente necessari per l'effettiva attuazione della sua funzione. Secondo tale concezione il consumatore non è soltanto il soggetto strutturalmente piú debole e neppure il soggetto informato ed illuminato, quindi responsabile[145]. Piuttosto, è la persona che consapevolmente adempie la sua funzione nel, e per il mercato interno in virtú dei poteri di volta in volta giuridicamente concessigli[146]. La tutela del consumatore va dunque fondamentalmente letta come disciplina del relativo ruolo di domanda svolto da tale soggetto sul mercato. La «protezione» del consumatore in effetti non si esaurisce nella tutela di questo quale parte debole del rapporto contrattuale. Pur esistendo una parziale sovrapposizione tra tali due problematiche potendo presentarsi il consumatore quale contraente debole, si è tuttavia già da tempo evidenziato che non si può giungere a una loro completa identificazione in quanto, da un lato, il contraente debole può non essere consumatore, mentre, dall'altro, quest'ultimo a volte è preso in considerazione dall'ordinamento non nella veste di contraente[147].

Elementi centrali della figura in esame sono la persona fisica (elemento soggettivo), l'agire per acquistare o cedere un bene o un servizio o prestare una garanzia (elemento oggettivo), lo scopo non imprenditoriale o professionale dell'acquisto o dell'utilizzo (elemento funzionale).

Dal punto di vista dell'elemento soggettivo, la definizione appare restrittiva poiché soltanto la persona fisica può essere qualificata come consumatore o utente. Nelle proposte di iniziativa parlamentare e nelle proposte formulate in sede dottrinale si auspicava invece una definizione più ampia che ricomprendesse anche le persone giuridiche non votate al perseguimento di intenti di lucro, come i comitati e le associazioni di ogni genere.

ed., Baden-Baden, 1999, p. 328, che accolgono l'idea dell'«aktiver Binnenmarkt-Verbraucher» e della sua funzione di «Binnenmarkt-Akteur».

145 Sul concetto di consumatore responsabile assunto dalla giurisprudenza europea, v. Causa C-238/89, Pall Corp., in *Raccolta*, 1990, p. I-4849.

146 Cfr. Micklitz, H.-W.: *Vorbemerkung Vor §§ 13, 14,* cit., p. 370 s.: «Der im Binnenmarktkonzept geforderte Verbraucher muß für die Wahrnehmung seiner Rolle und Funktion erst rechtlich mit den notwendigen Kompetezen und Befugnissen ausgestattet werden. Insofern reicht der Verbraucherbegriff des Binnenmarktes über die freiheitliche Privatrechtsordnung hinaus»; Heinrich, C.: *Formale Freiheit und materiale Gerechtigkeit*, cit., p. 157. In materia di liceità delle misure restrittive della libera circolazione delle merci la Corte di giustizia (Causa C-220/98, Estée Lauder Cosmetics, in *Raccolta*, 2000, p. I-146 s., e Causa C-210/96, Gut Springenheide e Tusky, *ivi*, 1998, p. I-4657) ha assunto quale criterio di valutazione l'aspettiva presunta di un consumatore medio, normalmente informato e ragionevolmente attento ed avveduto.

147 Cosí, Rizzo, V.: *Condizioni generali del contratto e predisposizione normativa*, Esi, Camerino-Napoli, 1983, p. 108 ss. V. anche, per tutti, Roppo, V.: *Contratti standard. Autonomia e controlli nella disciplina delle attività negoziali d'impresa*, Giuffrè, Milano, 1975, p. 153 s.; Mazzoni, C.M.: *Contratti di massa e controlli nel diritto privato*, Giuffrè, Milano, 1975, p. 149 s.

Dalla prospettiva dell'elemento oggettivo la definizione risulta invece formalmente estensiva, in quanto l'espressione consumatore non riguarda solo la persona fisica che "consuma" un bene, ma anche l'utente di un servizio pubblico o privato. È chiaro che quasi in tutti i paesi dell'Unione ed anche nel linguaggio normativo europeo la definizione di consumatore ricomprende implicitamente non solo chi consuma beni, ma anche chi utilizza servizi. Dal punto di vista del diritto italiano la definizione è comunque innovativa poiché l'espressione «servizio» non è definita legislativamente con formule di tenore generale, a differenza di quanto accade per la definizione di «bene», contenuta nell'art. 810 cod. civ., ponendosi cosí la questione della sua individuazione. Poiché nell'accezione di servizio della disciplina europea si includono anche i servizi bancari e i servizi di investimento in valori mobiliari così come i servizi assicurativi, si può ritenere che la disciplina quadro in esame si applichi anche ai consumatori-risparmiatori, ai clienti delle compagnie di assicurazione, ai clienti degli intermediari finanziari e così via, senza limitazioni, salvo quella incentrata sullo scopo dell'acquisto o dell'utilizzazione, che non deve essere riferibile all'attività imprenditoriale e professionale dell'acquirente e dell'utente.

L'elemento funzionale è previsto in negativo potendo cosí rientrare nella definizione qualsiasi tipo di acquisto o di utilizzo di bene o di servizio, purché non destinati a fini professionali o imprenditoriali. La previsione dell'elemento funzionale non pone dunque alcun problema in merito alla qualificazione come consumatore anche del professionista/imprenditore che compia un acquisto o utilizzi un servizio per scopi estranei alla propria attività professionale/imprenditoriale. Questo sembra essere il senso della decisione della CGUE che non ha quindi innovato la nozione di consumatore.

Si può certamente configurare la necessità di estendere le tutele e può essere anche condivisa. Tuttavia, si ritiene che questa estensione non possa sfociare in una totale parificazione tra professionisti e consumatori per due ragioni. In primo luogo, la situazione delle piccole e medie imprese e dei professionisti non è sempre parificabile a quella dei consumatori in quanto spesso non vi sono né quelle posizioni strutturali di debolezza, né le asimmetrie informative che fondano invece gli interventi giusconsumeristici; là dove invece dette posizioni si rinvengono, ben può essere ampliata la platea dei destinatari delle tutele, come peraltro già è avvenuto, ad esempio, nel caso delle pratiche commerciali scorrette e nel settore finanziario, ove si discorre genericamente di clienti al dettaglio. In secondo luogo, la situazione di detti soggetti è fondamentalmente diversa e per loro sembra più opportuno destinare una disciplina di settore che risolva specificamente i loro problemi, come accaduto ad esempio con la legge sulla subfornitura, nel rispetto del principio di proporzionalità.

