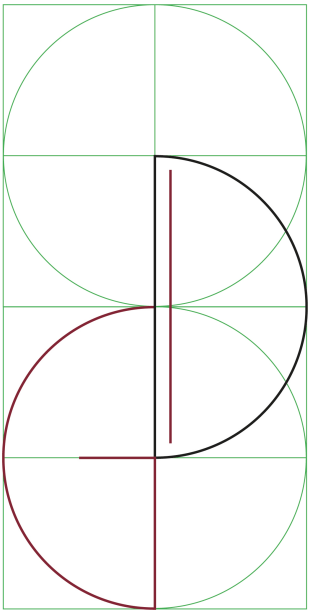
Materiali e documenti

Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2021 Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo



University Press

SAPIENZA UNIVERSITÀ EDITRICE

Collana Materiali e documenti 75

Annuario 2021
Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2021
Juridical Observatory on Digital Innovation

a cura di Salvatore Orlando e Giuseppina Capaldo

SAPIENZA
UNIVERSITÀ EDITRICE
2021

Sapienza Università Editrice
Piazzale Aldo Moro 5 – 00185 Roma

www.editricesapienza.it
editrice.sapienza@uniroma1.it

Iscrizione Registro Operatori Comunicazione n. 11420

ISBN 978-88-9377-186-3

DOI 10.13133/9788893771863

Pubblicato nel mese di luglio 2021

Impaginazione/layout a cura di: Enzo Maria Incutti

In copertina: Michela Tenace, *Studio per il logo OGID/JODI* (2021), archivio dell'A.

Indice

Prefazione

L'idea e la realizzazione del presente *Annuario* sono maturate nell'ambito delle attività seminariali, di confronto e di studio promosse nel corso del 2020 dall'Osservatorio Giuridico sull'Innovazione Digitale (OGID), costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università Sapienza di Roma (https://web.uniroma1.it/deap/ogid).

L'Osservatorio promuove lo studio delle relazioni tra le tecnologie digitali e il diritto privato, attraverso una serie di attività, tra le quali la tenuta di *webinar* con cadenza settimanale, la cura di pubblicazioni e la partecipazione alle procedure di consultazione pubblica delle istituzioni della Unione europea sulle proposte normative aventi ad oggetto le tematiche dell'innovazione digitale.

Nel corso del 2020 OGID ha organizzato 27 *webinar*, e circa 30 nel 2021. I relatori provengono da numerose Università italiane e straniere. Alcuni *webinar* sono tenuti in lingua inglese, e anche i relatori non accademici sono italiani e stranieri.

OGID cura dal 2020 la rubrica di aggiornamento "*Diritto e nuove tecnologie*" della rivista trimestrale *Persona e Mercato* (rivista di fascia A)[1].

---

[1] Numeri del 2020: 1/2020 – http://www.personaemercato.it/wp-content/uploads/2020/03/Osservatorio-1-2020.pdf; 2/2020 – http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf; 3/2020 – http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf; 4/2020 – http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf
Numeri del 2021: 1/2021 – http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf; 2/2021 - http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf

I contributi pubblicati in questo *Annuario* hanno ad oggetto temi trattati dagli Autori nei *webinar* dell'Osservatorio (nei quali hanno preso parte come relatori) o nella Rubrica "Diritto e nuove tecnologie" sulla rivista *Persona e Mercato*.

Sono contributi che coprono una varietà di temi di diritto privato legati all'innovazione digitale.

Li presentiamo seguendo l'ordine alfabetico degli Autori.

Buona lettura!

I Curatori

Salvatore Orlando Giuseppina Capaldo

1. Natura finanziaria delle cripto-attività e riflessi sul regime del capitale sociale

Attilio Altieri

1.1. Introduzione

Il fenomeno oramai noto come *FinTech* sta progressivamente plasmando il modo attraverso cui la ricchezza circola: uno dei passaggi fondamentali di questo nuovo "flusso" è dovuto, senz'altro, all'introduzione della DLT (Distributed Ledger Technology), grazie alla quale si è in grado di catturare una delle tappe della transizione dalla società dell'informazione[1] alla società del valore[2]. Infatti, guardando espressamente a questo nuovo contesto, un ruolo assolutamente predominante è interpretato dalla c.d. *blockchain* (la DLT più famosa), che ha "registrato" il transito dall'«*internet of information*» all'«*internet of value*»[3], in cui ogni tipo di *asset* può essere conservato, trasferito e gestito

---

1 Sulle funzioni di riproduzione e rappresentazione legate alle attività di natura informativa, v. S. ORLANDO, *Le informazioni*, Padova, 2012, p. 23 ss, e p. 63 ss.

2 V. R.T. AINSWORTH, V. VITASAARI, *Payroll Tax & the Blockchain*, in SSRN-id2970699, 2017; in senso critico nei confronti della *blockchain*, v. E. SCHUSTER, *Cloud Crypto Land*, in *SSRN-id3476678*, 2020, soprattutto quando essa è accostata ai beni immobili.

3 Cfr., ampiamente, le riflessioni di Luciano Floridi sull'«infosfera», che da ambiente informazionale sta progressivamente mutando in realtà: L. FLORIDI, *The Philosophy of Information,* Oxford, 2011; ID, *La rivoluzione dell'informazione*, Torino, 2012; ID, *The Ethics of Information*, Oxford, 2013; ID, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017; ID, *The Logic of Information: A Theory of Philosophy as Conceptual Design*, Oxford, 2019 (trad, it., *Pensare l'infosfera. La filosofia come design concettuale*, Milano, 2020); e da ultimo, con un testo a carattere divulgativo, ID, *Il verde e il blu*, Milano, 2020.

in modo decentrato, senza intermediari[4]. E sembra che proprio la "disintermediazione" rappresenti la cifra caratteristica della circolazione della ricchezza nell'era digitale[5].

Tale affermazione, però, perde la sua pregnanza nel momento in cui ci si sposta dalla disciplina dell'atto a quella dell'attività: in particolare, quando si passa dalla disposizione della ricchezza (con il suo mezzo tipico, ovvero il contratto) al luogo di produzione della ricchezza (la società), una qualche forma di intermediazione (umana) assume il carattere della necessità.

Il campo di verifica che qui si propone di esaminare è proprio quello della formazione del capitale sociale (sia in fase di costituzione che di aumento) delle società di capitali, dove – come si cercherà di dimostrare – taluni principi hanno la forza di resistere alla «destrutturazione delle regole societarie»[6], anche quando si passa per la «destrutturazione delle regole del mercato»[7], la cui inclinazione "ingegneristica" ha, da ultimo, generato le c.d. cripto-attività. E proprio da queste ultime – quali possibile oggetto di conferimento in società – si prenderanno le misure per avviare il discorso, al fine di comprendere se la

---

4 V. D. Tapscott, A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*, New York, 2018.

5 Cfr. M.T. Paracampo (a cura di), *Fintech*[2], Torino, 2019; G. Finocchiaro, V. Falce (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019; M. Cian, C. Sandei (a cura di), *Diritto del Fintech*, Milano, 2020. In verità, il problema dovrebbe porsi in termini di assenza di intermediazione umana, visto che un *medium* sembra sempre esserci, seppure costituito da una macchina. Sul processo di sostituzione dell'uomo da parte della macchina, v. E. Severino, *Il destino della tecnica*, Milano, 1998; N. Irti, E. Severino, *Dialogo su diritto e tecnica*, Bari-Roma, 2001. V. anche G. Agamben, *Homo sacer*, Torino, 2005; G. Teubner, *Ibridi ed attanti. Attori collettivi ed enti non umani nella società e nel diritto* (trad. it.), Milano-Udine, 2015; Id, *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten*, in *Archiv für die civilistische Praxis*, 218 (2018), p 155 ss., donde la soluzione per il riconoscimento agli agenti *software* lo *status* di attori parzialmente provvisti di capacità giuridica («*Für das Autonomierisiko ist es eine adäquate Antwort, den Softwareagenten den Status als teilrechtsfähige Akteure zuzuerkennen*», p. 204). Da ultimo, R. Bodei, *Dominio e sottomissione*, Bologna, 2019. Per i problemi legati ad internet, cfr. M. Hindman, *La trappola di internet*, Torino, 2019. E per certi versi anche S. Zuboff, *Il capitalismo della sorveglianza*, Roma, 2019.

6 V. Santoro, *Tentativi di sviluppo di un mercato secondario delle quote di società a responsabilità limitata*, in *Dir. banc. fin.*, 2020, 1, p. 32. E riguardo alla crisi denunciata dalla dottrina circa la rilevanza e la funzione del capitale sociale, su cui, per tutti, v. M.S. Spolidoro, *Capitale sociale* (voce), in *Enc. dir.*, IV Aggiornamento, Milano, 2000, p. 235 ss., con ampi riferimenti bibliografici.

7 V. Santoro, *Tentativi di sviluppo*, cit., p. 32.

loro natura possa avere delle ricadute in termini di disciplina allorquando le si accosti a quell'entità numerica che rappresenta il capitale sociale minimo.

1.2. Le ICOs e le cripto-attività

Le *Initial Coin Offerings* (altrimenti abbreviate in ICOs) costituiscono una "nuova" forma di raccolta di capitale utilizzato per finanziare iniziative o progetti imprenditoriali, tramite piattaforme basate sulla DLT, a fronte della emissione di *Coin* o *Token*[8], ovvero di *asset* crittografici[9]. Tali "cripto-attività", quindi, si differenziano per la particolare tipologia di corrispettivo dietro dazione (comunemente) di danaro: infatti, le ICOs, accumunate dalla capacità di emettere "rappresentazione di un valore", si distinguono, dal punto di vista dell'offerta (e quindi della sottoscrizione) a seconda che l'oggetto sia costituito da *Coin* o *Token*. I *Coins* sono una rappresentazione di valore creata direttamente nella rispettiva *Blockchain* (l'esempio tipico è dato da *Bitcoin* ed *Ether*, ovvero dalle c.d. cripto-valute o cripto-monete); mentre i *Tokens* sono una rappresentazione tecnica dei diritti che vengono implementati da parte degli emittenti solo successivamente nella *Blockchain* esistente[10].

La letteratura sull'argomento ha proposto varie tassonomie, tra cui, quella più utile ai fini della presente ricerca sembra essere quella basata sulla funzione economico-sociale dei *Tokens*[11]: si distinguono i *Currency Token* (che esprimono una funzione di pagamento e che coincidono con i *Coins*), gli *Utility Token* (che rispecchiano una funzione di

---

8 Per tutti, v. N. WOLF, *Initial Coin Offerings*, Berlin, 2020.

9 Cfr. sull'uso della crittografia per mettere in sicurezza le "relazioni" sulla rete N. SZABO, *Formalizing and Securing Relationships on Public Networks*, in *First Monday*, 1997, 2(9), reperibile al seguente indirizzo https://firstmonday.org/ojs/index.php/fm/article/view/548.

10 Cfr. N. WOLF, *Initial Coin Offerings*, cit., p. 41, il quale utilizza per i coin il termine "*Wertträger*", mentre per i Token, la locuzione "*die technische Repräsentation von Rechten*". V. anche S. ADHAMI, G. GIUDICI, S. MARTINAZZI, *Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings*, in SSRN-id3046209, 2018.

11 Classificazione operata da P. HACKER, C. THOMALE, *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*, in SSRN-id3075820, 2019, p. 12, sulla scorta di una diffusa analisi dei *Whitepaper* più rilevanti in circolazione sui mercati. In verità, questa è anche la classificazione adoperata dalla Finma, ovvero dall'Autorità federale di vigilanza sui mercati finanziari della Svizzera: v. https://www.finma.ch/it/news/2018/02/20180216-mm-ico-wegleitung/

consumo o d'uso) e i *Security/investment Token* (che denotano una funzione finanziaria o d'investimento)[12].

I tentativi di classificazioni sono vieppiù complessi poiché allo stato attuale non c'è una definizione "legale" né nazionale né comunitaria delle cripto-attività; gli unici dati normativi sono costituiti dalla direttiva 2018/843/UE e dal d.lgs. 231/2007 (modificato dal d.lgs. 90/2017) che offrono una sistemazione della valuta virtuale alla stregua di una «rappresentazione digitale di valore», e dall'art. 8-*ter* d.l. 135/2018 che puntualizza la portata delle DLT. Sul versante delle Autorità indipendenti, la Consob, la Banca d'Italia e l'ESMA si sono limitate ad emanare dei documenti di consultazione e dei report finali che al momento hanno la finalità, da un lato, di mettere in guardia soprattutto i consumatori circa i potenziali rischi delle operazioni che hanno ad oggetto le cripto-attività, dall'altro, di animare un dibattito fra studiosi ed esperti del settore che, sperabilmente, possa giungere ad una conclusione di carattere normativo[13].

A tal proposito, giova da ultimo segnalare il c.d. *Digital finance package*[14], un "conglomerato" di documenti, adottato dalla Commissione europea il 24 settembre 2020, dove sono confluite oltre alle linee guida in tema di *Digital finance strategy* e di sistemi di pagamento, anche una

---

12 Tra gli altri modelli proposti, vi è quello di J. Rohr, A. Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, in SSRN-id3048104, 2018, i quali prestano maggiore attenzione ai profili tecnici dei Token (classificazione proposta: *Protocol token*; *App token*; *Investment token*). Altra interessante tassonomia, è quella ordinata da N. Wolf, *Initial Coin Offerings*, cit., p. 48 ss. il quale attesta l'esistenza di cinque modelli più uno: *Currency Tokens, Utility Tokens, Debt Tokens, Ausübung von gesellschafterähnlichen Rechten Tokens, Equity Tokens* e gli *Hybrid Tokens*. Proprio quest'ultimo modello, quello dei *Token* ibridi appare essere quello di più complessa comprensione, in quanto lo stesso è basato prevalentemente su una commistione tra *Utility e Investment Token*.

13 Fra gli innumerevoli documenti, si segnalano quelli più significativi: per la Consob, oltre al noto *Documento per la discussione* del 19 marzo 2019 (http://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/12117302-78b0-4e6e-80c4-d3af7db0fdae), v. anche il rapporto finale del 2 gennaio 2020 su offerte iniziali e scambi di cripto-attività (http://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1); per la Banca d'Italia, si segnala l'avvertenza del 2018 (https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali-2018/avvertenze-valute-virtuali-2018.pdf); per l'ESMA, un *advice* del gennaio 2019 specifico sulle ICOs e sulle cripto-attività (http://www.consob.it/documents/46180/46181/esma50-157-1391.pdf/dc2e5c1e-8481-4331-882a-826aa7368f0e).

14 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

serie di proposte legislative sulla regolamentazione delle cripto-attività e della DLT, e sulla ben nota "resilienza" digitale del settore finanziario. Dando uno sguardo d'insieme alla proposta di regolamento sui mercati di cripto-attività, una delle novità è senz'altro rappresentata dalla "corale" definizione di *crypto-asset* come rappresentazione digitale di valore o di diritti[15], inquadrata funzionalmente nel novero delle forme di finanziamento delle PMI. Scorrendo il testo dei considerando (dove sono state recepite molte delle riflessioni già formulate nei precedenti atti dell'UE e dell'ESMA, si percepisce un approccio sussidiario e proporzionale (tipico del legislatore europeo nel campo dei mercati finanziari), volto a tratteggiare un modello "bipolare": riconosciuto che la maggior parte delle cripto-attività non rientra nell'attuale perimetro delineato dall'UE[16], lo scopo del regolamento sarebbe quello di "catturare" questa zona grigia, in modo tale da escludere i *token* già strutturati come strumenti finanziari (che rientrerebbero nelle prerogative della MiFID II da emendare)[17] o come moneta elettronica (che ricadrebbero nella Electronic Money Directive); mentre, alle "nuove" cripto-attività si applicherebbe lo specifico regolamento[18].

Altrettanto interessante è l'introduzione del tema della tripartizione delle cripto-attività, recependo in tale modo la classificazione già adoperata dalla dottrina e dalle Autorità di vigilanza e sottolineando la peculiarità degli *Utility token* (spesso aventi un contenuto non finanziario)[19]. Infine, particolare attenzione è stata dedicata ai *whitepaper*,

---

15 V. considerando n. 2.

16 V. considerando n. 3 sui pagamenti elettronici e gli strumenti finanziari.

17 Infatti, il grande assente di questa proposta di regolamento è rappresentato proprio dal *security/investment token*: la scelta è dettata (almeno da quanto traspare dal *Digital finance package*) dalla volontà di regolamentare questa tipologia di cripto-attività direttamente nella MiFID e negli altri regolamenti che si occupano di mercati finanziari.

18 V. considerando nn. 5 e 6.

19 I considerando nn. 10 e 11 si occupano dei *Payment token*, dividendolo in due tipologie: gli *asset-referenced tokens* e gli *electronic money token* (o *e-money token*). I primi (cons. n. 10) avrebbero una funzione di pagamento ma il loro valore sarebbe determinato da un sottostante (con una forte similitudine con i derivati) che può essere di diversi tipi (una valuta, una *commodity*, un'altra cripto-attività o un insieme variabile di queste componenti); i secondi (cons. n. 11) appaiono essere degli *stable coins*, giacchè sono legati ad una moneta *fiat*.

descritti in maniera piuttosto analitica (l'impressione è che si tratti di un surrogato del prospetto)[20].

1.3. La natura giuridica delle cripto-attività

La considerevole diffusione delle ICOs[21] unita ad una sostanziale incertezza sulla qualificazione dei *token* e dei *coin* ha contribuito ad accendere un intenso dibattito circa la natura giuridica delle cripto-attività. Al momento, l'unico elemento certo è costituito dal dato empirico che accomuna tutte le ipotesi di cripto-attività, ovvero quello di costituire un bene (digitale) suscettibile di acquisire un valore d'uso (mancando, come visto, un valore legale)[22].

Passando brevemente in rassegna le posizioni assunte in dottrina, occorre recuperare la classificazione *supra* tratteggiata. E quindi, partendo dai *Currency Token* (ovvero le monete virtuali), essi sono stati accostati alla moneta non avente corso legale nello Stato, per la loro indole ad essere usati come mezzo di pagamento[23]; c'è chi, invece, ne ha sottolineato la natura obbligatoria o contrattuale (argomentando *ex* art. 1322 c.c.)[24]; l'opinione prevalente ha più correttamente definito le cripto-monete come un bene (mobile) di cui all'art. 810 c.c.[25] o semplicemente come una merce[26].

---

20 V. considerando n. 16 e ss.

21 Anche se con una recente flessione. V. nt. 1.

22 A. Del Pozzo, *I rischi delle ICO e degli Exchange: che fare?*, in B. Russo (a cura di), *L'evoluzione dei sistemi e dei servizi di pagamento nell'era del digitale*, Padova, 2020, p. 137 ss.

23 M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, in *Riv. dir. civ.*,_2019, 1, p. 201.

24 V. De Stasio, *Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi,* in M. Cian, C. Sandei (a cura di), *Diritto del Fintech*, Milano, 2020, p. 233 ss. Anche C. Lanfranchi, *Profili giuridici delle valute virtuali*, in *Ciberspazio e diritto,* 2019, 1-2, p. 59.

25 A.M. Gambino, C. Bomprezzi, Blockchain *e criptovalute*, in G. Finocchiaro, V. Falce (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019, p. 276; A. Caloni, *Bitcoin: profili civilistici e tutela dell'investitore*, in *Riv. dir. civ.*, 2019, 1, pp. 171-172.

26 M. Cian, *La criptovaluta - alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca borsa tit. cred.*, 2019, 3, p. 315 ss., per il quale le criptovalute «vanno considerate, in linea di principio, alla stregua di "merce", cioè come beni digitali, oggetto di negoziazione in quanto beni e non in quanto denaro, con le relative conseguenze applicative». Nello stesso senso, anche la dottrina tedesca: S. Omlor, *Geld und Währung als Digitalisate*, in *JZ*, 2017, p. 754 ss., in part. p. 758, dove il bitcoin è paragonato ad un "*Immaterialgut*"; Id, *Kryptowährungen im Geldrecht*, in

Gli *Utility Token*, indubbiamente il *crypto-asset* di più complessa definizione, sono stati inquadrati seguendo il grado della loro "negoziabilità" (e, di conseguenza, della loro funzione speculativa): una parte della dottrina ha proposto la suddivisione tra prodotto finanziario e *voucher*[27]; altra parte, facendo ricorso ad un approccio "*top-down*", li distingue – in base alla tassonomia delle *trading venues*, in strumenti finanziari *ex* MiFID II o strumenti derivati[28].

Infine, gli *Investment Token* sono stati annoverati in vario modo: strumenti e/o contratti derivati su merci ai sensi della direttiva MiFID II[29]; strumenti finanziari o strumenti derivati[30]; prodotti finanziari[31];

ZHR, 2019, p. 311. Per le qualificazioni alternative, come "*Zahlungsmittel*", "*Recheneinheit*" o "*Wertaufbewahrungsmittel*", v. N. WOLF, *Initial Coin Offerings*, cit., pp. 48-49.

27 C. SANDEI, Initial coin offering *e appello al pubblico risparmio*, in M. CIAN, C. SANDEI (a cura di), *Diritto del Fintech*, Milano, 2020, p. 277 ss., in part. p. 290. Per l'assimilazione degli *utility token* ai vaucher, v. Risposta n. 14 del 28/09/2018 dell'Agenzia delle Entrate; ma anche art. 8 della legge della Repubblica di San Marino: "I token di utilizzo di cui all'articolo 7, comma 2, lettera a) sono da qualificarsi come voucher per l'acquisto di servizi o di beni offerti dall'Ente Blockchain".

28 F. ANNUNZIATA, *La disciplina delle* trading venues *nell'era delle rivoluzioni tecnologiche: dalle criptovalute alla* distributed ledger technology, in *ODC*, 2018, 3, p. 10 ss.; in particolare, p. 12.

Per la dottrina statunitense, invece, «*The nature of utility tokens makes categorical determinations about their status under U.S. securities laws impossible and subjects token sellers to significant uncertainty as to their regulatory obligations*», J. ROHR, A. WRIGHT, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, in SSRN-id3048104, 2018, p. 45.

In Germania, «*Die Ausgestaltung im Besonderen obliegt der Kreativität des initiierenden Unternehmens und ist lediglich durch die allgemeinen schuldrechtlichen Schranken (insbesondere §§ 134, 138, 242 BGB) und das technisch Mögliche beschränkt*», così N. WOLF, *Initial Coin Offerings*, cit., p. 50, che alla fine le definisce come «*Rechnungseinheiten*».

29 G. GITTI, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca borsa tit. cred.*, 2020, 1, p. 13 ss.

30 F. ANNUNZIATA, *La disciplina delle* trading venues, cit.; ID, *Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings*, in SSRN-id3332485, 2019.

31 C. SANDEI, Initial coin offering, cit. Cfr. anche L. FERRAIS, *Le* Initial Coin Offerings*: fattispecie in cerca d'autore*, in M.T. PARACAMPO (a cura di), *Fintech*(2), Torino, 2019, p. 291 ss., il quale afferma (p. 294) che bisognerebbe adottare un metodo sostanzialistico, dove dare prevalenza alla sostanza sulla forma e osservare, caso per caso, la componente finanziaria/speculativa.

rappresentazione sulla blockchain di azioni, obbligazioni ed altri strumenti di partecipazione societaria[32;33].

In verità, la disputa circa la natura giuridica dei *token*, così come impostata finora, evoca la descrizione di un "oggetto frattale", dove ciò che cambia risulta essere solo la proporzione del problema, rimanendo intatto il termine di paragone. Ed allora, partendo dai dati certi (che al momento sono solo quelli empirici), si tenterà di tratteggiare

---

32 N. de Luca, *Documentazione crittografica e circolazione della ricchezza*, in M. Cian, C. Sandei (a cura di), *Diritto del Fintech*, Milano, 2020, p. 418.

33 Negli USA, per l'inquadramento nelle *securities*, a seguito del risultato positivo del "Howey Test" vedi il DAO report della SEC, consultabile su https://www.sec.gov/litigation/investreport/34-81207.pdf; SEC, *Framework for "investment Contract"-Analysis of Digital Assets* (2019), https://www.sec.gov/corpfin/framework-investment-contract-analysisdigital-assets; per la giurisprudenza, v. United States District Court Eastern District of New York - United States of America c. Maksim Zaslavskiy, edita in *Società*, 2019, 1, p. 55 ss. con nota di P. Giudici, *ICO e diritto dei mercati finanziari: la prima sentenza americana*. Per la dottrina, L. Reiners, *Fintech Regulation in the United States*, in M. Cian, C. Sandei (a cura di), *Diritto del Fintech*, Milano, 2020, p. 645 ss.

In Germania, sono considerati prodotti finanziari: infatti, l'autorità di regolamentazione finanziaria (BaFin) ha recentemente approvato un primo prospetto di *securities token offerings* (v. https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs.html); cfr. Anche il recentissimo intervento normativo relativo alla definizione di *Tatbestand des Kryptoverwahrgeschäfts* (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_200302_kryptoverwahrgeschaeft.html?nn=9450978#U1). V. anche N. Wolf, *Initial Coin Offerings*, cit., p. 52 ss.

La Francia ha fornito, a livello legislativo, una definizione di Token, nell'art. L. 552-2 del *Code monétaire et financier*: «*constitue un jeton tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien*». La definizione ampia tenta di ricostruire il concetto di "proprietà" e di "bene immateriale" legato ai token. Sul punto F. Barriere, *Le crowdfunding, ou l'adaptation du droit au service des investissements*, in *RIDC*, 2019, p. 331 ss.; Ph. Dider, *Le crowdlending*, in *RDBF*, 20(2) (2019), dossier 17; A.-V. Le Fur, *Les nouveaux services de crédit alternatif: la pratique du peer to peer lending ou l'uberisation du crédit*, in *RDBF*, 18(1) (2017), dossier 7.

Nel Regno Unito, la FCA ha pubblicato il Policy Statement 19/22: Guidance on cryptoassets – feedback and final guidance to CP19/3 (PS19/22), consultabile su https://www.fca.org.uk/publication/policy/ps19-22.pdf, dove, a p. 15, gli investment tokens sono paragonati alle securities e, secondo l'autorità di vigilanza britannica, sono soggetti alle regole dei prodotti finanziari.

una possibile soluzione, anche per evitare quelle «operazioni di mera cosmesi lessicale»[34].

Come già ricordato, le ICOs si basano su un sistema DLT[35], di cui la *blockchain* rappresenta l'esemplare maggiormente diffuso: essa, come noto, nasce per risolvere il problema del *double spending* di un'informazione di valore[36], abilitando il menzionato concetto di Internet del valore, in quanto permette di maneggiare entità digitali non riproducibili ma divisibili. Ciò consente di scambiare anche una frazione del valore e, nel caso dei *token*, nasce la possibilità di scindere l'equivalente digitale di un bene fisico (si pensi ad un'opera d'arte, ma anche ai cavalli purosangue[37]) aumentandone la liquidità[38]. A sua volta il *token* è una rappresentazione digitale di valore[39], il cui "supporto materiale" è costituito da bit informatici: invero, da un punto di vista tecnico, «un *token* è una scritturazione informatica a favore di un determinato partecipante della rete»[40], ovvero una rappresentazione digitale di valore, basato sulla crittografia ed emessa da un soggetto che «a fronte dello stesso *token* riserva al titolare del medesimo una posizione giuridica attiva»[41].

Ponendoci nell'ottica contrattuale e guardando allo scambio che avviene tra due parti (ci si riferisce, semplificando, all'ipotesi tipica in cui si verifichi una vendita di *token* contro danaro)[42], l'attenzione cade

---

34 M. Onza, L. Salamone, *Prodotti, strumenti finanziari, valori mobiliari*, in *Banca borsa tit. cred*., 2009, 5, p. 567 ss.

35 Definito dal legislatore all'art. 8-*ter* d.l. 135/2018

36 P. Gallo, *DLT,* blockchain *e* smart contract, in M. Cian, C. Sandei (a cura di), *Diritto del Fintech*, Milano, 2020, p. 137 ss.

37 Cfr. M. Bottinelli, Blockchain – *Tokenizzazione, ovvero la parcellizzazione dei beni*, in *Medium*, 6 gennaio 2020.

38 P. Gallo, *DLT,* blockchain *e* smart contract, cit., p. 138.

39 Unico dato sancito dal legislatore, sia italiano che europeo, atteso che sia la direttiva 2018/843/UE che il d.lgs. 231/2007 definiscono le valute virtuali come tali: concetto facilmente trasferibile ai token, visto che quest'ultimo rappresenta il *genus* delle valute virtuali.

40 N. de Luca, *Documentazione crittografica*, cit., p. 411.

41 V. De Stasio, *Le monete virtuali*, cit., p. 223.

42 Allontanandoci per un momento dal contratto di società e dall'impostazione "associativa": v. P. Ferro-Luzzi, *I contratti associativi*, Milano, 2001, p. 222 ss.

sull'oggetto del contratto (*rectius*, sulla prestazione)[43] e sul suo contenuto in senso sostanziale[44], dovendo comprendere se la situazione giuridica attiva sia riferibile ad una cosa oppure ad un diritto relativo: in altre parole, quando si acquista un *token*, ci si relazione con un bene o con un credito? E le conseguenze non hanno solo rilevanza all'interno della sintassi negoziale (si pensi ai requisiti dell'oggetto[45] o agli effetti del contratto[46]), ma anche sulla disciplina dei conferimenti[47].

Distinguendo il contenuto dal contenitore, invece, si può affermare che quest'ultimo è formato da bit informatico, già da tempo riconosciuto come bene giuridico mobile[48]; mentre il contenuto è costituito, genericamente, da un valore**.** Quindi, da un punto di vista strutturale, i *token* possono essere paragonati ai titoli di credito[49], in quanto strumenti di mercato[50] che adattano una nuova tecnica di circolazione e che possono essere sottoposti, secondo una valutazione caso per caso, alla disciplina cartolare, stante la non necessità di avere un documento (o in generale un supporto materiale)[51] e dove si verifica una dematerializzazione senza una società di gestione accentrata[52]: infatti, siamo

---

43 Per tutti, v. G. De Nova, *L'oggetto del «contratto di informatica»: considerazioni di metodo*, in *Dir. inf.*, 1986, 3, pp. 804-805.

44 C.M. Bianca, *Il contratto*[2], vol. III, Milano, 2000, p. 320.

45 V. Roppo, *Il contratto*[2], Milano, 2011, p. 315 ss.

46 Cfr. R. Sacco, G. De Nova, *Il contratto*[(4)], Torino, 2016, p. 943 ss.

47 V. *infra*; ma si pensi anche alle conseguenze in termini di disciplina dei conferimenti richiamate dall'art. 2342, comma 3, c.c. e, quindi, agli artt. 2254 e 2255 c.c.

48 «In tal modo la scrittura in bit diviene giuridicamente un nuovo bene, possibile oggetto autonomo di negozi giuridici, una cosa materiale suscettibile di possesso e di danneggiamento», così R. Borruso, *Informatica giuridica* (voce), in *Enc. dir.*, Agg., Milano 1997, p. 645. Sui beni, v. A. Gambaro, *I beni*, in *Tratt. Cicu-Messineo*, Milano 2012, p. 173 ss., per il discorso sulle "frontiere del diritto dei beni" e sul suo progressivo spostamento.

49 Cfr. E. Rulli, *Incorporazione senza* res *e dematerializzazione senza accentratore: appunti sui* token, in *ODC*, 2019, 1, p. 121 ss.; una posizione simile la si intuisce anche in V. Santoro, *Tentativi di sviluppo*, cit., p. 23 ss.

50 F. Chiomenti, *Il titolo di credito. Fattispecie e disciplina*, Milano, 1977, p. 209.

51 F. Chiomenti, *Il titolo di credito*, cit., p. 208, dove parla di «scartolarizzazione». *Contra*, A. Stagno d'Alcontres, *Tipicità e atipicità nei titoli di credito*, Milano, 1992, p. 77 ss.

52 V. E. Rulli, *Incorporazione senza* res, cit., p. 122 ss.

in presenza del noto fenomeno di «trasformazione mobiliare delle istituzioni economiche»[53], dove al «documento "cosale"»[54] si sostituisce l'informazione "relazionale"[55]. Una conferma della similitudine tra "tokenizzazione" e cartolarizzazione[56] è offerta dalla recente legislazione del Liechtenstein, la *Gesetz über Token und VT-Dienstleister (Token- und VT-Dienstleister-Gesetz; TVTG*), approvata nell'ottobre 2019 ed entrata in vigore il 1° gennaio di quest'anno, che all'art. 2 definisce il *token* come un'informazione presente su un *VT-System*[57], che può rappresentare diritti di credito (*Forderungsrechte*) o diritti di partecipazione sociale (*Mitgliedschaftsrechte*) nei confronti di un soggetto, diritti sulle cose/beni (*Rechte an Sachen*) o altri diritti assoluti o relativi (*andere absolute oder relative Rechte*)[58]; ma, l'aspetto più interessante (ed utile) è contrassegnato dall'art. 5 (*Verfügungsgewalt und Verfügungsberechtigung*), che in qualche modo ricalca l'art. 1994 c.c. (e quindi gli effetti del possesso in buona fede).

Passando dalla "forma cartolare" a quella "mobiliare" e quindi procedendo dalla finalità circolatoria alla destinazione al mercato[59], dovremmo essere in grado di rintracciare la natura finanziaria dei *token*

---

53 P. SPADA, *Introduzione al diritto dei titoli di credito. Documenti circolanti, circolazione intermediata e password*(3), Torino, 2012, p. 26

54 *Ivi*, p. 99.

55 V., da ultimo, L. FLORIDI, *Il verde e il blu*, cit., cap. 3.

56 Sul processo di "tokenizzazione", anche con riferimento al diritto di proprietà, v. R. DE CARIA, *Il diritto di fronte alla tokenizzazione dell'economia*, in *Dir. econ.*, 2020, 1, p. 855 ss.

57 Ovvero «*„VT-Systeme": Transaktionssysteme, welche die sichere Übertragung und Aufbewahrung von Token sowie darauf aufbauende Dienstleistungserbringung mittels vertrauenswürdiger Technologien ermöglichen*» (art. 2, § 1, lett. b), TVTG), ovvero un sistema basata sulla *vertrauenswürdige Technologien* (lett. a).

58 La proposta di regolamento europeo sui mercati di cripto-attività, all'art. 3, lett. b) adotta una definizione di cripto-attività (e non di *token*) con un approccio più "generalista": infatti, essa consiste in "*a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger or similar technology*". Viene in parte mutuata la definizione di valuta virtuale di cui alla direttiva 2018/843/UE, aggiungendo, oltre alla rappresentazione di diritti (evidentemente per farvi rientrare sia gli *utility* che gli *investment token*), anche il concetto di trasferimento e deposito tramite la DLT.

59 Cfr. C. MOTTI, *Dalla destinazione alla circolazione alla destinazione al mercato: i "nuovi" titoli di massa*, in *I battelli del Reno*, 23 dicembre 2014, p. 4, la quale, avvertendo della potenziale inespressività o ripetizione dei due concetti, tuttavia ne sottolinea l'importanza allorquando si tratta di identificare la disciplina applicabile (tutela dell'investitore e regolazione dei rapporti interprivati).

(non solo per quelli d'investimento, ma anche per quelli di pagamento e di utilità): infatti, se la riconducibilità alla fattispecie cartolare risulta essere funzionale alla negoziabilità[60] e la trama che sviluppano coglie le tre condizioni dell'impiego di un capitale, dell'assunzione di un rischio e dell'aspettativa di un rendimento[61], all'interprete non resta che muoversi «dal generico riferimento alla funzione finanziaria (*rectius*, di investimento finanziario) dell'operazione, ad una analisi puntuale del tipo di bisogno economico soddisfatto (ossia all'identificazione del mercato di riferimento)»[62]. Invero, adottando un approccio tipologico, se per i *security* o *investment token* la natura finanziaria appare intrinseca[63], per i *payment* e gli *utility token* il discorso è parzialmente diverso: in questo caso sarà necessario indagare non solo se l'operazione sia effettivamente polarizzata, dal principio alla fine, intorno al danaro[64], ma, a prescindere dai motivi soggettivi, se il bene-*token* «sia oggettivamente negoziabile e sia dunque in grado di dar vita a un sistema di scambi per contanti (il cosiddetto mercato secondario)»[65]. Quindi per gli *utility token*, occorrerà indagare la possibilità di riacquisto o la loro ammissione alla negoziazione sugli *exchange*[66]; discorso analogo dovrà essere condotto con riferimento ai *payment token* (e si pensi al caso *Bitcoin*, dove la maggior parte dei possessori sono investitori con finalità speculative[67]).

---

60 E, quindi, funzionale al compimento potenzialmente innumerevole dello schema investimento/disinvestimento, tipico dei titoli di massa. Sul punto, v. G. Castellano, *I titoli di massa*, in *Banca borsa tit. cred.*, 1987, I, p. 22 ss.; P. Spada, *Dai titoli di credito atipici alle operazioni atipiche di raccolta del risparmio*, in *Banca borsa tit. cred.*, 1986, I, p. 13 ss.

61 Cfr. oltre alle comunicazioni Consob, anche, *ex multis*, R. Costi, *Il mercato mobiliare*(10), Torino, 2016, p. 8 ss.; F. Annunziata, *La disciplina del mercato mobiliare*(10), Torino, 2020, p. 91 ss.

62 C. Motti, *Dalla destinazione alla circolazione*, cit., pp. 10-11.

63 V. P.P. Pirani, *Gli strumenti della finanza disintermediata:* Initial Coin Offering *e* blockchain, in *AGE*, 2019, 1, p. 327 ss.

64 P. Ferro-Luzzi, *Attività e «prodotti finanziari»*, in *Riv. dir. civ.*, 2010, 2, p. 134.

65 G. Guizzi, *Mercato finanziario* (voce), in *Enc. dir., Agg.*, Milano, 2001, p. 749.

66 C. Sandei, *Le* initial coin offering *nel prisma dell'ordinamento finanziario*, in *Riv. dir. civ.*, 2020, 2, p. 404.

67 Cfr. S. Athey, I. Parashkevov, V. Sarukkai, J. Xia, *Bitcoin Pricing, Adoption, and Usage: Theory and Evidence*, in *SSRN-id2826674*, 2016, ove un'ampia analisi sul "mercato secondario" della moneta virtuale.

In definitiva, possiamo affermare che da un punto di vista costitutivo, i *token* si concretano in una costante concettuale[68] che li "riduce" alla nota nozione di bene di secondo grado[69], in modo tale da assicurare «la soddisfazione di un interesse: 1) *propter ius* […]; ma anche 2) *di natura strumentale*, che può trovare realizzazione solo attraverso una tecnica di protezione strumentale»[70]. Tale fattispecie complessa[71] (che contiene anche l'antifattispecie cartolare[72]) è idonea a far circolare quella "ricchezza assente"[73], metonimia della "merce finanziaria"[74] o, in ogni caso, di un valore negoziabile.

1.4. I riflessi sul regime del capitale sociale

Il risultato positivo circa la natura finanziaria delle cripto-attività, come già annunciato, non ha lo scopo "tipico" di compiere l'ulteriore passaggio circa la riconducibilità nel sistema dei "cerchi concentrici"[75] del T.u.f. e, quindi, di attrarre nella nozione di strumento o prodotto

---

68 Riferendosi all'atipicità dei titoli di credito, sull'atipicità dei titoli di credito, v. M. LIBERTINI, *Profili tipologici e profili normativi nella teoria dei titoli di credito*, Milano, 1969, p. 97 ss.; A. STAGNO D'ALCONTRES, *Tipicità e atipicità nei titoli di credito*, Milano, 1992, p. 141 ss.; B. LIBONATI, *Titoli atipici e non (I certificati di associazione in partecipazione)*, in *Banca borsa tit. cred.*, 1985, I, p. 468 ss.; P. SPADA, *Titoli atipici* (voce), in *Enc. giur.*, Roma, 1994, p. 1 ss.