IX. L'EVOLUZIONE TECNOLOGICA E LE TUTELE NEL PRISMA DEL PRINCIPIO DI SOSTENIBILITÀ.

L'impatto delle nuove tecnologie sulla realtà e, di riflesso, sull'ordinamento giuridico è molto forte, introducendo trasformazioni epocali che incidono profondamente sul tessuto sociale e imprenditoriale. Tra l'altro, cambiano i paradigmi di funzionamento dei mercati, mutano gli equilibri socioeconomici della società, emergono nuove esigenze di tutela. In presenza di siffatte evoluzioni, una delle difficoltà da affrontare è quella di trovare una sintesi normativa efficace che sia in grado di comporre gli opposti interessi all'interno di una visione globale della realtà che non sia schiacciata sul presente o sul futuro prossimo, ma che sia capace di guardare lontano. Il richiamo è dunque alla sostenibilità, assurta oggi a vera e propria chiave di lettura del contesto temporale e dei mutamenti sociali che investe pressoché tutti gli àmbiti tematici che vanno, tra l'altro, dall'ambiente all'economia, dall'agricoltura al turismo, dalla *governance* societaria alle stesse strutture della democrazia.

Lo strumento normativo che consente di conciliare le diverse esigenze nell'ottica di lungo periodo è il principio di sostenibilità, menzionato già da tempo nell'art. 3, § 3, TUE e di recente introdotto negli artt. 9, comma 3, e 41, comma 2, cost. La disposizione unionale affida all'Unione il compito di adoperarsi «per lo sviluppo sostenibile dell'Europa, basato su una crescita economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente. Essa promuove il progresso scientifico e tecnologico». La Costituzione assegna alla Repubblica il compito di tutelare «l'ambiente, la biodiversità e gli ecosistemi, anche nell'interesse delle future generazioni» e prescrive che l'iniziativa economica privata, libera, non possa svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana, alla salute e all'ambiente. Come emerge da queste disposizioni, il concetto di sviluppo sostenibile non è facilmente definibile in maniera univoca.

A livello internazionale, il principio lo si ritrova nel celebre rapporto del 1987 della Commissione Bruntland delle Nazioni Unite[148], intitolato «Report of the World Commission on Environment and Development: Our Common Future»[149]. Il rapporto ne elabora una prima definizione identificando come sostenibile lo «sviluppo che soddisfi i bisogni della generazione presente senza compromettere la possibilità delle generazioni future di soddisfare i propri». Da allora, la sostenibilità

148 Sulle attività dell'ONU in tema, v. *https://sustainabledevelopment.un.org*.

149 Il documento è consultabile in *https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf*.

è diventata un canone etico e politico che ha conquistato ampi spazi nelle scelte politiche e nelle decisioni giuridiche e normative, anche di livello costituzionale[150].

Secondo il glossario predisposto dall'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), la sostenibilità è «la continuità dei benefici prodotti da un intervento di sviluppo dopo la sua conclusione e la probabilità di ottenere benefici di lungo periodo. Il criterio verifica inoltre la resistenza al rischio dei flussi di benefici netti nel corso del tempo»[151].

A livello interno, l'art. 3 *quater*, comma 1, d.lgs. n. 152 del 2006 (Codice dell'ambiente), intitolato «Principio dello sviluppo sostenibile», dispone che «Ogni attività umana giuridicamente rilevante ai sensi del presente codice deve conformarsi al principio dello sviluppo sostenibile, al fine di garantire che il soddisfacimento dei bisogni delle generazioni attuali non possa compromettere la qualità della vita e le possibilità delle generazioni future».

Il concetto, rispetto alle sue prime versioni, ha fatto registrare una profonda evoluzione che, partendo da una visione centrata preminentemente sugli aspetti ecologici, è approdata verso un significato più globale, che tiene conto, oltre che della dimensione ambientale, di quella economica e di quella sociale. I tre aspetti sono stati comunque considerati in un rapporto sinergico e sistemico e, combinati tra loro in diversa misura, sono stati impiegati per giungere a una definizione di progresso e di benessere che superasse in qualche modo le tradizionali misure della ricchezza e della crescita economica basate sul PIL. La sostenibilità, dunque, ha oggi molte accezioni: ambientale, finanziaria, economica, istituzionale, socioculturale, tecnologica.

La sostenibilità ambientale indica se e quanto l'iniziativa produce effetti negativi sull'ambiente e come affronta le problematiche ambientali, facendo particolare riferimento a quanto previsto in materia dalla normativa vigente, che prevede la c.d. Valutazione di Impatto Ambientale (VIA) e la Valutazione Strategica (VAS).

150 Cfr., per tutti, D'Aloia, A.: *Sostenibilità e responsabilità sociale delle imprese. Note preliminari*, in AA. VV.: *Sostenibilità, responsabilità sociale d'impresa e nuove aspettative dei consumatori: nuovi paradigmi di qualità?* (a cura di M. Cocconi), Napoli, 2019, p. 7 ss.

151 Per un primo riferimento, da varie prospettive, sulla sostenibilità, v. Perlingieri, P.: "«Sostenibilità», ordinamento giuridico e «retorica dei diritti»", *Foro nap.*, 2020, p. 101 ss.; *Sostenibilità, responsabilità sociale d'impresa e nuove aspettative dei consumatori: nuovi paradigmi di qualità?*, cit.; Caterini, E.: *Sostenibilità e ordinamento civile. Per una riproposizione della questione sociale*, Esi, Napoli, 2018; Bologna, G.: *Manuale della sostenibilità. Idee, concetti, nuove discipline capaci di futuro*, 2 ed., Giuffrè, Milano, 2008; D'Aloia, A. e Bifulco, R. (a cura di): *Un diritto per il futuro. Teorie e modelli dello sviluppo sostenibile e della responsabilità intergenerazionale*, Esi, Napoli, 2008; Castellucci, L.: "Sviluppo sostenibile", *Dizionario di Economia e Finanza*, Treccani, Torino, 2012; Daly, H.E.: *Oltre la crescita. L'economia dello sviluppo sostenibile*, Roma, 2001; Davico, L.: *Sviluppo sostenibile. Le dimensioni sociali*, Roma, 2004; Dedeurwaerdere, T.: *Sustainability Science for Strong Sustainability*, Université catholique de Louvain, 2013; Griggs, D., Stafford-Smith, M., Gaffney, O., Rockström, J., Öhman, M. C., Shyamsundar, P., Steffen, W., Glaser, G., Kanie, N. e Noble, I.: "Policy: Sustainable development goals for people and planet", *Nature*, n. 495, 20 marzo 2013, p. 305 ss.

La sostenibilità finanziaria si concentra sull'equilibrio finanziario dell'iniziativa dal punto di vista unicamente del soggetto responsabile della sua esecuzione e del suo funzionamento, che deve accertare l'equilibrio tra entrate ed uscite finanziarie in modo da evitare che l'iniziativa si blocchi o fallisca per mancanza di liquidità finanziaria.

La sostenibilità economica fa riferimento, invece, all'intera collettività di riferimento del progetto o iniziativa, prendendo in considerazione i costi e ricavi o benefici di natura economica e sociale dell'intervento, presenti e futuri, non legati dunque alle uscite o entrate di cassa. In sostanza, si guarda alla possibilità per i beneficiari di accedere ai servizi o prodotti, alle modalità e grado di copertura dei costi, alla capacità di sopportare lo sfasamento tra risultati economici e impegni finanziari.