69 T. ASCARELLI, *Riflessioni in tema di titoli azionari, personalità giuridica e società tra società*, in *Banca, borsa, tit. cred.*, 1952, I, p. 385; ID, *Saggi di diritto commerciale*, Milano, 1955, p. 239.

70 Così L. SALAMONE, *Unità e molteplicità della nozione di valore mobiliare*, Milano, 1995, p. 111.

71 Cfr. R. SCOGNAMIGLIO, *Fattispecie* (voce), in *Enc. giur.*, XIV, Roma, 1989, p. 6 ss.; ma anche A. CATAUDELLA, *Fattispecie* (voce), in *Enc. dir.*, XVI, Milano, 1967; P.G. MONATERI, *Fattispecie* (voce), in *Digesto disc. priv., Sez. Civ.*, 1992; R. SACCO, *Fattispecie* (I agg.) (voce), in *Digesto disc. priv., Sez. Civ.*, 2010.

72 Stante la ricomprensione anche dei documenti di legittimazione e dei titoli impropri: sul punto, v. N. DE LUCA, *L'antifattispecie cartolare. Contributo allo studio dei titoli di credito*, in *Banca borsa tit. cred.*, 2017, 1, p. 93 ss.; N. DE LUCA, *Circolazione delle azioni e legittimazione dei soci*, Torino, 2007, *passim.*

73 P. SPADA, *La circolazione della ricchezza assente alla fine del millennio (riflessioni sistematiche sulla dematerializzazione dei titoli di massa)*, in *Banca borsa tit. cred.*, 1999, 4, p. 407 ss.; ma sui pericoli di una trasformazione da ricchezza assente a "inesistente", cfr. P. SPADA, *Dalla ricchezza assente alla ricchezza inesistente - divagazioni del giurista sul mercato finanziario*, in *Banca borsa tit. cred.*, 2010, 4, p. 401 ss.

74 P. SPADA, *Dalla ricchezza assente alla ricchezza inesistente*, cit., § 3.

75 V. V.V. CHIONNA, *Strumenti finanziari e prodotti finanziari*, cit., p. 1 ss.; ma già ID, *Le forme dell'investimento finanziario*, Milano, 2008, p. 1 ss., p. 121 ss.

finanziario i *token*: in altre parole, la prospettiva che si è scelto di adottare non coinvolge l'*Individualrecht* con le sue manifestazioni "consumeristiche" o di tutela dell'investimento (e si pensi alle conseguenza in tema di applicazione della disciplina MiFID o del prospetto informativo), ma ha l'intento di vagliare il rapporto che si istituisce tra i *crypto-asset* e il capitale sociale, crocevia dove appare più fragile la disintermediazione frutto della tecnica. E qui si inserisce il discorso sulla valutabilità economica e i relativi criteri che attingono alla "finanziarietà" dei *token*, le cui ricadute sono utili in riferimento a quelli con funzione di pagamento e di utilità, dove la relativa valutazione è agevolata dalla dialettica negoziale vista (*id est*, mercato primario/mercato secondario). Ma, anticipando già in parte le conclusioni, la natura finanziaria delle cripto-attività, in realtà, sposta in misura non rilevante gli argomenti ai fini della qualificazione nell'ottica del conferimento, poiché l'alternativa che si pone il diritto societario è quella rappresentata dalla triade denaro, beni in natura e crediti.

Prima, però, è necessario risolvere il problema della conferibilità dei *token* nel prisma delle società di capitali[76] (nello specifico s.p.a. e s.r.l.), atteso che il quesito investe la formazione del capitale sociale in

---

[76] Tema affrontato dalla giurisprudenza: oltre a Trib. Verona, 24 gennaio 2017 (in *Banca borsa tit. cred.*, 2017, p. 467 ss., con nota di M. PASSARETTA, *Bitcoin*: *il* leading case *italiano*, p. 471 ss.), che definisce il bitcoin come uno strumento finanziario, ai sensi dell'art. 1, comma 2, TUF, vi sono stati due arresti giurisprudenziali specifici sul conferimento di moneta virtuale, che hanno negato la conferibilità della stessa, seppure con motivazioni divergenti: Trib. Brescia, 25 luglio 2018, n. 7556 (in *Giur. it.*, 2019, 1, p. 118 ss., con nota di R. Razzante, *Criptovalute e conferimenti aziendali*, p. 119 ss.) e App. Brescia, 20 ottobre 2018 (in *Società*, 2019, 1, p. 26 ss. con nota di F. Murino, *Il conferimento di* token *e di criptovalute nelle S.r.l.*, p. 29 ss.). Mentre Trib. Brescia assimila le cripto-valute a un bene in natura, escludendo in concreto la conferibilità in società di capitali della specifica cripto-moneta, App. Brescia equipara le cripto-valute al danaro, negando in astratto la conferibilità. In particolare, in una prospettiva *de jure condendo* e guardando sia al *Digital Finance Package* che al Report della BCE sull'"euro digitale" del 2 ottobre 2020 (consultabile al seguente indirizzo https://www.ecb.europa.eu/euro/html/digitaleuro-report.en.html), la presunta "volatilità" della cripto-moneta (denunciata dalla Corte d'appello) verrebbe meno nel momento in cui si adottasse lo schema degli *stable coins* (v. *electronic money token* o *e-money token* di cui all'art. 3, lett. d) della proposta di regolamento sui *crypto-assets*); quanto all'"inattendibilità" (lamentata dal Tribunale), sembra rispondere la possibile introduzione di un euro digitale, una sorta di moneta digitale *fiat*, emessa direttamente dalla BCE (e dalla stessa "garantita"). Su quest'ultimo punto, le ipotesi (più licenziose) forse potrebbero tendere alla completa equiparazione con la valuta corrente e portare a paragonare, sul piano dei conferimenti in società, l'euro digitale al danaro.

due momenti fondamentali: la costituzione e l'aumento del capitale; insomma, occorre comprendere se l'oggetto del conferimento (*rectius*, della prestazione) possa essere costituito da una cripto-attività; successivamente, qualora la risposta fosse affermativa, occorrerà indagare le modalità attraverso le quali i soci (e successivamente gli amministratori nella loro funzione di controllo) possono procedere a conferire questa particolare attività.

1.4.1. L'iscrivibilità in bilancio

La questione preliminare che si pone intorno alla conferibilità passa necessariamente attraverso l'analisi dell'iscrivibilità in bilancio delle cripto-attività. A tal fine è possibile affermare che le cripto-attività sono entità economicamente valutabili: ciò si desume, oltre che dalla loro natura finanziaria, anche dai diversi interpelli e risoluzioni dell'Agenzia delle Entrate – confermate di recente dal Tar Lazio Sentenza 1077 del 27 gennaio 2020(77) – che definiscono e inquadrano le cripto-attività tra le componenti del reddito, e, in più, dalla circostanza che le cripto-attività sono o, comunque, possono essere elementi dell'attivo patrimoniale e, come tali, possono essere iscritti in bilancio secondo determinati criteri, su cui da ultimo si è pronunciato l'IFRIC - International Financial Reporting Interpretations Committee[78]. La conferma giunge dall'analisi dei principi contabili, la cui validità è corroborata dalla loro natura di regole tecniche con funzione interpretativa[79]: le cripto-valute, in base alla funzione che svolgono nel sistema economico, sia generale, sia particolare[80], possono essere considerate come valori di magazzino – se l'impresa compravende per sua naturale attività le cripto-valute – o come immobilizzazioni immateriali –

---

77 V. P.R. AMENDOLA, B. MASCAGNI, *L'inquadramento delle criptovalute: TAR del Lazio, sent. n. 01077/2020 del 27 gennaio 2020*, in *Diritto Bancario*, 5 marzo 2020.

78 Comitato dello IASB, succeduto al SIC (Standing Interpretation Committee) nel 2001 nell'incarico di stendere le interpretazioni ufficiali del contenuto dei principi contabili internazionali (v. IAS, IFRS). Gli IFRS (International Financial Reporting Standard) sono subentrati agli IAS (International Accounting Standard) pubblicati dal precedente International accounting standard Committee (IASC).

79 Per tutti, v. G.E. COLOMBO, *Il bilancio d'esercizio*, in G.E. COLOMBO E G.B. PORTALE (diretto da), *Trattato delle società per azioni*, vol. 7, t. 1, Torino, 1994, p. 211 ss.; per i principi contabili internazionali, v. S. FORTUNATO, *Bilancio e contabilità d'impresa in Europa*, Bari, 1993, p. 153 ss., p. 182 ss.

80 F. PONTANI, *Le criptovalute nel bilancio di esercizio delle società di capitali*, in *Economia Aziendale Online*, 2020, 1, p. 82.

in caso di un loro impiego a medio-lungo termine; gli *Utility Token* sono inquadrabili alla stregua di un *Intangible Asset* ai sensi dello IAS 38[81]; ai *security Token* si applicano l'IFRS 9 e lo IAS 32[82]. Da ciò si desume non solo la valutabilità in concreto delle cripto-attività, ma anche la loro iscrivibilità nel bilancio d'esercizio di una società di capitali.

A questo punto, per comprendere se l'iscrivibilità in bilancio sia anche sufficiente per conferire un bene, bisogna, seppur brevemente, guardare alla funzione del capitale sociale. In particolare, la funzione di garanzia nei confronti dei creditori sociali[83] consente di conferire solo beni espropriabili in una procedura esecutiva[84] o realizzabili dai creditori[85]: in verità, il patrimonio della società (che comprende le componenti passive, anch'esse destinate a produrre reddito) non coincide con il concetto di patrimonio come garanzia generica *ex* art. 2740 c.c. (che comprende le sole componenti attive). La funzione produttiva[86] considera l'idoneità dell'impresa ad essere gestita economicamente e produttivamente come la migliore garanzia per i creditori e comporta che il bene, per essere conferibile, debba essere recuperabile (la società deve entrare immediatamente nella disponibilità effettiva del bene senza la collaborazione del socio conferente)[87].

---

81 A. Incorvaia, *L'iscrizione in bilancio dei* cryptoassets *secondo i principi contabili internazionali IAS-IFRS*, in *Riv. dott. comm.*, 2020, 1, p. 21 ss., al quale si rinvia per maggiori precisazioni

82 A. Incorvaia, *L'iscrizione in bilancio*, cit.

83 E. Simonetto, *Concetto e composizione del capitale sociale. Parte I*, in *Riv. dir. comm.*, 1956, 1-2, p. 48 ss.; Id, *Concetto e composizione del capitale sociale. Parte II*, in *Riv. dir. comm.*, 1956, 3-4, p. 112 ss.; Id, *Responsabilità e garanzia nel diritto delle società*, Padova, 1959, p. 18 ss.

84 E. Simonetto, *Responsabilità e garanzia*, cit., *passim*.

85 G. Olivieri, *I conferimenti in natura nella società per azioni*, Padova, 1989, p. 65 ss.; Id, *I conferimenti nella società per azioni*, in F. d'Alessandro (diretto da), *Commentario romano al nuovo diritto delle società*, vol II, t. 1, Padova, 2010, p. 169.

86 G.B. Portale, *Capitale sociale e conferimenti nella società per azioni*, in *Riv. Soc.*, 1970, p. 33 ss.; Id, *I conferimenti in natura atipici nella s.p.a.,* Milano, 1974, p. 25 ss.; F. Di Sabato, *Capitale e responsabilità interna nelle società di persone*, Napoli, 1967, *passim*.

87 M. Miola, *La tutela dei creditori ed il capitale sociale: realtà e prospettive*, in *Riv. soc.*, 2012, 2-3, p. 237 ss.

In verità, l'ipotesi da preferire è quella organizzativa[88] nella sua accezione normativa[89]: parlandosi di capitale nominale, si evoca la funzione di una disciplina e, quindi, il capitale svolge tante funzioni quanti sono i sistemi di regole di riferimento. Guardando alla disciplina del capitale minimo, oltre alle regole relative al capitale nominale, il legislatore ha fornito il sistema di un articolato complesso di norme con lo scopo di assicurare che le risorse attualmente impiegate nell'impresa presentino un valore, contabile, in grado di preservare sempre la copertura non solo del capitale minimo, ma anche del capitale nominale statutario, e di salvaguardare la costante presenza, nell'attivo patrimoniale, del capitale reale. Facendo riferimento alle disposizioni volte a regolare l'investimento dei soci nella società, invece, si richiama la disciplina della valutazione dei conferimenti dei soci, che sembra, allo stesso modo, diretta ad assicurare che il valore effettivo delle risorse investite dai soci corrisponda almeno all'importo del capitale statutario[90].

In definitiva, la tesi della funzione organizzativa, funzionale all'applicazione della relativa disciplina, richiede solo la iscrivibilità in bilancio, la quale non opera come mero indizio della suscettibilità di valutazione economica del conferimento in natura[91]: la sussistenza di un valore tale da permettere l'iscrizione nel bilancio rappresenta, bensì, il presupposto della conferibilità (infatti, in mancanza di iscrizione in bilancio non vi sarebbero all'attivo cespiti corrispondenti al capitale sociale).

1.4.2. I *token* come "bene in natura"

Il secondo problema da risolvere per accertare la conferibilità delle cripto-attività attiene al loro inquadramento nelle categorie predisposte dal legislatore: danaro o beni in natura/crediti (cfr. artt. 2342, co. 1

---

88 Intesa come misurazione del valore della partecipazione del socio nella società: per tutti, P. SPADA, *Dalla nozione al tipo della società per azioni*, in *Riv. dir. civ.*, 1985, I, p. 109.

89 G. FERRI *jr*, *Struttura finanziaria dell'impresa e funzioni del capitale sociale*, in *Riv. notariato*, 2008, 4, p. 741 ss.; ma v. anche A. PACIELLO, *La funzione normativa del capitale nominale*, in *RDS*, 2010, 1, p. 2 ss.; nonché S. FORTUNATO, *Capitale e bilanci nelle S.p.a.*, in *Riv. soc.*, 1991, p. 125 ss., in part. p. 134 ss.

90 Cfr. G. FERRI *jr*, *Struttura finanziaria dell'impresa*, cit.

91 G. OLIVIERI, *I conferimenti in natura*, cit., p. 109 ss.; v. anche M. MIOLA, *I conferimenti in natura*, in G.E. COLOMBO, G.B. PORTALE (diretto da), *Trattato delle società per azioni*, Torino, vol. 1, t. 3, 2004, p. 50.

e 3 per le s.p.a. e 2464, co. 3 e 5 per le s.r.l.). In questa specifica ottica, l'entità conferibile è il *token*, in quanto, come già detto *supra*, le cripto-attività sono identificabili – da un punto di vista "materiale" – nei *token*, a prescindere dalla specifica funzione assolta.

Attesa la non equiparabilità nemmeno delle monete virtuali (*token* con funzioni di pagamento) con il danaro, né tantomeno delle altre tipologie di *token*, ma classificati gli stessi alla stregue di merce (finanziaria)-valore, negoziabile, per il diritto societario (artt. 2342 ss. c.c.) essi dovrebbero essere ricondotti nell'alveo dei beni diversi dal danaro[92].

Ciò è dimostrato accedendo alla teoria che descrive il conferimento come atto di investimento: non collocando il conferimento né tra i beni giuridici in senso tecnico *ex* art. 810 c.c.[93] né tra i fattori produttivi in un'ottica aziendale[94], ma concependolo come valore economico[95], esso può essere descritto in termini di «impiego di ricchezza da parte del socio. […] Più che di trasferimento di un bene dovrebbe parlarsi, a proposito del conferimento, di trasformazione di un valore»[96]. Stante l'indole delle cripto-attività a non essere associabile al danaro ma, in ogni caso, ascrivibile all'espressione di un valore[97], è possibile affermare che le cripto-attività, nell'ottica del conferimento, costituiscono un bene in natura.

A questo punto, deve applicarsi la disciplina relativa al tipo di società in favore della quale avviene l'attribuzione patrimoniale e, quindi, occorre individuare il corretto procedimento di stima da effettuare. A tal proposito, le possibilità sono tre, individuabili negli artt.

---

92 Si rinvia alle considerazioni del § 3.

93 Per tale impostazione, v. G.B. Portale, *Principio consensualistico e conferimento di beni in proprietà*, in *Riv. soc.*, 1970, p. 913 ss.; E. Simonetto, *Concetto e composizione del capitale sociale*, cit., p. 48 ss.

94 Per tutti, v. P. Ferro-Luzzi, *I contratti associativi*, Milano, 2001, p. 316; ma anche C. Angelici, *La società nulla*, Milano, 1975, p. 67 ss.; G. Olivieri, *I conferimenti in natura*, cit., p. 27 ss.

95 G. Ferri *jr*, *Investimento e conferimento*, Milano, 2001, p. 25 ss. Infatti, questa concezione risulta, coerentemente, da una visione *normativa* del capitale sociale, allorchè si analizza la disciplina positiva proprio in tema di oggetto del conferimento in natura.

96 *Ivi*, p. 32 e nt. 62; ma anche p. 33 e nt. 63.

97 In tal senso si esprimono anche la direttiva 2018/843/UE e il d.lgs. 231/2007, che, in sede di definizione della valuta virtuale, l'associano ad una "rappresentazione digitale di valore".

2343 (relazione di stima) e 2343-*ter*, commi 1 e 2, c.c. (senza relazione di stima).

Cominciando dall'art. 2343-*ter*, comma 1, può senz'altro dirsi che non può trovare applicazione nel caso dei *token*: infatti, come noto, il conferimento di beni in natura senza relazione di stima di cui al primo comma deve avere ad oggetto valori mobiliari negoziati in un mercato regolamentato o strumenti del mercato monetario, per tali dovendosi comprendere, in base all'art. 111-*bis*, comma 2, disp. att. c.c., quelli definiti dall'art. 1 commi 1-*bis* e 1-*ter* TUF (quindi, riconducibili alla categoria degli strumenti finanziari)[98]. Ora, a parte la possibilità di qualificare i *token* (o almeno determinati tipi) quali valori mobiliari nel senso appena detto, essi, per ora, non sono negoziati in mercati regolamentati, bensì in altri tipi di *trading venues* (*exchange*). In più, per la loro assimilazione agli strumenti di mercato monetario, si dovrebbe dimostrare che il token in questione svolge effettivamente la funzione di investimento di liquidità a breve/brevissimo termine, che contraddistingue (insieme all'effettiva negoziazione) gli strumenti del mercato monetario[99].

Discorso in parte differente deve essere condotto in riferimento all'ipotesi di cui all'art. 2343-*ter*, comma 2, c.c., che regola i conferimenti che hanno ad oggetto ogni altra entità in natura diversa da quella presa in considerazione al primo comma. Infatti, alla lettere a) e b) vi sono due ulteriori parametri, attraverso i quali definire il valore massimo di conferimento dei beni diversi dai valori mobiliari e strumenti del mercato monetario: quindi, idealmente, potrebbero rientrarvi i *token*.

La lettera a) individua il valore massimo di conferimento nel *fair value* al quale il bene conferito sia stato "iscritto nel bilancio dell'esercizio precedente quello nel quale è effettuato il conferimento a condizione che il bilancio sia sottoposto a revisione legale e la relazione del revisore non esprima rilievi in ordine alla valutazione dei beni oggetto del conferimento": così, il socio è legittimato a conferire il bene per un valore non superiore a quello di iscrizione, il quale non deve essere "nuovamente" valutato, non ricorrendo la necessità di presentare una

---

98 V. G. Ferri *jr*, *2343*-ter, in P. Abbadessa, G.B. Portale (diretto da), *Le società per azioni. Codice civile e norme complementari*, T. 1, Milano, 2016, p. 419.

99 M. Notari, *Il regime alternativo della valutazione dei conferimenti in natura in società per azioni*, in *Riv. soc.*, 2009, p. 62.; N. Abriani, *Il nuovo regime dei conferimenti in natura senza relazione di stima*, in *Riv. not.*, 2009, I, p. 302.

specifica relazione giurata[100]. Per "*fair value*" deve intendersi la sua accezione tecnica assunta come criterio di valutazione nell'ambito dei principi contabili internazionali adottati dall'Unione europea (v. art. 2343-*ter*, comma 5)[101]: secondo la definizione contenuta nei principi IAS/IFRS, il *fair value* combacia infatti con il valore di scambio in quanto esso è il corrispettivo al quale «un'attività potrebbe essere scambiata in una libera transazione fra parti consapevoli e disponibili»[102].

La lettera b) consente, in alternativa al *fair value*, di usare come valore massimo di conferimento quello che emerge da una "valutazione riferita ad una data precedente di non oltre sei mesi il conferimento e conforme ai principi e criteri generalmente riconosciuti per la valutazione dei beni oggetto del conferimento, a condizione che essa provenga da un esperto indipendente". Quanto ai criteri di valutazione, data la rilevanza accordata al prezzo degli strumenti finanziari di cui al comma 1 dell'art. 2343-*ter*[103] e al *fair value* della lettera a), comma 2, art. 2343-*ter*, si può affermare che essi si concentrino sul valore di scambio, come unico criterio generalmente riconosciuto per la valutazione dei conferimenti[104].

Entrambe le tecniche di conferimento, però, paiono difficilmente applicabili al caso dei *token*, poiché pagano il problema del dato temporale, dato l'alto tasso di volatilità che influenza i *token*: infatti, nel caso del *fair value*, può farsi riferimento al bilancio dell'esercizio precedente; mentre, nel caso della valutazione dell'esperto indipendente, la relazione può essere redatta nel periodo di sei mesi. Si correrebbe il rischio di entrare in possesso di una valutazione non più attuale[105], con la conseguente attivazione dell'art. 2343-*quater*, comma 2, che prevede, su iniziativa degli amministratori, una nuova valutazione *ex* art.

---

100 Cfr. G. Perone, *La nuova disciplina della stima dei conferimenti diversi dal danaro in società per azioni*, in *Riv. dir. comm.*, 2010, I, p. 238 ss.

101 F. Corsi, *Conferimenti in natura "senza stima": prime valutazioni*, in *Giur. Comm.*, 2009, I, p. 13.

102 Il paragrafo 9 dello IAS 39 "Strumenti finanziari: rilevazione e valutazione" fornisce la seguente definizione di *fair value*: "*the amount for which an asset could be exchanged, or a liability settled, between knowledgeable, willing parties in an arm's lenght transaction*".

103 V. G. Strampelli, *I regimi alternativi di stima dei conferimenti in natura in società per azioni: appunti*, in *Riv. dir. civ.*, 2011, 2, p. 230 ss.; G. Perone, *La nuova disciplina della stima*, cit., p. 230 ss.

104 *Ex multis*, M. Notari, *Il regime alternativo della valutazione*, cit., p. 91.

105 O, in ogni caso, meno attuale di quella di cui all'art. 2343 c.c.

2343[106]. Inoltre, vi sarebbe una forte responsabilizzazione degli amministratori in sede di attestazione.

Allora, per conferire i *token* (e quindi le cripto-attività) dovrà procedersi secondo l'art. 2343 c.c.: chi conferisce le cripto-attività dovrà presentare una relazione giurata di stima di un esperto designato dal tribunale nel cui circondario ha sede la società. La stima, quindi, dovrà contenere "la descrizione dei beni o dei crediti conferiti, l'attestazione che il loro valore è almeno pari a quello ad essi attribuito ai fini della determinazione del capitale sociale e dell'eventuale soprapprezzo e i criteri di valutazione seguiti"[107].

1.5. Conclusioni

La natura finanziaria delle cripto-attività, sebbene risulti essere una delle chiavi di lettura per comprendere la conferibilità come "evento", non gioca un ruolo primario nell'approccio "societario" prescelto, in quanto non aiuta a selezionare tra le categorie dell'art. 2342 c.c. (forse più ruvide rispetto ad altri contesti, ma sicuramente molto funzionali): infatti, questo "nuovo" bene, nella prospettiva del conferimento, "perde" la sua "originalità" a vantaggio della categoria dei beni in natura. Ma, come si è avuto modo di dimostrare, ciò non basta, poiché il diritto delle società impone che una forma di intermediazione sia comunque presente allorquando quel "valore digitale" si trasformi in un valore non solo contabile ma "reale" o, con un termine ora antiquato, "analogico".

L'elemento di curiosità si annida proprio nella diversa consistenza dei registri (di partenza e di arrivo): la DLT partorisce un'informazione distribuita e disintermediata, mentre quella stessa informazione, per essere "annotata", necessita del *medium* umano, quando dall'«infosfera» il flusso informativo affluisce in una struttura corporativa. Una sorta di nemesi per cui se è vero che «la tecnica raggiunge la forma massima di potenza quando diventa cosciente dell'assenza di limiti assoluti al proprio agire»[108], è proprio il capitalismo, con le sue regole

---

106 M. SPERANZIN, *2343*-quater, in P. ABBADESSA, G.B. PORTALE (diretto da), *Le società per azioni. Codice civile e norme complementari*. T. 1, Milano, 2016, p. 430 ss.

107 Allo stesso modo si procederà per in conferimenti in natura in una s.r.l., con l'unica differenza della procedura semplificata di cui all'art. 2465 c.c., dove l'esperto non sarà designato dal tribunale, essendo sufficiente che si tratti di un revisore o di una società di revisione iscritti nell'apposito registro.

108 E. SEVERINO, *Democrazia, tecnica, capitalismo*, Brescia, 2009, p. 124.

organizzative, a rinviare quell'«ormai inevitabile amministrazione economica generale della terra»[109].

[109] F. Nietzsche, *Frammenti postumi 1887-1888*, v. VIII, t. II, Milano, 1971, p. 113.

2. La strategia digitale dell'Unione Europea verso un mercato unico sostenibile

Giuseppina Capaldo

2.1. Oggetto e scopo dell'indagine

Nell'ambito di queste pagine desidero dare conto della Risoluzione del Parlamento europeo del 25 novembre 2020 sul tema "*Verso un mercato unico più sostenibile per le imprese e i consumatori*" (2020/2021 INI; nel prosieguo Risoluzione 2020/2021), nella specifica parte in cui si occupa della strategia digitale al servizio di un mercato sostenibile[1]. Dopo una prima parte in cui mi soffermo sul contesto normativo attuale (par. 2) della sostenibilità (par. 3), provo a delineare il ruolo che il digitale assume (par. 4), discutendo alcuni temi trattati dalla Risoluzione 2020/2021. In particolare, intendo richiamare la questione delle piattaforme (par. 5) e quella della economia circolare (par. 6).

Peraltro, se è certamente vero che le tematiche digitali regolate nella Risoluzione 2020/2021 non sono né quelle principali, né quelle decisive, è allo stesso modo vero che il digitale riguarda in modo trasversale tutte le politiche e rappresenta l'infrastruttura della maggior parte delle attività economiche. Anzi, queste brevi note, appunti di una ricerca ancora in itinere, proveranno dunque a dimostrare la relazione attuale tra due temi, sostenibilità e digitale, i quali costituiscono, oggi, problemi giuridici in quanto oggetto di numerosissimi atti normativi. In questo senso, la linea di ricerca proposta muove anche dalla convinzione che la futura strategia dell'UE volta appunto alla creazione di un mercato sostenibile utilizzi tutte le opportunità della rivoluzione digitale in tutte le sue molteplici declinazioni[2].

---

1 Il testo della risoluzione è disponibile presso il sito www.europarl.europa.eu.

2 M. Robinson, *Climate Justice. Manifesto per un futuro sostenibile*, Roma, 2020, p. 23.

2.2. Le fonti della costruzione di un mercato unico sostenibile nell'Unione Europea

La Risoluzione 2020/2021 si inserisce in un quadro di evoluzione della normativa comunitaria, volto a costruire una rinnovata opzione macroeconomica di sistema che faccia propria la dimensione della sostenibilità, attraverso un insieme di regole e di riconoscimenti di diritti e tutele fondamentali.

2.2.1. Le fonti primarie

Il punto di partenza per la comprensione di questo sforzo di costruzione di un'Europa sostenibile e digitale è la struttura del mercato unico. Come dichiarato nel Preambolo dei Trattati, l'Unione Europea promuove il progresso economico e sociale dei popoli degli Stati dell'Unione, tenendo conto del *principio dello sviluppo sostenibile* nel contesto della *realizzazione del mercato interno* e del *rafforzamento della coesione e della protezione dell'ambiente*. In tal senso, la norma fondante è l'art. 3 TUE, nel quale il legislatore comunitario, dopo aver dichiarato che si prefigge la promozione della pace, dei suoi valori e del benessere dei suoi popoli e che offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui è assicurata la libera circolazione delle persone, al terzo comma si concentra sulle caratteristiche del mercato interno. In tale disposizione, si legge infatti che "*L'Unione instaura un mercato interno. Si adopera 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. L'Unione combatte l'esclusione sociale e le discriminazioni e promuove la giustizia e la protezione sociali, la parità tra donne e uomini, la solidarietà tra le generazioni e la tutela dei diritti del minore. Essa promuove la coesione economica, sociale e territoriale, e la solidarietà tra gli Stati membri. Essa rispetta la ricchezza della sua diversità culturale e linguistica e vigila sulla salvaguardia e sullo sviluppo del patrimonio culturale europeo*".

Allo stato, quindi, il mercato interno è "fortemente" competitivo, ma su un sistema di economia sociale di mercato, di crescita equilibrata e di stabilità di prezzi. Peraltro, oltre ad aspirare alla piena occupazione, alla tutela ambientale e al progresso sociale, l'UE ribadisce la

tutela di molteplici diritti, di prerogative, e di libertà fondamentali[3]. In questo senso, mentre nella fase iniziale la normazione comunitaria si è rivolta alla creazione di un diritto dei mercanti, è attualmente indiscutibile che l'Unione europea sia impegnata a tutelare i diritti della persona ed è attenta alla solidarietà, alle libertà e ai diritti fondamentali di tutti i cittadini dell'Unione Europea[4]. Anche al co. 5 della citata disposizione si ribadisce il principio per cui "*l'Unione afferma e promuove i suoi valori e interessi, contribuendo alla protezione dei suoi cittadini. Contribuisce alla pace, alla sicurezza, allo sviluppo sostenibile della Terra, alla solidarietà e al rispetto reciproco tra i popoli, al commercio libero ed equo, all'eliminazione della povertà e alla tutela dei diritti umani, in particolare dei diritti del minore, e alla rigorosa osservanza e allo sviluppo del diritto internazionale, in particolare al rispetto dei principi della Carta delle Nazioni Unite*".

2.2.2. Le fonti secondarie

La forte caratterizzazione del mercato unico europeo nel senso ora indicato dai Trattati passa per diverse fonti secondarie (regolamenti, direttive e risoluzioni), che, nel loro intento di declinare il libero mercato verso scopi ulteriori a quello della concorrenza, sono da considerare come i logici predecessori della Risoluzione 2020/2021.

In particolare, tra i provvedimenti normativi rilevanti quanto alla sostenibilità, si deve segnalare, innanzitutto, il Regolamento (UE) 2020/852 del Parlamento Europeo e del Consiglio del 18 giugno 2020 relativo all'istituzione di un quadro che favorisce gli investimenti sostenibili[5].

Questo Regolamento stabilisce i criteri per determinare se un'attività economica possa considerarsi ecosostenibile al fine di individuare il grado di ecosostenibilità di un investimento e rappresenta un passo fondamentale verso l'obiettivo di un'unione a impatto climatico zero. Al primo considerando il testo richiama appunto l'art 3, co. 3 TUE,

---

[3] F. EKARDT, *Sustainability, Trasformation, Governance, Ethics, Law*, Berlin, 2019, p. 113 ss., delinea la libertà e I diritti fondamentali nell'ambito dell'Unione Europea e anche a livello internazionale in una ricostruzione della sostenibilità come obiettivo normative. L'idea è che esistano delle precondizioni elementari di questa libertà, sotto forma di cibo, acqua, sicurezza, stabilità climatica, istruzione, assenza di guerre ecc.

[4] G. VETTORI, *Contratto e Rimedi*, Milano, 2017, p. 38 intorno alla funzione del Trattato di Lisbona nel passaggio da un'Europa dei mercanti a un'Europa dei diritti.

[5] Il testo del regolamento è disponibile in https://eur-lex.europa.eu.

confermando il carattere primario e l'essenzialità di uno sviluppo sostenibile, che sia basato sulla equilibrata crescita e sulla tutela ambientale, per lo sviluppo del mercato interno.

Nel secondo considerando del Regolamento 2020/852 viene esplicitamente citata la comunicazione della Commissione Europea del 22 novembre 2016[6] che fece propri gli Obiettivi di Sviluppo Sostenibile di cui all'Agenda 2030, adottata il 25 settembre dall'Assemblea generale delle Nazioni Unite[7], riguardanti le tre dimensioni della sostenibilità e cioè la *governance* economica, sociale ed ambientale. Nel Regolamento 2020/852, peraltro, si ricorda l'Accordo di Parigi sui cambiamenti climatici, approvato dall'Unione in data 5 ottobre 2016 laddove ci si impegna a rendere "i flussi finanziari coerenti con un percorso che conduca a uno sviluppo a basse emissioni di gas a effetto serra e resiliente ai cambiamenti climatici" (considerando 3)[8].

Il Regolamento (UE) 2020/852 restituisce, quindi, un chiaro esempio di come oggi sostenibilità e transizione ad una economia climaticamente neutra, ovvero un economia che sia più efficiente in termini di risorse, e circolare rappresentino l'opzione strategica per garantire la competitività economica dell'Unione Europea nel lungo termine.

Orbene, al fine di declinare il mercato verso obiettivi di sostenibilità, è chiaro che diventa indispensabile predisporre gli strumenti a livello di politiche dell'Unione al fine di risolvere il problema che tutti gli economisti pongono e cioè il modo di attrarre la finanza verso gli investimenti sostenibili[9]. In tal senso, muove la comunicazione della

---

6 Si tratta della Comunicazione "Il futuro sostenibile dell'Europa: prossime tappe", il cui testo si legge in https://eur-lex.europa.eu. Il secondo considerando richiama anche le conclusioni del 20 giugno 2017 del Consiglio europeo e una comunicazione della Commissione sul "*Green Deal Europeo*" dell'11 dicembre 2019.

7 Testo disponibile in https://unric.org/it/agenda-2030/.

8 In argomento, S. Latouche, *Le pari de la décroissance*, Arthème Fayard, 2006, trad. it., *La scommessa della decrescita*, Milano, 2007, p.73; P. Greco, A.Pollio Salimbeni, *Lo sviluppo insostenibile. Dal vertice di Rio a quello di Johannesburg*, Milano, 2003, p. 31 ss.; N. Klein, *The shock doctrine*, (*trad. it.*) *Shock Economy. L'ascesa del capitalismo dei disastri*, Milano, 2007.

9 R. Henderson, *Nel mondo che brucia*, Roma, 2020, p. 117. R.G. Eccles, S. Klimenko, *The Investor Revolution*, in *Harvard Business Review*, May-June 2019, p. 106 ss. Indicano sette criteri valutare la sostenibilità di un investimento, lo screening cd. negativo, che eliminando società in settori o paesi ritenuti discutibili; lo Screening basato sulle norme (che per es. elimina aziende che violano alcune serie di norme); Screening

Commissione dell'8 marzo 2018 con cui si è aperto il tema della finanza sostenibile[10]. Uno degli obiettivi fissati in quel piano di azione è il riorientamento dei flussi di capitale verso investimenti sostenibili finalizzato a raggiungimento di una crescita sostenibile e inclusiva" (considerando 6). Queste evoluzioni si inseriscono nel solco delle nuove istanze delle teorie economiche che vedono nel capitalismo cd. *triple bottom line*, *Planet, People and Profit*[11] e nel bilanciamento di questi interessi[12] – anche attraverso la *governance* – il modo per rinnovare dall'interno il sistema economico e il nostro modo di vivere.

positivo (come la selezione di società con performance ESG particolarmente elevate; la valutazione del tipo di investimenti incentrati sulla sostenibilità (come in un fondo incentrato sull'accesso all'acqua pulita o all'energia rinnovabile); Integrazione ESG (inclusi i fattori ESG nell'analisi fondamentale); Proprietà attiva (impegnarsi a fondo con le società in portafoglio); Impact investing (ricerca di società che abbiano un impatto positivo su una questione ESG pur ottenendo un ritorno di mercato).

10 COM/2018/097, testo disponibile in https://eur-lex.europa.eu.

11 Si tratta degli studi iniziati da John Elkington, a prendere le mosse dal saggio J. ELKINGTON, *Towards the Sustainable Corporation Win-Win-Win Business Strategies for Sustainable Development*, in *California Management Review*, 1994, 1, p.90; fino a ID., *The Power of Unreasonable People (2008),* with Pamela Hartigan, Harvard Business School Press, 2008; ID.,*The Zeronauts: Breaking the Sustainability Barrier* (2012); ID., *The Breakthrough Challenge: 10 Ways to Connect Today's Profits With Tomorrow's Bottom Line*, Jossey-Bass, (2014); J. STIGLITZ, *People, Power, and Profits. Progressive Capitalism for an Age of Discontent*, 2019; trad. it. *Popolo, potere e profitti. Un capitalismo progressista in un'epoca di malcontento*, Torino, 2020, p.5 ss.; S. ZAMAGNI, *Disuguali*, Sansepolcro, 2020, p. 9 ss.

12 F. EKARDT, *Sustainability, Trasformation, Governance, Ethics, Law*, cit., p. 113 ss. *"Ethical and legal decisions can only be understood as a balancing situation (between various freedoms, elementary preconditions of freedom, further free- dom promoting conditions and everything that can be derived from all of the above). Any sustainability decision is thus marked by normative and factual uncertainties (which is usually overlooked). Concrete problems such as "strong versus weak sustainability" or the relevance of a specific argument can only be meaningfully resolved within this theoretical framework. The ethical and legal theory of sustainability is also developed as a trans- formed theory of democracy and of balance of powers.*". Ne consegue che la regola più importante per il contesto della sostenibilità e che non deve essere rovinata la base del bilanciamento.

Sempre nell'ambito dei provvedimenti che, analogamente a quanto avvenuto con la risoluzione dello scorso 25 novembre, l'UE ha recentemente emanato al fine di coniugare il mercato unico secondo l'obiettivo della sostenibilità si deve fare riferimento anche al Regolamento (UE) 2019/2088 del Parlamento Europeo e del Consiglio del 27 novembre 2019 relativo all'informativa sulla sostenibilità sempre nel settore dei servizi finanziari.

2.2.3. Le fonti interne

Ovviamente, questi interventi normativi euro-unitari hanno ricadute sul nostro ordinamento. Tra le normative di attuazione delle direttive, si segnalano in materia di sostenibilità diversi decreti. Ad esempio, il d.lgs. 254/2016 attua la direttiva 2014/95/UE del Parlamento europeo e del Consiglio del 22 ottobre 2014 e offre la disciplina relativa alla comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni. In seno a tale decreto, la norma che sollecita maggiore attenzione è certamente l'art. 3 che stabilisce il contenuto della dichiarazione individuale di carattere non finanziario[13].