La sostenibilità socioculturale si focalizza sulla rispondenza del progetto o dell'iniziativa ai bisogni e alle aspettative del gruppo destinatario dell'intervento stesso e della collettività in generale. In particolare, analizza come le diverse componenti della società siano coinvolte e ottengano benefici dal progetto, là dove le persone non sono viste come meri beneficiari passivi, ma come protagonisti attivi del cambiamento politico. Implicitamente, il termine assume il concetto di equa distribuzione delle condizioni di benessere umano (sicurezza, salute, istruzione), quindi del rafforzamento delle capacità e opportunità di tutta la popolazione.

Il concetto di sviluppo sostenibile è dunque una categoria giuridica ancora imperfetta nei contenuti e nella capacità vincolativa a causa della sua dimensione olistica, essendo trasversale a tutte le grandi aree tematiche. Ma si è già affermato quale un principio generale del diritto che, come tale, deve essere necessariamente elaborato e maggiormente puntualizzato nei contenuti.

Come evidenziato da autorevole dottrina, parlare di sviluppo sostenibile significa innanzi tutto chiedersi qual è il senso del progresso[152], prendendo atto che le decisioni e i comportamenti di oggi avranno una influenza sul futuro di cui occorre tenere conto assumendosene la responsabilità. In tal senso, due sono le implicazioni fondamentali del principio in esame. Sostenibilità significa, in primo luogo. guardare al futuro con una attenzione protettiva, custodiale e pertanto inserire nel sistema giuridico un dovere di protezione degli interessi delle generazioni future. Il costituzionalismo contemporaneo di regge su due pilastri: ragionevolezza e consapevolezza che diritti e doveri fanno parte di un'unica visione dell'uomo e di un disegno unitario di società: il futuro è dunque un bene giuridico da proteggere e la sostenibilità ne è lo strumento di protezione. In secondo

152 D'Aloia, A.: "Sostenibilità e responsabilità sociale delle imprese. Note preliminari", cit., p. 8; Id.: "Generazioni future (diritto costituzionale)", *Enc. Dir., Annali*, IX, Milano, 2016, p. 331 ss.

luogo, alla luce della Costituzione la sostenibilità è una «impresa "collettiva"» che ha bisogno di condivisione, partecipazione, impegno da parte di tutti i soggetti pubblici e privati dell'ordinamento. Quindi anche dei soggetti economici e, in particolare; delle imprese che hanno in tal senso una grande responsabilità, fondata sul rovesciamento virtuoso dell'art. 41, comma 2, cost. per il quale il limite della sicurezza e dignità umana diviene impegno di costruire una società più giusta ed inclusiva per oggi e per domani grazie ad un'attività economica ispirata al principio di sostenibilità[153].

La sostenibilità deve dunque essere il principio di riferimento per bilanciare all'interno degli interventi le esigenze di tutela della persona, dell'ambiente in tutte le sue declinazioni, del consumatore e dell'impresa con gli interessi del sistema economico e finanziario in una prospettiva di medio e lungo periodo che sia volta a garantire la continuità dei benefici prodotti da un intervento di sviluppo dopo la sua entrata in vigore e la probabilità di ottenere benefici di lungo periodo di natura economica e sociale. Questa potrebbe essere la linea da seguire per evitare regolazioni contraddittorie e incerte quanto agli effetti che si vogliono produrre e i soggetti che si pensa di tutelare, omettendo una - oramai - imprescindibile visione duratura da porre alla base degli interventi. Effetti che nel breve periodo possono forse proteggere l'impresa, il consumatore e, più in generale, la persona, ma nel tempo possono ripercuotersi contro i beneficiari per le reazioni indotte negli *stakeholder* e nel sistema da effetti negativi non sufficientemente ponderati: si tratta di soggetti e di mercati che sono, tutti, comunque parte del complesso sistema impresa-consumatore-mercato-ambiente-società dalla cui considerazione complessiva e prospettica non è (più) possibile prescindere.

In questa ottica operativa di interventi normativi improntati sulla sostenibilità quale criterio di bilanciamento tra contrapposti interessi e principi, una ulteriore importante indicazione di metodo potrebbe essere quella che si coglie in un interessante studio sulla rinnovata concezione economica del rapporto tra pubblico e privato che devono cooperare sulla base di un obiettivo comune[154]. Si afferma che, al momento, è raro trovare governi che operino con obiettivi chiari e che magari collaborino tra loro, come anche dovrebbero collaborare pubblico e privato ma con fini delineati e condivisi. Il problema si pone quando lo Stato finanzia privati o autorizza *outsourcing* che però non hanno *target* condivisi. Lo studio rileva che si assiste ad una "ultrafinanziarizzazione" del settore privato: le aziende top del S&P 500 hanno recentemente investito 4 trilioni di dollari nel riacquisto di loro azioni o in *bonus*, ma non nell'economia. Gli investimenti, gestiti da pubblico e privato, devono invece avere un obiettivo chiaro e comune per tutte le istituzioni

153 D'Aloia, A.: *o.c.*, p. 8 ss.

154 V. l'interessante studio di Mazzucato, M.: *Mission Economy. A Moonschoot Guide to Changin Capitalism*, London, 2021.

e i soggetti coinvolti. Per questo bisogna reinventare il capitalismo, che è in crisi in quanto la finanza oramai finanzia sé stessa, molte aziende si basano principalmente sulle trimestrali e i governi esitano invece di essere veri *leader*. Vi è poi il nodo del cambiamento climatico, che impone una rivoluzione del sistema. Per questo, per ripartire anche dopo la pandemia, i governi, le imprese, la finanza e l'economia dovrebbero basarsi su regole competitive e su un investimento pubblico più strategico. Pertanto, servono una *leadership* con una visione, innovazione, agilità e flessibilità organizzative, ma soprattutto un'alleanza vera tra Stato e settore privato, non solo a livello finanziario, ma anche in termini di obiettivi e sfide comuni.

Quanto ora scritto induce a spostare l'attenzione sulle imprese che sono i motori primari dei processi globali. Le loro azioni generano effetti positivi o negativi sulla sostenibilità economica e sugli obiettivi sostenibili. Non sorprende quindi che negli ultimi anni il ruolo delle corporazioni, principalmente delle multinazionali, sia stato oggetto di studi giuridici e politici[155]. Tale valutazione ha portato alla definizione dei nuovi principi sulla responsabilità sociale d'impresa (CSR) e ne ha favorito l'applicazione nelle legislazioni a livello internazionale e nazionale. Tuttavia, la CSR non è sufficiente per impedire alle imprese di danneggiare l'ambiente e di incidere a volte negativamente sulla crescita della società, soprattutto nel lungo periodo. Occorre in proposito osservare che le imprese possono agire in diversi paesi e sono legalmente considerate come gli attori in grado di perseguire o minacciare obiettivi di lungo termine. Storicamente le corporazioni sono state create come persone giuridiche per superare i limiti di agenzia dei semplici individui. Di conseguenza, la loro azione è stata significativa, a volte più dei governi colpiti dall'instabilità politica, per i processi economici e le trasformazioni durevoli che in qualche modo oggi rappresentano una minaccia per il pianeta e le generazioni future. Questa caratteristica intrinseca, che dipende dalla loro natura giuridica, è ovviamente rilevante quando si tratta di sostenibilità e obiettivi sostenibili che, a loro volta, consistono nel soddisfare i bisogni delle generazioni attuali senza compromettere i bisogni delle generazioni future, garantendo al tempo stesso un equilibrio tra crescita economica, tutela dell'ambiente e benessere sociale. Va evidenziato che la prima forma corporativa non è stata creata per scopi commerciali o, per lo meno, la teoria dell'incorporazione non mirava a servire direttamente scopi economici. Tracce di questa natura originaria si colgono in alcuni elementi della forma societaria, nello specifico la perpetuità e le finalità.