---

[13] La norma più interessante è all'art. 3 del d.lgs. 254/2016, che detta il contenuto della dichiarazione individuale di carattere non finanziario per gli Enti di Interesse pubblico (sui medesimi criteri sono redatte le dichiarazioni volontarie di cui all'art. 7 del medesimo decreto) *"1. La dichiarazione individuale di carattere non finanziario, nella misura necessaria ad assicurare la comprensione dell'attività di impresa, del suo andamento, dei suoi risultati e dell'impatto dalla stessa prodotta, copre i temi ambientali, sociali, attinenti al personale, al rispetto dei diritti umani, alla lotta contro la corruzione attiva e passiva, che sono rilevanti tenuto conto delle attività e delle caratteristiche dell'impresa, descrivendo almeno: a) il modello aziendale di gestione ed organizzazione delle attività dell'impresa, ivi inclusi i modelli di organizzazione e di gestione eventualmente adottati ai sensi dell'articolo 6, comma 1, lettera a), del decreto legislativo 8 giugno 2001, n. 231, anche con riferimento alla gestione dei suddetti temi; b) le politiche praticate dall'impresa, comprese quelle di dovuta diligenza, i risultati conseguiti tramite di esse ed i relativi indicatori fondamentali di prestazione di carattere non finanziario; c) i principali rischi, generati o subiti, connessi ai suddetti temi e che derivano dalle attività dell'impresa, dai suoi prodotti, servizi o rapporti commerciali, incluse, ove rilevanti, le catene di fornitura e subappalto;*

2. In merito agli ambiti di cui al comma 1, la dichiarazione di carattere non finanziario contiene almeno informazioni riguardanti: a) l'utilizzo di risorse energetiche, distinguendo fra quelle prodotte da fonti rinnovabili e non rinnovabili, e l'impiego di risorse idriche; b) le emissioni di gas ad effetto serra e le emissioni inquinanti in atmosfera; c) l'impatto, ove possibile sulla base di ipotesi o scenari realistici anche a medio termine, sull'ambiente nonché

Altre discipline rilevanti in materia sono il d.lgs. 147/2018, attuazione della direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio del 14 dicembre 2016, relativa alle attività e alla vigilanza degli enti pensionistici aziendali o professionali[14], e il d.lgs. 49/2019 Attuazione della cd. *Shareholders Rights* II, direttiva 2017/828 del Parlamento europeo e del Consiglio, del 17 maggio 2017, che modifica la direttiva 2007/36/CE per quanto riguarda l'incoraggiamento dell'impegno a lungo termine degli azionisti.

2.3. La risoluzione 2020/2021 e la sostenibilità del mercato

In un recente scritto[15], mi interrogavo su come, una volta chiarita l'opzione macroeconomica fatta propria dai Trattati UE, l'indagine potesse volgere a definire la sostenibilità ed individuarne il contesto normativo[16]. Finora, il legislatore dell'UE conosceva lo sviluppo sostenibile, la società sostenibile, l'economia sostenibile e anche il futuro sostenibile[17], ma la formula del mercato sostenibile di per sé non era adottata in modo frequente dal legislatore comunitario. Anzi, in questo contesto variegato e in continua evoluzione, la definizione – dal punto di vista dell'Unione europea – di mercato sostenibile è anch'essa

sulla salute e la sicurezza, associato ai fattori di rischio di cui al comma 1, lettera c), o ad altri rilevanti fattori di rischio ambientale e sanitario; d) aspetti sociali e attinenti alla gestione del personale, incluse le azioni poste in essere per garantire la parità di genere, le misure volte ad attuare le convenzioni di organizzazioni internazionali e sovranazionali in materia, e le modalità con cui è realizzato il dialogo con le parti sociali; e) rispetto dei diritti umani, le misure adottate per prevenirne le violazioni, nonché le azioni poste in essere per impedire atteggiamenti ed azioni comunque discriminatori; f) lotta contro la corruzione sia attiva sia passiva, con indicazione degli strumenti a tal fine adottati". Sul tema ampiamente in M. MAUGERI, *Informazione non finanziaria e interesse sociale*, in *Rivista delle Società*, fasc. 5, 1, p. 992 ss.; S. FORTUNATO, *L'informazione non-finanziaria nell'impresa socialmente responsabile*, in *Giurisprudenza Commerciale*, fasc. 3, p. 415 ss.

14 Si veda Regolamento IVASS n. 38/2018 recante disposizioni in materia di governo societario.

15 G. CAPALDO, *Linee evolutive in tema di soggetti per una società sostenibile*, in *Persona e Mercato*, 2020, 4, p. 334 ss.

16 Secondo P. MARCHETTI, *Editoriale*, in *Riv. Società*, 2020, p. 349 ss. "la sostenibilità non è utopia, alibi, corpo estraneo, ma concretissima esigenza che ridisegna responsabilità e obiettivi".

17 Parere del Comitato economico e sociale europeo su "Ascoltare i cittadini d'Europa per un futuro sostenibile" (2019/C 228/06).

in fieri, in quanto è l'effetto di una serie di norme che sono in corso di emanazione nell'arco dell'ultimo paio d'anni. Orbene, proprio la Risoluzione "*Verso un mercato unico più sostenibile per imprese e consumatori*" contribuisce a dare rilevanza alla locuzione "mercato sostenibile". Essa, infatti, pone un ulteriore tassello – la locuzione mercato unico sostenibile – con l'introduzione della dimensione di sostenibilità del mercato.

Il mercato unico è al centro dell'integrazione europea, sin dalle sue origini. Tuttavia oggi, come visto, la dimensione del mercato unico non è più soltanto economica, ma è diventata anche sociale ed ambientale[18]. La dimensione sociale era una dimensione ormai acquisita, basata nei trattati in cui l'economia sociale di mercato è divenuta in fondo il nuovo paradigma macroeconomico di riferimento dell'Unione europea[19]. La dimensione ambientale si è ormai inserita come elemento es-

---

[18] In argomento, la letteratura è sterminata: si vedano L. Wallach, M. Sforza, *WTO. Tutto quello che non vi hanno mai detto sul commercio globale*, Milano, 2000; S. George, *Fermiamo il WTO*, Milano, 2002; R. Vji, *Globalization and Welfare. A critical reader*, New York, 2007; L.S. Rossi (a cura di), *Commercio internazionale sostenibile*?, Bologna, 2003; P. Fitoussi, *La democrazia e il mercato*, Milano, 2004; J. Ziegler, *La privatizzazione del mondo. Padroni, predatori e mercenari del mercato globale*, Milano, 2003; *Dalla parte dei deboli. Il diritto all'alimentazione*, Milano, 2004; Id., *L'impero della vergogna*, Milano, 2006. Su alcune delle conseguenze dell'assenza di una regolazione etica dell'economia globale, tra gli altri, A. Gore, *L'assalto alla ragione*, Milano, 2007; N. Chomsky, V. Shiva, J. Stiglitz, *La debolezza del più forte. Globalizzazione e diritti umani*, Milano, 2004; K. Bales, *I nuovi schiavi*, Milano, 2000; N. Roozen, F. van der Hoff, *Max Havelaar. L'avventura del commercio equo e solidale*, Milano, 2003. V.Shiva, *Ritorno alla terra. La fine dell'ecoimperialismo*, Roma, 2009; Ead., *Le nuove guerre della globalizzazione. Sementi, acqua e forme di vita*, Torino, 2005; J. Bové, F. Dufour, *Il mondo non è in vendita. Agricoltori contro la globalizzazione alimentare*, Milano, 2000.

[19] Per un quadro delle questioni sociali ed economiche dell'epoca si richiamano, in una letteratura ricchissima, alcuni saggi tra i quali U. Beck, *I rischi della libertà. L'individuo nell'epoca della globalizzazione*, Bologna, 2000; Id., Conditio Humana. *Il rischio nell'età globale*, Roma-Bari, 2008; W. Sachs e T. Santarius (a cura di), *Per un futuro equo. Conflitto sulle risorse e giustizia globale*, Milano, 2007; P. Artus - M.P. Virard, *Globalisation. Le pire est à venir*, Paris, 2008; Z. Bauman, *Dentro la globalizzazione. Le conseguenze sulle persone*, Roma-Bari, 2001; G. Bolton. *Poor story. An insider uncovers how globalisation and good intention have failed the world's poor*, Great Britain, 2007; J. Kultalahti, I. Karppi, O. Kultalahti, E. Todisco (a cura di), *Globalisation. Challenges to Research and Governance*, Helsinki, 2009; M.C. Nussbaum, *Le nuove frontiere della*

senziale della opzione di mercato macroeconomico dell'Unione Europea e il mercato deve crescere in modo sostenibile, deve favorire l'innovazione, attrarre investimenti, promuovendo una competitività che sia anch'essa sostenibile. Quindi, quando il Trattato di Lisbona ci diceva che la base della opzione macroeconomica è quella di una economia sociale di mercato fortemente competitiva ecco che questa forte competitività deve tenere conto comunque di due dimensioni quella ambientale e quella sociale.

Tutto questo discorso della sostenibilità ha delle ricadute concrete.

Una crescita sostenibile significa che la crescita non dovrebbe fondarsi solo sulla quantità, ma anche (e in realtà persino di più) sulla qualità, il che significa: *i) nessuno sfruttamento dell'ambiente o del lavoro, ii) condizioni di vita eque, iii) crescita economica misurata sulla base non solo dei flussi annuali, ma anche delle riserve di ricchezza e della loro distribuzione, iv) soddisfacimento dei bisogni di tutti nel limite delle risorse del pianeta, v) sviluppo di economie che ci consentono di prosperare, indipendentemente dalla loro crescita o meno, e vi) un flusso chiuso relativo al ciclo delle entrate tra nuclei familiari, imprese, banche, governo e commercio, che operi in modo sociale ed ecologico*[20].

A differenza del passato, quando oggi nel discorso europeo parliamo di competitività si deve fare riferimento a un modello che trova un equilibrio tra prosperità economica questioni ambientali e inclusione sociale. In modo analogo, il diffuso indice di competitività globale va adeguato alla sostenibilità e deve tenere conto di due dimensioni quella ambientale e quella sociale.

Per avere conferma della concretezza del discorso e della sua pervasività nella costruzione della società, basti pensare che anche, per

---

giustizia, Bologna, 2007; A. SEN, *La democrazia degli altri. Perché la libertà non è un'invenzione dell'occidente*, Milano, 2004; ID., *Lo sviluppo è libertà. Perché non c'è crescita senza democrazia*, Milano, 2000; P. SINGER, *One world. L'etica della globalizzazione*, Torino, 2003; J.E. STIGLITZ, *In un mondo imperfetto. Mercato e democrazia nell'era della globalizzazione*, Roma, 2001; ID., *Bancarotta. L'economia globale in caduta libera*, Torino, 2010. M. YUNUS, *Il banchiere dei poveri*, Milano, 1998; ID., *Un mondo senza povertà*, Milano, 2008; ID., *Si può fare! Come il business sociale può creare un capitalismo più umano*, Milano, 2010.

20 "Ascoltare i cittadini d'Europa per un futuro sostenibile" (2019/C 228/06). Il §1.5 prosegue: "L'energia, i materiali, il mondo naturale, la società umana, il potere e la ricchezza che condividiamo: tutti questi elementi sono assenti nel modello attuale. Il lavoro non retribuito dei prestatori di assistenza, principalmente le donne, è ignorato, sebbene nessuna economia potrebbe funzionare senza di loro".

esempio, nel diritto privato delle società e in particolare del diritto commerciale europeo è stato introdotto il riferimento all'ambiente nella definizione di scopo delle società. In Francia, le società *benefit*, che erano state introdotte prima in USA come *Benefit corporation*[21], sono state codificate come *entreprise à missiòn* - con la *loi Pacte*[22] che ha modificato anche l'art. 1833 del *code civil* in materia di oggetto della società, inserendo dei riferimenti alla tutela dell'ambiente "*La société est gérée dans son intéret social, en prenant en considération les enjeux sociaux et environnementaux de son activité*" (1833, co. 2 c.c.)[23].

2.4. Il ruolo del digitale nella costruzione europea di un mercato sostenibile

La Risoluzione 2020/2021 dedica un capo alla strategia digitale, in tal modo confermando, ove ve ne fosse la necessità, il fatto che questa rivoluzione, con tutte le sue possibili ricadute, rappresenta uno degli assi portanti del mercato sostenibile.

D'altra parte, già nella comunicazione del 19 febbraio 2020 "Plasmare il futuro digitale dell'Europa" con cui la Commissione aveva fissato, per i prossimi cinque anni, tre obiettivi principali volti a realizzare la trasformazione digitale della nostra società, consentendo altresì

---

21 Che la *B Corp* non rappresenti la soluzione per un nuovo capitalismo R. Henderson, *op. cit*., p. 143 ss. e rilievi critici in punto di disciplina; così anche A.Frignani- P.Virano, *Le società benefit davvero cambieranno l'economia?*, in *Contr. Impr*., 2017, p. 503 ss.

22 Si tratta della *Loi 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises*, il cui testo è disponibile in www.legifrance.gouv.fr.

23 I. Tchotourian, J. Turcotte, *Le droit des sociétés*, cit., p. 11. S. Toepler, *Do Benefit Corporations Represent a Policy Threat to Nonprofits*, in *Nonprofit Policy Forum*, 2019, p.1 ss. esamina il tema della competizione tra le forme giuridiche, a seguito dell'inserimento della benefit corporation, rispetto alle altre forme per l'imprenditoria sociale. N. Kurkland, *Esop Plus Benefit Corporation: Ownership Culture With Benefit Accountability*, in *California Management Review*, 2018 , 60(4), p. 51-73; I. Tchotourian, J. Turcotte, *Le droit des sociétés au service d'une gouvernance d'entreprise sociétalement responsable? Incertitudes sur les conséquences de l'adoption de la Benefit Corporation*, in *La Revue des Sciences de Gestion*, 2018, 11; L. A. Cooper, J. Weber, *Does Benefit Corporation Status Matter to Investors? An Exploratory Study of Investor Perceptions and Decisions*, in Business & Society, Jan 2020, p. 1; D. Brakman Raiser, *Benefit Corporations – A sustainable Form of organization?*, in *Wake Forest Law Review*, 2012, p. 591 ss.

all'Europa di assumere un ruolo trainante nel panorama globale vi era un riferimento all'economia sostenibile. In particolare, secondo quella comunicazione la prossima agenda euro-unitaria deve realizzare: "*i) una tecnologia al servizio delle persone: sviluppare, diffondere e adottare tecnologie che migliorino sensibilmente la vita quotidiana delle persone. Un'economia forte e competitiva che domini e plasmi la tecnologia nel rispetto dei valori europei; ii) un'economia equa e competitiva: un mercato unico senza attriti, in cui le imprese di tutte le dimensioni e in qualsiasi settore possano competere in condizioni di parità e possano sviluppare, commercializzare e utilizzare tecnologie, prodotti e servizi digitali su una scala tale da rafforzare la loro produttività e la loro competitività a livello mondiale, e in cui i consumatori possano essere certi che i loro diritti vengano rispettati; iii) una società aperta, democratica e sostenibile: un ambiente affidabile in cui i cittadini siano autonomi e responsabili nel modo in cui agiscono e interagiscono, anche in relazione ai dati che forniscono sia online sia offline. Un approccio europeo alla trasformazione digitale che rinforzi i nostri valori democratici, rispetti i diritti fondamentali e contribuisca a un'economia sostenibile, a impatto climatico zero ed efficiente nell'impiego delle risorse*".

La indicata consapevolezza dell'Unione Europea circa la crescente digitalizzazione come fenomeno idoneo a fornire alla società nuovi canali per la condivisione delle informazioni utili alla realizzazione di un mercato sostenibile non resta senza concrete manifestazioni.

Vi sono tantissimi profili di interconnessione tra digitale e sostenibilità che riguardano la tutela dei dati, la responsabilità di chi li gestisce, la responsabilità dei soggetti. Tutti questi profili presentano spunti di disciplina privatistica estremamente rilevanti e su cui occorre meditare.

2.5. Informazioni, piattaforme on-line e trasparenza nel mercato sostenibile

Un tema centrale in questo discorso è quello della regolazione delle piattaforme *online* e, più precisamente, della responsabilità di fornire agli informatori e ai consumatori le indicazioni sui prodotti e i servizi che esse offrono. Non a caso, la Risoluzione 2020/2021 al considerando S ripropone il problema strategico dell'informazione. Da un lato c'è la necessità di condividere l'informazione e dall'altro c'è l'esigenza che la piattaforma - cuore pulsante dell'economia digitale - fornisca ai consumatori notizie affidabili sui prodotti e i servizi che offre. Il 15 dicembre

2020 è stato varato il *Digital Services Act* (DSA)[24], che unitamente al *Digital Market Act* (DMA)[25], si pone l'obiettivo di regolamentare in modo trasparente e all'avanguardia le piattaforme online e le attività e i rapporti che con esse si instaurano. In particolare, il DSA disciplina sia i servizi di intermediazione, che di *hosting*, sia le piattaforme on line che quelle di grandi dimensioni.

Evidentemente la regolazione chiara e trasparente delle piattaforme incide non solo sulla attività di autonomia privata, ma anche sulla trasparenza come valore stesso della società[26], che acquisisce, attraverso le piattaforme, un carattere rilevante per le democrazie. La recente storia europea e nordamericana dimostra come per la qualità della rappresentatività di un Paese sia di fondamentale rilevanza che non possa realizzarsi alcun processo di alterazione, sottrazione, manipolazione dei dati.

In generale quando si discorre di sostenibilità, la dimensione della trasparenza non va coniugata semplicemente sul piano delle relazioni b2b e b2c, bensì a livello di società e di istituzioni. L'accesso alle piattaforme, la diffusione delle informazioni (si veda anche il considerando R della Risoluzione 2020/2021) possono rappresentare la garanzia per costruire un diverso tipo di democrazia, se non diretta, certamente maggiormente partecipata[27]. E le garanzie di cui devono essere dotate le informazioni e i processi connessi alle piattaforme on line devono tener conto di queste implicazioni.

2.6. La sostenibilità e la valutazione dell'impatto ambientale dell'infrastruttura digitale

Il considerando T della Risoluzione 2020/2021 conferma il ruolo del settore digitale nel contribuire all'innovazione e alla promozione di

---

24 Il testo della Proposta è disponibile in https://ec.europa.eu.

25 Il testo è disponibile in https://ec.europa.eu/.

26 S. Zamagni, *Disuguali*, cit., p.133 ss. L. Floridi, *Il verde e il blu. Idee ingenue per migliorare la politica*, Milano, 2020, p. 255 ss.; T. Piketty, *Capitale e ideologia*, Milano, 2020, p. 13 ss.; S. Zuboff, *Il capitalismo della sorveglianza.Il futuro dell'umanità nell'era dei nuovi poteri*, Milano, 2019, p. 367 ss.

27 Rob Reich, *Just Giving: Why Philantropy is Failing Democracy and How It Can Do Better*, Princeton, 2018, p. 151, M. D'Eramo, *Dominio. La guerra invisibile dei potenti contro i sudditi*, Milano, 2020, p. 78 e p. 84 ss; J. Stiglitz, *Popolo, potere e profitti*, cit., p.163.

un'economia sostenibile e ribadisce la necessità di valutare l'impatto ambientale dell'infrastruttura digitale[28].

In modo puntuale, nel capo della Risoluzione 2020/2021 specificamente dedicato alla strategia digitale al servizio di un mercato sostenibile, al paragrafo 21, si fa riferimento al *passaporto digitale dei prodotti*. L'Unione Europea accoglie con favore l'annuncio di uno spazio comune europeo dei dati per le *applicazioni circolari intelligenti* e vuole sviluppare appunto un passaporto digitale dei prodotti per migliorare tracciabilità e accesso alle informazioni sulle condizioni di produzione di un prodotto, la durabilità, la composizione di un prodotto, il riutilizzo, la riparazione e tutta una serie di aspetti che possono riguardare la riparabilità ed eventualmente anche la fase di smaltimento del prodotto.

Anche qui, il discorso non nasce con la Risoluzione 2020/2021. Già nel *Circular Economy Action Plan* del 11 marzo 2020 al fine di introdurre e sviluppare l'applicazione efficace ed efficiente del nuovo quadro per i prodotti sostenibili, si afferma che la Commissione: i) istituirà uno spazio europeo dei dati per le applicazioni circolari intelligenti contenente dati sulle catene di valore e informazioni sui prodotti; ii) intensificherà, in cooperazione con le autorità nazionali, gli sforzi volti a garantire il rispetto dei requisiti di sostenibilità applicabili ai prodotti immessi sul mercato dell'UE, in particolare mediante ispezioni concertate e azioni di vigilanza del mercato.

Lo spazio europeo dei dati per le applicazioni circolari intelligenti fornirà l'architettura e il sistema di governance per stimolare applicazioni e servizi, quali i passaporti dei prodotti, la mappatura delle risorse e l'informazione ai consumatori. Di fatto, il paragrafo 21 della Risoluzione 2020/2021 rappresenta l'esigenza di creare un sistema di dati che possa consentire di tracciare e accedere alle informazioni relative alla produzione di un certo prodotto, il che può essere facilmente costruito attraverso la tecnologia *Blockchain*. Strettamente correlato a questo tema c'è quello della certificazione, cui il passaporto

---

28 *Circular Economy Action Plan* 11 marzo 2020 (COM/2020/98) in https://eur-lex.europa.eu. I soggetti coinvolti e che promuovono la transizione attraverso ricerca, innovazione e digitalizzazione sono il Fondo Europeo di sviluppo regionale, LIFE e Orizzonte Europa. A sua volta l'Istituto europeo di innovazione e tecnologia coordinerà iniziative in materia di innovazione sull'economia circolare in collaborazione con università, organismi di ricerca, l'industria e PMI all'interno delle comunità della conoscenza e dell'innovazione.

offre una base documentata. La sfida futura, sul tema, muove dall'esigenza di tenere conto anche di tanti aspetti poi più strettamente economici, quali eventualmente la proporzionalità dei costi relativi al riciclo rispetto al valore del prodotto e le esigenze di piccole e medie imprese[29].

A fronte del significativo impatto ambientale del settore digitale, il paragrafo 23 della Risoluzione 2020/2021, per quanto concerne la produzione di beni e la fornitura di servizi, invita la Commissione a valutare in che misura un indice di sostenibilità del digitale europeo che sia basato su un'analisi del ciclo di vita dei prodotti possa ottimizzare la produzione e il consumo sostenibili di tecnologie digitali, in quanto è estremamente importante scegliere un adeguato criterio di valutazione.

Nell'ambito dell'*Action Plan* sono state già approfondite alcune delle linee che qui vengono richiamate, facendo espresso rinvio alla futura adozione di un'iniziativa legislativa relativa ad una strategia in materia di prodotti sostenibili, nella quale la Commissione darà rilevanza anche alla "mobilitazione del potenziale di digitalizzazione delle informazioni relative ai prodotti, ivi comprese soluzioni come i passaporti, le etichettature e le filigrane digitali". L'*Action Plan* individua specifiche categorie catene del valore cui dare priorità, che

29 COM (2020) 103, *Una strategia per le PMI per un'Europa sostenibile e digitale*.

comprendono – quanto al settore in parola – l'elettronica e le TIC[30] e quelle relative alle batterie e ai veicoli[31].

---

[30] *Circular Economy Action Plan*, cit., sezione 3 dedicata alle Principali Catene di Valore dei Prodotti, 3.1 Elettronica e TLC: *"I rifiuti delle apparecchiature elettriche ed elettroniche continuano a costituire uno dei flussi di rifiuti in più rapida crescita nell'UE, con un tasso annuale pari attualmente al 2 %. Si stima che nell'UE meno del 40 % dei rifiuti elettronici sia riciclato. Si verifica una perdita di valore quando i prodotti del tutto o in parte funzionanti sono eliminati perché non si possono riparare, il software non è più supportato o i materiali incorporati nei dispositivi non sono recuperati. Circa due cittadini europei su tre vorrebbero poter utilizzare più a lungo i dispositivi digitali che possiedono, purché le prestazioni non siano compromesse in modo significativo. Per far fronte a queste sfide, la Commissione presenterà una "Iniziativa per un'elettronica circolare" che ricorrerà a strumenti nuovi e esistenti. In linea con il nuovo quadro strategico in materia di prodotti sostenibili, l'iniziativa promuoverà l'allungamento della durata di vita dei prodotti e comprenderà, tra l'altro, le azioni seguenti: i) misure di regolamentazione per l'elettronica e le TIC, compresi i telefoni cellulari, i tablet e i laptop a norma della direttiva sulla progettazione ecocompatibile, in modo che i dispositivi siano progettati per l'efficienza energetica e la durabilità, la riparabilità, la possibilità di upgrading, la manutenzione, il riutilizzo e il riciclaggio. Il prossimo piano di lavoro sulla progettazione ecocompatibile conterrà ulteriori dettagli al riguardo. Le misure riguarderanno anche le stampanti e i materiali di consumo come le cartucce, a meno che il settore non concluda un ambizioso accordo volontario entro i prossimi sei mesi; ii) particolare attenzione sarà rivolta alle TIC in quanto settore prioritario in cui concretizzare il "diritto alla riparazione" includendovi il diritto di aggiornare i software obsoleti; iii) misure di regolamentazione per i caricabatterie dei telefoni cellulari e i dispositivi analoghi, ivi compresi l'introduzione di un caricabatterie universale, il rafforzamento della durabilità dei cavi di ricarica e incentivi per separare l'acquisto dei caricabatterie dall'acquisto di nuovi dispositivi; iv) miglioramento della raccolta e del trattamento dei rifiuti di apparecchiature elettriche ed elettroniche, anche esaminando la possibilità di istituire a livello di UE un sistema di resa per restituire o rivendere telefoni cellulari, tablet e caricabatterie usati; riesame delle norme dell'UE sulle restrizioni dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche e elaborazione di orientamenti per migliorare la coerenza con la legislazione applicabile, tra cui il regolamento REACH e la direttiva sulla progettazione ecocompatibile"*.

Circular Economy Action Plan, cit., 3.2: *"Le batterie e i veicoli sostenibili sono alla base della mobilità del futuro. Per progredire rapidamente nel rafforzamento della sostenibilità della catena di valore emergente delle batterie per la mobilità elettrica e aumentare il potenziale di circolarità di tutte le batterie, quest'anno la Commissione proporrà un nuovo quadro normativo per le batterie. Questa proposta legislativa si baserà sulla valutazione della direttiva relativa alle pile e sul lavoro della "European batteries Alliance", tenendo conto degli elementi seguenti: i) regole sul contenuto riciclato e misure per migliorare i tassi di raccolta e riciclaggio di tutte le batterie, garanzia del recupero dei materiali di valore e elaborazione di orientamenti destinati ai consumatori; ii) il problema delle pile non ricaricabili al fine di eliminare progressivamente il loro utilizzo laddove esistono alternative;*

Il paragrafo 24 della Risoluzione 2020/2021 riguarda la potenziale impronta ambientale dei dati che non siano necessari e cioè applicazioni quali file, video, foto, messaggi di posta elettronica che siano indesiderati e cioè, quindi, vedere come producendo una qualunque impronta ambientale causino un eccessivo dispendio energetico. L'utilizzo della infrastruttura digitale richiede un forte consumo energetico, pertanto il Parlamento sollecita una valutazione dell'impronta di carbonio e ambientale, nonché del suo impatto sul comportamento dei consumatori e dell'adozione di adeguate misure per ridurlo. A questo profilo si affianca al paragrafo 25, quello che concerne l'istituzione di sistemi di ricarica universale per ridurre la produzione e ridurre anche i rifiuti e i rifiuti elettronici.

2.7. Economia circolare, appalti e digitale

L'economia circolare rappresenta una delle linee della trasformazione industriale verso temi centrali della sostenibilità, quali la neutralità climatica e la competitività a lungo termine. Essa sfrutta le tecnologie digitali per quanto riguarda la tracciabilità, la rintracciabilità e la mappatura delle risorse e delle tecnologie verdi. Ancora una volta in modo esatto, il legislatore comunitario prende atto che le tecnologie digitali apportano una forte innovazione anche per quello che riguarda l'economia circolare. Il paragrafo 22 della Risoluzione invita puntualmente la Commissione a sviluppare norme e protocolli specifici in materia di economia circolare.

La proposta è di adottare protocolli per accedere a dati interoperabili e condividerli tra aziende, investitori e autorità sempre allo scopo di sviluppare opportunità commerciali e favorire nell'ambito del nuovo QFP i finanziamenti a favore della ricerca e dell'innovazione nelle tecnologie sostenibili.

Un ulteriore elemento degno di nota riguarda la digitalizzazione degli appalti, al paragrafo 26, in quanto gli appalti pubblici debbano essere posti al centro del piano di ripresa economica in linea con il

---

iii) i requisiti di sostenibilità e trasparenza per le batterie tenendo conto, ad esempio, dell'impronta di carbonio del processo di produzione delle batterie, dell'approvvigionamento etico di materie prime e della sicurezza dell'approvvigionamento, agevolando il riutilizzo, il cambio di destinazione e il riciclaggio".

Green Deal europeo sostenendo gli sforzi di innovazione del settore privato e i processi di digitalizzazione degli appalti pubblici stabilendo incentivi adeguati per promuovere la produzione e il consumo sostenibili chiedendo che sia data priorità alla incentivazione della domanda di beni e servizi ecologici con una minore impronta ambientale nella promozione di criteri sociali ed ambientali.

3. Digitalizzazione e proprietà intellettuale

Lucio Casalini

3.1. Premessa

Il diritto di accesso alla conoscenza[1] è ampiamente regolato dalle norme sulla proprietà intellettuale. Su questo complesso impianto normativo si fondano le condizioni affinché la circolazione delle opere dell'ingegno e dei prodotti della conoscenza – ossia di beni immateriali – possa soddisfare gli interessi dei diversi soggetti coinvolti, amplificati dal loro dispiegarsi nella cd. società dell'informazione[2].

Con riferimento a tali peculiari interessi vi è, in primo luogo, l'interesse dell'autore dell'opera, il quale vanta, secondo la ricostruzione

---

1 Ai fini dell'analisi da intendersi come «[l]a conoscenza che, in rete, non ha il carattere naturale della scarsità, ed è quindi suscettibile di usi non rivali, configurandosi propriamente come un *common*», cfr. RODOTÀ, *Il diritto di avere diritti,* Laterza, 2012, p. 113. E, più diffusamente sul rapporto tra accesso e conoscenza, cfr. *ibidem*, p. 130.

2 L'espressione "società dell'informazione" è usata soprattutto dai sociologi per indicare l'attuale società post-industriale. Ciò che più spiccatamente la caratterizza è il prevalere di un bene immateriale come l'informazione rispetto all'industria, il settore dell'economia che è stato trainante per tutto il XX secolo. Si veda in argomento la voce "società dell'informazione" in *Enciclopedia della scienza e della tecnica Treccani* ove si legge che «l'elevato dinamismo che caratterizza la società contemporanea colloca l'informazione in posizione centrale, attribuendole il ruolo di risorsa strategica che condiziona l'efficienza dei sistemi, divenendo fattore di sviluppo sociale ed economico, di crescita e di ricchezza culturale. La società dell'informazione è un contesto in cui le nuove tecnologie informatiche e di telecomunicazione assumono un ruolo fondamentale nello sviluppo delle attività umane». Per un ulteriore approfondimento cfr. ORLANDO, *Le informazioni*, CEDAM, 2012, qui l'Autore delinea distinte nozioni giuridiche di informazione, a partire dalla configurazione di due funzioni fondamentali associate alle attività di natura informativa giuridicamente rilevanti: la funzione di riproduzione e quella di rappresentazione.

dualistica tradizionale[3], da un lato diritti di natura *morale* (ovvero, *in primis*, la possibilità di rivendicare in qualsiasi luogo e momento la paternità dell'opera), dall'altro diritti di natura *patrimoniale* (ovvero le diverse facoltà di sfruttamento economico dell'opera stessa). Vi è, poi, l'interesse di un numero indeterminato di potenziali fruitori, che di quella stessa opera intendano *lato sensu* godere e disporre, per un personale sviluppo ed arricchimento.

Secondo una interpretazione costituzionalmente orientata, il diritto d'autore è chiamato a svolgere un ruolo cruciale, poiché dirimente sia sul piano sociale – sono coinvolti valori fondamentali costituzionalmente protetti, come il pieno e il libero sviluppo della persona umana (art. 2 Cost.) e la promozione e lo sviluppo della cultura e della ricerca scientifica e tecnica (art. 9 Cost.) – sia sul piano economico – poiché il suo corretto funzionamento è precondizione indispensabile per innescare l'innovazione e la crescita, oltre che per garantire l'eguaglianza (art. 3 Cost.) nell'accesso alle risorse e la funzione sociale della proprietà (art. 42 Cost.).

Al fine di favorire – ad un tempo – creatività, innovazione e la più ampia diffusione della conoscenza, il processo di modernizzazione del diritto d'autore, in armonia con il nuovo contesto digitale, prima ancora che un'opportunità risulta, allora, essere un'esigenza.

3.1.1. Struttura e finalità dell'analisi

Questa ricerca, lungi dal voler pervenire a conclusioni definitive, mira, all'opposto, ad interrogarsi sui punti di congiunzione e di frizione tra il dirompente fenomeno di digitalizzazione delle risorse e l'auspicato processo di modernizzazione del diritto d'autore.

In particolare, dopo aver individuato il quadro normativo e delimitato il campo dell'indagine (§ 3.2), tale peculiare rapporto verrà riletto alla luce del recente attivismo del legislatore europeo in questo settore (§ 3.3), confluito da ultimo nella direttiva UE 790/2019 (§ 3.4). Si proverà, quindi, a mettere a fuoco le principali novità introdotte ricorrendo all'ausilio delle nuove tecnologie al regime di eccezioni e limitazioni (§ 3.4.1), in particolare attraverso le tecniche del cd. *text and data*

---

[3] Cfr. Spedicato, *Principi di diritto d'autore*, Il Mulino, 2020, p. 85, che richiama l'immagine del *Doppelrecht*, utilizzata dai giuristi tedeschi di impostazione kohleriana per riferirsi a questo tipo di diritti composti da due parti distinte e tra loro reciprocamente autonome.

mining (§ 3.4.2), nonché le ambiguità insite nella componente tecnologica. Da ultimo si cercherà di delineare, *de iure condendo*, le prospettive di analisi in tema di digitalizzazione, *open access* e proprietà intellettuale (§ 3.5), in vista del recepimento della direttiva nel nostro ordinamento.

3.2. Quadro normativo e delimitazione del campo dell'indagine.

Come anticipato, il diritto a beneficiare dell'accesso ad internet ed alle fonti della conoscenza disponibili in rete occupa, dunque, una posizione centrale [4]. Tuttavia, il quadro normativo *in subjecta materia* si presenta assai articolato e multilivello. Pertanto, pare opportuno preliminarmente delimitare il campo dell'indagine.

Nell'ampio *genus* della proprietà intellettuale si tende a ricomprendere tanto i diritti di privativa industriale, quanto il diritto d'autore ed i diritti ad esso connessi[5].

Tuttavia, nella prospettazione tradizionale, con tale espressione si suole fare riferimento al solo campo del diritto d'autore, mentre per gli altri diritti si parla, specificamente, di proprietà industriale. Distinzione che ha trovato un contrappunto in due fondamentali Convenzioni internazionali della fine del sec. XIX: la Convenzione di Berna del 1886 (ratificata dall'Italia con L. 20 giugno 1978, n.399, nel testo di Parigi del 24 luglio 1971), dedicata alla materia del diritto d'autore, e la Convenzione di Parigi del 1883 (ratificata dall'Italia con L. 28 aprile

---

[4] In un saggio scritto nel 2000 dal titolo *L'Era dell'Accesso. La rivoluzione della new economy*, l'economista ed attivista statunitense Jeremy Rifkin sostiene con lucidità e lungimiranza la progressiva perdita di rilevanza della proprietà fisica a favore del controllo dei flussi di valore e, dunque, l'importanza strategica del concetto di "accesso" alle reti ed alle informazioni, che prenderà il sopravvento sul mero titolo di proprietà dei beni, cfr. RIFKIN, *The age of access: the new culture of hypercapitalism, where all of life is a paid for experience*, 2000. Sul punto cfr. inoltre l'approfondita riflessione di DEHART, KLOZA, *Internet (access) as a new fundamental right,* in *European Journal of Law and Technology,* 2012.

[5] Per fare il punto sulla disciplina, si rinvia integralmente a UBERTAZZI, *Commentario breve alle leggi su proprietà intellettuale e concorrenza,* Padova, 2012; ID. (a cura di), *La proprietà intellettuale,* Torino, 2011; FERRETTI, *Il nuovo diritto d'autore. Manuale operativo,* Miano, 2012; GALLI, GAMBINO, *Codice commentato della proprietà industriale e intellettuale,* Torino, 2011; COLANGELO, *Diritto comparato della proprietà intellettuale,* Bologna, 2011; SPEDICATO, *op. cit.*

1976, n.424, nel testo di Stoccolma del 14 luglio 1967), che ha gettato le basi per la protezione della proprietà industriale.

I due settori sono, poi, confluiti nella più ampia nozione di proprietà intellettuale, sotto l'azione congiunta di altri due fondamentali accordi internazionali: la Convenzione di Stoccolma del 1967 (ratificata dall'Italia con L. 28 aprile 1976, n.424), istitutiva dell'Organizzazione mondiale della proprietà *intellettuale* (WIPO), e l'accordo TRIPs del 1994 (ratificato dall'Italia con L. 29 dicembre 1994, n.747).

Nel nostro ordinamento, sul piano sostanziale, ciò che attualmente caratterizza la proprietà intellettuale è la struttura dominicale dei diritti che, conformemente alla tradizione romanistica, si configurano come diritti esclusivi su beni immateriali. Oggetto del diritto è, infatti, una *res incorporales,* ovvero – mutuando le espressioni della dottrina tomistica – il cd. *corpus mysticum* (l'opera letteraria o l'idea innovativa) e non anche il supporto materiale, il cd. *corpus mechanicum* (ad es. il libro che incorpora un romanzo)[6].

L'uso del termine "proprietà" è dunque influenzato da ragioni storiche di egemonia culturale e dogmatica del diritto di proprietà come categoria concettuale, con tutte le conseguenze in termini di esclusività, pienezza ed assolutezza che esso porta con sé[7]. I diritti di proprietà intellettuale, dunque, sono quei particolari diritti di esclusiva

---

6 Cfr. Spedicato, *op. cit.*, p. 23.

7 Nella manualistica cfr. Trabucchi, *Istituzioni di diritto civile,* Cedam, 2019, p. 725; Gazzoni, *Manuale di diritto privato,* ESI, 2019, p. 211; Perlingeri, *Istituzioni di diritto civile*, 2020, p. 114.

che consentono a chi ne è titolare uno sfruttamento economico, limitato nel tempo[8], con temporanea sottrazione dalle regole della concorrenza. Si realizza così un monopolio[9], assistito da efficaci rimedi giudiziari *ad hoc*, anche di natura cautelare, per impedirne l'utilizzazione a terzi in assenza di consenso[10].

Il nostro codice civile contempla alcune norme a carattere generale (artt. 2563-2595 c.c.), collocate nel Libro V dedicato al lavoro, ma l'analisi verrà delimitata alla materia del diritto d'autore, regolata fondamentalmente dagli artt. 2575-2579 c.c. e dalla L. 22 aprile 1941, n. 633[11] e successive modificazioni, soprattutto di matrice comunitaria[12], volte al rafforzamento dei diritti di esclusiva e all'ampliamento dei beni tutelabili[13].

Quanto al contenuto del diritto d'autore troviamo un chiaro referente normativo nell'art. 2577 c.c., ove è compiuta la scomposizione, *supra* accennata, in una componente *morale*, illimitata nel tempo e nello spazio, accanto ad una componente *patrimoniale*, assoggettata a limiti di tempo e suscettibile di formare oggetto di contrattazione. A

---

8 Per il diritto d'autore i diritti di utilizzazione economica dell'opera durano fino a 70 anni dopo la morte dell'autore; mentre per i diritti di brevetto il limite arriva a 20 anni. In entrambi i casi, tale limite è improrogabile e, alla scadenza, il bene entra nel pubblico dominio.

9 Cfr. CASO, *I libri nella "tempesta perfetta": dal copyright al controllo delle informazioni digitali,* in *Riv. crit. dir. priv.,* XXXI, n. 1, 2013, ove afferma che «[l]a scelta del legislatore è una scelta di equilibrio. Monopolio sì, ma limitato nel tempo e in ampiezza». Poi aggiunge che «esistono margini di libertà della fruizione grazie a meccanismi come le libere utilizzazioni e il fair use». Più ampiamente, cfr. FERRI, *Manuale di diritto commerciale*, Utet, 2019, p. 131.

10 Nell'apparato rimediale a disposizione del titolare si annoverano, ad esempio, l'inibitoria, il sequestro, assegnazione in proprietà dei beni contraffatti, il plagio.

11 La disciplina della proprietà industriale si rinviene, invece, nel relativo codice, emanato con il d.lgs. 10 febbraio 2005, n. 30, noto come codice della proprietà industriale (c.p.i.).

12 La Legge sul diritto d'autore è stata attraversata da numerosi interventi modificativi nel corso degli oltre settanta anni dalla sua entrata in vigore. Per una panoramica, cfr. DE SANCTIS, *Manuale del nuovo diritto d'autore,* Editoriale Scientifica, 2012.

13 Ciò ha portato anche ad un accentuarsi del dibattito, soprattutto internazionale, sul rapporto tra proprietà intellettuale e diritto della concorrenza. Mette conto rilevare che, in taluni casi, per temperare la portata dell'esclusiva si è fatto ricorso alle regole in materia *antitrust* (*Magill,* Corte di Giustizia C-241/91 e *IMS Health* C-418/01).

quest'ultimo riguardo, la L. n. 633/1941 regola anche i principali contratti[14] per mezzo dei quali l'autore dispone dei relativi diritti patrimoniali.

La cornice normativa si chiude con il recente regolamento sul ruolo dell'Autorità Garante per le Garanzie nelle Comunicazioni (AGCOM)[15] in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica[16], che introduce un particolare *iter* amministrativo a tutela dei diritti violati in rete[17].

3.3. L'azione dell'Unione Europea

Sul piano comunitario, il diritto di proprietà intellettuale e, in particolare, il diritto d'autore che qui ci occupa sono stati oggetto di attenzione crescente.

Questa è testimoniata dal singolare fermento legislativo degli ultimi anni, che ha trovato la propria base giuridica, anzitutto, nell'art. 17 della stessa Carta dei diritti fondamentali dell'Unione Europea[18], oltre che in due fondamentali norme dei Trattati: l'art. 3 TUE (in particolare al co. 3, dove si «promuove il progresso scientifico e tecnolo-

---

14 Gli artt. 118-136, ad esempio, disciplinano il contratto di edizione, con il quale l'autore concede (in via esclusiva, salvo patto contrario) ad un editore l'esercizio del diritto di pubblicare l'opera, per conto e a spese dell'editore. Quest'ultimo s'impegna a riprodurre l'opera e metterne in vendita le riproduzioni, pagando all'autore il compenso pattuito, generalmente determinato in misura percentuale sul prezzo di copertina.

15 Allegato A alla Delibera n. 680/13/Cons del 12 dicembre 2013.

16 Per una efficace analisi delle disposizioni si veda Orofino, *L'intervento regolamentare dell'AGCOM in materia di diritto d'autore: profili di criticità formale e sostanziale,* in Pizzetti (a cura di), *Il caso del diritto d'autore,* II ed., Torino, 2013, ove l'Autore sottolinea che «la regolamentazione del diritto d'autore non è andata di pari passo con l'evoluzione tecnologica».

17 Ad oggi sono molteplici le violazioni segnalate all'AGCOM, ma la scelta di delegare la repressione del fenomeno della pirateria in rete alla regolamentazione amministrativa è considerato in dottrina assai controverso ed ha sollevato particolari perplessità, tanto da non poter essere considerato, secondo alcuni, parte del processo di modernizzazione del diritto d'autore. Cfr. Bertoni, Montagnani, *La modernizzazione del diritto d'autore e il ruolo degli intermediari Internet quali propulsori* delle *attività creative in rete,* in *Diritto dell'Informazione e dell'Informatica,* 1, 2015; Papa (a cura di), *Il diritto d'autore nell'era digitale*, Giappichelli, 2019, pp. 1-13, 39-47, 57-73.

18 Per un'analisi critica, puntuale ed approfondita, si rinvia integralmente a Sganga, *Propertizing European Copyright. History, Challenges and Opportunities*, Elgar, 2018.

gico») e l'art. 179 TFUE (che auspica la realizzazione di uno Spazio Europeo della Ricerca, entro cui persone e contenuti possano circolare liberamente, in virtù di una «quinta libertà»[19], essenziale allo sviluppo dell'Europa).

Prima tappa fondamentale del processo di armonizzazione in tema di diritto d'autore è stata, certamente, l'adozione della direttiva 29/2001/CE, del 27 settembre 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (cd. direttiva *infosoc*).

Questo primo significativo intervento del legislatore europeo è volto al superamento del principio di territorialità, ormai atavico, che informa la materia. In essa sono previste eccezioni e limitazioni al diritto di esclusiva dell'autore e dei titolari dei diritti connessi, al fine di dare maggiore flessibilità all'intero sistema del *copyright*, perennemente costretto ad adeguarsi ai rapidi avanzamenti dell'innovazione tecnologica[20]. È interessante rilevare fin d'ora che la direttiva lascia ampia facoltà ai singoli Stati membri di stabilire eccezioni e limitazioni ai diritti esclusivi sull'opera (ad es. riproduzione, comunicazione, distribuzione)[21].

In seguito, si è registrato un nuovo deciso impulso dell'Unione Europea, con l'affermazione di un principio di notevole portata. Attraverso raccomandazioni della Commissione ed un corposo *impact assessment*, ha stabilito che i risultati della ricerca scientifica condotta mediante l'utilizzo di risorse pubbliche debbano essere resi utilizzabili

---

19 L'espressione compare per la prima volta nelle conclusioni del Consiglio Europeo del 13 e 14 marzo 2008, che invita a creare una «quinta libertà» al fine di eliminare gli ostacoli alla libera circolazione delle conoscenze.

20 Nella direttiva è tracciata la linea di *discrimen* tra diritto esclusivo e libera utilizzazione, quale fondamentale momento per stabilire quale sia la tutela riconosciuta al diritto d'autore. Da qui vengono stabilite le deroghe alla sua esclusività, per tre ordini di ragioni: i) tutela della cultura e di interessi superiori; ii) ovviare ad illeciti imperseguibili; iii) forme di utilizzazione effimere.

21 Come noto, l'impianto legislativo di eccezioni e limitazioni è costruito attorno alla elencazione dell'art. 5 dalla direttiva 29/2001/CE, ove sono tipizzate le ipotesi consentite di utilizzazione dell'opera ed inoltre è data facoltà agli Stati membri di introdurne di nuove all'interno del proprio ordinamento statale, purché i titolari dei diritti ricevano un *equo compenso*. La norma si chiude stabilendo che le eccezioni e le limitazioni in essa contemplate «sono applicate esclusivamente in determinati casi speciali che non siano in contrasto con lo sfruttamento normale dell'opera o degli altri materiali e non arrechino ingiustificato pregiudizio agli interessi legittimi del titolare».

da parte della collettività ed essere, perciò, sottoposti inderogabilmente ad un regime di libero accesso[22].

Questa presa di posizione della Commissione rinsalda la connessione tra accesso e libera circolazione della conoscenza, spostando l'angolo visuale: l'esito di uno studio condotto con fondi pubblici può dirsi *ab origine* bene comune accessibile a tutti. Ad un'attenta osservazione non sfugge come tale principio sia destinato ad avere una portata dirompente sulla prassi contrattuale nel perimetro del mercato unico digitale europeo.

3.4. Prime riflessioni attorno alla direttiva 790/2019/UE: tra armonizzazione e nuovi assetti a geometria variabile

Proprio al fine di promuovere la piena realizzazione del mercato unico digitale è stata adottata, da ultimo, la direttiva 790/2019/UE del Parlamento europeo e del Consiglio, il 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale, che modifica le direttive 96/9/CE e 2001/29/CE.

Con essa, il legislatore europeo si pone l'obiettivo di rafforzare l'armonizzazione del quadro normativo comunitario del diritto d'autore nel peculiare ambito delle nuove tecnologie digitali e, in particolare, di Internet.

A questo fine, sembra, *prima facie*, legittimare l'utilizzo di alcune attività estremamente rilevanti per la libera e piena diffusione delle informazioni e dei dati, in particolare della ricerca scientifica, sull'onda delle più evolute tecniche di estrazione di dati e dei processi di digitalizzazione.

Il riferimento corre alle cd. tecniche di *text and data mining* (TDM), finalizzate all'estrazione di informazioni e dati (artt. 3-4), nonché all'utilizzo di opere nell'ambito delle attività didattiche digitali (art. 5), alla conservazione del patrimonio culturale (art. 6), all'utilizzo di opere fuori commercio possedute da istituti di tutela del patrimonio culturale (art. 7). Tutte attività che, come sottolinea il considerando 8 della medesima direttiva, «possono arrecare beneficio […] alla comunità di ricerca e, in tal modo, sostenere l'innovazione».

---

22 Cfr. Raccomandazione della Commissione del 17 luglio 2012 sull'accesso all'informazione scientifica e sulla sua conservazione (2012/417/UE), in *eur-lex.europa.eu*.

Soffermando, in particolare, l'attenzione sugli artt. 3 e 4, è possibile constatare come si riconoscano, attraverso il *text and data mining* specifiche eccezioni a favore degli organismi di ricerca e degli istituti di tutela del patrimonio culturale con riferimento ai diritti di cui all'art. 5, lett a) e all'art. 7, par. 1, della direttiva 1996/9/CE, nonché ai diritti di cui all'art. 2 della direttiva 2001/29/CE.

Ne consegue che, in caso di estrazione di dati e informazioni per scopi di ricerca scientifica da opere alle quali si ha legalmente accesso, gli organismi di ricerca non debbano essere sottoposti alle più restrittive previsioni prescritte nell'ambito della tutela giuridica delle banche dati e, soprattutto, in materia di riproduzione, le quali sono destinate a riconoscere in via esclusiva agli autori la possibilità di autorizzare o vietare la riproduzione, diretta o indiretta, delle proprie opere.

Al fine di garantire tale obiettivo, il par. 4 dell'art.3 attribuisce, altresì, agli Stati membri il precipuo compito di instaurare un dialogo tra titolari dei diritti ed enti in modo da consentire l'individuazione concorde di nuove *best practises* per l'applicazione di tali eccezioni.

Più in generale, quindi, se, da una parte, la Convenzione di Berna introduce le cd. libere utilizzazioni e, dall'altra, la direttiva 2001/29/CE le qualifica come deroghe limitate e specifiche, da recepire facoltativamente a livello nazionale[23], con la direttiva *copyright* il decalogo degli usi leciti delle opere protette, che è tale se sussiste la previa autorizzazione del titolare, diventa obbligatorio, salvo che per l'eccezione di ricerca scientifica e di insegnamento, e non più discrezionalmente rimesso alla volontà degli Stati membri[24].

Tuttavia, la dottrina ha accolto con un certo sfavore la nuova disciplina, rilevandone le molteplici contraddittorietà, probabilmente frutto del travagliato iter di adozione nelle sedi istituzionali europee[25].

---

[23] Fatta eccezione per le cd. copie temporanee, *ex* art. 5, co. 1, di cui se ne sancisce l'obbligatorietà.

[24] Così FALCE, *Direttiva Copyright 2019: fair use ed eccezioni al copyright tra esigenze di "apertura" e necessità di indirizzo*, in *Filodiritto*, 2019. Paradigmatico, in questo senso, è la previsione, all'art. 5 della direttiva *infosoc,* di ben 21 eccezioni e limitazioni ai diritti di riproduzione e comunicazione al pubblico, di cui una sola obbligatoria per gli Stati membri. Almeno su questo piano, dunque, la recente direttiva *copyright* si pone in decisa controtendenza rispetto al precedente approccio europeo.

[25] Cfr. CASO, *The academic copyright in the age of commodification of scientific research*, in *SCIRES-IT – SCIentific RESearch and Information Technology*, 2020, p. 25; PAPA (a cura di), *op. cit.*, p. 11.

A ben vedere, infatti, il regime delle eccezioni e delle limitazioni si presenta ancora non pienamente armonizzato, essendo agevole rilevare diversi profili di disomogeneità che, prevedibilmente, non verranno risolti in sede di recepimento. Di tal guisa, sembrerebbe tradito uno dei principali obiettivi che lo stesso legislatore europeo si è prefissato con questo intervento: al considerando 5, infatti, riconosce apertamente che, in specifici settori, «la natura facoltativa delle eccezioni e limitazioni di cui alla direttiva 96/9/CE, 2001/29/CE e 2009/4/CE […] può avere un impatto negativo sul funzionamento del mercato interno».

Sebbene lo sforzo appaia apprezzabile – almeno nei limiti in cui, da una parte, viene acceso finalmente un primo faro sull'attività precipuamente svolta dagli organismi di ricerca e, dall'altra, si cerchi di introiettare tecniche avanzate di digitalizzazione e trattamento di informazioni e dati, incentivando l'uso di software a ciò deputati – il quadro che emerge sembra ancora piuttosto confuso. Ne consegue un nuovo assetto a geometria variabile: in parte armonizzato, laddove si sancisce il carattere obbligatorio delle eccezioni e limitazioni, in parte ancora disomogeneo, ove affidato all'autonomia normativa dei singoli legislatori nazionali[26].

Nel paragrafo che segue, si cercherà di mettere in luce ulteriori criticità che sembrano emergere dal dato normativo, già a partire dai problemi definitori[27].

3.4.1. (segue) Sull'eccezione di *text and data mining*

Il Titolo III della direttiva *copyright* è significativamente intitolato "Misure miranti ad adeguare le eccezioni e limitazioni all'ambiente digitale e al contesto transfrontaliero" e all'art. 7, di chiusura al medesimo titolo, si sancisce l'imperatività delle norme in esso contenute.

In particolare, ai sensi dell'art. 2 della direttiva, con *text and data mining* si deve intendere «qualsiasi tecnica di analisi automatizzata volta ad analizzare testi e dati in formato digitale avente lo scopo di

---

26 Cfr. Spedicato, *op. cit.*, p. 191.

27 Sui problemi definitori dei termini «dato» e «informazione» cfr. Strowel, *Big Data and Data Appropriation in the EU*, in Aplin (ed.), *Research Handbook on Intellectual Property and Digital Technologies*, Cheltenham, UK-Northampton, MA, USA, Edward Elgar, 2020, p. 107.

generare informazioni inclusi, a titolo non esaustivo, modelli, tendenze e correlazioni»[28].

All'interno dei singoli Stati membri dovrà essere introdotta un'eccezione per le riproduzioni e le estrazioni di testo e di dati, da opere o altri materiali cui si abbia legalmente accesso, a condizione che l'utilizzo delle stesse non sia stato espressamente riservato dai titolari dei diritti, ad esempio attraverso strumenti che consentano la lettura automatizzata di contenuti resi pubblicamente disponibili online[29].

L'art. 3, nel tratteggiare l'ambito dell'eccezione in tema di riproduzioni ed estrazioni per scopi di ricerca scientifica, richiama soggettivamente gli organismi di ricerca e gli istituti di tutela del patrimonio culturale. Ai sensi dell'art. 2 della direttiva, rubricato "Definizioni", per "organismo di ricerca" deve intendersi «un'università, comprese le relative biblioteche, un istituto di ricerca o qualsiasi altra entità il cui obiettivo primario sia condurre attività di ricerca scientifica oppure condurre attività didattiche che includano altresì attività di ricerca scientifica: a) senza scopo di lucro o reinvestendo tutti gli utili nella propria attività di ricerca scientifica, o b) con una finalità di interesse pubblico riconosciuta da uno Stato membro, in modo che non sia possibile l'accesso su base preferenziale ai risultati generati da detta ricerca scientifica da parte di un'impresa che esercita un'influenza determinante su tale organismo». Per "istituto di tutela del patrimonio culturale", invece: «una biblioteca accessibile al pubblico, un museo, un archivio o un istituto per il patrimonio cinematografico o sonoro».

Il legislatore europeo ha scelto di offrire, pertanto, una elencazione esemplificativa dei soggetti che possono ricondursi a tale definizione, il che appare, *prima facie*, eccessivamente restrittivo e foriero di ambiguità. Inoltre, non si preoccupa di chiarire chi, in concreto, sarà investito del ruolo di riproduzione ed estrazione. Sennonché, è appena il

---

[28] Per un eccellente inquadramento si rinvia ai lavori del Max Planck Institute, che in tema di eccezioni ha fornito importanti spunti in parte considerati dalle Istituzioni Europee in sede di finalizzazione e approvazione della stessa direttiva. Cfr. HILTY, HEIKO, *Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules Part B Exceptions and Limitations*, Max Planck Institute for Innovation & Competition Research Paper, n. 17-02, disponibile al sito: papers.ssrn.com/sol3/papers.cfm?abstract_id=2900110.

[29] «Sia l'eccezione *ex* art. 3, sia quella *ex* art. 4 sono subordinate al fatto che chi effettua il TDM deve avere legalmente accesso alle opere o agli altri materiali. Ciò implica l'aver stipulato una licenza con il titolare del diritto o che il contenuto sia stato messo a disposizione gratuita su Internet», così CASO, *op. cit.*, p. 20.

caso di notare come difetti una definizione di dati e di informazioni e come, gli stessi, non siano protetti in quanto tali dal diritto autoriale, che si limita, come noto, a proteggere la forma creativa di un'opera, senza estendere le tutele del diritto esclusivo alle informazioni e ai dati incorporati nell'opera stessa[30]. Alcuni interpreti hanno sostenuto al riguardo che il TDM è tuttora un'attività non toccata dal diritto di riproduzione, in base all'assunto che il diritto di riproduzione riguarda pur sempre l'opera e la sua valenza comunicativa, non i dati di cui è composta[31].

Non sembra fare chiarezza neppure il considerando 8, ove si sottolinea che «in alcuni casi, l'estrazione di testo e di dati può riguardare atti protetti dal diritto d'autore dal diritto *sui generis* sulle banche dati, o entrambi, in particolare la riproduzione di opere o altro materiale, l'estrazione di contenuti da una banca dati o entrambi, come avviene ad esempio quando i dati vengono normalizzati nel processo di estrazione di testo e di dati. Se non sussistono eccezioni né limitazioni è richiesta un'apposita autorizzazione ai titolari dei diritti».

E nemmeno il successivo art. 4 fa particolarmente luce sul punto. La norma dispone un'eccezione per le riproduzioni e le estrazioni effettuate da opere o altri materiali cui si abbia legalmente accesso ai fini dell'estrazione di testo e di dati, a condizione che l'utilizzo delle opere e di altri materiali non sia stato espressamente riservato dai titolari dei diritti in modo appropriato. Certamente non facile sarà prevedere cosa si intenderà per "riserva appropriata" in sede applicativa[32].

---

30 Sul punto ha aperto un primo dibattito dottrinario Hugenholtz, *Data Property: Unwelcome Guest in the House of IP*, Institute for Information Law (IViR), in *Lohsse, Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden-Baden, Nomos, 2017, p. 75-99. Sulle opportunità ed i rischi dell'uso dei Big Data nella scienza cfr. Leonelli, *La ricerca scientifica nell'era dei Big Data. Cinque modi in cui i Big Data danneggiano la scienza, e come salvarla*, Meltemi, 2018. Ad ogni modo, l'estrazione di testo e di dati non dovrebbe, né potrebbe, qualificare una forma di sfruttamento coperta da diritti di esclusiva, diritti d'autore o altri diritti *sui generis*. Critico sul punto Caso, *Il conflitto tra diritto d'autore e ricerca scientifica nella disciplina del text and data mining della direttiva sul mercato unico digitale*, in *Trento LawTech Research Papers*, nr. 38, 2020, p. 22. che afferma «[i]n definitiva, questa disciplina sembra più puntata a creare un mercato secondario del TDM consegnandolo nelle mani dei titolari dei diritti che a liberare l'analisi dei dati».

31 Cfr. Caso, *op. cit.*, p. 16, in particolare nota 33.

32 Ai sensi dell'art. 5 gli Stati membri dovranno altresì consentire l'utilizzo digitale di opere e altri materiali esclusivamente per finalità illustrativa ad uso didattico, nei limiti di quanto giustificato dallo scopo non commerciale perseguito, purché tale

In conclusione, sarà giocoforza rimesso agli Stati membri individuare in maniera più stringente e analitica il perimetro della nuova eccezione, costretti tra i due poli del difficile bilanciamento tra tutela autoriale e diffusione della conoscenza[33]. E laddove con il recepimento nazionale non si colmino queste incertezze, si lascerà all'autorità giudiziale il compito – non facile – di interpretare tali norme.

3.5. Prospettive di analisi *de iure condendo*

Il processo di digitalizzazione spiana la strada ad una rimeditazione profonda della disciplina della proprietà intellettuale.

Come avvenuto nel XV sec. con la rivoluzione guthemberghiana, che ha segnato il passaggio dalla cultura manoscritta alla cultura tipografica con l'invenzione della stampa, nel XXI sec. è la rivoluzione digitale, caratterizzata dalla smaterializzazione dei beni, a scardinare il vecchio sistema e a rivelarsi potenzialmente in grado di arginare quella che, dalla migliore dottrina, è stata definita una deriva protezionistica del diritto di proprietà intellettuale[34].

Anche in questo settore, si registra, infatti, ancora una volta, la natura ancipite del processo di digitalizzazione. Se da una parte consente la massima diffusione possibile della conoscenza, condizionata unicamente dalla possibilità di accesso alla rete; dall'altra offre uno strumentario tecnologico che, se piegato a certi utilizzi, ne determina una indesiderabile *overprotection*[35].

Si pensi, ad esempio, ai cd. *digital rights management* (DRM), programmi informatici attraverso cui è possibile fissare cosa si possa e non

---

utilizzo: i) avvenga sotto la responsabilità di un istituto di istruzione, nei suoi locali o in altro luogo o tramite un ambiente elettronico sicuro accessibile solo agli alunni o studenti e al personale docente di tale istituto; ii) sia accompagnato dall'indicazione della fonte, compreso il nome dell'autore, tranne quando ciò risulti impossibile.

33 Ancora aspramente critico CASO, *op. cit.*, p. 23, ove afferma che «la disciplina delle eccezioni e limitazioni contenuta nella direttiva CDSM risulta alquanto deludente. Avrebbe dovuto rappresentare un argine all'ordine privato, ma si rivela confusa, debole e inefficace. Ciò vale anche per le eccezioni e limitazioni riferite alle attività di TDM. Alcuni correttivi sono auspicabili in sede di attuazione della direttiva. Tuttavia, i difetti dell'impostazione di fondo rimangono tutti».

34 Cfr. GHIDINI, *Proprietà intellettuale: per una prospettiva sistematica*, in *Dir. merc. tecnol.*, 2013; ID., *Opere dell'ingegno: più libertà per i «derivati culturali»*, in *Dir. merc. tecnol.*, 2014.

35 Cfr. SPEDICATO, *op. cit.*, p. 21.

si possa fare di un *file* digitale. Con questi strumenti informatici diventa possibile abilitare e disabilitare facoltà e scindere le diverse prerogative che spettano tradizionalmente al proprietario – copiare, leggere, ascoltare, rivedere –, con un livello di efficacia impossibile da raggiungere per un bene materiale. In definitiva, è il codice, ossia il software installato nel file, a stabilire le condizioni d'uso[36].

Non mancano, infatti, norme che forniscono copertura giuridica ad atti di autotutela tecnologica unilateralmente posti in essere da parte dei titolari dei diritti di esclusiva[37].

Ciò si ripercuote, inevitabilmente, sull'autonomia negoziale, ove si tende ad imporre clausole escludenti in forza di una consustanziale asimmetria tra le parti[38] che trova nello strumento tecnologico un sicuro alleato.

Come emerso nel corso dell'analisi, già ad una prima lettura di parte delle disposizioni contenute nella direttiva *copyright*, pare potersi aderire a quella dottrina che intravede, ancora una volta, un'esigua

---

36 Cfr. Quarta, Smorto, *Diritto privato dei mercati digitali,* Le Monnier, 2020, p. 62.

37 Così Spedicato, *op. cit.,* p. 27, che richiama, oltre ai DRM, le cd. misure tecnologiche di protezione (TPM), di cui alla direttiva *infosoc*. A questo riguardo, si è parlato di «trionfo della forza d'autore», cfr. Spada, *Copia privata ed opere sottochiave*, in *Rivista di diritto industriale*, 2002, p. 603.

38 Cui negli anni ha cercato di porvi rimedio la giurisprudenza della Corte di Giustizia Europea; cfr. *ex multis*, Corte di Giustizia UE, C-355/12, noto come caso Nintendo. Più in generale, alcune ultime pronunce dei giudici di Lussemburgo lasciano intravedere qualche margine di irrobustimento delle eccezioni e limitazioni, sebbene sia ancora presto per tirare le somme. Cfr. Corte di Giustizia UE, Grande Sez., 29 luglio 2019, n. C-69/17, *Funke Medien NRW GmbH* c. Repubblica federale di Germania, punto 70: «tuttavia, sebbene l'articolo 5 della direttiva 2001/29 sia intitolato "Eccezioni e limitazioni", occorre rilevare che siffatte eccezioni o limitazioni comportano a loro volta diritti a vantaggio degli utenti di opere o di altri materiali protetti (v., in tal senso, sentenza dell'11 settembre 2014, *Eugen Ulmer*, C-117/13, EU:C:2014:2196, punto 43)»; ancora, sentenza del 29 luglio 2019, n. C-516/17, *Spiegel Online GmbH c. Volker Beck*, punto 54. Sugli ultimi sviluppi giurisprudenziali v. Sganga, *A Decade of Fair Balance Doctrine, and How to Fix It: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online* (August 1, 2019), in *European Intellectual Property Review*, 11, 2019.

dose di coraggio nelle scelte di politica legislativa del legislatore europeo[39]. Quando non addirittura una certa confusione, a fronte della natura ambivalente della componente tecnologica, che pare essersi riversata anche nella trasposizione normativa.

In questo scenario, appare arduo raggiungere quegli ambiziosi ed auspicati obiettivi di armonizzazione e, *lato sensu*, di modernizzazione del diritto d'autore, permeabile ai principi dell'*open access*, quantomeno con riferimento ai prodotti della ricerca scientifica[40]. A questo specifico riguardo, non solo la giurisprudenza della Corte di Giustizia Europea, ma anche la comunità accademica internazionale nel suo complesso evidenziano, da qualche decennio, tutti i limiti dell'approccio dominicale ai risultati della ricerca, soprattutto quando tali risultati siano il frutto di attività finanziate con fondi pubblici.

Prendendo le mosse da talune iniziative condotte a livello internazionale[41], vari Paesi hanno intrapreso i primi passi legislativi, volti a favorire una transizione, quantomeno parziale, del mondo della ricerca scientifica da un modello basato sulla rigida applicazione della disciplina autoriale ad uno ispirato ai valori dell'*open access* (e, in una prospettiva ancora più generale, a quelli dell'*open science*).

In Italia, un primo importante passo che muove in questa direzione si è registrato con la legge 7 ottobre 2013, n. 112 – che ha convertito, con modificazioni, il d.l. 8 agosto 2013, n. 91 recante "Disposizioni urgenti per la tutela, la valorizzazione e il rilancio dei beni e delle attività culturali e del turismo" – il cui art. 4 impone ai soggetti pubblici preposti all'erogazione o alla gestione dei finanziamenti della ricerca

---

39 In questo senso cfr. PAPA (a cura di), *op. cit.*, p. 158, ove si parla di «occasione sostanzialmente persa», per non aver introdotto norme esplicitamente e direttamente dedicate ai principi dell'*open access*, che ancora poggia su un fragile sistema di *soft law*.

40 «Dimensioni elefantiache, linguaggio confuso, prescrizioni normative contraddittorie e incapacità di condurre a un'effettiva armonizzazione consegnano agli Stati membri un testo di difficile attuazione e interpretazione. È facile prevedere che la direttiva darà adito a un gigantesco contezioso giudiziario (oltre che a una copiosa produzione dottrinale), nel quale il dialogo tra la Corte di Giustizia e le corti nazionali deciderà – al prezzo di una moltiplicazione esponenziale dei costi di transazione e di gestione delle controversie – gli esiti (mai definitivi) dello scontro tra i molteplici interessi che ruotano attorno al diritto d'autore», così CASO, *op. cit.*, p. 9.

41 Risale al 2003 la ben nota *Dichiarazione di Berlino* sull'accesso aperto alla letteratura scientifica, pietra miliare nella storia europea dell'*Open Access*. Obiettivo della dichiarazione, quello di garantire la massima diffusione possibile delle pubblicazioni scientifiche mediante l'utilizzo di Internet.

scientifica di adottare le misure necessarie per la promozione dell'accesso aperto ai risultati della ricerca finanziata per una quota pari o superiore al 50% con fondi pubblici.

Si tratta di un *paradigm shift* – per mutuare il lessico kuhniano[42] – tuttora in pieno svolgimento: molte sono le questioni ancora oggetto di discussione, sia sul piano teorico, che applicativo. Sotto tale ultimo aspetto, occorre trovare soluzioni – giuridiche, oltre che gestionali – che consentano di contemperare adeguatamente gli interessi e i diritti dei vari soggetti coinvolti nell'attività di ricerca.

In una prospettiva *de iure condendo*, soprattutto alla luce dell'imminente recepimento della direttiva *copyright*[43], sembra opportuno proseguire l'indagine, orientando l'analisi sulla disciplina giuridica di riferimento e, in una prospettiva anche applicativa, sull'elaborazione delle *best practices* e di nuovi modelli negoziali.

---

42 L'espressione è stata coniata da Thomas Kuhn nella sua fondamentale opera *La struttura delle rivoluzioni scientifiche*, per descrivere un cambiamento nelle assunzioni basilari all'interno di una teoria scientifica dominante. L'opera rappresenta una pietra miliare nel dibattito epistemologico moderno e alla sua influenza si deve l'introduzione nel gergo scientifico e filosofico del termine *paradigma*. Cfr. Kuhn, *The structure of scientific revolutions*, University of Chicago Press, 1962.

43 In Italia, il Senato della Repubblica ha dato il via libera il 29 ottobre 2020 (con 134 voti favorevoli, 64 contrari e 31 astenuti) al disegno di legge di delegazione al Governo per il recepimento di 33 direttive europee in vari settori. Tra queste anche la direttiva 790/2019/UE. Si tratta del primo passo dell'iter di recepimento del provvedimento, che passa all'esame della Camera. Ai sensi dell'art. 29 della stessa direttiva, tutti gli Stati membri dovranno conformarsi entro il 7 giugno 2021.

4. *Smart contract*: disciplina, criticità e risvolti pratici

Ettore William Di Mauro

4.1. *Blockchain*: la tecnologia di supporto

Gli *smart contracts*[1] sono un'evoluzione del protocollo *bitcoin*[2] e trovano applicazione diffusa sul finire degli anni 90 negli Stati Uniti grazie allo sviluppo della tecnologia *blockchain*[3].

---

1 La locuzione «*smart contract*» è stata coniata da N. SZABO, *Smart Contracts: Building Blocks for Digital Markets*, in www.fon.hum.uva.nl, 1997, in szabo.best.vwh.net/idea.html., definendo il nuovo fenomeno quale «a set of promis, including protocols within the parties perform on the these promises» e riconosce nella *vending machine* l'antesignano del contratto automatico; R. DE CARIA, *The legal meaning of smart contracts*, in *European Review of Private Law*, 2019, p. 735.

2 Il *bitcoin* è un *software peer to peer* che si pone quale alternativa ai tradizionali canali di pagamento. Cfr. S. NAKAMOTO, *Bitcoin: a Peer-to-peer Electronic Cash System*, 2011, bitcoin.org/bitcoin.pdf.

3 I. FERLITO, *"Smart Contract". Automazione contrattuale ed etica dell'algoritmo*, in *Comp. dir. civ.*, 2020, p. 661; F. SCUTIERO, Smart contract *e sistema di diritto, un connubio tutta da definire*, in *Foro nap.*, 2019, p.113; K. KELLY, Out of control. *La nuova tecnologia delle macchine, dei sistemi sociali e del mondo dell'economia*, Milano, 1996, p. 6 ss.; V. ARIOSI, *Il cammino della Tecnologia. Invenzioni e scoperte che hanno segnato la storia dell'uomo*, Tricase-Lecce, 2017, *passim*; G. RINALDI, Smart contract*: meccanizzazione del contratto nel paradigma della* blockchain, in corso di pubblicazione; M. GIULIANO, *La* blockchain *e gli* smart contracts *nell'innovazione del diritto nel terzo millennio*, in *Diritto dell'informazione e dell'informatica*, 2018, p. 989 ss.; F. FAINI, Blockchain *e diritto: la "catena del valore" tra documenti informatici,* smart contracts *e* data protection, in *Resp. civ. prev.*, 2020, p. 297 ss.; G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2002, pp. 61-66; A. PALLADINO, *Dall'*homo loquens *all'*homo smart*: la contrattualistica del terzo millennio*, in *De Iustitia*, 2020, p. 90 ss.; K. WERBACH e N. CORNELL, *Contracts ex machina*, in *Duke Law Journal*, 2017, p. 314 ss.; F. DELFINI, Blockchain, Smart Contracts *e innovazione tecnologica: l'informatica e il diritto dei contratti*, in *Riv. dir. priv.*, 2019, p. 167; C. PERNICE, Smart contract *e automazione contrattuale, potenzialità dei rischi della negoziazione algoritmica nell'era digitale*, in *Dir. merc. ass. fin.*, 2019, p. 117 ss.; G. LEMME, *Gli* smart contracts *e le tre leggi della robotica*, in *An. giur. econ.*, 2019, p. 133; A.U. JANSSEN e F.P.

Quest'ultima è finalizzata alla conservazione e gestione di transazioni attraverso la creazione di un *database* distribuito tra gli utenti di una rete[4]. In altri termini la *blockchain* consiste in un registro pubblico e condiviso[5] in grado di aggiornarsi automaticamente su ciascuno dei nodi che partecipano alla catena, e che di fatto sono dei computer. Tale registro è strutturato in blocchi, ognuno dei quali rappresenta un numero di transazioni la cui provenienza e ora di esecuzione sono attribuite in modo indelebile e immutabile attraverso un meccanismo di crittografia a chiave asimmetrica[6] e una marcatura temporale (c.d. *timestamping*).

Patti, *Demistificare gli* smart contracts, in *Oss. dir. civ. comm.*, 2020, p. 32 ss.; E. Giorgini, *Algorithms and Law*, in *The Italian Law Journal*, 2019, p. 131 ss.; A. Nuzzo, *Algoritmi e potere*, in *An. giur. econ*., 2019, p. 39 ss.; L. Avitabile, *Il diritto davanti all'algoritmo*, in *Riv. it. scienze giuridiche*, 2017, p. 315 ss.

4 L. Parola, P. Merati e G. Gavotti, Blockchain *e* smart contract*: questioni giuridiche aperte*, in *Contratti*, 2018, p. 681 ss.; M.L. Perugini e P. Dal Checco, *Introduzione agli* smart contrats, 2016, in www.papers.ssrn.com; M. Giaccaglia, *Considerazioni su* blockchain *e* smart contracts *(oltre le criptovalute)*, in *Contr. impr*., 2019, p. 941 ss.; G. Rinaldi, Smart contract*: meccanizzazione del contratto nel paradigma della* blockchain, cit., in corso di pubblicazione; R. De Caria, *The legal meaning of* Smart Contracts, cit., pp. 732-733, il quale definisce la *blockchain* quale «a type of database takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is the "chained" to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions»; K. Werbach e N. Cornell, *Contracts ex machina*, cit., p. 324 ss.; P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 107 ss.; F. Faini, Blockchain *e diritto: la «catena del valore» tra documenti informatici,* smart contracts *e* data protection, cit., p. 299 ss.; M. Manente, Blockchain*: la pretesa di sostituire il notaio*, in *Notariato*, 2016, p. 211.

5 La distribuzione di un database tra gli utenti di una rate rappresenta il tratto distintivo delle c.d. distributed ledgers technology (DLT), di cui la *blockchain* rappresenta l'esempio più famoso. Il concetto di distribuzione della gestione di un database si contrappone alla tradizionale logica della gestione centralizzata di dati (ad esempio, istituzioni finanziarie e banche per dati finanziari, enti pubblici per dati personali, ecc.), sottoposti al controllo di una (sola e sovraordinata) autorità centrale. Nel DLT non esiste un ordine gerarchico, ma tutti gli utenti della rete sono allo stesso livello e possono agire soltanto con il consenso della maggioranza.

6 Nella crittografia asimmetrica ogni utente possiede una coppia di chiavi (una privata e una pubblica) univocamente correlate. Quella privata è tenuta segreta dal suo possessore, mentre quella pubblica, generata dalla chiave privata, viene comunicata alla controparte. La chiave privata serve per decifrare il testo cifrato con la chiave pubblica. Tale meccanismo tecnico di cifratura è alla base della firma digitale. La chiave pubblica può essere condivisa apertamente, ad esempio, perché inviata lungo la rete ad un altro soggetto. Tuttavia, essa può crittografare un messaggio ma non lo

Ciascun blocco è collegato irreversibilmente a quello precedente tramite una particolare operazione logaritmica, cd. funzione di *hash*[7], che forma la catena di blocchi (*blockchain*) accessibile e consultabile da tutti i nodi della rete. Prima di essere aggiunto alla catena, ogni blocco è controllato, validato e crittografato da alcuni dei nodi, detti *miners*, tramite la soluzione di una complessa operazione matematica.

La *blockchain* consente di verificare, approvare ed archiviare su tutti i nodi di una rete, i dati delle transazioni in essa registrate, senza la necessità di ricorrere a un soggetto terzo, o a una autorità centrale.

L'assenza di un sistema centrale di controllo potrebbe determinare rischi di *double spending*, ovvero l'utilizzo di medesime risorse virtuali per molteplici operazioni. La soluzione adottata è quella di prevedere non un'unica piattaforma, ma appunto blocchi di registrazione condivisa. Una volta eseguita la transazione la stessa diventa immutabile e non modificabile a meno che non ci sia una nuova operazione di segno opposto e che ci sia l'accordo di tutti i nodi abilitati o la maggioranza di essi, condizioni difficilmente realizzabili.

Su tale tecnologia operano gli *smart contract*, non solo per il semplice trasferimento di moneta virtuale da un soggetto ad un altro, ma

---

può decodificare. Solo la corrispondente chiave privata può decodificare o sbloccare i messaggi codificati con la chiave pubblica, motivo che impone la segretezza. Cfr. M. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, cit., pp. 999-1000.

7 La funzione di *hash* è la «catena» che lega i singoli blocchi. Si attua attraverso un meccanismo digitale che viene utilizzato per comprimere i dati in un formato specifico di una lunghezza determinata. La cd. impronta *hash* è una sequenza di lettere e cifre, ottenuta applicando un particolare algoritmo di calcolo alla sequenza di *bit* che formano il *file* o il testo. L'algoritmo non fa altro che scandire sequenzialmente uno dopo l'altro tutti i *byte* che costituiscono il *file* e ricavare, passo dopo passo, una serie di «impronte intermedie», ciascuna delle quali dipende dalla precedente, ottenendo, al termine della scansione, l'impronta *hash* definitiva. Ogni passo dell'elaborazione è influenzato da quelli precedenti e determina lo stato di quelli successivi, per questo motivo è sufficiente modificare anche un solo *bit* di tutto il *file* per ottenere una impronta *hash* diversa. Per verificare che un testo sia stato modificato è sufficiente verificare che gli *hash* dei due testi a confronto corrispondano. Un'altra caratteristica dell'impronta di *hash* è quella di non permettere di risalire al testo originario. L'algoritmo è pensato in modo da non consentire a nessuno di capire cosa abbia generato una determinata impronta. Nella *blockchain* l'*hash* viene utilizzato per creare un collegamento tra ciascun blocco specifico. Questo di ottiene scrivendo l'*hash* di ogni blocco precedente nel blocco successivo della catena. Quando viene creato un blocco, viene creato un *hash* di dati al suo interno e l'*hash* che viene creato include l'*hash* del blocco precedente.

anche per operazioni strutturalmente più complesse, ad esempio nel trasferire un bene virtuale, che nulla vieta sia la rappresentazione digitale di un bene materiale, immesso nel sistema a fronte del trasferimento di un prezzo. Le transazioni eseguite dagli *smart contract*, tradotte in algoritmo, formano i blocchi della struttura *blockchain.*

4.2. Il protocollo *smart contract*

Con la locuzione «*smart contract*» si indicano protocolli per computer attraverso i quali al ricorrere di una condizione predefinita e informaticamente verificabile, il sistema esegue in via automatica una determinata prestazione[8].