155 Sulla sostenibilità nel diritto societario, v. gli interessanti studi di Anello, G.: "Perpetuals by Nature. The Moral Core of Corporations", *Diacronia*, 2, 2022, (bozza dell'articolo gentilmente concessa dall'autore) e Anello, G., Arafa, M. e Gramitto Ricci, S.A.: "Sacred Corporate Law", *Seattle University Law Review*, vol. 45, 2021, p. 413 ss., di cui le considerazioni nel testo sono debitrici; in argomento, da diverse prospettive, v. Imbruglia, D.: "Mercato unico sostenibile e diritto dei consumatori", *Pers. merc.*, 2021, 3, p. 495 ss.; Tombari, U.: *"Potere" e "interessi" nella grande impresa azionaria*, Giuffrè, Milano, 2021; Id.: "Corporate Purpose e Diritto societario: scopo sociale: dalla supremazia degli interessi dei soci" alla libertà di scelta dello "scopo sociale"?", *Riv. soc.*, 2021, 1, p. 1 ss.; Capaldo, G.: "Linee evolutive in tema di soggetti per una società sostenibile", *Pers. merc.*, 2020, 4, p. 334 ss.

Siffatta natura continua a dettare il successo di questo strumento giuridico: la combinazione di lunga durata e la centralità degli interessi ha giustificato l'impresa nel suo insieme in quanto strumento perfetto per superare i limiti temporali della vita umana e raggiungere obiettivi di vasta portata. Non è un caso che, secondo questa logica, la forma societaria "moderna" sia stata definita come un soggetto giuridico autonomo con propri interessi, non influenzato da quelli di altri. Al giorno d'oggi, il profilo perpetuo della forma societaria originaria appare ancora trascurato. La forma corporativa è stata adottata nel diritto commerciale in modo del tutto acritico, senza alcuna approfondita revisione delle sue peculiari origini escatologiche e delle sue conseguenze sull'agenzia legale e sui suoi poteri. Anche se le società sono state considerate entità efficienti, auto-rinnovantisi e "immortali" sin dalle loro origini, ci sono solo poche norme riguardanti le implicazioni per le società commerciali dell'agire in una prospettiva di lungo termine, e sono pochi gli studi sulla morale e sulle implicazioni giuridiche del raggio d'azione perpetuo delle persone giuridiche commerciali. Nell'esperienza angloamericana il diritto, i giudici e gli avvocati hanno ribadito la dottrina che una società è un'entità "eterna", ma nonostante l'enorme effetto che la perpetuità ha avuto nella storia del diritto le sue implicazioni nel settore economico di oggi sono in gran parte sotto esame. Per questo motivo, la natura perpetua delle società commerciali dovrebbe essere studiata e collegata alla sostenibilità e agli obiettivi sostenibili, giacché tale perpetuità porta con sé conseguenze sociali ed economiche ampiamente sottovalutate. È quindi importante evidenziare la connessione ontologica tra perpetuità e forma corporativa per individuarne le implicazioni allo stato attuale e governarle. Un'indagine su questo argomento può offrire una visione più profonda delle implicazioni sociali e a lungo termine della teoria delle corporazioni. Ma può rivelarsi utile anche per motivi pratici: attualmente, una serie di questioni relative alla teoria della corporazione dipendono dai presupposti del comportamento degli attori legali coinvolti nell'attività di impresa quali ad esempio la visione di lungo e breve periodo, i problemi di agenzia, la separazione e la titolarità della proprietà, il primato dei soci.

Oltre agli aspetti sopra evidenziati, vi è anche un'altra dimensione applicativa del principio di sostenibilità che non può non manifestarsi in sede ermeneutica e applicativa, considerato il suo rango di principio ancorato nel TFUE e nella Costituzione.

A proposito della responsabilità civile, autorevole dottrina osservava il «punto centrale della responsabilità oggi, infatti, non è tanto l'*an* (l'individuazione della meritevolezza dell'interesse - là dove ormai alcuni interessi di rilevanza costituzionale non possono essere tenuti fuori dalla tutela anche risarcitoria), ma il

quantum damni in una prospettiva di solidarietà sostenibile, attenta al bilanciamento dei principi e valori costituzionali»[156].

Altro spunto sin coglie a proposito di quanto scritto in un altro contesto tematico e in citazione di risalente letteratura tedesca si afferma relazione alla giurisprudenza che «sacra non è la legge ma il diritto e il giudice a sua volta è subordinato solamente al diritto. In una visione ottimistica quindi la legge dovrebbe possedere tutti quei caratteri per sostenere una costruzione sostenibile del diritto positivo»[157].

La sostenibilità sembra dunque assumere anche il ruolo di strumento ermeneutico che orienta l'operatore verso soluzioni applicative del diritto che siano anche sostenibili, ossia porta l'interprete ad individuare un punto di equilibrio fra gli interessi contrapposti che travalichi la dimensione del caso concreto proiettandolo in una visione sistemica rivolta al futuro attraverso un bilanciamento che tenga conto non soltanto degli interessi delle parti, ma anche di interessi generali di natura sistemica che li salvaguardi nel medio nel lungo periodo.

Questa sembra essere oggi la sfida per gli operatori del diritto, consistente nella valutazione dal punto di vista della sostenibilità della disciplina applicabile al caso concreto quale *enforcement* del relativo principio.

156 Così, Perlingieri, P.: "Le funzioni della responsabilità civile", *Rass. dir. civ.*, 2011, p. 118.

157 Favale, R.: "Nullità di protezione dei contratti d'investimento mobiliare e l'ascesa del principio di buona fede", in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), Esi, Napoli, 2020, p. 454. V. anche per le indicazioni interessanti sul tema, Goldschmidt, J.: "Gesetzesdämmerung", *JW*, 1924, p. 245 ss.

BIBLIOGRAFIA

AA. VV.: *Diritto dell'informatica*, (a cura di F. Delfini e G. Finocchiario), 2014, Torino

Alpa, G. (a cura di): *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020

Amidei, A.: "La proposta di Regolamento UE per un Artificial Intelligence Act: prime riflessioni sulle ricadute in tema di responsabilità", *Tecnologie e Diritto*, 2022, 1, p. 1 ss.