Si pensi, ad esempio, ad una vendita con riserva di proprietà. A fronte della mancata registrazione del pagamento del prezzo il bene viene ritrasferito automaticamente al venditore, in esecuzione dell'impostazione dell'algoritmo, evitando i costi ed i tempi di un giudizio.

Le previsioni negoziali vengono convertite in un codice informatico e inserite in un registro logico, basato sul binomio *if-then*, in forza del quale «al verificarsi di un dato evento (*if*) si produce l'effetto digitalmente collegato (*then*), che può consistere tanto nella mera esecuzione

---

8 C.D. Clack, V.A. Bakshi e L. Braine, *Smart contract templates: foundations, design landscape and research directions*, in researchgate.net, definiscono gli *smart contract* come «an automable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer»; K. Werbach e N. Cornell, *Contracts ex machina*, cit., p. 338 ss. Molte sono le definizioni date dagli autori americani. Solo per citarne alcuni: R. O'Shields, *Smart contracts: legal agreements for the blockchain*, in *N.C. Banking Inst.*, 2017, p. 179 lo definisce come «self-executing electronic instructions drafted in computer code»; T. Hingley, *A smart new world: blockchain and smart contracts*, in www.freshfields.com/en-gb/our-thinking/campaigns/digital/fintech/block chain-and-smart-contract , come «a piece of computer code that is capable of monitoring, executing and enforcing an agreement»; G. Jaccard, *Smart contracts and the role of law*, in papers.ssrn.com, come «a software, with which computer code binds two, or multitude, of parties in view of the execution of predefined effects, and that is stored on a distributed ledger»; L.W. Cong e Z. He, *Blockchain disruption and smart contracts*, in papers.ssrn.com, come «digital contracts allowing terms contingent on decentralized consensus that are self-enforcing and tamperproof through automated execution».

delle clausole pattuite, quanto nell'adeguamento della prestazione al verificarsi di eventi sopravvenuti»[9].

L'automazione può essere totale o parziale[10], così come è variabile il potere di scelta dell'algoritmo, il contenuto ed il sistema di accertamento delle condizioni predefinite.

L'*input* (*if*) può basarsi su elementi interni del contratto (ad esempio l'apposizione di un termine), o esterni ad esso (ad esempio il prezzo del bene), e può avere ad oggetto dati che risultano da fonti pubbliche o istituzionali o che richiedono un sistema di conferma allargata: nel primo caso il codice farà discendere l'esecuzione da questa verifica; nel secondo il riscontro dell'evento necessiterà dell'intervento di un «oracolo»[11], «una piattaforma che "interroga" la rete sulla condizione da appurare e ne dà conferma al raggiungimento di un determinato numero di riscontri positivi»[12]. In altri termini, è un programma esterno alla *blockchain* che lega la rete alla realtà.

Alcuni esempi possono chiarire meglio il funzionamento degli *smart contract*. Si ponga il caso della vendita di una licenza. Supponiamo che Tizio crei uno *smart contract* al quale allega l'informazione x (la licenza) programmando che essa venga trasferita al pagamento di una somma y[13]. Tizio lancia lo *smart contract* nella *blockchain*. Nel caso

---

9 C. PERNICE, Smart contract *e automazione contrattuale*, cit., p. 119, la quale precisa che «una volta inserito nella *blockchain* lo *smart contract* funziona autonomamente, diventa "inarrestabile": l'attuazione dell'accordo sfugge alla volontà e al controllo dell'uomo il quale non può in alcun modo interromperne l'esecuzione».

10 Le parti possono decidere se affidare all'algoritmo tutta o parte dell'esecuzione.

11 P. CUCCURU, Blockchain *ed automazione contrattuale, riflessioni sugli* smart contract, cit., p. 111, il quale descrive gli oracoli quali «programmi indipendenti dalla *blockchain* che monitorano dati esterni al sistema decentralizzato, come gli indici delle quotazioni azionarie o il database del venditore, e comunicano agli *smart contract* collegati il soddisfacimento delle condizioni rilevanti»; L. PIATTI, *Dal Codice civile al codice binario:* blockchain *e* smart contracts, in *Cib. dir.*, 2016, p. 334, li descrive come «un riferimento fidato, per il contratto e per le parti, che accerta il compimento di determinati avvenimenti del mondo fisico e restituisce un *input* al contratto stesso»; F. SCUTIERO, Smart contract *e sistema di diritto*, cit., p. 122.

12 C. PERNICE, Smart contract *e automazione contrattuale*, cit., p. 119.

13 Secondo M.L. PERUGINI e P. DAL CHECCO, *Introduzione agli* smart contract, cit., p. 10 «l'utilizzo delle funzioni di *blockchain* impone alcuni limiti di carattere tecnico: le prestazioni di commercio elettronico indiretto non sono eseguibili in via informatica. Sono, così, escluse dall'applicazione tutte le clausole che abbiano riguardo a beni o servizi che, pur acquistati in rete, abbiano una consistenza tangibile o debbano essere eseguiti nel mondo materiale come, ad esempio, la consegna di un libro o il servizio di pulizia di un locale»; di diverso avviso P. CUCCURU, Blockchain *ed*

in cui Caio voglia acquistare la licenza, sarà sufficiente interagire con il protocollo creato da Tizio e trasferire la somma y. Una volta integrate le condizioni dello scambio l'algoritmo rilascerà la licenza a Caio e trasferirà la somma di denaro a Tizio[14].

Tale meccanismo trova spazio anche nella fornitura e pagamento dell'energia elettrica e nella fruizione di contenuti musicali. Nella prima ipotesi, al consumo registrato dal contatore, che, in questo caso, rappresenterebbe l'oracolo che collega il codice alla realtà esterna, ne consegue una bollettazione precisa ed un puntuale pagamento della fattura. Nella seconda ipotesi, gli utenti di una piattaforma musicale (ad esempio UjoMusic) possono ascoltare musica e pagare direttamente gli artisti, senza ricorrere ad alcun intermediario[15].

Il prevedere una serie di condizioni, al verificarsi delle quali le prestazioni delle parti vengono declinate in maniera puntuale, permette di ottenere, nell'esecuzione del contratto, una risposta automatica e immediata da parte del sistema, senza alcuna valutazione di sorta[16] né intermediazione.

4.3. I tentativi di inquadramento

L'impatto delle tecnologie informatiche sul mondo dei traffici ha condotto una parte della dottrina a ritenere che ci si trovi di fronte a un vero e proprio declino dell'accordo, inteso nel senso di una progressiva scomparsa della reciproca dialogicità tra le parti, sostituita da surrogati della comunicazione linguistico-verbale o dal mero scambio delle prestazioni, tanto che lo stesso contratto finirebbe per scomporsi

---

automazione contrattuale. Riflessioni sugli smart contracts, cit., p. 108, il quale ritiene che «ogni tipo di informazione intesa può essere rappresentata digitalmente, inserita e conservata in una *blockchain*»: beni immateriali, diritti, dati personali, licenze, testamenti, bilanci aziendali.

14 C. Pernice, Smart contract *e automazione contrattuale*, cit., p. 120, descrive un altro esempio: «ipotizziamo che un'agenzia di *web marketing* chieda ad alcuni *sponsor* di finanziare il proprio video garantendo un certo numero di visualizzazioni in un determinato tempo. In questo caso verrà creato uno *smart contract* a termine con oracolo che avrà il compito di comunicare il numero delle visualizzazioni su *Youtube*.

15 L. Parola, P. Merati e G. Gavotti, Blockchain *e* smart contract*: questioni giuridiche aperte*, cit., p. 685.

16 F. Scutiero, Smart contract *e sistema di diritto*, cit., p. 123.

nella combinazione di due atti unilaterali, dando vita a «scambi senza accordo»[17].

Un'altra parte della dottrina nega la natura contrattuale agli *smart contract* riconoscendogli soltanto la funzione di strumento per «la negoziazione, conclusione e/o automatica applicazione di rapporti contrattuali o relazioni para-contrattuali: un canale per la conclusione e gestione degli accordi, piuttosto che accordi in senso stretto»[18].

---

[17] N. IRTI, *Norma e luoghi. Problemi di geo-diritto*, cit., p. 182 ss., precisa che «il declino dell'accordo, derivante dalla crisi della parola e del dialogo, dissolve il contratto nella combinazione di due atti unilaterali: atti leciti, dell'esporre e del preferire, richiedenti soltanto la riferibilità a un autore e la naturale capacità d'intendere e di volere. Le parti dello scambio assumano decisioni, che nascono e restano separate»; G. LEMME, *Gli* smart contracts *e le tre leggi della robotica*, cit., p. 140 conferma il pensiero di Irti ritenendo che l'insigne Maestro «preconizza il passaggio dall'*homo loquens* all'*homo videns*: da colui che, attraverso il dialogo, contribuisce alla formazione del negozio, a colui che passivamente subisce, senza esprimersi con il linguaggio parlato, una eteroformazione del contenuto contrattuale»; A. PALLADINO, *Dall'*homo loquens *all'*homo smart*: la contrattualistica del terzo millennio*, ritiene che «le rinnovate esigenze dell'*homo digitalis* si sono orientate verso la più completa oggettivizzazione dello scambio, prediligendo dinamiche volte alla riduzione dell'elemento della volontà e del potere delle parti di incidere sulla struttura negoziale, al fine di mitigare i rischi connessi all'asimmetria informativa e ai costi della negoziazione»; U. BRECCIA, *Sub art.* 1321, in *Comm. c.c.* Gabrielli, Torino, 2011, p. 7 ss.; V. ROPPO, *Il contratto del duemila,* Torino, 2011, p. 25 ss.; M. FARINA, Smart contract *tra automazione contrattuale e disumanizzazione dei rapporti giuridici*, cit., p. 4. *Contra* G. OPPO, *Disumanizzazione del contratto?*, in *Riv. dir. civ.*, 1998, p. 525 ss. Sul punto di v. anche P. PERLINGIERI, *Metodo, categorie, sistema nel diritto del commercio elettronico*, in ID., *Il diritto dei contratti fra persona e mercato*, Napoli, 2003, p. 652 ss.; C.M. BIANCA, *Acontrattualità dei contratti di massa?*, in *Vit. not.*, 2001, p. 1120 ss.

[18] F. DI CIOMMO, Blockchain, smart contract, *intelligenza artificiale (IA) e "trading" algoritmo: ovvero, del regno del non diritto*, cit., p. 4, afferma che «quando il contratto si conclude esclusivamente attraverso l'attività di uno o più *software*, l'accertamento automatizzato dei presupposti fattuali di perfezionamento dello stesso dovrà svolgersi in ossequio a regole prefissate dalle parti, a monte di un contratto quadro o, comunque, in un regolamento contrattuale»; L. PAROLA, P. MERATI e G. GAVOTTI, Blockchain *e* smart contract*: questioni giuridiche aperte*, cit., p. 685 ss. Si consideri, ad esempio, l'acquisto di licenza d'uso di un'opera di proprietà intellettuale, o il trasferimento di un qualsiasi altro dato, come le preferenze di una certa categoria di persone, desunte dalle loro attività *online*, a fini pubblicitari. Tizio crea uno *smart contract*, al quale allega l'informazione x (la licenza o le preferenze), programmando che essa venga trasferita al soddisfacimento di determinate condizioni (ad esempio una controprestazione in valuta virtuale y), e lancia il protocollo su di una *blockchain*. Nel momento in cui Caio intende ottenere x, essa interagisce col protocollo creato da Tizio, trasferendo, in caso di accettazione dei termini dello scambio, la somma y. Essendo integrate le condizioni dello scambio, l'algoritmo dello *smart contract* rilascia x a Caio e trasferisce y a Tizio, eliminando il divario temporale tra le prestazioni

Si tratterebbe di contratti «al cui perfezionamento si può giungere anche secondo gli schemi tradizionali di conclusione dell'accordo, che vengono tradotti in programmi informatici e che, attraverso questi, si autoeseguono»[19].

Il vantaggio funzionale di utilizzare uno *smart contract* risiederebbe soltanto nel fatto che esso possa prevedere un numero indefinito di clausole che stabiliscono, in un dato momento e tenendo conto delle circostanze concrete, il contenuto delle prestazioni delle parti. In altri termini, si avrebbero delle semplici *vending machine* ma altamente digitalizzate.

Altra dottrina[20], sulla scia di quella americana[21], ritiene, invece, che gli *smart contract* siano in grado di sostituirsi completamente ai contratti tradizionalmente intesi e che il codice informatico costituisca, in tutto, il contratto. Gli *smart code* avrebbero forza di legge tra le parti ai sensi dell'art. 1372 c.c. e sarebbero, quindi, autosufficienti, autoeseguiti e autoimposti, con la conseguenza che potrebbero porsi al di là di ogni possibile controllo da parte degli Stati e della relativa giurisdizione legale.

---

collegate, nonché ogni spazio per il volontario inadempimento delle parti. Il meccanismo imita un deposito presso terzi. Cfr. C. Pernice, Smart contract *e automazione contrattuale: potenzialità e rischi della negoziazione algoritmica nell'era digitale*, cit., pp. 133-134.

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

20 M. Giuliano, *La* blockchain *e gli* smart contracts *nell'innovazione del diritto nel terzo millennio*, cit., p. 989 ss.; M. Durovic e F. Lech, *The Enforceability of Smart Contracts*, in *The Italian Law Journal*, 2019, p. 493 ss.

21 Per i giuristi americani gli *smart contract* configurano veri e propri contratti ogni volta che contengano uno scambio di promesse dalle quali potersi desumere un *do ut des* e una *contractual intention*. Cfr. Secondo S. Aceto di Capriglia, *Contrattazione algoritmica. Problemi di proliferazione e prospettive operazionali. L'esperienza "pilota" statunitense*, in *Federalismi.it*, 2019, pp. 6-7; I. Ferlito, «Smart contract». *Automazione contrattuale ed etica dell'algoritmo*, cit., p. 12; altri autori ritengono addirittura che gli *smart contract* siano indipendenti dal diritto, A. Savelyev, *Contract law 2.0: «smart» contracts as the beginning of the end of classic contract law*, in reaserchgate.net p. 17 ss.; V. Zeno Zencovich, *«Smart contracts», «granular norms» and non discrimination*; R. Pardolesi e A. Davola, «Smart contract»*: lusinghe ed equivoci dell'innovazione purchessia*, p. 297 ss.; F. Di Ciommo, *Smart contract e (non-)diritto. Il caso dei mercati finanziari*, p. 257 ss.; Id., «Blockchain, smart contract», *intelligenza artificiale (AI) e «trading» algoritmico: ovvero, del regno del non diritto*, in *Riv. infortuni e delle malattie professionali*, 2019, p. 1 ss.; P. Cuccuru, Blockchain *ed automazione contrattuale, riflessioni sugli* smart contract, cit., p. 110 ss.; A.J. Kolber, *Not-so-Smart Blockchain contracts and artificial responsability*, in *Stanford Technology Law Review*, p. 198 ss.

Una tesi maggiormente condivisibile, e più vicina alla prassi, li colloca all'interno del sistema giuridico tradizionale, sottolineando una non conformità tra l'accordo delle parti e il protocollo codificato e, dunque, l'esigenza che i medesimi debbano necessariamente integrarsi con ulteriori elementi espressione della volontà delle parti[22]. Tale posizione fa leva sul cd. *split contracting model* o *hybrid agreement* che consiste nella redazione contestuale di un contratto in linguaggio naturale unitamente a una copia in codice, ovvero con l'inclusione nel testo contrattuale di alcune parti codificate e auto-eseguibili[23].

Nella prassi la stesura del contratto avviene, di solito, attraverso una interfaccia *web*, ossia un modulo che contiene, da un lato, il testo in linguaggio naturale, e dall'altro, i parametri computabili in codice informatico, relativi ad informazioni da raccogliere da fonti esterne per eventuali condizioni a cui è subordinata l'esecuzione e o la sua modifica[24].

4.4. I vantaggi

Gli *smart contract* e la *blockchain* suscitano interesse da parte dei cittadini che intravedono in questa tecnologia uno strumento di indipendenza e risparmio, capace di assicurare la certezza delle transazioni in misura maggiore rispetto ai sistemi di certificazione ed esecuzione tradizionali, atteso che le informazioni sono criptate, permanenti, tracciabili e autoeseguibili[25].

---

22 L. PAROLA, P. MERATI e G. GAVOTTI, Blockchain *e* smart contract*: questioi giuridiche aperte*, cit., p. 681 ss.; F. DI CIOMMO, Blockchain, smart contract*, intelligenza artificiale (IA) e "trading" algoritmo: ovvero, del regno del non diritto*, cit., p. 4 ss.; F. FAINI, Blockchain *e diritto: la «catena del valore» tra documenti informatici,* smart contract *e* data protection, cit., p. 297 ss.; A. STAZI, *Automazione contrattuale e "contratti intelligenti"*, cit., p. 161; A. PALLADINO, *Dall'*homo loquens *all'*homo smart*: la contrattualistica del terzo millennio*, cit., p. 90 ss. Sul tema della rilevanza dell'adempimento negli *smart contract*, I. FERLITO, "Smart contract". *Automazione contrattuale ed etica dell'algoritmo*, cit., p. 17.

23 A. STAZI, *u.l.o.c.*; V. PASQUINO, Smart contracts*: caratteristiche, vantaggi e problematiche*, in *Dir. proc.*, 2017, p. 245; P. DE FILIPPI e A. WRIGHT, *Blockchain and the Law: The Rule of code*, Cambridge, 2018, pp. 76-78.

24 Spesso indicato come *smart contract* ma che dal punto di vista giuridico in realtà ne costituisce soltanto la parte relativa all'esecuzione automatica.

25 C. PERNICE, Smart contract *e automazione contrattuale: potenzialità e rischi della negoziazione algoritmica nell'era digitale*, cit., p. 121.

In effetti gli *smart contract* basati su tecnologia *blockchain* sembrano potere ridurre al minimo il rischio di inadempimento[26]. La fiducia nello spontaneo adempimento della controparte «perde necessariamente rilevanza allorquando l'esecuzione dell'accordo viene affidata ad una rete di computer che non si ha modo di influenzare: una volta lanciato nella *blockchain*, lo *smart contract* è indipendente dal susseguente volere delle parti, segue unicamente le istruzioni impartitegli e si auto-esegue al compimento delle condizioni programmate»[27].

Il contratto «tradizionale» è garantito e protetto dal suo carattere giuridicamente vincolante determinato da una fonte normativa esterna a sé. Di conseguenza, le parti possono volontariamente violare le promesse fatte e/o le corti e i giudici essere chiamati a modificare, annullare o fare eseguire coattivamente le obbligazioni assunte. Fintanto che una delle parti è disposta a subire le conseguenze legali del suo comportamento è, fondamentalmente, libera di non adempiere al contratto stipulato[28].

L'accordo inserito in una *blockchain*, invece, non fa affidamento sulla vincolatività legale o sulla sanzione della parte inadempiente quali strumenti a tutela della sua esecuzione. L'effettività e la garanzia di esecuzione dei rapporti derivano direttamente dal *code layer* nel quale essi sono eseguiti, ovvero dalla struttura tecnologica che li ospita[29].

---

26 L. Parola, P. Merati e G. Gavotti, Blockchain *e* smart contract*: questioi giuridiche aperte*, cit., p. 687, precisano che «nonostante l'adempimento dei contratti intelligenti sia automatizzato, potrebbero sorgere contestazioni tra le parti in merito all'esattezza dell'adepimento» e al ruolo della buona fede. Altra questione è posta da F. Scutiero, Smart contract *e sistema di diritto, un connubio tutto da definire*, cit., pp. 127-129, il quale pone il problema della rilevanza del silenzio per la formazione dell'accordo in uno *smart contract;* E. Mik, *Smart contract: Terinology, Technical Limitations and real-world complexity*, in *Law, Innovation and Technology*, 2017, pp. 14-15.

27 P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 112.

28 P. Cuccuru, *o.l.u.c.*; C.J. Goetz e R.E. Scott, *Liquidated damages, penalties and the just compensation principle: some notes on an enforcement model and a theory of efficient breach,* in *Columbia Law Review*, 1977, pp. 554-558.

29 Il carattere normativo implicito negli ecosistemi digitali è stata concettualizzata da L. Lessig, *Code and other Laws of Cyberspace*, New York, 1999, p. 1 ss.; Id., *The future of ideas: the fate of the Commons in a connected world*, New York, 2001, p. 246, precisa che un «code layer» o un «logical layer» è «the space where code decide show content and applications flow, and where code could control how innovation develops».

Il vantaggio è rappresentato dalla possibilità di prevedere innumerevoli variabili nel programma informatico, giungendo così a «neutralizzare» il rischio di sopravvenienze e di garantire un sicuro adempimento secondo i tempi e le modalità previste dall'algoritmo, perché l'esecuzione automatizzata consiste nell'inevitabilità dell'effetto[30]. Al verificarsi di una condizione propria dell'algoritmo l'effetto si produce automaticamente.

Con un simile meccanismo si potrebbero ottenere diversi benefici. In primo luogo, ridurre drasticamente il rischio di frodi: poiché l'adempimento di Tizio è subordinato ed inscindibile da quello di Caio, l'esecuzione dei termini dell'accordo è idealmente simultanea, così che non sarebbe possibile, ad esempio, che una delle parti trattenga il pagamento y senza consegnare il bene promesso x, o che, viceversa, il pagamento y possa essere annullato una volta che si è ottenuto x.

In secondo luogo, delegare ad una rete di computer decentralizzata l'esecuzione dell'accordo permetterebbe di fare a meno dell'intermediazione di terzi, con conseguente riduzione dei costi e della possibilità di errore e, quindi, con la riduzione di dispendiose controversie, il cui esito rimane sempre incerto[31].

In terzo luogo, visto l'elevato grado di certezza e sicurezza delle transazioni che gli *smart contract* potenzialmente offrono, le parti potrebbero non stipulare clausole penali o meccanismi di monitoraggio dell'accordo, con evidente semplificazione delle trattative e risparmio nell'economia generale dell'affare[32].

In quarto luogo, il linguaggio informatico, caratterizzato dall'essere inequivoco e altamente prevedibile, potrebbe tendere ad eliminare i profili di incertezza derivanti dall'ambiguità intrinseca del linguaggio naturale, poiché non lascerebbe spazio alcuno per attività ermeneutiche. Il rigore e la rigidità del codice impedirebbero letture discordanti

---

30 D. Di Sabato, *Gli* smart contracts*: robot che gestiscono il rischio contrattuale*, cit., p. 398.

31 Cfr. R. De Caria, *The legal meaning of smart contracts*, cit., pp. 740-741; A. Savelyev, *Contract law 2.0: "Smart" contracts as the beginning of the end of classic contract law*, in *Information and Communication Technology Law*, 2017, p. 18.

32 P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., pp. 112-113, precisa nella nota 29 che «gli *smart contract* non necessitano di meccanismi addizionali di risoluzione delle controversie, poiché essi stessi sono un meccanismo preventivo di risoluzione delle dispute: il loro *design* subordina l'adempimento di una parte a quello della controparte, non vi è nessuno dei due versanti del rapporto sinallagmatico che può compiersi in assenza dell'altro».

delle clausole contrattuali, evitando l'insorgere di dispute fondate sulla differente interpretazione delle locuzioni utilizzate, specialmente nei traffici internazionali[33].

Infine, l'utilizzo di uno *smart contract* raggiungerebbe profili di certezza formale, derivanti dal «timbro» (il *timestamping*), contenente ora esatta e data, apposto digitalmente ogni volta che una istruzione viene inserita nella *blockchain*[34].

In pratica i principali vantaggi individuati dai sostenitori della tecnologia *blockchain* applicata agli *smart contract* tendono tutti verso una maggiore efficienza delle relazioni contrattuali, che si tradurrebbero in un minore dispendio di risorse nella fase negoziale e di esecuzione del contratto, una maggiore velocità ed immediatezza delle prestazioni, nonché una significativa riduzione del rischio di insorgenza di controversie tra le parti.

4.5. I profili critici

Al pari dei vantaggi, le criticità degli *smart contract* emergono dalle stesse caratteristiche del sistema digitale e dell'architettura decentralizzata nel quale operano.

In via preliminare si pone il problema della comprensibilità e della naturale rigidità dello strumento. L'immutabilità dei registri decentra-

---

33 D. Di Sabato, *Gli* smart contracts*: robot che gestiscono il rischio contrattuale*, cit., p. 398, precisa che «il programma può contenere infinite variabili, ma solo quelle programmate hanno rilievo, per il resto non sono ammessi spazi di tolleranza, non c'è margine per una valutazione in termini di ragionevolezza che possa indurre a considerare doveroso un comportamento diverso dalla controparte»; H. Surden, *Computable Contracts*, in *UC Davies Law Review*, 2012, p. 634; P. De Filippi e A. Wright, *Decentralized blockchain technology and the rise of lex cryptographia*, cit., pp. 24-25.

34 In questo modo si potrebbero prevenire ipotetiche difficoltà derivanti dall'incerto contesto temporale dell'accordo. Una tale caratteristica è utile nella registrazione di beni (anche materiali) dei quali si voglia certificare la provenienza o verificare la proprietà. In merito risulta interessante uno studio del UK Government Office for Science, *Distributed Ledger Technology: beyond block chain*, in assets.publishing.service.gov.uk/government, p. 56, per l'utilizzo della *blockchain* per tracciare la provenienza dei diamanti e seguire la catena delle loro alienazioni.

lizzati sembrerebbe ostacolare qualsiasi intervento esterno, ad esempio un intervento giudiziale inibitorio, facendo emergere importanti questioni di controllabilità e governabilità degli *smart contract*[35].

È indubbio come la maggior parte delle persone non possegga un complesso di competenze informatiche e di programmazione tale da consentire loro di scrivere un accordo in *bit*. La traduzione dell'accordo in codice è operazione complessa, a maggior ragione ove si considerino la varietà di interessi che animano le parti e le molteplici sfumature che le clausole contrattuali possono assumere[36].

La negoziazione e la predisposizione degli *smart contract*, quindi, richiedono necessariamente la collaborazione e la partecipazione di soggetti capaci di scrivere e di leggere algoritmi. In questa prospettiva, l'inesperienza tecnico digitale della maggior parte dei contraenti risulterà sortire l'effetto contrario, reintroducendo l'intermediazione in questo tipo di relazioni[37].

Il professionista sarà chiamato ad intervenire non più con riferimento alla fase dell'esecuzione dell'accordo, bensì con riguardo alla fase di *design* dell'accordo stesso. Questo comporterà anche l'aumento dei costi che si sposteranno dal piano dell'esecuzione a quello della creazione, portando con sé, inoltre, l'inevitabile rischio di minare quella certezza e quella prevedibilità che dovrebbero, invece, caratterizzare gli *smart contract*. Programmatori e informatici, in sede di trasposizione dell'accordo contrattuale in codice, potrebbero non eseguire un'esatta e corretta traduzione della volontà, conducendo lo *smart contract* ad effetti inattesi o diversi rispetto alle concrete decisioni

---

35 P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., pp. 113-114; sui limiti si v. R. De Caria, *The legal meaning of smart contracts*, cit., p. 743 ss.; K. Werbach e N. Cornell, *Contracts* ex machina, cit., p. 352 ss.

36 I. Ferlito, «Smart contract». *Automazione contrattuale ed etica dell'algoritmo*, cit., p. 20; G. Rinaldi, Smart contract*: meccanizzazione del contratto nel paradigma della* blockchain, cit., in corso di pubblicazione; L. Piatti, *Dal codice civile al codice binario*, cit., pp. 337-338; G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, cit., p. 455-456; I. Morea, *Il consenso*, in A. Fusaro (a cura di), *I vizi del consenso*, Milano, 2013, p. 59.

37 I. Ferlito, *o.u.l.c.*; M. Manente, Blockchain*: la pretesa di sostituire il notaio*, in *Notariato*, 2018, pp. 217-218; P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 114, precisa che «programmatori, prestatori di servizi o software di "traduzione" costituirebbero terze parti necessarie di ogni rapporto».

delle parti, perché spesso tendono a semplificare le istruzioni loro impartite per facilitare la comprensibilità ed esecuzione da parte del sistema informatico[38].

Il desiderio degli ideatori degli *smart contract* di ridurre al minimo o addirittura di rendere assente l'intervento umano sembra non riuscito.

Del resto, eliminare qualsivoglia contributo interpretativo nelle relazioni umane non può essere considerato una conquista del terzo millennio, non si può ritornare all'antico brocardo in *claris non fit interpretatio* poiché il caso concreto verte su interessi sempre diversi e le dinamiche umane risultano difficilmente inquadrabili in semplificazioni binarie[39]. Efficienza, automazione e semplificazione sono valori che andranno bilanciati con altri caratterizzanti la persona umana, primo fra tutti la sua dignità, contenuti nei princìpi normativi costituzionali e caratterizzanti la nostra collettività.

La pretesa di tradurre in codice tutte le circostanze che possono interessare un contratto nel suo «concreto vivere» appare ambiziosa e poco realistica, stante l'imprevedibilità delle stesse e l'impossibilità oggettiva di tradure alcuni criteri ermeneutici essenziali nei rapporti contrattuali, quali la buona fede e la ragionevolezza[40].

---

38 P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 115 ritiene che l'ostacolo linguistico potrebbe, col tempo, rilevarsi temporaneo. Secondo l'a. non è escluso che «la progressiva diffusione di competenze di programmazione e ingegneria informatica, in ambienti legali e non, possa eliminare alla radice il problema della comprensibilità del codice. Lo sviluppo della tecnologia informatica potrebbe, inoltre, permettere ai computer di comprendere ed elaborare complesse istruzioni espressa in linguaggio naturale, un compito che, attualmente, non sono in grado di svolgere»; D.K. Citron, *Technological Due Process*, in *Washington University Law Review*, 2008, p. 1249.

39 C. Pernice, Smart contract *e automazione contrattuale: potenzialità e rischi della negoziazione algoritmica nell'era digitale*, cit., p. 123; P. Perlingieri, *L'interpretazione della legge come sistematica ed assiologica. Il broccardo* in claris non fit interpretatio*, il ruolo dell'art. 12 disp. prel. c.c. e la nuova scuola dell'esegesi*, in *Rass. dir. civ.*, 1985, p. 990 ss.; A. Gentili, *Il diritto come discorso*, Milano, 2013, p. 3.

40 I. Ferlito, «Smart contract». *Automazione contrattuale ed etica dell'algoritmo*, cit., pp. 21-22 precisa che «dettagliare ogni possibile evenienza in modo completo, univoco, senza lasciare spazio per interpretazioni richiederebbe, ammesso che sia fattibile, la redazione di contratti molto lunghi, con conseguente incremento del rischio di incorrere in errori di programmazione»; J.I.H. Hsiao, *Smart contract on the blockchain. Paradigm shift for contract law*, in *US-China Law Review*, 2017, p. 694, ribadisce che «smart contract is based on a binary zero-sum logic that does not appear in all real-

Inoltre, «se il codice è la traduzione informatica del linguaggio naturale per forza di cose all'ambiguità del primo seguirà l'incompletezza del secondo; se polisenso è il testo da tradurre altrettanto lo sarà il testo tradotto; se carente è l'informazione impartita altrettanto lo sarà l'*input* che lo rappresenta»[41].

La partecipazione di programmatori ed informatici nella stesura dell'algoritmo aumenta, di fatto, il rischio di divergenza tra volizione e dichiarazione così come il pericolo che il contraente, soprattutto quello debole, si trovi a aderire ad un accordo non del tutto consapevolmente.

I costi addizionali, le difficoltà di traduzione ed i rischi relativi all'intermediazione dei programmatori potrebbero scoraggiare l'utilizzo degli *smart contract*[42].

Inoltre, la rigidità del codice e la decentralizzazione, che degli *smart contract* e della *blockchain* dovrebbero essere punti di forza, pongono, invece, ulteriori limiti.

Sussiste il rischio di configurare un «ecosistema *online* autoreferenziale», sottratto a qualsiasi sindacato esterno, ancorché si tratti di intervento legittimo in quanto finalizzato alla correzione di disfunzioni e alla salvaguardia delle norme imperative di un ordinamento.

L'irreversibilità dei rapporti automatizzati e dei relativi effetti sembrerebbe precludere alle parti di ricorrere a strumenti di autotutela a fronte di accordi illegittimi, viziati o comunque iniqui[43].

---

life contract case»; G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, p. 35 ss., sottolinea che «la certezza del diritto non è un dato acquisito del sistema ma un obiettivo al quale deve tendere l'attività del giurista»; ID., *Sul criterio di ragionevolezza*, in C. PERLINGIERI e L. RUGGERI (a cura di), *L'incidenza della dottrina sulla giurisprudenza nel diritto dei contratti*, Napoli, , 2016, p. 29 ss. ; F. FAINI, Blockchain *e diritto: la «catena del valore» tra documenti informatici,* smart contract *e* data protection, cit., pp. 307-308; D. DI SABATO, *Gli* smart contract*: robot che gestiscono il rischio contrattuale*, cit., p. 399 ss.

41 C. PERNICE, Smart contract *e automazione contrattuale: potenzialità e rischi della negoziazione algoritmica nell'era digitale*, cit., p. 125; S. CAPACCIOLI, Smart contracts*: traiettorie di un'utopia divenuta attuabile*, cit., p. 37.

42 Tuttavia, sembrerebbe che un ampio margine per lo sviluppo degli *smart contract* possa invece aversi in accordi altamente standardizzati e relativamente semplici, predisposti da professionisti imprese e prestatori di servizi che possono sopperire ai costi di codificazione con un'applicazione su larga scala delle clausole «smart» codificate.

43 P. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 116 aggiunge che non solo le parti non potrebbero, ad esempio rifiutare la prestazione ove l'accordo risulti essere fraudolento o viziato e, allo stesso tempo, «le

L'inevitabilità dell'effetto al verificarsi dell'*input* determinea, ad esempio, una rinuncia alla proponibilità dell'eccezione di inadempimento.

Una tale circostanza suscita un problema di coordinamento con l'art. 1341 c.c. laddove dispone che non hanno effetto, se non specificatamente approvate per iscritto, le condizioni che stabiliscono limitazioni alla facoltà di proporre eccezioni.

Un esempio può meglio chiarire il concreto operare degli *smart contract*.

Si ponga il caso dell'acquisto di un biglietto del treno. Ricorrendo le modalità tradizionali di conclusione ed esecuzione dell'accordo, in caso di ritardo l'utente dovrebbe recarsi allo sportello ed avviare una procedura di rimborso che richiede tempo e vari adempimenti burocratici. Con l'utilizzo di uno *smart contract*, invece, il pagamento verrebbe sbloccato solo se il treno non arrivi in orario: in caso di ritardo l'algoritmo accrediterà all'utente una parte della somma versata a titolo di rimborso[44].

Essendo l'esecuzione contestuale viene meno l'interesse di prevedere misure rafforzative dell'esecuzione. Non essendo ipotizzabile l'inadempimento non può nemmeno porsi l'eccezione diretta a farlo valere[45], imponendo alle parti una rinuncia «forzata» alla medesima.

Un altro problema, ad esempio, si pone in termini di responsabilità, del debitore o per fatto illecito.

Alla luce dell'evoluzione tecnologica e del diffondersi di *software* sempre più sofistacti nella vita quotidiana sembra non ci si possa limitare a una semplice ripartizione della responsabilità tra i diversi soggetti in qualche modo coinvolti nell'utilizzo di uno *smart contract.* All'interprete si impone una scelta di fondo tra la possibilità di considerare il *software* uno strumento tecnologico avanzato, ma comunque

---

autorità pubbliche avrebbero difficoltà nell'assicurare il rispetto di scelte politico-legislative (basti ipotizzare uno *smart contract* che rilascia automaticamente e dietro corrispettivo la chiave di accesso a materiale pedo-pornografico archiviato in rete)».

44 C. Pernice, Smart contract *e automazione contrattuale: potenzialità e rischi della negoziazione algoritmica nell'era digitale*, cit., p. 133, precisa che tale meccanismo ricorda quello del deposito presso terzi. «In concreto gli *smart contracts* sono agenti indipendenti ai quali viene affidato un patrimonio che viene gestito in conformità delle istruzioni impartite: una volta che l'obbligazione è adempiuta da un lato il protocollo esegue automaticamente e simultaneamente la controprestazione, eliminando il divario temporale tra gli adempimenti».

45 C. Pernice, *o.c.*, p. 134.

uno strumento la cui attività rimarrà sempre riconducibile all'uomo, oppure la possibilità di considerare il *software* come un «soggetto», al quale imputare l'attività svolta, nella misura in cui si tratti di algoritmi dotati di capacità cognitive e di apprendimento[46].

Tale problema fa emergere un ulteriore profilo critico in ordine all'identificazione del titolare[47] e al coordinamento con le norme in materia di *data protection*[48].

Il sistema della *blockchain* consente, infatti, un anonimato relativo.

Chiunque può prendere parte alle attività registrate nel *database*, senza la necessità di accertare l'identità di coloro che effettuano le transazioni stesse, purché in possesso delle chiavi di accesso. In un simile contesto, l'interlocutore dichiara di essere un certo soggetto, ma non vi è alcuna validazione della dichiarazione, con la conseguenza che si rinuncia a creare ogni legame tra profilo informatico e profilo «reale».

Una ibridizzazione delle piattaforme decentralizzate permetterebbe la creazione di *blockchain* private, cd. *permissioned*, e potrebbe

---

[46] Il 26 ottobre 2017, l'Arabia Saudita ha concesso la cittadinanza onoraria a Sophia, un robot umanoide creato dalla compagnia di Hong Kong Hanson Robotics, dotato di intelligenza artificiale e in grado di dialogare, riconoscere le emozioni umane e rispondere in tempo reale, sorridendo e cambiando la propria espressione facciale. Cfr. I. FERLITO, «Smart contract». *Automazione contrattuale ed etica dell'algoritmo*, cit., p. 26; sulla differenza tra naturale e artificiale G. ZAGREBELSKY, *Intorno alla legge. Il diritto come dimensione del vivere comune*, Torino, 2009, p. 40. Il tema ha ricevuto riscontro anche dal Parlamento europeo nella Risoluzione del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica. In tale occasione Il Parlamento, consapevole dell'esistenza di almeno tre livelli di robotica, con distinti e crescenti livelli di autonomia, che vanno dai robot totalmente tele-operati a quelli che apprendono dalla loro esperienza, nonché dei diversi tipi di interazione che la macchina è in grado di avere con l'uomo e l'ambiente; ed allarmato dai nuovi scenari, ha sollecitato la Commissione all'adozione di un intervento normativo volto alla risoluzione dei problemi in tema d'imputazione dell'attività e di responsabilità per i danni prodotti dalla robotica, evidenziando con forza la necessità che vengano indicate precisazioni circa la possibilità per gli androidi di godere di personalità giuridica propria.

[47] F. SCUTIERO, Smart contract *e sistema di diritto, un connubio tutto da definire*, cit., p. 133; F. FAINI, Blockchain *e diritto: la "catena del valore" tra documenti informatici,* smart contracts *e* data protection, cit., p. 310 ss.; M. GIULIANO, *La* blockchain *e gli* smart contracts *nell'innovcazione del diritto nel terzo millennio*, cit., p. 1012 ss.

[48] Sul punto si v. M. GIULIANO, *La* blockchain *e gli* smart contracts *nell'innovazione del diritto nel terzo millennio*, cit., p. 1010, il quale sostiene che i caratteri principali della tecnologia *blockchain*, ossia la trasparenza, la condivisione, la decentralizzazione, la disintermediazione e l'irreversibilità dovrebbero conciliarsi con i princìpi fissati nel GDPR (Regolamento UE n. 2016/679) sul trattamento dei dati personali.

dare una soluzione al problema della identificazione perché consentirebbe di restringere l'accesso dei potenziali utenti a soggetti determinati, come avviene per la firma digitale. Il fatto che i computer che svolgono l'attività di elaborazione degli *smart contract* siano preindentificabili farebbe in modo che gli interventi normativi, le decisioni giudiziali e le istanze delle parti abbiano un concreto destinatario. Nodi identificabili rappresentano, in sostanza, il punto di incontro tra la *blockchain* e l'ordinamento giuridico, fornendo la piattaforma di una «entrata di emergenza» ogni volta l'intervento o la modifica delle istruzioni sia necessario[49].

Ogni soluzione volta a trasformare il sistema in *permissioned*, tuttavia, pone il rischio di negare l'essenza fondamentale dell'architettura *blockchain*, basata proprio su di un sistema *permissionless.*

4.6. La normativa internazionale ed europea

A livello internazionale solo un numero ristretto di Paesi si è dotato di una normativa specifica in tema di *smart contract*. Un esempio significativo proviene dallo Stato dell'Arizona, negli Stati Uniti, che nel marzo del 2017, ha emendato la propria disciplina in materia di transazioni elettroniche, riconoscendo agli *smart contract* e alle *blockchain*

[49] P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., pp. 116-117 ritiene che «la blockchain di tipo *permissioned* sembra essere, inoltre, la struttura che maggiormente si adatta allo sfruttamento commerciale della tecnologia. Due ordini di ragioni fanno protendere per tale ipotesi. In primo luogo, sembra improbabile una concreta diffusione dei registri decentralizzati senza che sia chiara la loro accettazione quale mezzo legittimo nella gestione di accordi in un ecosistema digitale. Legittimazione che, come desumibile da quanto detto poc'anzi, è fortemente dipendente dalle possibilità di regolabilità delle blockchain e, di conseguenza, dalla presenza di identificabili nodi, intesi quali soggetti passivi della regolamentazione».

pieno valore giuridico[50]. Sulla medesima scia, poi, si sono allineati gli Stati del Nevada[51], dell'Ohio[52] e del Tennesee[53].

A livello europeo[54], il Parlamento, con la risoluzione del 3 ottobre 2018 ha evidenziato le potenzialità delle tecnologie *blockchain* e, in merito agli *smart contract* ha rilevato la necessità che la Commissione effettui una approfondita valutazione sul piano del diritto, invitando all'esame del caso concreto per favorire la loro diffusione attraverso il

---

50 Arizona House Bill n. 2417, «An Act Amending Section 44-7003, Arizona Revised Statutes; amending title 44, chapter 26, Arizone Revised Statutes, by adding article 5; relating to electronic transactions». In particolare dispone che (a) «a signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature», (b) «a record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record» e che (c) «smart contracts may exist in commerce. A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term». Cfr. R. De Caria, *The legal meaning of smart contracts*, cit., p. 738.

51 Nevada Senate Bill n. 398, «An act relating to electronic transactions; recognizing and authorizing the use of blockchain technology; prohibiting a local government from taxing or imposing restrictions upon the use of a blockchain; and providing other matters properly relating thereto».

52 Ohio Senate Bill n. 220, «An act to amend sections 1306.01 and 3772.01 and to enact sections 1354.01, 1354.02, 1354.03, 1354.04 and 1354.05 of the Revised Code to provide a legal safe harbor to covered entities that implement a specified cybersecurity program, to allow transactions recorded by blockchain technology under the Uniform Electronic Transactions Act, and to alter the definition of "key employee" under the Casino Gaming Law».

53 Tennessee Senate Bill n. 1662, «an act to amend Tennessee Code Annotated, Title 12; Title 47; Title 48; Title 61 and Title 66, relative to electronic transactions». Cfr. M. Durovic e F. Lech, *The enforceability of smart contracts*, cit., p. 499 ss.

54 Al di là delle prime analisi del fenomeno compiute dalle proprie istituzioni volte ad incentivare una disciplina armonizzata tra i vari Stati membri in materia di *blockchai* e *smart contract*, in materia si ricorda il lavoro redatto dall'*European Parliamentary Research Service*, intitolato *How Blockchain Technology Could Change Our Lives*, nel quale viene evidenziata la necessità che i legislatori operino per armonizzare e collegare le regole del diritto contrattuale con gli *smart contract*, l'istituzione di un Osservatorio e *Forum* sulle *blockchain*, il progetto *Blockchain4EU* e la creazione dello *European Blockchain Partnership* (EBP), anvente anche l'obiettivo di realizzare un'infrastruttura condivisa per migliorare l'accesso e la fruizione dei servizi pubblici digitali transfrontalieri nel quadro dell'Unione europea. Cfr. *European Commission launches the EU Blockchain Observatory and Forum*, in europa.eu; P. Boucher, S. Nascimento e M. Kritikos, *How Blockchain Technology Could Change Our Lives*, Brussels, 2017; S. Nascimento, A. Polvora e J.S: Lourenco, *#Blockchain4EU: Blockchain for Industrial Transformations*, Lussemburgo, 2018.

coordinamento giuridico o il riconoscimento reciproco tra gli Stati membri in materia di contratti intelligenti[55].

Successivamente, il 4 dicembre 2018, i Paesi dell'Europa meridionale appartenenti all'EuroMed 7 (Italia, Cipro, Francia, Grecia, Malta, Portogallo e Spagna) hanno sottoscritto una dichiarazione con la quale si sono impegnati ad intraprendere una stretta collaborazione tecnologica, con lo scopo di promuovere la comprensione e lo sviluppo condiviso delle tecnologie *blockchain*, nel rispetto dei princìpi fondamentali europei. Nella dichiarazione gli *smart contract* sono considerati un potenziale elemento di svolta, capace di trasformare la fornitura e la fruizione di servizi in àmbiti quali «la certificazione dell'origine dei prodotti, l'istruzione, i trasporti, la mobilità, la navigazione marittima, i registri catastali, le dogane, gli albi delle imprese e la sanità»[56].

Nonostante il favore comunitario, tuttavia, solo Malta risulta essere lo Stato provvisto della disciplina più avanzata e organica in materia[57].

La normativa maltese distingue gli *smart contract* in senso informatico, definiti dei protocolli per computer, dagli *smart contract* suscettibili di costituire un vincolo giuridico, considerati dei veri e propri accordi contrattuali, redatti e conclusi, parzialmente o totalmente, in forma digitale. Essi ricevono tutela attraverso i meccanismi di esecuzione automatica delle pattuizioni negoziali previsti all'interno del loro codice informatico, oppure mediante il ricorso ai tradizionali rimedi giudiziali. Inoltre, il governo maltese ha posto un importante tassello per costruire l'intelaiatura normativa necessaria agli operatori *blockchain*, dotandosi di un'Autorità indipendente avente la funzione di promuovere e sviluppare tutte le soluzioni e servizi che utilizzano tecnologie innovative[58].

---

55 Parlamento UE, Risoluzione n. P8_TA-PROV(2018)0373, del 3 ottobre 2018, *Tecnologie di registro distribuito e blockchain: creare fiducia attraverso al disintermediazione*.

56 Dichiarazione ministeriale dei Paesi dell'Europa meridionale sulle tecnologie basate sui registri distribuiti, Bruxelles, 2018, p. 2, consultabile in sviluppoeconomico.gov.it

57 Il quadro normativo maltese è composto di tre testi: il *Virtual Financial Assets Act*, il *Malta Digital Innovation Autorty Act* e l'*Innovative Technology Arrangements and Services Act*.

58 Art. 8 *Malta Digital Innovation Autorty Act*. Anche la Francia, seppure distante dalle posizioni anglosassoni, ha riconosciuto la valenza del nuovo meccanismo digitale, applicando fiorentemente lo stesso nei contratti di *escrow* nonché nel settore cinematografico e musicale per generare una più equa distribuzione della remunerazione inerente ai diritti d'autore tra tutti gli *stakeholders*, che partecipano alla filiera produttiva. Cfr. C. Waignier, *Blockchains et smart contracts: premiers retours d'expérience*

4.7. La normativa italiana

La scelta normativa italiana[59], nonostante l'entusiasmo iniziale, è risultata poco felice ponendo più problemi che soluzioni.

L'art. 8 -*ter*, comma 2, del d.l., 14 dicembre 2018, n.135, convertito in l. 11 febbraio 2019, n. 12 dispone che uno *smart contract* è «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».

Per potere comprendere meglio il senso della norma occorre ritornare all'idea di base di Nick Szabo. Secondo l'informatico americano

---

dans l'industrie musicale, in *Annales des Mines-Réalités industrielle*, 2017, pp. 46-49. Inoltre, ha consentito il ricorso alla tecnologia *blockchain* per i *minibons* e per la registrazione ed il trasferimento di titoli finanziari non quotati come sistema alternativo rispetto alla tradizionale registrazione in libri contabili e societari, e con eguali effetti giuridici. Nel dicembre 2018 il Parlamento francese ha reso noto di volere finanziare l'implementazione della tecnologia *blockchain* nella pubblica amministrazione, nei prossimi tre anni, con lo stanziamento di 500 milioni di euro. Cfr. N. RICHARD e R. BLOCH, *Des parlementaries préconisent d'investir 500 millions dans la blockchain en trois ans*, in *lesechos.fr*.; S. ACETO DI CAPRIGLIA, *Contrattazione algoritmica. Problemi di profilazione e prospettive operazionali. L'esperienza "pilota" statunitense*, in *Federalismi.it*, 2019, p. 32, rileva che, in Spagna, gli *smart contract* non vengono considerati dei veri contratti ma come una innovativa modalità di conclusione o, in alternativa, «come forma addizionale rispetto a quelle tradizionali (atto pubblico, scrittura privata, accordo totale, fatti concludenti)».

59 I. FERLITO, «Smart contract». *Automazione contrattuale ed etica dell'algoritmo*, cit., p. 693, fa riferimento al comunicato stampa dell'ottobre 2017 da parte del Consiglio Nazionale del Notariato, in cui viene presentata la «*Notarchain*», una nuova modalità di archiviazione dei dati digitali in una duplice modalità ossia i registri diffusi (*blockchain*) e i registri volontari digitali; «o ai diversi progetti quali, ad esempio, la "Torrefazione Caffè San Domenico", il "*Wine Blockchain EY*", che si avvalgono della tecnologia *blockchain* per traciare il percorso di filiera del prodotto finito. Sul tema si v. S. MORABITO, *L'applicabilità della Blockchain nel diritto dell'arte*, in businessjus.com; G. MAGRI, *La Blockchain può rendere più sicuro il mercato dell'arte?*, in *Aedon*, 2019; M. GIACCAGLIA, *Considerazioni su blockchain e smart contracts (oltre le criptovalute)*, in *Contr. impr.*, 2019, p. 941 ss.

molte clausole contrattuali (come la garanzia, l'assunzione dell'obbligazione la delimitazione del diritto di proprietà, ecc…) possono essere incorporate in un *hardware* e in *software*[60].

Szabo immagina che grazie alla combinazione di *hardware* e *software* installati in uno stesso autoveicolo, ad esempio, lo *smart contract* entra in azione per disabilitare la messa in moto dell'auto in caso di mancato pagamento di un certo numero di rate, se acquistata in modo dilazionato[61].

Se questa è l'idea di base un rapido confronto con la disposizione pone subito in rilievo la mancanza del riferimento alla componente *hardware.* La norma definisce lo *smart contract* solo come un «programma per elaboratore» (quindi solo un *software*) mentre nell'idea originaria doveva essere una integrazione tra *software* e *hardware.*

Infatti, una *vending machine* ha una componente *software* (che contiene le istruzioni) e anche una componente *hardware* che materialmente eroga il prodotto. Allo stesso modo dovrebbe avvenire nell'esempio dell'autovettura, in cui sarà necessario un *hardware* che materialmente inibisca l'accensione fisica del motore «eseguendo» gli *input* ricevuti[62].

Di conseguenza per fare «girare» uno *smart contract* un semplice «programma per elaboratore» non sembra sufficiente, occorrendo un ulteriore dispositivo su cui il medesimo sarà programmato ad agire[63].

Altro problema che emerge dal confronto con la disposizione in esame si trova nella locuzione «effetti predefiniti dalle parti», perché, da un lato, sembra lasciare immaginare il momento di formazione

---

60 N. Szabo, *Formalising and Securing Relationships on Public Networks*, 1997, in firstmonday.org.

61 N. Sazbo, *Secure Property Title with Owner Authority*, in nakamotoinstitute.org.

62 M. Manente, Smart contract *e tecnologie basate su registri distribuiti*, in *Studio n.1_2019 DI del Consiglio Nazionale del Notariato*, 2019, p. 2 ss.; M. Farina, Smart contract *tra automazione contrattuale e disumanizzazione dei rapporti giuridici*, cit., p. 14.

63 Invero l'ulteriore dispositivo potrà essere un apparato *hardware* ma anche un altro apparato *software*, ma comunque sembra non bastare il solo algoritmo. Secondo M. Farina, *o.u.l.c*, «la mancata previsione non necessariamente rappresenterebbe una carenza normativa, perché potrebbe essere interpretata come una volontà precisa del legislatore di lasciare un margine di libertà evitando di vincolare eccessivamente l'àmbito di utilizzo di questi nuovi strumenti»; G. Rinaldi, Smart contract*: meccanizzione del contratto nel paradigma della* blockchain, cit., in corso di pubblicazione (pp. 27-28), precisa che «la medesima disposizione omette di distinguere, a differenza ad esempio della legislazione maltese, tra *smart contract* in senso informatico e *smart contract* in senso giuridico».

dell'accordo precedente allo *smart contract*, mentre dall'altro lato, indica il medesimo come fonte di vincolo giuridico tra le parti ponendosi così in contrasto con la preesistenza di un rapporto contrattuale. Se lo *smart contract* è già fonte giuridica di un vincolo «renderebbe inutile la previsione di un vincolo ulteriore»[64].

Infine, la norma in esame riconosce agli *smart contract* valore di documento avente forma scritta, circostanza che finirebbe per avvicinarli ad un contratto vero e proprio, ma aprendo il problema della loro forma.

Nonostante il dato testuale dell'art. 1325 c.c. sembra affermare l'essenzialità della forma solo nei casi in cui è prevista dalla legge sotto pena di nullità, una «generica» forma del contratto è «sempre essenziale» [65], perché è sempre necessario che la decisione sia portata all'esterno o dichiarata[66].

La regola generale del sistema rimane la libertà di forma ma non la sua assenza.

Il tema acquista particolare rilevanza laddove si considerino quei contratti per i quali viene prevista dal legislatore la forma *ad substantiam*.

A quest'ultima viene riconosciuta una duplice funzione. Da un lato, esprime la cd. funzione di prova, ossia è volta ad avere la certezza dell'esatto contenuto delle dichiarazioni delle parti, dall'altro lato, esprime la cd. funzione di consapevolezza, ossia richiama l'attenzione delle parti sull'importanza dell'atto che stanno per compiere[67].

In questi termini, notevoli difficoltà sorgono nell'incorporare l'accordo delle parti, posto che, proprio come negli *smart contract*, non

---

64 M. MANENTE, Smart contract *e tecnologie basate su registri distribuiti*, cit., p. 3.

65 M. GIULIANO, *La* blockchain *e gli* smart contracts *nell'innovazione del diritto nel terzo millennio*, cit., p. 1030.

66 P. PERLINGIERI, *Manuale di diritto civile*, 9° ed., Napoli, 2018, p. 512, precisa che «se la forma viene considerata, in senso lato, come il veicolo (dichiarazione o comportamento concludente) mediante il quale l'assetto di interessi composto dalle parti risulta oggettivamente riconoscibile, per contro, la forma, quale requisito autonomo, si identifica nel documento (atto pubblico, scrittura privata o documento informatico) dal quale risulta la manifestazione di volontà. Delle due nozioni soltanto l'ultima integra la forma come requisito del negozio, mentre la prima riassume solo il diverso problema della necessaria esteriorizzazione delle manifestazioni di volontà dei contraenti»; N. IRTI, *Studi sul formalismo negoziale*, Padova, 1997, p. 137 ss.

67 M. MANENTE, Smart contract *e tecnologie basate su registri distribuiti*, cit., p. 4.

sempre il documento contenente il contratto possa essere redatto materialmente dalle parti interessate, per cui occorrerà individuare uno strumento che sia idoneo a rappresentare correttamente la decisione delle parti a vincolarsi nel contratto, anche nel caso in cui il documento sia predisposto dai terzi.

Normalmente tale strumento è la sottoscrizione ma, in materia di *smart contract*, porta con sé il problema dell'imputabilità dell'atto e dell'identificazione delle parti[68].

Infatti, la disposizione in esame non prevede espressamente alcuna forma di sottoscrizione, delegando all'Agenzia per l'Italia digitale (AgID) la determinazione dei requisiti necessari per l'identificazione delle parti[69].

La somiglianza dal punto di vista testuale della formula utilizzata dal legislatore per gli *smart contract*, rispetto a quella già usata nel Codice dell'Amministrazione Digitale (cd. CAD) per la firma digitale apre ulteriori questioni.

---

[68] La sottoscrizione esprime tre funzioni: indicativa, perché permette di identificare l'autore del documento; dichiarativa, perché permette l'assunzione della paternità del documento; probatoria, perché dimostra l'autenticità del documento. Cfr. G. Petrelli, *Documento informatico, contratto in forma elettronica e atto notarile*, in *Notariato*, 1997, p. 567; G. Casu, *L'atto notarile tra forma e sostanza*, Milano-Roma, 1996, p. 148 ss.

[69] La novella sembra porsi in linea con quanto disposto dagli artt. 20, comma 1 *-bis* e 21, comma 2*-bis*, d.lg., 5 marzo 2005, n. 82, cd. CAD, che rispettivamente prevedono: «Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità» e « Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo».

In primo luogo, dalla formulazione usata dal legislatore emerge che questo «processo di identificazione» sembri rappresentare qualcosa di diverso e alternativo rispetto a quanto previsto dal CAD.

La lettura sistematica delle norme potrebbe sollevare il problema se sia consentito ad AgID, nell'àmbito della delega attribuitagli, prevedere comunque l'utilizzo di firme digitali per l'imputabilità di uno *smart contract* o se, come previsto per il documento informatico, debba trattarsi di processi differenti ed ulteriori rispetto all'apposizione di una firma[70].

In secondo luogo, la delega ad AgID sembra eccessivamente ampia per attribuire a tale Ente in via esclusiva la responsabilità di adottare misure idonee ad evitare fenomeni di sostituzione di persona, senza una minima copertura normativa in merito.

Nella disposizione in esame, quindi, sembra mancare un meccanismo che consenta di documentare una manifestazione inequivoca della volontà delle parti[71], anche se la locuzione «la cui esecuzione vincola automaticamente due o più parti» ne fa intravedere alcune tracce.

Il termine «esecuzione» si riferisce a quella fase del rapporto contrattuale successivo alla sua conclusione, in cui le prestazioni vengono eseguite dalle parti.

In questo modo la norma sembra esprimere un nonsenso giuridico, perché l'esecuzione, intesa come adempimento, non può generare vincoli, in quanto semmai determina l'estinzione di una obbligazione e non il suo sorgere.

Se, invece, si provi a cercare il significato del termine «esecuzione», contenuto nella disposizione in esame, in un altro registro linguistico

---

70 M. MANENTE, Smart contract *e tecnologie basate su registri distribuiti*, cit., p. 6, nota 4, sottolinea che sarebbe necessario verificare la compatibilità di tale impianto con il Regolamento UE, n. 910/2014 del Parlamento e Consiglio UE, nel quale «la nozione di "firma elettronica" è indicata come l'insieme di "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare"».

71 G. RINALDI, Smart contract*: meccanizzazione del contratto nel paradigma della* blockchain, in corso di pubblicazione; M. NICOTRA, *L'Italia prova a normare gli smart contract, ecco come: pro e contro*, in agendadigitale.eu; M. GIULIANO, Blockchain*, i rischi del tentativo italiano di regolamentazione*, in agendadigitale.eu; ID., *La* blockchain *e gli* smart contracts *nell'innovcazione del diritto nel terzo millennio*, cit., p. 34 ss. DeJure; M. FARINA, Smart contract *tra automazione contrattuale e disumanizzazione dei rapporti giuridici*, cit., p. 15.

che non sia quello giuridico, forse la questione non si risolve necessariamente in un nonsenso.

Nel linguaggio informatico il termine «esecuzione» è la traduzione di «execution»[72] che significa «avvio» di un programma, ossia lettura delle istruzioni caricate e loro memorizzazione all'interno del sistema[73].

L'azione materiale del «dare avvio» al programma potrebbe produrre la prova della manifestazione del consenso di una parte di accettare le istruzioni in esso contenute, e quindi l'«avvio congiunto» del programma, ad opera delle parti interessate, la prova dell'avvenuto accordo.

Tuttavia, la formulazione legislativa rimane una scelta terminologica confusa.

Sul piano funzionale, inoltre, sarà ancóra più difficile dimostrare la causa di uno *smart contract.* Un programma per elaboratore può contenere solo istruzioni di tipo esecutivo e non di tipo descrittivo, in quanto esse non sono istruzioni, ma il frutto di un procedimento ermeneutico che la logica binaria di un computer non potrà mai realizzare.

Se, infatti, si può immaginare la causa di uno *smart contract* che sovrintenda al funzionamento di un distributore di bevande, non altrettanto lo si può fare per uno che semplicemente contenga l'istruzione di pagamento di una somma da una persona ad un'altra. Un simile pagamento potrebbe in concreto trovare la sua causa in molteplici schemi negoziali (ad esempio compravendita, mutuo, liberalità).

Residua «uno spazio alla valutazione della conformità del regolamento contrattuale nel suo complesso e delle singole pattuizioni tradotte in altrettante formule *if-then* ai canoni di buona fede, correttezza, ragionevolezza e proporzionalità»[74].

---

72 Letteralmente «the performance of an instruction or program». Cfr. oxforddictionaries.com/definition/execution.

73 M. Manente, Smart contract *e tecnologie basate su registri distribuiti*, cit., p. 6; G. Rinaldi, Smart contract*: meccanizzazione del contratto nel paradigma della* blockchain, in corso di pubblicazione.

74 D. Di Sabato, *Gli* smart contracts*: robot che gestiscono il rischio contrattuale*, cit., p. 401; C. Pernice, Smart contract *e automazione contrattuale, potenzialità dei rischi della negoziazione algoritmica nell'era digitale*, cit., pp. 124-125; F. Scutiero, Smart contract *e sistema di diritto, un connubio tutta da definire*, cit., p. 131. Sulla interpretazione si v. E. Betti, *Interpretazione della legge e degli atti giuridici*, Milano, 1949, p. 168; Id., *Interpretazione della legge e sua efficienza evolutiva*, in Id., *Diritto, metodo, ermeneutica*, Milano,

Gli *smart contract* possono rendere meno probabile l'insorgere di un imprevisto, ma non possono escluderlo del tutto.

La rigidità dello strumento informatico, che rappresenterebbe la prerogativa di un eventuale successo degli *smart contract*, potrebbe costituire il loro principale difetto.

È proprio l'adeguamento al caso concreto dei contenuti giuridici uno dei problemi applicativi più difficili da affrontare da tali strumenti tecnologici.

4.8. Sviluppi futuri e il ruolo del giurista

Nell'àmbito della generale e inarrestabile tendenza verso la meccanizzazione di attività che in passato erano riservate esclusivamente all'intervento umano, gli *smart contract* costituiscono una delle maggiori espressioni di tale indirizzo nell'interazione negoziale[75].

1991, p. 536 ss.; ID., *Teoria generale dell'interpretazione*, Milano, 1990, *passim*; P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, Napoli, 2006, p. 563 ss.; ID., *Interpretazione e legalità costituzionale*, Napoli, 2012, p. 113 ss.; ID., *Applicazione e controllo nell'interpretazione giuridica*, in *Riv. dir. civ.*, 2010, p. 317 ss.; ID., *Controllo e conformazione negli atti di autonomia negoziale*, in *Rass. dir. civ.*, 2017, p. 204 ss.; ID., *Interpretazione e controllo di conformità alla Costituzione*, in *Rass. dir. civ.*, 2018, p. 593 ss.; ID., *Interpretazione ed evoluzione dell'ordinamento*, in *Riv. dir. priv.*, 2011, p. 159 ss.; N. IRTI, *Princìpi e problemi di interpretazione contrattuale*, in *Riv. trim. dir. proc. civ.*, 1999, p. 1139 ss.; ID., *Sulla positività ermeneutica*, in *Riv. dir. civ.*, 2016, p. 923.

75 G. RINALDI, Smart contract*: meccanizzazione del contratto nel paradigma della* blockchain, in corso di pubblicazione; I. FERLITO, *"Smart Contract". Automazione contrattuale ed etica dell'algoritmo*, cit., p. 696, riporta in merito il dialogo intercorso tra Natalino Irti e Emanuele Severino, il primo giurista e il secondo filosofo. Nella visione del giurista emerge «la concezione positivistica del diritto, fatto di norme aventi esclusivamente validità procedurale, non già verità di contenuto, "nomodotti" all'interno delle quali le proposizioni ideologico-politiche o economiche, i molteplici *lógoi*, devono tradursi per riuscire ad ottenere efficacia; e la consapevolezza che la tecnica sia segnata dalla medesima astrattezza, o se si vuole dall'indeterminatezza, e perciò non in grado di rispondere alle domande fondamentali del diritto». Nella visione del filosofo, invece, «la tecnica è destinata a diventare il principio regolatore di ogni materia, la volontà che regola ogni altra volontà». Sembra che «la tecnica tenda all'onnipotenza». Cfr. N. IRTI e E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, 2001, p. 12; N. IRTI, *Nichilismo giuridico*, Roma-Bari,2004, p. 18 ss.; ID., *Il salvagente della forma*, Roma-Bari, 2007, p. 45 ss. *Contra* O. DE BERTOLIS, *Elementi di antropologia giuridica*, Napoli, 2010, p. 89 ss., spec. p. 94, il quale precisa che «è scopo di una legislazione che procede con scienza e coscienza sempre più puntuale permettere, per il bene nostro e dei posteri, interventi tecnologici sul mondo esterno rispettosi dell'equilibrio naturale dei beni e delle risorse»; ID., *La moneta del diritto*, Milano, 2012, p. 73 ss.; ID., *L'ellisse giuridica*, Padova, 2011, p. 69 ss.

In effetti la tecnologia *blockchain* consente agli *smart contract* di espandere potenzialmente il loro raggio d'azione[76].

Una delle prime implementazioni la si può vedere nel *car sharing*. Il proprietario della flotta inserisce uno *smart contract* la cui funzione è di verificare l'avvenuto pagamento del servizio e di conseguenza sbloccare le portiere dell'auto e consentirne l'avviamento[77]. Lo *smart contract*, oltre ad essere *self-executing* contiene anche le condizioni generali di utilizzo e gestisce la loro approvazione da parte dell'utente[78].

Allo stesso modo è possibile utilizzarli per i sistemi di guida autonoma e per l'informatica automobilistica: ad esempio per l'acquisto di servizi accessori quali le guide turistiche, report sulle condizioni del traffico e servizi di intrattenimento[79].

La possibilità di strutturare uno *smart contract* in una serie indefinita di opzioni permetterebbe di modificare le prestazioni, e quindi il contenuto del rapporto contrattuale, secondo quanto previsto dall'algoritmo. Un esempio potrebbe trovarsi nel contratto di assicurazione per la responsabilità da circolazione dei veicoli: un sistema rileva i chilometri percorsi e l'algoritmo modula il premio che viene immediatamente addebitato sul conto corrente dell'assicurato[80].

Un'altra possibile applicazione è il cd. *smart construction contract*, attraverso il quale possono gestirsi tutti i rapporti di fornitura per la

---

76 G. Lemme, *Gli* smart contracts *e le tre leggi della robotica*, cit., p. 145.

77 In parte già avviene per i servizi di *car sharing* diffusi, ad esempio *Enjoy* e *Car2go*.

78 J.M. Sklaroff, *Smart contracts and the Cost of Inflexibility*, in researchgate.net, 2017.

79 G. Lemme, *Gli* smart contracts *e le tre leggi della robotica*, cit., p. 146; F. Rundo e S. Conoci, *Tecnologia blockchain: dagli smart contract allo smart driving*, in *Dir. giust.*, 2017. Secondo R. De Caria, *The legal meaning of smart contracts*, cit., p. 747, compie una interessante riflessione sul funzionamento di Netflix: «there are in fact very few differences between the functioning of a smart contract and that of a mechanical vending machine. Netflix allows users to legally watch streaming videos in exchange for a monthly payment; in case of missing payments, the software will simply supsend the service, not allowing users to log in. The fact that the interruption is performed by humans, by software, or by smart contracts with a record in the blockchain, does not in practice seem to make a relevant legally speaking difference».

80 F. Scutiero, Smart contract *e sistema di diritto, un connubio tutta da definire*, cit., p. 126; A.J. Casey e A. Niblett, *Self-driving contracts*, in *The Journal of Corporation Law*, 2017, p. 5 ss.

costruzione di un edificio, che l'algoritmo mette in relazione con il progetto per l'automatizzazione e la velocizzazione del lavoro d'impresa[81].

Non mancano, infine, ipotesi più o meno surreali come lo *smart love*. Si tratterebbe di un accordo matrimoniale formato su base *peer to peer* tramite la manifestazione di consenso dei «coniugi». L'ufficiale di stato civile diventerebbe la rete e alle norme che regolamentano gli effetti civili del matrimonio si sostituirebbero le istruzioni date allo *smart contract* dal proprio algoritmo[82].

Nonostante una tale ampiezza applicativa, i vantaggi associati a questa nuova tecnologia sembrano, allo stato dell'arte, «sovrastimati»[83].

In primo luogo, la probabile non conoscenza dei linguaggi di programmazione tra le parti pone in dubbio la concreta intellegibilità dell'accordo tra i contraenti e, ulteriormente, apre l'ingresso ad anomalie e vulnerabilità informatiche, cd. *bug*, oppure in errori nella traduzione in algoritmo dell'assetto di interessi che le parti intendono perseguire. La necessità, quindi, di rivolgersi a soggetti terzi, informatici e programmatori, per il confezionamento di uno *smart contract* non permetterebbe una riduzione significativa dei costi.

In secondo luogo, non del tutto vero è l'affermazione secondo la quale gli *smart contract* assicurerebbero un giudizio «oggettivo», riducendo se non azzerando l'attività interpretativa degli operatori del diritto, e la contestuale riduzione delle controversie. La negoziazione algoritmica non esclude in radice la possibilità di sindacare l'effetto prodotto tecnologicamente, ma semplicemente l'intervento giudiziario viene rinviato in una fase successiva. Anzi, «l'impossibilità per le

---

81 L. STOUGIANNOS e A. MAGNERON, *BIM, Blockchain and the Smart Construction Contract*, 2018, in millerthomson.com/en/blog/breaking-ground-mt-construction-law/bim-blockchain-smart-construction-contract.

82 G. LEMME, *Gli* smart contracts *e le tre leggi della robotica*, cit., p. 146; A. CARACCIOLO, *L'amore ai tempi della blockchain*, in *Annali del Dipartimento Jonico*, 2017, p. 55 ss., il quale rileva che è possibile ipotizzare anche *smart contract* illeciti, ad esempio nel furto dei dati; I. FERLITO, *"Smart Contract". Automazione contrattuale ed etica dell'algoritmo*, cit., p. 696; M. NASTRI, *Nuove tecnologie: l'ultima domanda*, in *Notariato*, 2018, p. 485 ss.; G. LAURINI, *Il notariato di domani: identità e innovazione*, in *Notariato*, 2010, p. 237 ss.

83 C. PERNICE, Smart contract *e automazione contrattuale, potenzialità dei rischi della negoziazione algoritmica nell'era digitale*, cit., p. 136; G. RINALDI, Smart contract*: meccanizzazione del contratto nel paradigma della* blockchain, in corso di pubblicazione.

parti di "correggere", anticipatamente l'ingiustizia della soluzione programmata potrebbe paradossalmente portare all'attenzione dell'autorità giudiziaria situazioni convenzionalmente rimediabili»[84].

Queste riflessioni fanno protendere verso la considerazione che il diritto non debba piegarsi alla tecnica lasciando che questa, con la sua potenza, imponga la regolazione, anzi, rinforza l'idea che lo scrutinio del giurista, quindi l'interpretazione, sia necessario ed essenziale, oggi più che mai. Il giurista rimane l'unico in grado di plasmare il diritto esistente al nuovo che avanza, nel rispetto dei princìpi di ciascuno ordinamento nel quale il fenomeno è analizzato e di una componente «etica» irrinunciabile[85].

Il diritto non potrà di certo impedire la diffusione delle nuove tecnologie, ma dovrà comunque disciplinarne gli sviluppi, non rinunciando al proprio ruolo di elemento regolatore della società e del mercato, perché non è una tecnica come le altre ma è «un tecnica di umanizzazione della tecnica»[86].

Il riferirsi immediatamente all'uomo gli conferisce «uno statuto epistemologico completamente diverso dalle tecniche»[87], le quali si rapportano invece a degli oggetti.

L'importanza del caso concreto diventa dirompente. Occorre compiere un'analisi attenta di tutti i suoi elementi e peculiarità, compresi quelli che, a prima vista, potrebbero sembrare poco rilevanti per poi

---

84 C. Pernice, Smart contract *e automazione contrattuale, potenzialità dei rischi della negoziazione algoritmica nell'era digitale*, cit., p. 137.

85 I. Ferlito, *"Smart Contract". Automazione contrattuale ed etica dell'algoritmo*, cit., p. 698; G. Perlingieri, *Garanzie «atipicihe» e rapporti commerciali*, in *Riv. dir. impr.*, 2017, p. 45 sottolinea che «deve rifuggire da ragionamenti logico-deduttivi, da astratte simmetrie concettuali e deve limitarsi a individuare, in relazione al caso concreto, la normativa piú *adeguata* e *congrua* alle peculiarità dei beni, degli interessi che reclamano soddisfazione e dei valori normativi coinvolti». Cfr. Id., *Profili applicativi della ragionevolezza nel diritto civile*, cit., p. 114; E. Betti, *Teoria generale della interpretazione*, cit., p. 59 ss.; P. Perlingieri, *Interpretazione e applicazione: profili dell'individuazione normativa*, in *Dir. giur.*, 1975, p. 826 ss.; B. Troisi, *Interpretazione della legge e dialettica*, in Aa.Vv., *Legge, Giudici, Giuristi*, (Atti del Convegno tenuto a Cagliari nei giorni 18-21 maggio 1981), Milano, 1982, p. 13 ss.; P. Perlingieri, *Complessità e unitarietà dell'ordinamento giuridico vigente*, in *Rass. dir. civ.*, 2005, p. 188 ss.; Id., *L'interpretazione della legge come sistematica e assiologica. Il broccardo* in claris non fit interpretatio*, il ruolo dell'art. 12 disp. prel. c.c. e la nuova scuola dell'esegesi*, cit., p. 275 ss.; Id., *Interpretazione assiologica e diritto civile*, in *Corti salernitane*, 2013, p. 465 ss.

86 O. De Bertolis, *Elementi di antropologia giuridica*, cit., p. 59.

87 O. De Bertolis, *o.c.*, p. 96.

individuare, nel suo àmbito, la disciplina da applicare in modo che risulti la più ragionevole ed adeguata al caso in esame[88].

Sorge, in altri termini, la necessità di disciplinare i comportamenti e le attività al fine di non rendere tutto ciò che è tecnologicamente possibile giuridicamente legittimo[89].

Ai tempi del *web*, in cui la persona diventa dato e viene lanciata nell'arena del digitale, l'unica soluzione sembra essere quella di mantenere la bussola puntata sul principio di tutela della dignità umana[90].

Il rapporto tra uomo e macchina rimane di complementarietà[91]. Uno *smart contract* potrà porsi prevalentemente come «strumento» di supporto o come «parte» di un più ampio accordo contrattuale, magari

---

88 P. Perlingieri, *Complessità e unitarietà dell'ordinamento giuridico vigente*, cit., p. 189 ss.; Id., *Equilibrio delle posizioni contrattuali ed autonomia privata. Sintesi di un convegno*, in Id., *Il diritto dei contratti*, cit., p. 468; P. Grossi, *La formazione del giurista e l'esigenza di un odierno ripensamento epistemologico*, in Id., *Società, diritto, Stato. Un recupero per il diritto*, Milano, 2006, p. 46, il quale osserva che «la complessità dell'attuale paesaggio giuridico obbliga il giurista a una nuova messa a fuoco e a nuovi strumenti di osservazione», riconoscendo implicitamente la diretta incidenza della complessità del sistema sulla teoria dell'interpretazione; P. Perlingieri e P. Femia, *Nozioni introduttive e princípi fondamentali del diritto civile*, Napoli, 2004, p. 78. Sulla ragionevolezza e adeguatezza si v. G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, p. 2 ss.; Id., *Sul criterio di ragionevolezza*, in C. Perlingieri e L. Ruggeri (a cura di), *L'incidenza della dottrina sulla giurisprudenza nel diritto dei contratti*, Napoli, 2016, p. 29 ss.; Id., *La scelta della disciplina applicabile ai c.dd. «vitalizi impropri». Riflessioni in tema di aleatorietà della rendita vitalizi e di tipicità e atipicità nei* contratti, cit., p. 529 ss.; A. Fachechi, Rent to buy *e variabilità della disciplina applicabile*, cit., p. 105 ss.; L. D'Andrea, *Ragionevolezza e legittimazione del sistema*, Milano, 2005, p. 2; P. Perlingieri, *La «grande dicotomia» diritto positivo – diritto naturale*, in Id., *L'ordinamento vigente e i suoi valori. Problemi del diritto civile*, Napoli, 2006, p. 555 s.; E. Navarretta, *Buona fede e ragionevolezza nel diritto contrattuale europeo*, in *Eur. dir. priv.*, 2012, p. 971 ss.; N. Lipari, *Diritto e valori sociali. Legalità condivisa e dignità della persona*, Roma, 2004, p. 7.

89 O. De Bertolis, *Elementi di antropologia giuridica*, cit., p. 94.

90 P. Perlingieri, *La persona e i suoi diritti. Problemi di diritto civile*, Napoli, 2005, p. 45 ss.; I. Ferlito, *"Smart Contract". Automazione contrattuale ed etica dell'algoritmo*, cit., p. 699, precisa che «"solo così sarà possibile superare le sfide sempre più complesse che il progresso tecnologico ci pone davanti", magari attraverso l'individuazione di standard etici a livello sovranazionale che sappiano garantire il rispetto della dignità personale».

91 C. Pernice, Smart contract *e automazione contrattuale, potenzialità dei rischi della negoziazione algoritmica nell'era digitale*, cit., p. 137; D. Di Sabato, *Gli* smart contracts*: robot che gestiscono il rischio contrattuale*, cit., pp. 401-402.

redatto secondo forme più «tradizionali», curandone e semplificandone l'aspetto relativo all'adempimento delle obbligazioni pattuite[92].