Anello, G., Arafa, M. e Gramitto Ricci, S.A.: "Sacred Corporate Law", *Seattle University Law Review*, vol. 45, 2021, p. 413 ss.

Anello, G.: "Perpetuals by Nature. The Moral Core of Corporations", *Diacronia*, 2, 2022

Ashley, K.D.: *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambrigde University Press, 2014

Barenghi, A.: "Il dibattito tedesco sulla fideiussione bancaria: a proposito di un recente saggio", *Banca borsa tit. cred.*, 1995, p. 101 ss.

Barenghi, A.: "Una pura formalità. A proposito di limiti e di garanzie dell'autonomia privata in diritto tedesco", *Nuova giur. civ. comm.*, 1995, I, p. 202 ss.

Battaglini, R. e Giordano, M.T. (a cura di): Blockchain e smart contract. *Funzionamento, profili giuridici e internazionali, applicazioni pratiche*, Giuffrè, Milano, 2019

Bellomia, V.: "Il contratto intelligente: questioni di diritto civile", *www.judicium.it/contratto-intelligente-questioni-diritto-civile/*, 2020

Benedetti, A.M.: "Contrattazione, algoritmi e diritto civile transnazionale: cinque questioni e due scenari", in *Rapporti civilistici e intelligenze artificiali*, Atti Convegno SISDIC, Napoli, 2021

Bologna, G.: *Manuale della sostenibilità. Idee, concetti, nuove discipline capaci di futuro*, 2 ed., Giuffrè, Milano, 2008

Börding, A., Jülicher, T., Röttgen, C. e von Schönfeld, M.: *Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht: Praxis und Rechtsdogmatik*, in *Computer und Recht*, 2017, p. 134-140

Borruso, R.: *Computer e diritto*, II, *Problemi giuridici dell'informatica*, Giuffrè, Milano, 1988

Bourque, S. e Fung Ling Tsui, S.: *A Lawyer's Introduction to Smart Contracts*, in *Lask: Scientia Nobilitat*, 2014, p. 4-23

Brägelmann, T. e Kaulartz, M. (a cura di): *Rechtshandbuch Smart Contracts*, München, 2019

Brägelmann, T.: *Incomplete Contracts: Eine Sisyphusaufgabe für Legal Tech-Fans*, in *REthinking Law*, 2018, 1, p. 34 ss.

Bravo, F.: *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018

Buchleitner, C. e Rabl, T.: *Blockchain und Smart Contracts*, in *ecolex*, 2017, p. 4-14

Capaldo, G.: "Linee evolutive in tema di soggetti per una società sostenibile"*, Pers. merc.*, 2020, 4, p. 334 ss.

Casey, A.J. e Niblett, A.: *Self-Driving Contracts*, in 43 *Journal of Corporation Law*, 2017, p. 1-33

Casonato, C. e Marchetti, B.: "Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale", *Bio-Law Journal*, 2021, 3, p. 415 ss.

Castellucci, L.: "Sviluppo sostenibile", *Dizionario di Economia e Finanza*, Treccani, Torino, 2012

Catchlove, P.: *Smart Contracts: A New Era of Contract Use*, ssrn.com/abstract=3090226

Caterini, E.: "Il «germe» dell'intelligenza artificiale", in AA. VV.: *Scritti in onore di Antonio Flamini*, I, (a cura di R. Favale e L. Ruggeri), Esi, Napoli, 2020, p. 211 ss.,

Caterini, E.: *L'intelligenza artificiale «sostenibile» e il processo di socializzazione del diritto civile*, Napoli, 2020

Caterini, E.: *Sostenibilità e ordinamento civile. Per una riproposizione della questione sociale*, Esi, Napoli, 2018

Clarizia, R. (a cura di): *I contratti informatici*, in *Trattato dei contratti* diretto da P. Rescigno e E. Gabrielli, Torino, 2007

Clarizia, R.: *Informatica e conclusione del contratto*, Giuffrè, Milano, 1985

D'Alessio, A.: "La responsabilità civile dell'intelligenza artificiale antropocentrica", *Persona e merc.*, 2022, 2, p. 243 ss.

D'Aloia, A. e Bifulco, R. (a cura di): *Un diritto per il futuro. Teorie e modelli dello sviluppo sostenibile e della responsabilità intergenerazionale*, Esi, Napoli, 2008

D'Aloia, A.: "Generazioni future (diritto costituzionale)", *Enc. Dir., Annali*, IX, Milano, 2016, p. 331 ss.

D'Aloia, A.: *Sostenibilità e responsabilità sociale delle imprese. Note preliminari*, in AA. VV.: *Sostenibilità, responsabilità sociale d'impresa e nuove aspettative dei consumatori: nuovi paradigmi di qualità?* (a cura di M. Cocconi), Napoli, 2019, p. 7 ss.

d'Avack, L.: "La rivoluzione tecnologica e la nuova era digitale: problemi etici", in Ruffolo, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 23

Daly, H.E.: *Oltre la crescita. L'economia dello sviluppo sostenibile*, Roma, 2001

Davico, L.: *Sviluppo sostenibile. Le dimensioni sociali*, Roma, 2004

De Filippi, P. e Wright, A.: *Blockchain and the Law: The Role of the Code*, Harvard University Press 2018

De Franceschi, A.: *La circolazione dei dati personali tra privacy e contratto*, Esi, Napoli, 2017, p. 67 ss.

De Mari Casareto Dal Verme, T.: "Verso la nuova Product Liability Directive: la proposta della Commissione europea del 28 settembre 2022 per una nuova direttiva sulla responsabilità da prodotto difettoso che abroga la Direttiva 85/374/CEE", *Persona e mercato*, 2022, 1, p. 502 ss.

Dedeurwaerdere, T.: *Sustainability Science for Strong Sustainability*, Université catholique de Louvain, 2013

Delfini, F.: "Il commercio elettronico", in Vaccà, C. (a cura di): *Il commercio elettronico*, Giuffrè, Milano, 1999, p. 27 ss.

Delfini, F.: *Contratto telematico e commercio elettronico*, Giuffrè, Milano, 2002

Di Giovanni, F.: "Sui contratti delle macchine intelligenti", in Ruffolo, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, p. 251 ss.

Di Gregorio, V.: "Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie", *Danno e resp.*, 2022, 1, p. 51 ss.

di Martino, A.: "Intelligenza artificiale e decisione amministrativa automatizzata", *Tecn. dir.*, 2020, 1, p. 83 ss.

Di Nella, L.: "La tutela del garante nell'esperienza tedesca e negli ordinamenti europeo e italiano: la Mithaftung von Nahbereichpersonen", *Rassegna di diritto civile*, 2012, 4, p. 1191 ss.

Di Nella, L.: "Smart Contract, Blockchain e interpretazione dei contratti", *Rass. dir. civ.*, 2022, p. 48 ss.