Il legislatore e il giurista avranno il difficile compito di relazionare i nuovi fenomeni sociali entro i valori e gli ideali che costituiscono la base della società attuale, magari aiutando i programmatori nella progettazione degli algoritmi ad inserire quei princìpi che confermino una dimensione antropocentrica, i caratteri non replicabili della nostra unicità.

La necessità di individuare la disciplina da adottare implica una scelta di fondo tra la possibilità di considerare gli *smart contract* come uno strumento tecnologico avanzato, ma pur sempre un mezzo per lo svolgimento dell'attività che deve in ogni caso essere ricondotta all'uomo che se ne avvantaggia e ne risponde, e l'eventualità fantascientifica, ma forse non più di tanto, di valorizzare la capacità degli *smart contract* di operare scelte e quindi di essere imputabili dell'attività compiuta.

Si sta realizzando ciò che Asimov aveva immaginato e quindi considerare che le tre leggi[93] della robotica, da lui elaborate, possano svolgere il ruolo di legge fondamentale, in riferimento alle attività svolte

---

92 M. Manente, Smart contract *e tecnologie basate su registri distribuiti*, cit., p. 7; F. Di Ciommo, «Blockchain, smart contract», *intelligenza artificiale (AI) e «trading» algoritmico: ovvero, del regno del non diritto*, cit., p. 4; C. Pernice, Smart contract *e automazione contrattuale, potenzialità dei rischi della negoziazione algoritmica nell'era digitale*, cit., p. 137 ritiene che gli àmbiti applicativi più diffusi sembrano da rinvenirsi nel settore assicurativo, bancario e finanziario. Un protocollo, ad esempio, potrebbe prevedere di vendere o acquisire un certo numero di partecipazioni azionarie al raggiungimento di una determinata quotazione. Inoltre, gli *smart contract* potrebbero essere impiegati al fine di agevolare la raccolta di informazioni nei mercati bancari e assicurativi per ridurre tempi e costi delle procedure di erogazione dei mutui e rimborso delle polizze.

93 Prima legge: «Un robot non può recar danno a un essere umano né può permettere che a causa del proprio mancato intervento un essere umano riceva danno». Seconda legge: «Un robot deve obbedire agli ordini impartiti dagli esseri umani purché tali ordini non contravvengano alla prima legge». Terza legge: «Un robot deve proteggere la propria esistenza, purché questa autodifesa non contrasti con la Prima e con la Seconda Legge». Esse furono elaborate da Asimov nel 1942 e illustrate in una rivista scientifica. Successivamente in Io, Robot (1950) Isaac Asimov enuncia una quarta legge: «Un robot non può recar danno all'umanità e non può permettere che, a causa di un suo mancato intervento, l'umanità riceva danno». G. Lemme, *Gli* smart contracts *e le tre leggi della robotica*, cit., p. 150, rileva che «in fondo, scopo dei robot di Asimov era proteggere l'Uminità. Anche contro le mille sfumature della stupidità ed irrazionalità umana, spesso autolesionistica, ma anche alla base dell'evolversi della società. Gli *smart contract*, in fondo, sono pensati per «proteggere» l'uomo dalla

con l'impiego di macchine sempre più automatizzate, oppure possiamo ancora considerare applicabile la *summa divisio* di Aristotele[94], che distingueva gli strumenti a disposizione dell'uomo per amministrare il suo patrimonio in «strumenti inanimati» e «strumenti animati», ovvero i servi, e classificare gli *smart contract* tra i primi?

fatica di leggere condizioni contrattuali, dal verificarne l'adempimento, dal richiedere prestazione controprestazione tra le parti. Se questa protezione sarà paragonabile a quella di un amorevole genitore o a quella di un sovrano dispotico, solo il futuro – prossimo – potrà dirlo».

94 *Politica, Libro I.*

5. *Sharenting* e riservatezza del minore in rete

Massimo Foglia

5.1. Introduzione

Se si vuole giungere, nell'era tecnologica, al significato di identità personale nella sua piena comprensione biografica, occorre monitorare quella propaggine di noi stessi che germoglia dal terreno d'un altro mondo, quello della rete[1]. I cosiddetti nativi digitali si muovono con naturalezza nel contesto dei *social media* sin dai primi anni di vita; essi hanno una connaturata propensione a "vivere in pubblico" e una parte rilevante della loro vita (ma ormai pure quella dei loro genitori) si svolge in questa dimensione elettronica[2].

È in tale contesto che appare interessante osservare *come* la responsabilità genitoriale debba operare nel rispetto di quei doveri di cura e di controllo che garantiscono lo sviluppo della personalità e dell'identità dei figli minori[3]. Un angolo prospettico particolarmente favorevole

---

1 V. per tutti RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Milano, 2006, p. 103 e p. 108 e ID., *Il diritto di avere diritti*, Roma-Bari, 2012, p. 327, il quale si chiedeva se, in tale contesto, avessero ancora senso regole che privilegiano un bisogno di vita privata.

2 Sul concetto di identità personale nell'era tecnologica sia consentito il rinvio a FOGLIA, *L'identità personale nell'era della comunicazione digitale*, in BILOTTA e RAIMONDI, *Il soggetto di diritto. Storia ed evoluzione di un concetto nel diritto privato*, Napoli, 2020, p. 265 ss.

3 In dottrina la tematica è stata approfondita, in particolare, da GIARDINA, *Interesse del minore: gli aspetti identitari*, in *Nuova giur. civ. comm.*, 2016, p. 159; ID., *Morte della potestà e capacità del figlio*, in *Riv. dir. civ.*, 2016, p. 1609 ss.; THIENE, *Riservatezza e autodeterminazione del minore nelle scelte esistenziali*, in *Fam. dir.*, 2017, p. 172; SESTA, *Famiglia e figli a quarant'anni dalla riforma, in Fam. dir.*, 2015, p. 1009; FERRANDO, *Stato unico di figlio e varietà dei modelli familiari*, in *Fam. dir.*, p. 952; AL MUREDEN, *La responsabilità genitoriale tra condizione unica del figlio e pluralità dei modelli familiari*, in *Fam. dir.*, 2014, p. 466; DE CRISTOFARO, *Dalla potestà alla responsabilità genitoriale. Profili problematici di*

a tale disamina è rappresentato dal diritto alla riservatezza del minore[4]. Occorre chiarire sin d'ora quale significato dare al concetto di riservatezza nell'ambito di questa breve riflessione. Due sono le prospettive che interessa ora indagare: la prima riguarda la tutela dei dati personali del minore (ad esempio, l'immagine)[5] nei confronti di terzi e del mondo esterno al contesto familiare[6] (si parlerà, a questo riguardo, del fenomeno dello *sharenting*); la seconda concerne il divieto di intromissione nella vita privata del minore (si pensi alla segretezza della comunicazione e al rispetto della corrispondenza)[7].

Entrambe le questioni vanno risolte nell'ambito del rapporto tra identità e autonomia[8], che all'interno del diritto di famiglia conduce quasi fisiologicamente ad un conflitto tra autorità e libertà[9]. Se l'autonomia postula il potere di autodeterminazione soggettiva, inteso come

---

una innovazione discutibile, in *Nuova giur. civ. comm.*, 2014, in particolare pp. 782 e 788. Tra le opere monografiche più recenti v. C. M. Bianca, *La riforma della filiazione*, Padova, 2015; Id., *Diritto civile*, II, 1, Famiglia, Milano, 2017, p. 377; A. Gorgoni, *Filiazione e responsabilità genitoriale*, Padova, 2017.

4 Sul dibattito, nella letteratura italiana, sul diritto alla riservatezza v. Giampiccolo, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. e proc. civ.*, 1958, p. 458 ss. e Pugliese, *Il diritto alla «riservatezza» nel quadro dei diritti alla personalità*, in *Riv. dir. civ.*, I, 1963, p. 605 ss. Il diritto alla riservatezza, diretto a tutelare principalmente l'intimità privata del soggetto tutelato dalle ingerenze da parte di terzi, va tenuto distinto dal diritto alla privacy, inteso come corretto trattamento dei dati personali. Sottolinea opportunamente tale distinzione M. Bianca, *Il minore e i nuovi media*, in Senigaglia (a cura di), *Autodeterminazione e minore d'età. Itinerari di diritto minorile*, Pisa, 2019, p. 151 ss.

5 Sul concetto di "dato personale" alla luce del Codice in materia di protezione dei dati personali, così come modificato dal d.lgs. 10 agosto 2018, n. 101, in adeguamento al regolamento UE 2016/679/UE (GDPR), v. C. Irti, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus*, 2, 2020, p. 379 ss.

6 Per un approfondimento su tale profilo v. M. Bianca, *Il minore e i nuovi media*, cit., p. 145 ss.

7 Per un'ampia e recente indagine sul punto v. C. Camardi, *Minore e privacy nel contesto delle relazioni familiari*, in Senigaglia (a cura di), *Autodeterminazione e minore d'età*, cit., p. 117 ss., nonché Id., *Relazione di filiazione e privacy. Brevi note sull'autodeterminazione del minore*, in *Juscivile*, 2018, p. 6 ss.

8 Per un quadro generale sul tema dell'autonomia del minore v. A. Belvedere - M. De Cristofaro, *L'autonomia dei minori tra famiglia e società*, Milano, 1980.

9 Pone in luce questa prospettiva, di recente, Senigaglia, *Le misure di protezione dell'interesse del soggetto minore di età tra autonomia ed eteronomia*, in Senigaglia (a cura di), *Autodeterminazione e minore d'età*, cit., p. 43 ss., svolgendo alcune riflessioni sulla considerazione giuridica del minore d'età e sul ruolo dei genitori nella crescita del minore: «È evidente, infatti, che nei primi anni di vita il "fanciullo" necessiti di essere cresciuto, ovvero di ricevere tutti quegli stimoli e fattori educativi che gli consentano di farsi adulto, di costruire la propria personalità; stimoli esterni promananti da chi

«potere di controllare le modalità di costruzione della propria identità»[10], è opportuno sottolineare come la costruzione dell'identità personale, e in particolare di quella digitale, molto spesso sfugga al controllo del suo titolare: si parla, in tal senso, di identità "esterna", in quanto *da altri* imposta all'interessato[11].

È utile sottolineare che la tutela della riservatezza e dei dati personali del minore opera non soltanto nei confronti dei terzi[12], ma anche nei confronti dei genitori. A questi ultimi è imposto, per un verso, un divieto di intrusione incondizionata nella privacy del minore all'interno della famiglia o nei luoghi che il minore frequenta; per altro verso è dovere del genitore evitare esternazioni che abbiano ad oggetto

---

ne ha la responsabilità, anzitutto genitoriale, in nome della quale è chiamato a plasmare l'altrui persona attingendo, evidentemente, dalle proprie risorse identitarie. Successivamente, lo sviluppo della razionalità e del discernimento del soggetto alimenta l'identità individuale, che va a definirsi e con essa l'interesse all'autonomia e all'autodeterminazione, quali strumenti funzionali allo svolgimento e allo sviluppo della personalità (artt. 2 e 3 Cost.). Un interesse, quest'ultimo, che va senz'altro tutelato anche se, proprio in ragione della vulnerabilità sempre più residuale, sotto il controllo, graduato, di chi ha la cura dell'infradiciottenne» (p. 44).

10 MARINI, *La giuridificazione della persona. Ideologie e tecniche nei diritti della personalità*, in *Riv. dir. civ.*, 2006, I, p. 366.

11 Occorre chiedersi chi siano questi *altri*. In una prima approssimazione si potrebbe rispondere: chi raccoglie, conserva e diffonde i dati personali. A titolo esemplificativo, è noto infatti che chi gestisce i *social network* o i motori di ricerca può condizionare il nostro modo di pensare e di comportarci: emblematico di ciò è il meccanismo della *filter bubble* (sul punto si rinvia a M. BIANCA, *La* filter bubble *e il problema dell'identità digitale*, in *MediaLaws*, 2, 2019, p. 1 ss.). Non solo. Oggi tutti sanno quanto i *social media* possano influenzare le opinioni dei cittadini, l'integrità del confronto democratico, forse addirittura l'esito di elezioni politiche di paesi democratici (cfr. ORIGGI, *La democrazia può sopravvivere a Facebook? Egualitarismo epistemico, vulnerabilità cognitiva e nuove tecnologie*, in *Ragion pratica*, 2018, p. 445 ss.; RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, p. 199 ss.). È il fenomeno della postverità e delle *fake news*, che dimostra come la tecnologia possa essere sfruttata dagli attivisti della disinformazione per scopi illeciti ed eversivi. È illuminante il libro di NICHOLS, *The Death of Expertise*, trad. it. *La conoscenza e i suoi nemici*, Roma, 2018, dove l'A. racconta come nel 2014 il «Washington Post» abbia chiesto agli americani se considerassero giusto intervenire militarmente in Ucraina in seguito all'aggressione russa. I più erano favorevoli, ma la cosa curiosa è che lo erano soprattutto coloro che non avevano idea, nemmeno lontanamente, di dove fosse l'Ucraina.

12 Sul punto v. CAMARDI, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 126; CARRIERO, *Privacy del minore e potestà dei genitori*, in *Rass. dir. civ.*, 2004, p. 1004, 1011; SCALISI, *Famiglia e diritti del minore*, in *Fam. pers. succ.*, 2006, p. 815, p. 821 ss.; THIENE, *Riservatezza e autodeterminazione del minore nelle scelte esistenziali*, cit., p. 173 ss.

dati personali del minore nei confronti di terze persone, che in tal modo ne vengano a conoscenza senza una ragione giustificatrice[13].

La questione che si vuol trattare si situa sul crocevia tra il diritto del minore alla privacy (che incorpora il potere di escludere le ingerenze altrui) e la responsabilità genitoriale (dotata invece della forza di invadere la sfera altrui nell'adempimento di un potere/dovere)[14]. Ad orientare l'asticella, come è noto, è il cosiddetto "*best interest of the child*"[15]; un principio, tuttavia, vuoto di contenuti specifici e la cui applicazione varia a seconda di molteplici elementi contestuali, imponendo così un'attenta analisi del caso concreto ed una valutazione delle personali circostanze di vita del minore.

5.2. Lo *sharenting* in Italia

Una condotta lesiva della riservatezza dei figli minori ad opera dei genitori si configura nei comportamenti mediante i quali gli stessi genitori diffondono immagini o informazioni riguardanti i figli minori sui *social network* o altrove, senza il loro consenso oppure all'insaputa

---

13 Camardi, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 129. Ulteriori pericoli che minacciano l'autonomia ed il governo dell'identità digitale del minore possono configurarsi nella possibilità che il profilo di un utente, presente in rete, possa essere accostato a testi, messaggi o immagini raffiguranti una falsa realtà dei gusti, delle opinioni o dei convincimenti della persona interessata; che la rappresentazione distorta e fuorviante del patrimonio intellettuale e personale dell'interessato possa integrare una lesione del diritto all'onore ed alla reputazione; che l'immagine di un utente venga diffusa senza il consenso dell'interessato e che venga sottratta l'identità digitale altrui. Tale casistica è tratta da Pasquino, *Identità digitale della persona, diritto all'immagine e reputazione*, in Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 106. Tutti questi esempi mettono in luce la potenziale pericolosità di un luogo, quello della rete, che non conosce confini geografici.

14 In questi termini Camardi, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 117.

15 Sul punto v. Scalisi, *Il superiore interesse del minore. Ovvero il fatto come diritto*, in *Riv. dir. civ.*, 2018, p. 405; Lenti, *Note critiche in tema di interesse del minore*, in *Riv. dir. civ.*, 2016, p. 86; Senigaglia, *Status filiationis e dimensione relazionale dei rapporti di famiglia*, Napoli, 2013, p. 85, 145 ss.; Salanitro, *Azioni di stato e favor minoris tra interessi pubblici e privati*, in *Nuova giur. civ. comm.*, 2018, p. 552; Lucchini Guastalla, *Maternità surrogata e best interest of the child*, in *Nuova giur. civ. comm.*, 2017, p. 1722; Falletti, *Vita familiare e vita privata nel caso Paradiso e Campanelli di fronte alla Grande Camera della Corte di Strasburgo*, in *Fam. dir.*, 2017, p. 729.

o nonostante l'opposizione dell'altro genitore[16]. In area anglofona tale fenomeno prende il nome di *sharenting*.

Lo *sharenting* (neologismo nato dalla combinazione di *parenting* e *sharing*)[17] indica quella diffusa tendenza dei genitori a condividere sul web tutto ciò che riguarda i propri figli: dal momento della nascita alla prima poppata, dal primo sorriso alle prime parole, dai primi passi al primo compleanno e via dicendo.

Negli Stati Uniti tale tendenza è oggetto di studio anche nella letteratura giuridica[18]. Di recente sono apparsi i primi contributi con riguardo al potenziale conflitto tra diritto dei genitori a condividere *online* immagini dei figli (oltre che discutere e confrontarsi sulla vita e l'educazione di questi ultimi) e, di contro, l'interesse dei minori alla tutela della loro privacy e identità digitale[19].

Nella società moderna, infatti, accade sovente che siano proprio i genitori a lasciare nella rete la prima *digital footprint*[20] dei loro figli; una traccia digitale indelebile, capace di resistere all'azione del tempo e rimanere nel web anche quando i figli diventeranno adulti, col rischio

---

16 In questa prospettiva il dovere di vigilanza dei genitori consiste pure nella protezione del minore e dei suoi dati dalla ingerenza di terzi soggetti. V. CAMARDI, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 130.

17 Per un'efficace rappresentazione del fenomeno, si consiglia la visione del video apparso nel sito del *New York Times* il 7 agosto 2019 al seguente url: https://www.nytimes.com/2019/08/07/opinion/parents-social-media.html (consultato il 27.5.2020).

18 Cfr. SHMUELI and BLECHER-PRIGAT, *Privacy for Children*, in 42 *Colum. Hum. Rts. L. Rev*. 759 (2011); HARMON COOLEY, *Guarding Against a Radical Redefinition of Liability for Internet Misrepresentation: The United States v. Drew Prosecution and the Computer Fraud and Abuse Act*, in 14 *J. Internet L.*, Feb. 2011, 1, 23; MCPEAK, *Social Media Snooping and Its Ethical Bounds*, in 46 *Ariz. St. L.J.* 845, 848 (2014).

19 V., in particolare, STEINBERG, *Sharenting: Children's Privacy In The Age Of Social Media*, in *Emory Law Journal* 66 (2017), 839-1007, secondo la quale le corti americane, seppur riconoscano un interesse alla privacy del minore come meritevole di protezione, attribuiscono maggior rilevanza al diritto dei genitori al controllo sull'educazione dei propri figli e ai limiti della loro privacy: «Current laws protecting children's privacy reflect the strong tradition of parental rights to control and shape the lives of their children. Many laws aimed at protecting children's privacy are written from the paternalistic viewpoint that the parent has exclusive control over the disclosure of a child's personal information».

20 Cfr. STEINBERG, *Sharenting*, cit., p. 849 s. Le tracce o impronte della propria identità costruita tramite informazioni pubblicate online sono destinate a perdurare negli archivi digitali ed avere conseguenze anche nel lungo periodo. Sono dati "persistenti" che in futuro potranno sempre influire sull'immagine dell'interessato diventato ormai "adulto". Cfr. MCPEAK, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, in 48 *Wake Forest L. Rev.* 887, 911 (2013).

che questi, in futuro, possano considerarla lesiva della propria identità personale e ricevere nocumento da tale indesiderata esposizione di sé[21].

È utile dunque svolgere qualche considerazione con riguardo al "valore" della propria immagine, quale frammento dell'identità personale dell'individuo sin dai primi anni di vita, per cogliere appieno il motivo di tanta preoccupazione relativamente alla divulgazione delle immagini nella rete.

Va sottolineato che l'immagine è, da un lato, la rappresentazione con mezzi tecnici o grafici dell'aspetto fisico di una persona; dall'altro essa costituisce l'espressione pubblica più generale della sua personalità. È stato detto che l'immagine di ciascun individuo è lo specchio di una memoria personale e, contemporaneamente, di una memoria sociale[22]. Tutto ciò evidentemente risulta amplificato nella dimensione digitale e nelle interazioni sociali sul web, dove mondo reale e mondo virtuale si trasformano reciprocamente al punto che «quando ci con-

---

21 Cfr. Caggiano, *"Privacy" e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 2018, p. 3 ss., la quale osserva che, anche in ragione dell'esibizionismo dei genitori, il minore si trova ad essere spesso online, pure prima di nascere, "sotto forma di ecografia". Si dà origine, così, ad una identità digitale che precede quella anagrafica e che non risponde alla proiezione del sé voluta dall'individuo una volta maturo. Sicché il minore ha bisogno di essere particolarmente protetto da un'esposizione o sovraesposizione di dati per i possibili rischi sullo sviluppo della sua personalità, per l'esteso tracciamento della persona (profilazione) nel corso dell'intera vita, per i furti di dati o di identità, che se relativi al minore possono avere ripercussioni più gravi. Per ulteriori approfondimenti sul tema del consenso del minore v. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pisa, 2020; A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019.

22 Eco, *Ero troppo preoccupato a fotografare e non ho guardato*, riflessioni sulla fotografia rese in occasione del XXXVIII Congresso dell'Associazione Italiana di Studi Semiotici, dal titolo «La fotografia: oggetto teorico e pratica sociale», tenutosi a Roma dall'8 al 10 ottobre 2010, reperibile in www.doppiozero.com/materiali/fuori-busta/umberto-eco-e-paolo-fabbri-due-riflessioni-sulla-fotografia (cit. da S. Peron, *Sul divieto di diffusione sui social network delle fotografie e di altri dati personali dei figli*, in *Resp. civ. prev*., 2018, p. 589).

frontiamo con la nostra immagine nello specchio della macchina arriviamo a vederci in modo diverso»[23], poiché «il mondo immateriale cattura la nostra vita e la ritraduce attraverso nuove convenzioni, artificiali e tecnologiche»[24].

Chiarito il ruolo fondamentale della propria immagine, può essere affrontato il profilo giuridico della questione, sul presupposto che la pubblicazione di una fotografia *online* si inquadra nel trattamento di dati personali e sensibili, e costituisce interferenza nella vita privata del minore, anche se si tratta dei propri figli[25].

Va detto che, di regola, i genitori devono rispettare la riservatezza della vita personale del minore a partire dall'età nella quale lo stesso comincia a manifestarla in relazione alla sua maturità[26]. Nel caso di minore munito della capacità di discernimento (è il caso del "grande minore"), questi potrà direttamente reagire contro i genitori, quantomeno manifestando una qualche forma di opposizione. Mentre

---

23 TURKLE, *La vita sullo schermo. Nuove identità e relazioni sociali nell'epoca di Internet*, Milano, 1997, p. 1.

24 RICCIARDI, *Lo schermo e lo specchio*, introduzione a TURKLE, *La vita sullo schermo*, cit., p. XIII.

25 Il quadro normativo, con riferimento particolare al diritto all'immagine, si articola su più livelli. Esso trae anzitutto fondamento nell'art. 2 Cost. ed è altresì ricavabile dall'art. 10 c.c. e dagli artt. 96 e 97 della legge sul diritto d'autore (l. 22 aprile 1941, n. 633). A queste norme deve poi aggiungersi il combinato disposto degli artt. 4,7,8 e 145 del d. lgs. 30-6-2003 n. 196 (riguardanti la tutela della riservatezza dei dati personali) nonché degli artt. 1 e 16, co. 1, della Convenzione di New York del 20.11.1989 ratificata dall'Italia con legge 27.5.1991 n. 176 (su cui v. DOGLIOTTI, *I diritti del minore e la convenzione dell'ONU*, in *Dir. fam. pers.*, 1992, p. 301 ss.). A livello europeo, una specifica normativa di tutela dei minori in relazione ai servizi della società dell'informazione è contenuta ora nell'art. 8 del Regolamento (UE) 679/2016 del 27 aprile 2016, laddove l'immagine fotografica dei figli costituisce dato personale e la sua diffusione integra un'interferenza nella vita privata. Il GDPR prevede disposizioni specifiche dedicate al minore. Il considerando n. 38, in particolare, dichiara che «I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali». Sulla specifica disciplina sul trattamento dei dati personali dei minori d'età dettata dal Regolamento UE 2016/679 v. C. PERLINGIERI, *La tutela dei minori di età nei "social networks"*, in *Rass. dir. civ.*, 2016, p. 1324 ss.; A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019 e ID., *L'accesso dei minori d'età ai servizi della c.d. società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul codice per la protezione dei dati personali*, in *Contr. impr.*, 2019, p. 614 ss.; MONTARULI, *La protezione dei dati personali e il minore*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO, RICCIUTO, Torino, 2019, p. 280 ss.

26 CAMARDI, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 134.

quando il fenomeno riguarda i cosiddetti *petits enfants*, per i quali non può che sussistere una tutela "dinamica" della persona affidata al controllo di autorità garanti[27], il potere del genitore di incidere sulla riservatezza del minore nella rete conosce ben pochi argini sotto il profilo giuridico, dacché molto dipende dall'educazione, dalla cultura e dalla sensibilità degli stessi genitori al rispetto della sfera privata del minore.

È ovvio che il rafforzamento del diritto del minore alla costruzione della propria identità digitale non può certo tradursi in un diritto esclusivo di autorappresentazione[28], ma i principi sin qui delineati dovrebbero essere sufficienti ad impedire l'abuso del potere dei genitori, consistente nel rendere pubblica la sfera privata del minore (e per conseguenza incidere negativamente sulla costruzione dell'identità digitale del figlio) senza tener conto del suo interesse[29].

---

27 V., da ultimo, M. Astone, *La protezione dei dati personali e il (possibile) ruolo dell'autorità garante per le comunicazioni*, in *Nuovo dir. civ.*, 2019, 3, p. 247 ss.

28 V. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 109: «Vi sono molti, e ben noti, motivi per rispondere dicendo che nessuno può avere il monopolio della propria presentazione "in pubblico", sì che sarebbero illegittime tutte le rappresentazioni diverse da quelle in cui l'interessato si riconosce pienamente». Con riguardo ai dati personali del minore sussiste in ogni caso un principio che riconosce il superiore interesse del minore da bilanciarsi con le esigenze di protezione, v. Montaruli, *La protezione dei dati personali e il minore*, cit., p. 280 ss.

29 Cfr. Forciniti, *Tutela cautelare e d'urgenza e diffusione di immagini di soggetti minori sui social networks*, in *Fam. dir.*, 2019, p. 591 ss., la quale giustamente osserva: «L'abitudine, sempre più diffusa, e talvolta addirittura compulsiva, di fotografare i momenti di vita dei bambini e di "immortalarli" postandoli immediatamente sui social, non consente loro di vivere momenti intensamente, ma anzi li induce a proiettarsi precocemente in un mondo non solo virtuale ma anche insidioso. È indubbio che, dalla disamina delle più importanti carte nazionali e sovranazionali, l'interesse del minore debba essere considerato sempre preminente. Dare l'esempio ai propri figli di una pubblicazione non controllata di foto personali sui social può predisporli altresì a subire le conseguenze di un uso distorto degli stessi». Cfr. anche Senigaglia, *Le misure di protezione dell'interesse del soggetto minore di età tra autonomia ed eteronomia*, cit., p. 49: «In sostanza, i genitori pur non essendo liberi rispetto al se (se educare, istruire, mantenere, assistere moralmente, ecc.), lo sono con riguardo al come, la cui definizione è demandata alla (ampia) discrezionalità (e non al mero arbitrio) degli stessi, sussistendo il (solo) limite di non arrecare pregiudizio all'interesse superiore del figlio. Un limite che con riguardo al "minore piccolo", la cui personalità è in formazione – evidentemente educata dall'identità valoriale dei genitori, fermo restando il modello imprescindibile dei "valori di libertà emergenti dalla Costituzione" –, è rappresentato dalla dignità umana (art. 1, Carta dei diritti fondamentali UE); con riferimento, invece, al "minore grande", la cui personalità si è già definita, il limite è rappresentato dalla sua identità, da tutto ciò che lo rende unico, distinguibile da chiunque altro».

Quale autonomia e quale rilevanza allora assegnare ai figli e alle proprie risorse identitarie rispetto al potere di ingerenza dei genitori nella vita privata del minore? Il dibattito dottrinale in Italia si può riassumere in due opposte visioni: un'impostazione più tradizionalista e rigida della "potestà" genitoriale (com'era definita prima dell'intervento legislativo del 2013)[30], da un lato; e l'opinione di chi, dall'altro, attribuisce all'identità del figlio un «criterio-guida imprescindibile dell'azione educativa e delle decisioni dei genitori», e alla capacità di discernimento «lo strumento indispensabile per garantire il rispetto di una personalità in divenire»[31].

L'analisi della giurisprudenza italiana, e in particolare delle pronunce di merito, dimostra quanto lo strumento del diritto sia inadeguato o comunque insufficiente ad affrontare un problema di tipo culturale che concerne anche l'educazione all'uso della rete. Alla base delle motivazioni dei provvedimenti di cui si dirà appresso, vi è infatti la preoccupante constatazione secondo cui «la diffusione incontrollata di fotografie e altri dati personali dei figli minori risponda più a un desiderio di riconoscimento e gratificazione del genitore, perseguiti attraverso il meccanismo della condivisione sui *social network* al fine di stimolare *like* e commenti da parte degli altri utenti, senza considerare le conseguenze che potrebbero derivare ai figli da tale condotta e, dunque, senza ponderare adeguatamente l'interesse oggettivo dei figli a non subire interferenza arbitrarie nella loro vita privata (quand'anche esse provengano da uno o da entrambi i genitori)»[32].

Una breve ricognizione di alcune pronunce delle corti italiane potrà risultare utile a definire le coordinate del problema.

5.3. Esistenza digitale del minore e rimedi civilistici

Nella giurisprudenza delle corti di merito italiane si trova ormai un'ampia casistica con riferimento al dovere di vigilanza e di controllo dei genitori sulla protezione del minore e dei suoi dati nella rete. È emblematica, ad esempio, la vicenda di un minore sedicenne (sottopo-

30 Cfr. RUSCELLO, *Autonomia dei genitori, responsabilità genitoriale e intervento "pubblico"*, in *Nuova giur. civ. comm.*, 2015, p. 717.

31 GIARDINA, *"Morte" della potestà e "capacità" del figlio*, in *Riv. dir. civ.*, 2016, p. 1620.

32 Così PERON, *Sul divieto di diffusione sui social network delle fotografie e di altri dati personali dei figli*, cit., p. 589 ss.

sto alla cura di un tutore a seguito della sospensione della responsabilità genitoriale di entrambi i genitori), il quale aveva ripetutamente segnalato ai servizi sociali, incaricati ad attuare il percorso di sostegno, il forte senso di disagio causato dai comportamenti della madre, responsabile di aver divulgato attraverso i social network *post* e immagini relativi al figlio, alla loro complessa storia familiare ed alle controversie giudiziarie da loro attraversate[33]. Il Tribunale aveva ritenuto che la volontà espressa dal ragazzo di proseguire gli studi all'estero fosse fondata «sulla necessità di allontanarsi dall'attuale contesto sociale, nel quale tutti i compagni» erano a «conoscenza delle sue vicende personali, rese note dalla madre con uso costante e sistematico dei *social network*». Ad avviso del Tribunale, tale «massiccia presenza mediatica della vicenda del minore» giustificava il «turbamento dello stesso e la resistenza a proseguire gli studi in un contesto nel quale particolari della propria vita personale, erano ampiamente noti». Sicché, a tutela del minore, il Tribunale disponeva l'immediata rimozione di immagini, informazioni, dati relativi al figlio inseriti su *social network* dai genitori, inibendo loro, pena il pagamento di una somma di denaro *ex* art. 614-*bis* c.p.c., la diffusione nella rete delle suddette immagini, informazioni o dati relativi al minore.

In altri casi registrati dalle corti italiane, benché il minore non si dichiari contrario alla pubblicazione di proprie immagini in rete, risulta mancare il consenso di entrambi i genitori alla divulgazione di tali immagini. È il caso riguardante una madre che aveva acconsentito alla pubblicazione su *Facebook* di fotografie della figlia sedicenne in pose allusive e provocanti, nonostante l'opposizione del padre[34]. Analogamente, in altra vicenda affrontata dal Tribunale di Mantova[35], il giudice aveva ordinato ad una madre, separata dal marito, presso la quale vivevano i due figli rispettivamente di tre anni e mezzo e di un anno e mezzo, di non inserire le foto dei minori sui *social network* e di

33 Trib. Roma (ord.), 23 dicembre 2017, in *Resp. civ. prev.*, 2018, p. 589, con nota di Peron, *Sul divieto di diffusione sui social network delle fotografie e di altri dati personali dei figli*, cit.

34 Trib. Prato, 28 ottobre 2016, reperibile nel database *DeJure*.

35 Trib. Mantova, 19 settembre 2017, con nota di Nitti, *La pubblicazione di foto di minori sui social network tra tutela della riservatezza e individuazione dei confini della responsabilità genitoriale*, in *Fam. dir.*, 2018, p. 380.

provvedere alla rimozione di tutte le immagini sino ad allora pubblicate senza il consenso del padre[36].

Questa breve ricognizione delle vicende più comuni nell'ambito del dovere di controllo dei genitori sui dati del minore nella rete mostra non solo come il problema esista, ma anche che ci sia sempre più esigenza di governarlo. Non è infrequente, difatti, che nell'ambito del ricorso congiunto per lo scioglimento del matrimonio i genitori si impegnino formalmente a non pubblicare o divulgare foto, immagini, video o altro materiale concernente il minore all'interno di una pagina *web*, un *blog*, un *social network* né come immagini di profilo su applicazioni come *WhatsApp* o e simili, senza il consenso congiunto di entrambi i genitori[37].

Gli strumenti di tutela in caso di violazione delle regole suddette, diretti a garantire una effettiva protezione del diritto di riservatezza del minore, possono essere incisivi, come si dirà ora, ma il vero problema è che quando un'immagine (o qualsiasi altra informazione o dato personale) viene immessa nella rete[38], la portata lesiva della sua divulgazione risulta particolarmente intensa poiché la perpetuità della rete determina inevitabilmente l'immanenza dell'informazione.

Ad ogni modo, al fine di proteggere la riservatezza del minore, il giudice può apprestare anzitutto una tutela inibitoria, come visto nella casistica giurisprudenziale suddetta, rivolgendo ai genitori l'ordine di

---

36 Il giudice mantovano ha ritenuto che, nel caso di specie, l'inserimento di foto dei minori sui *social network* costituisse un «comportamento potenzialmente pregiudizievole» per essi e che il pregiudizio per i minori fosse «insito nella diffusione della loro immagine sui *social network*»: «in quanto ciò determina la diffusione delle immagini fra un numero indeterminato di persone, conosciute e non, le quali possono essere malintenzionate e avvicinarsi ai bambini dopo averli visti più volte in foto *on-line*, non potendo inoltre andare sottaciuto l'ulteriore pericolo costituito dalla condotta di soggetti che "taggano" le foto *on-line* dei minori e, con procedimenti di fotomontaggio, ne traggono materiale pedopornografico da far circolare fra gli interessati, come ripetutamente evidenziato dagli organi di polizia».

37 V., *inter alia*, Trib. Ferrara, 5 giugno 2017; Trib. Trieste, 18 luglio 2017; Trib. Velletri, 27 aprile 2017; Trib. Brescia, 2 settembre 2017, tutte reperibili nel database *DeJure*.

38 Cfr. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Nuove leg. civ. comm.*, 2017, p. 1023 ss., il quale osserva: «[…] nel trattamento dei dati operato in internet, focalizzare l'attenzione sul comportamento del gestore del sito sorgente risulta evidentemente riduttivo. L'informazione collocata nel cyberspazio si presta ad essere "raccolta" da chiunque, indicizzata e intrecciata, per il tramite di algoritmi, ad altre informazioni, facendo emergere un'identità virtuale dell'individuo oggettivamente diversa, perché artificiosa, da quella reale».

immediata cessazione della diffusione sui *social network* di immagini, notizie e dettagli relativi alla vita privata del minore, nonché la rimozione di quanto già pubblicato in passato. È inoltre nel potere del giudice diffidare soggetti terzi dal diffondere tali informazioni, nonché consentire al genitore o al tutore di richiedere anche a terzi la rimozione di tali contenuti e ai gestori dei motori di ricerca di deindicizzare informazioni relative al minore[39].

Ulteriore strumento di grande rilevanza, poiché utile al fine di assicurare l'osservanza degli obblighi di fare, è rappresentato dall'istituto dell'*astreinte* di cui all'art. 614 *bis* del codice di procedura civile. Si tratta di una misura funzionale a favorire la conformazione a diritti della condotta della parte contro cui è disposta, nonché ad evitare la produzione di ulteriori danni, riducendo quindi l'entità del pregiudizio. In particolare, il giudice può stabilire che, in caso di mancata ottemperanza del genitore all'obbligo di interrompere la diffusione di immagini, video, informazioni relative al minore nei *social network*, ovvero di mancata ottemperanza all'obbligo di rimuovere tali dati, il genitore inadempiente dovrà corrispondere una somma di denaro al ricorrente (o al suo tutore) per la violazione posta in essere[40].

In proposito si è fatto notare che il contenuto generale della previsione di cui all'art. 614 *bis* c.p.c. non limita la concessione del rimedio dell'*astreinte* alle pronunce giudiziali di natura ordinaria rese al termine di controversia, essendo consentita la condanna a misure di coercizione indiretta, anche in sede cautelare[41], tutte le volte in cui la soddisfazione dell'interesse del ricorrente non possa prescindere dalla volontà e fattiva collaborazione dell'obbligato[42].

---

39 Il gestore del motore di ricerca deve essere considerato a tutti gli effetti di legge quale titolare del trattamento. Conseguentemente le azioni volte a chiedere la rimozione, cancellazione o deindicizzazione di un contenuto presente su internet possono essere rivolte sia a chi pubblica le informazioni sia ai gestori dei motori di ricerca.

40 V. Trib. Roma, 23 dicembre 2017, cit.

41 V. Trib. Rieti, 7 marzo 2019, in *Fam. dir*., 2019, p. 591 ss., con nota di commento di Forciniti, *Tutela cautelare d'urgenza e diffusione di immagini di soggetti minori sui social networks*, cit.; v. anche Trib. Mantova, 19 settembre 2017, cit.

42 V. Trib. Bari, 16 maggio 2016, in *Giur. it*., 2017, 839, con nota di Montanari, *Astreinte in sede cautelare ed azione di manutenzione del contratto*.

5.4. La tutela della riservatezza del minore nel contesto delle relazioni familiari

Un limite ulteriore che i genitori incontrano nel garantire il diritto alla riservatezza dei figli minori è rappresentato dal divieto di intromissione nella vita privata di questi ultimi. Ci si chiede, cioè, quando e fino a che punto i genitori possano intrudere nella sfera privata dei loro figli minorenni in un contesto sociale dominato dalle comunicazioni elettroniche e dai *social network*.

I comportamenti volti a "frugare" nella vita personale dei figli vanno dalla lettura non autorizzata della corrispondenza, degli appunti personali e di qualsiasi materiale che il minore ritenga riservato, fino alle cosiddette intrusioni informatiche, realizzate con qualunque mezzo, nei *device* usati dal minore per comunicare con terzi o per navigare. A ciò si aggiungano i sistemi di controllo a distanza mediante *webcam* o programmi utilizzati dai genitori per sorvegliare i figli, in casa o fuori.