Di Sabato, D.: "Autonomia negoziale e distibuted ladger technology", in Valentino, D. (a cura di): *Nuovi contratti della* digital economy, *Singoli contratti. Leggi collegate,* II, Commentario UTET, Torino, 2 ed., 2020, p. 245 ss.

Di Sabato, D.: "Gli Smart contracts: robot che gestiscono il rischio contrattuale", *Contr. impr.*, 2017, p. 378 ss.

Di Sabato, D.: "I dati non sensibili tra libero accesso e appartenenza pubblica necessaria!, in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), I, cit., p. 407 ss.

Djazayeri, A.: *Rechtliche Herausforderungen durch Smart Contracts*, in *jurisPR-BKR*, 2016, 12, no. 1

Durovic, M. e Janssen, A.: *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, *European Review of Private Law* (ERPL), p. ss.

Durovic, M. e Janssen, A.: *The Formation of Smart Contracts and Beyond: Shaking the Fundamentals of Contract Law?*, in *https://www.researchgate.net/publication/327732779_The_Formation_of_Smart_Contracts_and_Beyond_Shaking_the_Fundamentals_of_Contract_Law*

Favale, R.: "Nullità di protezione dei contratti d'investimento mobiliare e l'ascesa del principio di buona fede", in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), Esi, Napoli, 2020, p. 454.

Federico, A.: "Equilibrio contrattuale e contrattazione algoritmica", in *Rapporti civilistici e intelligenze artificiali*, Atti Convegno SISDIC, Napoli, 2021

Finck, M.: *Blockchain Regulation and Governance in Europe*, Cambridge, 2019, p. 161 ss.

Finck, M.: *Blockchains: Regulating the Unknown*, in *German Law Journal*, 2018, 19, p. 665-691

Finocchiaro, G. e Bomprezzi, C.: "A legal analysis of the use of blockchain technology for the formation of smart legal contracts", *Riv. dir. media*, 2020, 2, (*http://www.medialaws.eu/rivista/a-legal-analysis-of-the-use-of-blockchain-technology-for-the-formation-of-smart-legal-contracts/*), p. 1 ss.

Finocchiaro, G.: "Intelligenza artificiale e responsabilità", *Contr. e impresa*, 2020, 2, p. 713 ss.

Finocchiaro, G.: *I contratti informatici*, in *Tratt. Dir. comm. e dir. pubbl. econ.* diretto da F. Galgano, XXII, Padova, 1997

Follieri, L.: *Il contratto concluso in* Internet, Esi, Napoli, 2005

Franzoni, M.: "Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale", *Juscivile*, 2021, 1, p. 4 ss.

Frattari, F.: "Robotica e responsabilità da algoritmo. Il processo di produzione dell'intelligenza artificiale", *Contr. impr.*, 2020, 1, p. 458 ss.

Fries, M.: "PayPal Law and Legal Tech - Was macht die Digitalisierung mit dem Privatrecht?", *Neue Juristische Wochenschrift*, 2016, p. 2862 ss.

Fries, M. e Paal, B.P. (a cura di): *Smart Contracts*, Tübingen, 2019, p. 1 ss.

Gambini, M.: "Il danno (patrimoniale e non patrimoniale) da trattamento illecito di dati personali", in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), I, cit., p. 529 ss.

Gambino, A.: "I sette vizi capitali dei giudici-robot (tra blockchain e AI)", *www.agendadigitale.eu/cultura-digitale/i-sette-vizi-capitali-dei-giudici-robot-tra-blockchain-e-ai*, 11 dicembre 2018

Gambino, A.M.: "La circolazione dei dati personali, la configurabilità di un mercato e i diritti fondamentali", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, cit., p. 45 ss.

Giaccaglia, M.: "Considerazioni su Blockchain e smart contracts (oltre le criprovalute)", *Contr. impr.*, 2019, p. 944 ss.

Giaccaglia, M.: "Gli Smart Contracts. Vecchi e nuovi(?) paradigmi nella prospettiva della protezione dei consumatori", www.dimt.it/wp-content/uploads/2020/08/Giaccaglia-SmartContracts-completo.pdf

Giannantonio, E.: *Diritto dell'informatica*, Giuffrè, Milano, 1997

Giannantonio, E.: *Manuale di diritto dell'informatica*, Cedam, Padova, 1994

Giannone Codiglione, G.: "I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy", *Dir. inf.*, 2017, p. 418 ss.

Giova, S.: *La conclusione del contratto via* Internet, Esi, Napoli, 2000

Gless, S. e Seelmann, K. (a cura di): *Intelligente Agenten und das Recht,* Baden-Baden, 2016

Goldschmidt, J.: "Gesetzesdämmerung", *JW,* 1924, p. 245 ss.

Griggs, D., Stafford-Smith, M., Gaffney, O., Rockström, J., Öhman, M. C., Shyamsundar, P., Steffen, W., Glaser, G., Kanie, N. e Noble, I.: "Policy: Sustainable development goals for people and planet", *Nature*, n. 495, 20 marzo 2013, p. 305 ss.

Guggenheim, N.: *The Potentional of Blockchain for the Conclusion of Contracts*, in Schulze, R., Staudenmeyer, D. e Lohse, S. (a cura di): *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps,* Baden-Baden, 2017, p. 83-97

Harari, Y.N.: *Homo Deus. Eine Geschichte von Morgen*, traduzione dall'inglese di A. Wirthensohn, 2017, München, p. 465

Hassan, S. e De Filippi, P.: "The Expansion of Algorithmic Governance: From Code is Law to Law is Code", *Field Actions Science Reports The journal of field actions*, *Special Issue* 17|2017, *Artificial Intelligence and Robotics in the City,* scaricabile alla *URL: https://journals.openedition.org/factsreports/4518*

Heckelmann, M.: *Zulässigkeit und Handhabung von Smart Contracts*, in *NJW*, 2018, p. 504 ss.

Heiss, H.: *Verbraucherschutz im Binnenmarkt: Art. 129a EGV und die wirtschaftlichen Verbraucherinteressen*, in *ZEuP,* 1996, p. 641 ss.

Iaselli, M.: "Consiglio di Stato: quando si può parlare di intelligenza artificiale?", *www.altalex.com/documents/news/2021/12/10/consiglio-di-stato-quando-si-puo-parlare-di-intelligenza-artificiale*

I-H Hsiao, J.: *Smart Contract on the Blockchain-Paradigm Shift for Contract Law*, in *US-China Law Review*, 2017, 14, p. 685-694

Imbruglia, D.: "Mercato unico sostenibile e diritto dei consumatori", *Pers. merc.*, 2021, 3, p. 495 ss.

Jacobs, C. e Lange-Hausstein, C.: *Blockchain und Smart Contracts: zivil- und aufsichtsrechtliche Bedingungen*, in *IT-Rechts-Berater (ITBR)*, 2017, p. 10-15

Joerges, C. e Brüggemeier, G.: „Europäisierung des Vertragsrechts und Haftungsrechts", in Müller-Graff, P.-C.: *Gemeinsames Privatrecht in der Europäischen Gemeinschaft*, 2 ed., Baden-Baden, 1999, p. 328

Jünemann, M. e Kast, A.: *Rechtsfragen beim Einsatz der Blockchain*, in *Kreditwesen*, 2017, p. 531-536

Kaissis, A.: "Recourse to Courts in times of Alternative Dispute Resolution and Disruptive Technologies", in Apalagaki, C. e Pipsou, L.-M. (a cura di): *Dikaio Choris Synora - Liber Amicorum Athanassios Kaissis*, Atene-Salonicco, 2018., p. 301 ss.

Kaulartz, M. e Heckmann, J.: *Smart Contracts - Anwendung der Blockchain-Technologie*, in *Computer und Recht (CR)*, 2016, p. 618-624

Kaulartz, M.: *Die Blockchain-Technologie: Hintergründe zur Distributed Ledger Technology und zu Blockchain*, in *Computer und Recht (CR)*, 2016, p. 474 ss.

Kaulartz, M.: *Herausforderungen bei der Gestaltung von Smart Contracts*, in *Zeitschrift zum Innovations- und Technikrecht (InTeR)*, 2016, p. 201-206

Langhanke, C. e Schmidt-Kessel, M.: "Consumer data as consideration", *Journal of European Consumer and Market Law*, 2015, p. 218 ss.

Lazzarelli, F.: "E-commerce e contraente debole (non consumatore). Considerazioni sistematiche a margine dei recenti interventi del legislatore UE e della Corte di Giustizia", in AA. VV.: *Scritti in onore di Antonio Flamini* (a cura di R. Favale e L. Ruggeri), I, cit., p. 667 ss.

Lessing, L.: "Code Is Law. On Liberty in Cyberspace", *Harvard Magazine*, 1.1.2000 (*https://www.harvardmagazine.com/2000/01/code-is-law-html*)

LESSING, L.: *Code: And Other Laws of Cyberspace. Version 2.0,* New York, 2006

LINARDATOS, D.: *Smart Contracts – einige klarstellende Bemerkungen*, in *Kommunikation & Recht*, 2018, p. 85 ss.

MANN, M.: *Die Decentralized Autonomous Organization - Ein neuer Gesellschaftstyp? Gesellschaftrechtliche und kollisionsrechtliche Implikationen*, in *Neue Zeitschrift für Gesellschaftsrecht*, 2017, p 1014 ss.

MATERA, D.M.: "Patrimonializzazione dei dati e pratiche commerciali scorrette", *Tecnologie e Diritto*, 2022, 1, p. 155 ss.

MAUGERI, M.: Smart contracts e *disciplina dei contratti*, Bologna, 2021, p. 19 ss.

MAZZONI, C.M.: *Contratti di massa e controlli nel diritto privato*, Giuffrè, Milano, 1975, p. 149 s.

MAZZUCATO, M.: *Mission Economy. A Moonschoot Guide to Changin Capitalism*, London, 2021.

MEDICUS, D.: *Abschied von der Privatautonomie im Schuldrecht? Erscheinungsformen, Gefahren, Abhilfen*, Köln, 1994, p. 7 ss.

MESSINETTI, R.: "Circolazione dei dati personali e autonomia privata", in ZORZI GALGANO, N.: *Persona e mercato dei dati*, cit., p. 140 e 160 ss.

MESSINETTI, R.: "La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata", *Contr. impr.*, 2019, p. 861 ss.

MEZZACAPO, S.: *La regolamentazione dell'*algorithmic trading *nell'UE*, in TROIANO, V. e MOTRONE, R. (a cura di), *La MiFID II. Rapporti con la clientela - regole di* governance *- mercati*, cit., p. 341 ss.

MICKLITZ, H.-W.: *Vorbemerkung Vor §§ 13, 14,* in *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, vol. I, *Allgemeiner Teil*, 4 ed., München, 2001, p. 369 s.

MIK, E.: *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, in 10 *Journal of Law, Innovation and Technology (JLIT)*, 2017, p. 269-300

MÜLLER, M.: *Bitcoin, Blockchain und Smart Contracts. Technische Grundlagen und mögliche Anwendungsbereiche in der Immobilienwirtschaft*, in Zeitschrift für *Immobilienrecht*, 2017, p. 600 ss.

O'Shields, R.: *Smart Contracts: Legal Agreements for the Blockchain*, in 21 *North Carolina Banking Institute*, 2017, p. 177-194

Orlando, S.: "Verso l'Artificial Intelligence Act: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale", *Persona e mercato*, 2021, 2, p. 444 ss.

Paech, P.: *The Governance of Blockchain Financial Networks*, in 80 *Modern Law Review*, 2017, p. 1072-1100

Pardolesi, R. e Davola, A.: "«Smart contract»: lusinghe ed equivoci dell'innovazione purchessia", *Foro it.*, 2019, V, p. 195 ss.

Parisi, F.: *Il contratto concluso mediante computer*, Cedam, Padova, 1987

Paulus, D. e Matzke, R.: *Smart Contracts und das BGB. Viel Lärm um nichts?*, in *ZfPW*, 2018, p. 431 ss.; Idd.: *Digitalierung und private Rechtsdurchsetzung. Relativierung der Zwangsvollstreckung durch smarte IT-Lösungen?*, in *Computer und Recht (CR)*, 2017, p. 769 ss.

Pennalisico, M.: "La conclusione dei contratti on-line tra continuità e innovazione", *Dir. inf.*, 2004, p. 810 ss.

Perlingieri, C.: *Profili civilistici dei social networks*, Esi, Napoli, 2014.

Perlingieri, P.: "«Sostenibilità», ordinamento giuridico e «retorica dei diritti»", *Foro nap.*, 2020, p. 101 ss.

Perlingieri, P.: "Le funzioni della responsabilità civile", *Rass. dir. civ.*, 2011, p. 118

Perlingieri, P.: *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, II, *Fonti e interpretazione*, 4 ed., Esi, Napoli, 2020, p. 278 ss.

Pernice, C.: "Distributed ledger technology, blockchain e smart contracts: prime regolazioni", *Tecn. dir.*, 2020, 2, p. 490 ss.

Prosperetti, E.: "Obbligo di motivazione e procedimenti in cui non è nota a priori la logica dell'algoritmo", *www.dirittomercatotecnologia.it*

Quarta, A.: *Mercati senza scambi. La metamorfosi del contratto nel capitalismo*, Esi, Napoli, 2020

Rampone, F.: "Linee guida AGID e il paradosso della forma scritta", *https://associazioneblockchain.it/wp-content/uploads/2020/02/20.02.14-Le-Linee-Guida-dellAgID-su-smart-contract.pdf*, p. 2

Raskin, M.: *The Law and Legality of Smart Contracts*, in 1 *Georgetown Technology Review*, 2017, p. 305-341

Reich, N. e Micklitz, H.-W.: *Europäisches Verbraucherrecht*, 4 ed., Baden-Baden, 2003, p. 281 ss

Remotti, G.: "Blockchain smart contract: primo inquadramento e prospettive di indagine (commento all'art. 8 ter D.L. 14 dicembre 2018, n. 135)", *ODCC*, 2020, p. 189 ss.

Resta, G.: "Diritti fondamentali e diritti privato nell'era digitale", in Caggia, F. e Resta, G.: *I diritti fondamentali in Europa e il diritto privato*, Roma, 2019, p. 219 ss.

Resta, G.: "I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale* (a cura di V. Ricciuto e C. Solinas), Milano, 2022, p. 53.

Reyes, C.L.: *Conceptualizing Cryptolaw*, in 96 *Nebraska Law Review*, 2017, p. 384-445

Ricciuto, V. e Solinas, C.: "Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto", *Giust. civ.*, 2021, p. 3 ss.

Ricciuto, V. e Zorzi, N. (a cura di): *Il contratto telematico*, in *Tratt. di dir. comm. e dir. pubbl. econ.* diretto da F. Galgano, XXVII, Padova, 2002

Ricciuto, V.: "La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno", *Dir. inf.*, 2018, p. 689 ss.

Rizzo, V.: *Condizioni generali del contratto e predisposizione normativa*, Esi, Camerino-Napoli, 1983, p. 108 ss.

Rizzo, V.: *Interpretazione dei contratti e relatività delle sue regole*, Esi, Camerino-Napoli, 1985, p. 11 ss.

Rodotà, S.: *Elaboratori elettronici e controllo sociale*, Torino, 1973, p. 51.

ROPPO, V.: *Contratti standard. Autonomia e controlli nella disciplina delle attività negoziali d'impresa*, Giuffrè, Milano, 1975, p. 153 s.

RUFFOLO, U. (a cura di): *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020

RUNDO, F. e CONOCI, S.: "Tecnologia "blockchain": dagli smart contracts allo smart driving", *SeG_III_MMXVII* (*www.sicurezzaegiustizia.com, 2017, III*)

RUNDO, F. e CONOCI, S.: "Tecnologia "blockchain": dagli smarts contracts allo smart driving", *SeG_III_MMXVII* (*https://www.sicurezzaegiustizia.com*, 2017)

RYAN, P.: *Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain*, in 7 *Technology Innovation Management Review*, 2017, p. 10-17

SANTOSUOSSO, A.: *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Giuffrè, Milano, 2020.

SARTOR, G.: "Gli agenti software: nuovi soggetti del ciberdiritto?", *Contr. impr.*, 2002, II, p. 465 ss.

SARTOR, G.: *Intelligenza artificiale e diritto. Un'introduzione,* Giuffrè, Milano, 1996

SATTLER, A.: *Der Einfluss der Digitalisierung auf das Gesellschaftsrecht*, in Betriebsberater, 2018, p. 2243 ss.

SAVELYEV, A.: *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law*, ssrn.com/abstract=2885241

SCHOLZ, L.H.: *Algorithmic Contracts*, in 20 *Stanford Technology Law Review*, 2017, p. 101-147

SCHREY, J. e THALHOFER, T.: *Rechtliche Aspekte der Blockchain*, in *NJW*, 2017, p. 1431 ss.

SCHUHMACHER, E. e FATALIN, M.: "Compliance-Anforderungen an Hersteller autonomer Software-Agenten. Fünf Grundprinzipien für gesetzliche Instrumente", *Computer und Recht (CR)*, 2019, p. 200 ss.

SCORZA, G.: "Facebook non è gratis? Nota a Consiglio di Stato, sentenza 29 marzo 2021, n. 2631", *Dir. internet*, 2021, III, p. 561 ss.

SCORZA, G.: "Il dato personale: manifestazione della personalità vs. forma di ricchezza", in AA. VV.: *Fornitura di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, cit., pp. 85 ss.

SKLAROFF, J.M.: *Smart Contracts and the Cost of Inflexibility*, in 166 *University Pennsylvania Law Review*, 2017, p. 263-303

SÖBBING, T.: *Smart Contracts und Blockchain-Technologie. Definition, Arbeitswiese, Rechtsfragen*, in *ITRB*, 2018, p. 43 ss.

SPINDLER, G.: *Gesellschaftsrecht und Digitalisierung*, in *Zeitschrift für Gesellschaftsrecht*, 2018, p. 17 ss.

THOBANI, S.: "La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità", *Europa e dir. priv.*, 2016, 2, p. 513 ss

THOBANI, S.: "Operazioni di tying e libertà del consenso", *Giur. it.*, 2019, p. 530 ss.

THOBANI, S.: *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Giuffrè, Milano, 2018

TJONG TJIN TAI, T.F.E.: *Juridische aspecten van blockchain en smart contracts*, in 54 *Tijdschrift voor Privaatrecht*, 2017, p. 563-608

TJONG TJIN TAI, T.F.E.: *Smart contracts en het recht*, in 93 *Nederlands Juristenblad*, 2017, p. 176-182.

TOMBARI, U.: "Corporate Purpose e Diritto societario: scopo sociale: dalla supremazia degli interessi dei soci" alla libertà di scelta dello "scopo sociale"?", *Riv. soc.*, 2021, 1, p. 1 ss.

TOMBARI, U.: *"Potere" e "interessi" nella grande impresa azionaria*, Giuffrè, Milano, 2021

TOSI, E.: "La conclusione dei contratti on-line", in ID. (a cura di): *I problemi giuridici di Internet (dall'E-Commerce all'E-Business*), Giuffrè, Milano, 2003, p. 101 ss.

TREIBER, K.: *Aus der Praxis: Schuldscheindarlehen als Smart Contracts*, in *REthinking Law*, 2018, 1, p. 10 ss.

VORPEIL, K.: „Digitalisierung der Außenhandelfinanzierung - Neue ICC-Richtlinien zur elektronischen Vorlage von Dokumenten bei Akkreditiven und Imkassi - Teil I", *Zeitschrift für Wirtschafts- und Bankrecht*, 2019, 32, p. 1469 ss.

Weiss, S.: *Potenziale und Risiken der Blockchain Technologie im Bankenbereich*, München, 2018

Werbach, K. e Cornell, N.: *Contracts Ex Machina*, in 67 *Duke Law Journal*, 2017, p. 313-382

Wilsch, H.: „Die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts", *Deutsche Notar-Zeitschrift*, 2017, p. 761

Zimmermann, A.S.: *Blockchain-Netzwerke und Internationales Privatrecht oder: der Sitz dezentraler Rechtverhältnisse*, in *Praxis des Internationalen Privat- und Verfahrensrechts*, 2018, 6, p. 566 ss.

Zorzi Galgano, N. (a cura di): *Persona e mercato dei dati. Riflessioni sul GDPR*, Giuffrè, Milano, 2019; Irti, C.: *Consenso «negoziato» e circolazione dei dati personali*, Torino, 2021