Non v'è dubbio che il dovere di vigilanza dei genitori nei confronti dei figli includa anche un potere di sorveglianza e di ingerenza nella vita privata, inteso ad evitare la produzione di danni in capo ai figli medesimi o nei confronti di terzi, alla stregua degli artt. 2047 e 2018 del codice civile[43]. Tuttavia è altrettanto certo che tale ingerenza incontri un limite nel diritto di riservatezza del minore come sin qui descritto. È poi compito dell'interprete «elaborare un appropriato criterio di bilanciamento e tracciare il confine oltre il quale l'ingerenza dei genitori deve arrestarsi per non diventare "illecita"»[44], ma in via di principio si potrebbe affermare che il travalicamento da parte del genitore di quella sottile linea di confine che separa l'ingerenza legittima dall'intrusione ingiustificata (che nella realtà pratica rimane comunque difficile da tracciare nettamente) appare giustificato ogni qual volta l'intervento di questi risulti *funzionale* alla protezione del minore ovvero ad evitare la produzione di pregiudizi in capo a terzi.

A ciò si aggiunga che i riferimenti normativi applicabili alla casistica in esame sono piuttosto vaghi, nel senso che non offrono indicazioni concrete e definitive in ordine ai limiti di ingerenza dei genitori. Si pensi all'art. 315 *bis* del codice civile, secondo cui il rispetto delle

---

43 Camardi, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 130.

44 *Ibidem*.

capacità, delle inclinazioni naturali e delle aspirazioni del minore dovrebbe costituire la bussola per orientare i genitori nell'educazione dei propri figli; specialmente in quella fascia d'età che prende avvio attorno ai 12 anni (ma anche di età inferiore se il figlio fosse capace di discernimento) in cui il figlio minore «ha diritto di essere ascoltato in tutte le questioni e le procedure che lo riguardano».

Basti pensare all'esempio classico del genitore che accede alla pagina *Facebook* del figlio per verificare presunte condotte illecite del minore e in tale occasione venga a conoscenza di altri dati, concernenti attività altre o esperienze del minore che nulla hanno a che fare con le ragioni che hanno motivato l'intromissione del genitore[45]. La questione in dottrina è stata affrontata sotto un duplice profilo: con riguardo all'*an* del potere/dovere del genitore, la sua ingerenza si potrebbe giustificare allorquando il criterio del *best interest* richieda di violare la privacy del figlio[46]; mentre con riferimento al *quantum* e/o al *quomodo* il genitore possa spingersi nella conoscenza o nella ricerca dei dati riguardanti la vita personale del figlio, si è osservato che le norme civilistiche sulle relazioni familiari non danno alcuna specifica indicazione[47], ma il bilanciamento dell'interesse del minore con quello del genitore dovrebbe rispettare quei principi dettati dal Regolamento UE in materia di privacy[48] in virtù dei quali «i genitori dovrebbero prendere conoscenza o "prelevare" soltanto quei dati necessari alla soluzione del problema esistenziale del minore in ragione del quale l'accesso è stato motivato»[49].

5.5. Conclusioni

L'epoca di internet ha segnato un radicale cambiamento nella costruzione dell'identità personale[50], che ora conosce anche una dimensione tecnologica e virtuale. Le persone sono occupate a convertire le

---

45 È l'esempio proposto da Camardi, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 132.

46 Camardi, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 133.

47 Camardi, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 135.

48 Si allude in particolare ai principi della necessità e finalità, della pertinenza, della proporzione, della limitazione o non eccedenza dei dati.

49 Camardi, *Minore e privacy nel contesto delle relazioni familiari*, cit., p. 136.

50 Secondo un'ormai risalente definizione della Corte di Cassazione, «l'identità rappresenta una formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue specifiche caratteristiche e manifestazioni»: così Cass. 22.6.1985, n. 3769, in *Foro it*., 1985, I, p. 2211 ss. con nota di R. Pardolesi.

loro esperienze in dati che fluiscono liberamente nella rete e sui *social network*[51]; informazioni che, nel loro insieme, costituiscono un patrimonio digitale[52], destinato ad alimentarsi ogni volta che il suo titolare affidi al web dati che lo riguardano, attraverso, ad esempio, l'utilizzo di profili dei social, *e-mail*, *tweet*, file di testo, immagini, *chat*, *account*, *cloud computing* e via dicendo[53].

L'esistenza di tale patrimonio informativo pone in luce una nuova dimensione della persona – un "oltremondo" – che si realizza nella cosiddetta mediasfera, e cioè nel virtuale contesto dei *social media*[54]. Potrebbe sembrare un paradosso discutere di riservatezza su tali premesse, ma da uno sguardo più attento appare subito chiaro che il

---

51 M. BIANCA, *Il minore e i nuovi media*, cit., p. 150, osserva come «i nuovi media rispetto al soggetto minore d'età, proprio perché utilizzati da soggetti la cui personalità è ancora in formazione, sono diventati strumenti di costruzione della stessa esistenza e della identità dei giovani, e sono i fattori cui è principalmente addebitabile la formazione di una *esistenza digitale* che talvolta assorbe o prevarica la loro esistenza fisica non virtuale. La dimensione assorbente della *esistenza digitale* dei soggetti minori di età mostra lo scarto e la distanza rispetto all'uso dei nuovi media da parte dei soggetti adulti, denunciando la maggiore pericolosità e le insidie della loro infosfera digitale» (corsivo dell'A.).

52 Tale patrimonio "digitale" è destinato altresì a divenire oggetto di successione ereditaria. Per un approfondimento sul tema della c.d. "eredità digitale", v. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inform*., 2018, p. 92; MARINO, *La "successione digitale"*, in *Osserv. dir. comm*., 2018, p. 167 ss.; RESTA, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in MANTELERO e POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, p. 403 ss.; F.P. PATTI e BARTOLINI, *Digital Inheritance and* Post Mortem *Data Protection: The Italian Reform*, in *European Review of Private Law*, 5-2019, p. 1181 ss.; CINQUE, *La successione nel «patrimonio digitale»: prime considerazioni*, *Nuova giur. civ. comm*., 2012, p. 645 ss.; MAGNANI, *L'eredità digitale*, in *Riv. not*., 2014, p. 147 ss.; DEPLANO, *La successione a causa di morte nel patrimonio digitale*, in C. PERLINGIERI e RUGGIERI (a cura di), *Internet e diritto civile*, Napoli, 2015, p. 427 ss.; I. SASSO, *La tutela dei dati personali "digitali" dopo la morte dell'interessato alla luce del Reg. UE 2016/679*, in *Dir. succ. fam*., 2019, p. 181 ss.; VIZZONI, *Mandato* post mortem *ed eredità digitale*, in *RivistaFamilia.it*, 2019.

53 In area anglofona si è giunti a coniare un nuovo termine per indicare un fenomeno che taluni non esitano a definire una nuova religione: il dataismo (in inglese, *dataism*). Fenomeno che poggia sull'idea secondo cui le esperienze umane non avrebbero un valore intrinseco: il valore, cioè, non consisterebbe nel vivere esperienze, ma piuttosto nel trasformarle in dati e nel condividerle. Così HARARI, *Homo deus*, Firenze-Milano, 2018, p. 473.

54 Con riferimento ai concetti di corpo fisico e corpo "elettronico", quest'ultimo inteso come «l'insieme delle informazioni che costruiscono la nostra identità», v. RODOTÀ, *Diritto di avere diritti*, Roma-Bari, 2012, p. 315; RESTA, *Identità personale e "identità digitale"*, in ID., *Dignità, persone, mercati*, Torino, 2014, p. 335.

bisogno di tutela della propria intimità accresce proprio lì dove aumentano i rischi e i pericoli di una sua irrimediabile frustrazione.

È in tale cornice che emerge con solare evidenza non soltanto il ruolo fondamentale della protezione dei dati personali del minore, oggi intesa nella più moderna accezione di «forma di controllo sul modo in cui l'identità individuale può essere costruita»[55], ma anche del diritto alla riservatezza del minore.

Per un verso, tale diritto è stato qui inteso in maniera esemplificativa «quale diritto a che i genitori rispettino l'intimità della vita del minore sui *social networks*»[56]; per altro verso, si tratta di un diritto del minore alla costruzione della propria identità digitale che, in virtù del principio del *best interest*, pone un limite al potere dei genitori di rendere pubblica la sfera privata del minore senza tener conto del suo interesse.

Tuttavia, su tale controllo dei dati del minore, specialmente quando si tratta di *petits enfants*, appare decisivo il ruolo dei genitori nell'ambito dell'esercizio della loro responsabilità genitoriale. Parte della dottrina ritiene infatti che il concetto di educazione debba oggi ricomprendere anche un'educazione ad un buon uso dei *social network* per comporre in un giusto equilibrio opportunità e rischi[57]. E che tale problematica richieda altresì un cambiamento di paradigma relativamente ai soggetti coinvolti nella cura e nell'educazione del minore, rafforzando per tale via il ruolo della scuola e di altre istituzioni[58].

---

55 Marini, *La giuridificazione della persona*, cit., p. 364. Sulla definizione di *privacy* v. anche Rodotà, *Tecnologie e diritti*, cit., p. 80, dove afferma: «il riferimento alla *privacy* esprime l'indicazione di un valore tendenziale più che una vera e propria definizione legislativa. E questo è confermato dal fatto che tutta la legislazione sulla protezione dei dati non contiene al suo interno formali definizioni di *privacy*».

56 M. Bianca, *Il minore e i nuovi media*, cit., p. 163.

57 V. al riguardo Thiene, *Ragazzi perduti online: illeciti dei minori e responsabilità dei genitori*, in *Nuova giur. civ. comm.*, 2018, p. 1621: «Va da sé che nel percorso di istruzione circa l'utilizzo dei social media è fondamentale il ruolo educativo dei genitori, che non possono farsi trovare impreparati o peggio distratti di fronte agli strumenti informatici o di nuova generazione, compresi i siti di socializzazione e i servizi di messaggistica istantanea. Per favorire un ambiente online costruttivo e arricchente è necessario incoraggiare i fanciulli a sviluppare un pensiero critico e consapevole sulle opportunità ma anche sulle insidie del web».

58 V. M. Bianca, *Il minore e i nuovi media*, cit., p. 168.

6. Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR

Andrea Maria Garofalo

6.1. Introduzione

Di fronte alla disciplina del consenso al trattamento, che come ben noto costituisce una delle basi giuridiche ammesse dal GDPR per il trattamento dei dati personali, la sensazione che mi pare emerga è – usando un eufemismo – di insoddisfazione.

Tutto il GDPR, infatti, è percorso da una considerazione di fondo: gli individui, i singoli, le persone fisiche non sono idonee a tutelare i loro interessi in materia di protezione dei dati. Lo dimostra l'attenzione verso i controlli interni ed esterni dell'attività di trattamento[1]; lo attesta il principio di responsabilizzazione, che investe il titolare del trattamento dell'onere di valutare e gestire il rischio dello stesso trattamento[2].

Se questo è vero, suona a me quanto meno strano – sempre in senso eufemistico – che questi stessi individui, prima reputati inidonei a tutelarsi, siano abilitati a disporre dei loro stessi dati, addirittura creando una base per il loro trattamento e così rendendo quest'ultimo lecito.

Se lo si ammette, si apre uno scenario di ricerca assai interessante: v'è prima da chiedersi perché, apparentemente in modo contraddittorio, le discipline di protezione dei dati che si sono susseguite nel tempo abbiano ammesso il consenso e quali problemi emergano da questo riconoscimento legislativo[3]; v'è poi da domandarsi come il consenso

---

1 Artt. 24 ss.

2 Art. 24.

3 V. § 2.

sia attualmente regolato (a livello legislativo e interpretativo)[4]; ancora, v'è da verificare se anche l'attuale disciplina di questo atto di volontà presenti delle criticità[5]; infine, deve indagarsi se la ricostruzione dogmatica dell'atto di consenso o una revisione interpretativa o legislativa della sua disciplina consenta di ripianare – almeno in parte – quelle storture cui la stessa esistenza di una simile base legale dà vita e che ancora oggi risultino non superate[6].

A quest'indagine, da svolgere per lo più sul piano eurounitario, sono dedicate le pagine che seguono.

6.2. Funzioni e disfunzioni, da un punto di vista generale, del consenso

Come noto, il trattamento dei dati personali, allorché si rientri entro l'ambito di applicazione del GDPR (in linea di massima: trattamento automatizzato), può avvenire solo se è presente una "base" che lo rende lecito (art. 5, par. 1, GDPR). Tra le basi per il trattamento, accanto all'esecuzione di un contratto, all'adempimento di un obbligo legale o all'esecuzione di un compito in senso lato pubblico, alla salvaguardia di interessi vitali di una persona e al legittimo interesse, troviamo il consenso dell'interessato dal trattamento (art. 6, par. 1, GDPR). E anche con riferimento ai dati "sensibili" (o, meglio, ai dati rientranti in "categorie particolari") possiamo trovare, accanto a un divieto generale di trattamento e alla sua disapplicazione allorché sussistano talune specifiche basi (tra cui manca però l'esecuzione di un contratto e il legittimo interesse), il consenso dell'interessato quale condizione di liceità del corrispondente trattamento (art. 9, par. 2, GDPR).

Emerge con nitidezza, già da questi brevi cenni, la particolarità del consenso: mentre in ogni altro caso il bilanciamento tra gli interessi del titolare del trattamento e i rischi per le libertà, i diritti e gli interessi del *data subject* è stato già compiuto dal legislatore europeo (fermo restando che esso può e deve, in forme e modi di volta in volta diversi,

4 V. § 3.

5 V. § 4.

6 V. §§ 5 e 6.

venire specificato in concreto), nell'ipotesi del consenso il bilanciamento è posto in essere, a suo piacimento, dall'interessato[7]. In tal modo, dunque, viene inserita nel GDPR una condizione di liceità del trattamento che, anziché essere *content-based*, risulta *consent-based* e che, per l'effetto, permette di superare i margini del sistema del Regolamento ogni qual volta essi appaiano in concreto eccessivamente ristretti[8].

Se questa è, banalmente, la ragione fondante del consenso, altrettanto semplice è accorgersi delle disfunzioni che il consenso stesso reca in sé e, una volta ammesso, introduce nell'ordinamento.

Studi recenti hanno, infatti, confermato quanto è sotto gli occhi di tutti noi: la materia della protezione dei dati è dominata da un fortissimo disallineamento tra la realtà delle cose e l'esperienza che ogni utente ne fa giornalmente.

Senza scendere nei dettagli, basterà rilevare che, solitamente, le informative in materia di trattamento dei dati personali, così come le richieste di consenso, sono troppo lunghe per immaginare che il titolare dei dati le legga e le analizzi prima di scegliere se dare il suo consenso. Anche se poi ciò avvenisse, l'interessato difficilmente le capirebbe: o, meglio, comprenderebbe i rischi che il trattamento porta con sé. Difatti, gli utenti di regola sottovalutano i rischi che l'utilizzo dei loro dati comporta (rischi legati non solo e non tanto alla compressione della

---

7 Si consenta, su questi temi, il rinvio a A.M. GAROFALO, *Protection and Free Movement of Personal Data in EU Law*, in M. SCHMIDT-KESSEL, *European Economic Constitution. German-Italian Dialogue for a Solidarity-oriented Common Market*, Jena, 2020, in corso di pubblicazione.

8 Del resto, se è vero che il consenso non è la regola rispetto ad altre eccezioni (ossia, rispetto alle altre basi), è vero anche che esso formalmente non è altro che "una condizione tra le altre possibili" (in tal senso v. F. CAGGIA, *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Riv. dir. comm.*, 2019, I, p. 406; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in AA. VV., *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017, p. 138 ss.). Da un punto di vista sostanziale, tuttavia, il consenso è una condizione di liceità assai diversa dalle altre e, soprattutto, giocoforza residuale, benché il suo uso attuale nella prassi possa creare delle illusioni ottiche e farla sembrare prioritaria: e, infatti, va ribadito che del consenso vi è necessità solo quando mancano altre basi (peraltro, come oltre si dirà, tale priorità logica dovrebbe tradursi anche in una preminenza deontologica, nel senso che, ove vi è spazio per altre basi, il titolare del trattamento non dovrebbe ricorrere al consenso o comunque dovrebbe essere disincentivato a fare ricorso ad esso).

privacy, quanto alla limitazione di altri diritti, quale quello all'autodeterminazione commerciale); né hanno contezza del valore che i loro dati personali rivestono per le controparti (sicché sono portati ad accettarne la dismissione anche senza riceverne una vera e propria utilità in cambio). Per di più, spesso gli utenti suppongono che i loro dati sono già in circolazione che, quindi, non potendo più esercitare un controllo sugli stessi, risulta indifferente ammettere nuovi e ulteriori trattamenti.

Questi fenomeni possono venire raccolti sotto l'ampia dicitura di *privacy paradox*[9]: tanto più importante è la protezione dei dati in una società che evolve, tanto meno è, da un lato, strutturalmente attuabile tramite condotte dei singoli e, da un altro lato, avvertita e percepita come tale da questi stessi singoli. Potremmo, convenzionalmente, definire il primo ambito del "paradosso dell'attenzione" e il secondo del "paradosso della valutazione": il primo dipende dall'asimmetria del tempo tra chi tratta i dati e chi li fornisce, tale per cui al secondo non può essere richiesta la lettura analitica delle condizioni del trattamento; il secondo, invece, dalla mancanza di una cultura diffusa in tema di dati, sicché il loro trattamento non è – in breve – sentito come minaccia a certi valori.

Tali paradossi, ovviamente, rendono il consenso al trattamento dei dati una base potenzialmente distruttiva rispetto al sistema: da un lato, è ovvio che, se non perimetrato entro confini rigidissimi, il consenso fornito dall'interessato potrebbe fisiologicamente non corrispondere a una scelta reale o comunque a una scelta realmente ponderata; da un altro lato, è altrettanto evidente che, in tali situazioni, chiedere e ottenere il consenso al trattamento può costituire una facile scappatoia rispetto al sistema di liceità del trattamento.

Quest'ultima considerazione è tanto più vero, quanto più spesso avviene che i singoli forniscano il loro consenso (anziché rifiutarlo). Ma, a ben vedere, essa resta vera anche se statisticamente assenso o

---

[9] Cfr. S.B. Barnes, *A Privacy Paradox: Social Networking in the United States*, in *First Monday*, 2006. Alcune specificazioni di questo paradosso sono fornite da: S. Trepte. - D. Teutsch - P.K. Masur - C. Eicher - M. Fischer - A. Hennhöfer - F. Lind, *Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)*, in S. Gutwirth, R. Leenes e P. de Hert (a cura di), *Reforming European Data Protection Law*, Dordrecht-Heidelberg-New York, 2015, p. 333 ss.; D.J. Solove, *Introduction: Privacy Self-Management and The Consent Dilemma*, in *Harvard Law Review*, 2013, p. 1881 ss.; Id., *"I've Got Nothing to Hide" and Other Misunderstandigs of Privacy*, in *San Diego Law Review*, 2007, p. 745.

diniego si equivalgono e perfino se il rifiuto supera statisticamente il consenso: e, ciò, perché comunque la condizione di liceità *consent-based*, se non rigidamente regolata, non assicura la presenza di una volontà vera o comunque veramente ponderata nemmeno nei (pochi o statisticamente meno numerosi) casi in cui essa si presenta, finendo anzi per ridursi a una trappola per utenti inesperti da schivare[10].

Senza dire che nemmeno di fronte a un (fisiologico) rifiuto generalizzato al trattamento potremmo dirci appagati. Se, infatti, il rifiuto non deriva da un atto di volontà (vera e veramente ponderata), esso di per sé si accompagna a delle criticità: può accadere, infatti, che esso si ritorca contro gli stessi interessi del titolare dei dati, che avrebbe avuto convenienza ad accettare il trattamento, e di riflesso che pregiudichi proprio il titolare del trattamento. Il risultato sarà, inevitabilmente, l'inefficacia del sistema del consenso (assieme a un inevitabile pregiudizio di quel *free flow of personal data*, che tanto sta a cuore al legislatore eurounitario e più in generale all'economia moderna).

E, ancora, un simile rifiuto generalizzato finisce per rendere l'utente una sorta di burocrate, costretto a muoversi tra svariate richieste, che per il contesto in cui sono formulate spesso richiedono di venire lette quanto meno nelle prime parole, per poi essere pedissequamente rifiutate[11].

---

10 Del resto, spesso non vi è alcuna ragione per il titolare dei dati a dare il suo consenso; eppure, benché manchi tale interesse, il consenso viene prestato. Giacché le ipotesi in cui il *data subject* vuole consapevolmente arricchire la sua controparte, concedendole l'uso dei suoi dati, sono giocoforza limitate, è evidente che l'autorizzazione al trattamento finisce per essere un feticcio che non corrisponde ad alcuna volontà reale.

11 Le ultime ragioni indicate rendono, a mio avviso, poco credibile che un semplice incremento della "cultura dei dati" (pur auspicabile) possa risolvere tutti i problemi regolatori attualmente sussistenti. E, infatti, per quanto sia da guardare con favore quel cambio antropologico che porterà – così si crede o per lo meno si spera – a rendere i dati (la loro protezione e il loro trattamento) veri e propri valori, avvertiti socialmente e socio-giuridicamente e non solo disciplinati come tali dall'interno dell'ordinamento giuridico (in virtù dei riflessi che l'utilizzo dei dati personali inevitabilmente ha), comunque anche tale mutamento non escluderebbe i problemi legati al paradosso dell'attenzione e alla correlata necessità, per l'utente che vi si volesse sottrarre, di trasformarsi in un burocrate, continuamente raggiunto da richieste di consenso da leggere e valutare.

6.3. Regolazione e interpretazione del consenso, oggi

Già nelle disposizioni dedicate alle condizioni di liceità del trattamento il consenso, oltre a venire menzionato, trova alcuni cenni di disciplina: all'art. 6 si prevede che il consenso vada fornito "per una o più specifiche finalità"; all'art. 9 si aggiunge che esso, se relativo a dati "di categorie particolari", sia anche "esplicito".

Tuttavia, è soprattutto negli art. 4(11) e 7-8 che il consenso viene regolato. Ivi, in particolare, si definisce il consenso dell'interessato quale "manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento". Inoltre, si stabilisce che l'onere della prova del consenso sia a carico del titolare del trattamento; che, nel consenso di consenso prestato nel contesto di una dichiarazione scritta più ampia, la sua richiesta sia chiaramente distinguibile, comprensibile, facilmente accessibile; che la libertà del consenso debba essere valutata tenendo "nella massima considerazione l'eventualità … che l'esecuzione di un contratto … sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto". L'art. 8, poi, detta ulteriori condizioni riguardanti il "consenso dei minori in relazione ai servizi della società dell'informazione".

A lato, v'è anche da menzionare la Direttiva *ePrivacy* (volgarmente detta *cookie law*), ossia la Direttiva 2002/58/CE, la quale prevede quale unica base per il trattamento dei dati personali rientranti nel suo ambito di applicazione (e, quindi, in particolare i *cookie*[12]) il consenso dell'interessato. Consenso che, peraltro, "corrisponde al consenso della persona interessata di cui alla Direttiva 95/ 46/CE" (così l'art. 2, lett. f])[13].

Al fine di comprendere come debbano venire intese tali disposizioni appaiono della massima utilità, per la loro intrinseca condivisibilità, così come per la loro autorevolezza, le linee guida elaborate di

---

[12] Sulla profilazione mediante uso di *cookie* e strumenti simili v. oggi anche le Guidelines 8/2020 on the targeting of social media users, version 1.0., adopted on 2 September 2020.

[13] Oggi v. l'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.

recente dall'European Data Protection Board e che aggiornano e completano le linee guida del Gruppo di lavoro Articolo 29[14].

La "libertà" del consenso manca, secondo l'EPDB, se il soggetto è costretto di fatto a dare il suo consenso perché intende ottenere un bene o un servizio o perché il rapporto in cui agisce è fortemente squilibrato.

Il primo gruppo di casi richiama le cosiddette *tying practices*[15], rispetto alle quali il GDPR mantiene una posizione abbastanza equivoca all'art. 7, par. 4, e al considerando 43[16]: probabilmente, incrociando le varie tesi sostenute, allo stato deve ritenersi che la necessità di prestare il consenso per accedere a beni o servizi essenziali lo renda inevitabilmente invalido e che, invece, là dove si tratti di beni o servizi non essenziali il consenso possa essere validamente richiesto e prestato, purché ciò avvenga con modalità tali da far dubitare della libertà del consenso[17]. Ad esempio, sarebbe ammesso condizionare uno sconto al consenso; non, invece, condizionare l'accesso a una *app* già scaricata al

---

14 Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1., adopted on 4 May 2020.

15 Su cui molto si è scritto di recente: v. per tutti A. De Franceschi, *La circolazione dei dati personali tra* privacy *e contratto*, Napoli, 2017; C. Langhanke e M. Schmidt-Kessel, *Consumer Data as Consideration*, in *Journal of European Consumer and Market Law*, 2015, p. 218 ss.

16 Secondo cui, rispettivamente, va tenuta nella "massima considerazione" l'eventualità che l'esecuzione del contratto sia condizionata al consenso, "presumendosi" la mancanza di libertà se il trattamento dei dati non è necessario per tale esecuzione.

17 Sulla prima ipotesi v. l'*Handbook on European Data Protection Law*, Luxembourg, 2014, p. 58 (che parla, a dire il vero, di beni "sufficientemente importanti"); sulla seconda, in realtà, le Guidelines 05/2020 sostengono una tesi abbastanza restrittiva, secondo la quale la libertà mancherebbe ogni qual volta un servizio fosse richiesto verso la controprestazione di dati, anche se nel mercato fosse possibile reperirlo verso una controprestazione in denaro. Nondimeno, parrebbe lecito subordinare al consenso l'ottenimento di uno sconto, giacché in tal modo sarebbe ben chiara all'interessato la scelta che compirà concedendo il suo consenso. Le due ipotesi divergono, come meglio diremo oltre, poiché la prima si avvicina di più a una costrizione, la seconda a una influenza indebita. Resta qualche dubbio per il caso di iscrizione a una *newsletter*, ove non si può ritenere che il trattamento avvenga sulla base della necessità contrattuale, poiché lo stesso trattamento costituisce (di regola) remunerazione per il *data controller*; in tal caso appare ragionevole costruire il consenso quale negozio collegato che fornisce la controprestazione, a sua volta inserita in uno schema di scambio condizionale (cfr., sullo scambio di dati personali a fronte dell'iscrizione a una *newsletter*, Cass. civ., Sez. I, 2 luglio 2018, n. 17278, in *NGCC*, 2018, I, p. 1775).

consenso a un trattamento di dati non direttamente necessario per la stessa prestazione del servizio[18] o l'accesso a una pagina internet al consenso ai *cookie*, come avviene tramite i cosiddetti *cookie walls*[19].

Il secondo gruppo di casi richiama situazioni in cui il *data subject* versa in posizione di debolezza verso il titolare del trattamento, tanto da essere portato di fatto ad acconsentire al trattamento, senza poter esercitare una libera scelta. Si tratta, ad esempio, dei casi del lavoratore rispetto al suo datore o del privato verso un'autorità pubblica[20].

Sotto un punto di vista diverso, la "libertà" del consenso, e quindi l'"effettività" del volere, difetta se il consenso viene richiesto per un insieme di scopi, anziché "granularmente" per singoli e specifici scopi (come, del resto, confermano anche i considerando 32 e 43[21]).

Tale requisito si collega, poi, a quello della "specificità" del consenso, che di nuovo mira a garantire l'"effettività" del volere: il consenso deve venire prestato in relazione a uno o più scopi specifici, stabiliti anticipatamente dal titolare del trattamento. Del resto, è un principio generale, espressamente stabilito dal GDPR, quello per cui gli scopi del trattamento debbono essere già decisi prima della raccolta dei dati (cfr. art. 5, par. 1, lett. b])

La specificità, a sua volta, ci porta a considerare quello dell'"informazione": per ciascuno degli scopi specifici del trattamento basato sul consenso, ossia per ciascuno dei singoli atti di consenso che vengono richiesti, l'interessato deve essere sufficientemente informato.

L'informazione ha un contenuto minimo, desumibile in parte dei considerando, in parte dalle previsioni del GDPR, in parte da un'interpretazione sistematica e funzionale del testo di legge[22]. Secondo

---

18 In tal caso, peraltro, la base più appropriata per il trattamento sarebbe quella indicata nell'art. 6, par. 1, lett. b. Sulla pratica, molto comune, dei titolari del trattamento di munirsi del consenso anche ove vi è una diversa base per il trattamento v. *infra*.

19 Connesso al requisito in parola è quello della mancanza di pregiudizio (*detriment*), in base al quale il titolare del trattamento deve poter dimostrare che il rifiuto o la revoca del consenso non porta a costi o a svantaggi per il titolare dei dati (v. anche il considerando 42).

20 V. anche qui il considerando 43.

21 Secondo cui, rispettivamente, il consenso deve essere dato per tutti gli scopi di un trattamento, fermo restando che esso non è libero se non si permette al *data subject* di acconsentire separatamente a diverse operazioni di trattamento dei dati.

22 V., quanto al testo del GDPR, il considerando 42 e l'art. 7, par. 3.

l'EDPB, tale contenuto coincide – tra l'altro – con l'identità del titolare del trattamento, lo scopo di ciascuna operazione di trattamento, il tipo di dati raccolti e usati, il diritto di revocare il consenso.

Ancora più importante, però, è chiedersi come vanno fornite le informazioni, anche al fine di rispettare il principio di trasparenza e di permettere al *data subject* di porre in essere una decisione consapevole (il che, a ben vedere, ridonda ancora una volta nell'"effettività" del volere[23]). In ogni caso, la richiesta di consenso – che è il mezzo comune con cui il titolare del trattamento cerca di ottenere il consenso e che, soprattutto, è un mezzo sicuramente ammesso dal GDPR – deve essere redatta in modo chiaro e con linguaggio semplice, comprensibile ai presumibili destinatari della comunicazione[24]. È opportuno, inoltre, che le informazioni siano fornite in modo breve e conciso: a tal riguardo il titolare del trattamento si può servire di una costruzione a più livelli (*layered*), fornendo al primo livello alcune informazioni basilari e, poi, rinviando ad altre pagine per l'indicazione di dettagli via via più specifici[25].

Infine, l'atto di consenso deve risultare "non ambiguo", risultando altrimenti dubbia la presenza di una volontà "effettiva". In linea generale, si prescrive che il consenso sia prestato tra un "atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano" (così il considerando 32).

Più nel dettaglio, il GDPR (allo stesso considerando) specifica che, per quanto non vi siano oneri di forma particolari (sono possibili dichiarazioni scritte, anche con strumenti elettronici, o pure orali), non possono essere considerati validi atti di consenso il silenzio, le caselle

---

23 Insiste sulla consapevolezza "del fatto" e "della misura" il considerando 42.

24 Ai sensi dell'art. 7, par. 2, sembrerebbe che ciò sia richiesto solo laddove la richiesta di consenso sia parte di una dichiarazione scritta più ampia. In realtà, il requisito in parola ha una portata assai più estesa; semmai, nel caso in cui la richiesta sia parte di una dichiarazione più ampia, il GDPR prescrive anche che essa sia facilmente distinguibile e accessibile. V., del resto, il considerando 32.

25 In tal modo, scrive l'EPDB, si possono al tempo stesso rispettare i doveri – apparentemente contrastanti – di precisione e completezza, da un lato, e di semplicità, dall'altro.

pre-spuntate[26] o la semplice inattività; al contrario, possono esserlo le spunte di caselle durante la visita di una pagina *web* o anche semplicemente la scelta di impostazioni tecniche per i servizi della società dell'informazione (ad esempio, la scelta di impostazioni di un *browser*). Per l'effetto, non si può ad esempio considerare valido il consenso ai *cookie* prestato semplicemente continuando la navigazione in una pagina internet.

Per quanto riguarda i soli dati di cui all'art. 9 GDPR, il consenso dev'essere anche "esplicito": a tal fine, può consistere in una dichiarazione scritta e firmata, ma può essere sufficiente anche il riempimento di un modulo *online*, una *email* o l'*upload* di un documento firmato. Anche la forma orale potrebbe essere idonea; tuttavia, la necessità che il titolare del trattamento provi l'esistenza di tutte le condizioni richieste per il consenso esplicito rende assai difficile che questi si accontenti di una dichiarazione orale (tutt'al più, si possono immaginare dichiarazioni telefoniche registrate, ammesso che si riesca a provare in tal modo anche di aver fornito informazioni sufficienti in un modo chiaro, adeguato e trasparente).

Con riguardo a qualsiasi categoria di dati personali, il considerando 32 e l'art. 7, par. 3, prevedono anche che, quando la richiesta di consenso avviene tramite mezzi elettronici, la richiesta non deve "interferire immotivatamente con il servizio per il quale il consenso è espresso" e che la revoca del consenso deve essere tanto facile quanto la sua concessione. Tali disposizioni potrebbero avere un riflesso assai importante sul modo in cui viene ricostruito il consenso (e non solo la revoca); tuttavia, esse vengono a tutt'oggi per lo più intese in senso letterale: la prima, come volta a evitare fastidi nella navigazione sui siti (sicché il consenso, pur richiedendo un atto positivo e non ambiguo, non dovrebbe essere eccessivamente difficile da prestare) e, la seconda, come volta a regolare unicamente le modalità della revoca. Su questi punti torneremo comunque oltre.

6.4. Forza e debolezza dell'approccio attuale

Come si è visto, la tendenza dell'ordinamento eurounitario è nel senso di creare dei confini al trattamento dei dati, onde renderlo il più

---

[26] Cfr. Corte di Giustizia, 11 novembre 2020, C-61/19; v. anche Corte di Giustizia, 1 ottobre 2019, C-673-17, per il caso di caselle pre-spuntate e *cookie*.

possibile informato e libero. Tuttavia, restano probabilmente dei problemi, che l'approccio attuale non riesce a superare.

Per descrivere i punti di forza e di fragilità dell'attuale sistema, è necessario ampliare la prospettiva.

Qualsiasi sistema o sottosistema che si basi sulla volontà individuale non può, per forza di cose, richiedere un accertamento circa la presenza di una volontà psichica perfettamente formata di chi dichiara il suo volere. Nondimeno, il sistema può funzionare perché, di norma (fisiologicamente), chi dichiara il suo volere effettivamente ha posto in essere una scelta coincidente, sufficientemente ponderata almeno nei suoi elementi centrali[27].

E, difatti, solo se così è si può addebitare a un soggetto, in ragione della sua autoresponsabilità, una dichiarazione che (patologicamente) non corrisponde alla sua volontà. Questo è quanto avviene, di regola, nel sistema dei contratti, in cui chi dichiara sa o può sapere a cosa va incontro.

Più specificamente, chi dichiara è o può essere perfettamente consapevole degli elementi centrali del contratto, mentre per quelli di minore rilievo può ben demandare la disciplina, se non vuole interessarsene, all'ordinamento giuridico (confidando sul fatto che tale disciplina sarà la più equilibrata possibile). E lo stesso vale finanche dove ci si allontani dal sistema del codice civile, per approdare al contratto del consumatore: anche in tal caso, infatti, il contraente debole può scegliere l'*an* del contratto e può sindacarne i profili essenziali (bene o servizio, prezzo); quanto, invece, alla disciplina ulteriore, è proprio la fisiologica impossibilità di averne contezza (unitamente all'altrettanto fisiologica impossibilità di farne oggetto di trattativa) a consigliare un intervento correttivo da parte dell'ordinamento giuridico[28].

---

27 Rispetto a questa fisiologia possono ben sussistere situazioni patologiche, le quali tuttavia sono, per l'appunto, patologiche: si pensi, per il caso del contratto, al sistema dei tradizionali vizi del volere (errore, dolo, violenza, incapacità).

28 Patologia diversa è quella che emerge là dove un soggetto non sia in condizione di decidere l'*an* del contratto e si trovi quindi soggetto al potere altrui: si pensi ai casi di monopolio, oligopolio e anche, nell'ambito del terzo contratto, all'abuso di dipendenza economia. Simile, inoltre, è la condizione del soggetto vulnerabile: colui che, cioè, è portato – a causa della sua condizione o in ragione di un'influenza indebita di controparte – a concludere un certo contratto.

Il sistema del consenso al trattamento, tuttavia, non rispetta questi principi. In quei casi, infatti, la patologia diviene la normalità: è normale che chi presta il suo consenso non abbia piena contezza di quanto sta facendo. A fronte di ciò, l'ordinamento dovrebbe necessariamente ripristinare, tramite un suo intervento, l'effettività del consenso: in caso contrario il sistema non può funzionare o, comunque, finisce per essere inefficace.

L'ordinamento, a sua volta, può agire in astratto in due forme diverse: rendendo fisiologicamente reale il consenso; correggendo, sulla base degli interessi normali del titolare dei dati, la disciplina specifica del trattamento.

Il primo approccio è quello per lo più scelto a livello europeo. La ragione è di ordine logico: il consenso al trattamento attiene per lo più a una scelta su un elemento centrale, rispetto a cui è difficile supporre che un terzo possa, per quanto sulla base di un interesse normale della parte, sostituirsi (si finirebbe, di fatto, per sostituire al consenso una diversa condizione di liceità, vagamente corrispondente al legittimo interesse)[29]. Soltanto di fronte a una esorbitante mancanza di interesse in capo al *data subject* oppure per quanto attiene al *quomodo* del trattamento – il cui rilievo, però, è assai limitato – si può pensare a un intervento correttivo fondato sull'interesse normale del titolare dei dati (i rischi corsi e i benefici ottenuti, entrambi valutati secondo normalità e ragionevolezza).

In questo quadro possiamo allora inserire gli interventi regolatori di cui s'è detto nel precedente paragrafo: quando richiedono un consenso informato e libero, in realtà il più delle volte cercano di superare il *privacy paradox*, rendendo vera e veramente ponderata la volontà.

---

[29] E, infatti, in questo caso mancherebbe un criterio interno alla stessa pattuizione (proprio perché la verifica riguarderebbe un elemento centrale della pattuizione, che giocoforza non potrebbe essere al tempo stesso oggetto della valutazione e parametro della stessa; al contrario, laddove la verifica riguarda elementi accessori, è ovvio che la si può compiere sulla base di quell'economia interna allo stesso contratto). Il criterio esterno, su cui inevitabilmente basarsi, non sarebbe che quello dell'interesse "normale" a dare i dati: con la conseguenza che l'atto di consenso verrebbe pienamente materializzato e la volontà a sua volta totalmente compressa. Il consenso, così, lascerebbe di fatto spazio a un bilanciamento tra gli interessi del titolare del trattamento e i rischi (e gli interessi) del titolare dei dati; per l'effetto, si tradurrebbe in una sorta di legittimo interesse.

Così, la necessità di un consenso specifico (granulare), non inglobato in un testo contrattuale, dovrebbe assicurare che sia prestata attenzione a tutti i possibili trattamenti; inoltre, il dovere di informare chiaramente, in modo accessibile e breve (e con la necessità di rinviare ad altri testi per ulteriori spiegazioni), dovrebbe garantire circa l'esistenza dei presupposti di una scelta reale; l'esigenza di lasciare libero il consenso, evitando di subordinare l'accesso a siti allo stesso, dovrebbe tra l'altro scongiurare il rischio di una decisione frettolosa[30].

Al contrario, la valutazione di impatto preventiva può leggersi nel secondo ambito: l'art. 35 GDPR, infatti, nel prevedere che in determinati casi il titolare del trattamento sia tenuto a svolgere una tale valutazione, parrebbe implicarne un possibile esito negativo, con conseguente preclusione del trattamento previsto. Una simile interpretazione è peraltro confortata dalla lettura dell'art. 36 GDPR, che in tema di consultazione preventiva dell'Autorità di controllo non esclude affatto la possibilità che quest'ultima esprima parere negativo al trattamento, per l'assenza di misure adottate (anche se corrispondenti a tutte quelle adottabili) idonee ad attenuare sufficientemente i rischi[31].

Questi interventi senza dubbio debbono essere visti con favore, poiché essi percorrono una strada volta a superare i problemi indicati in

---

30 Anche il consenso al trattamento può mancare di libertà sotto un altro e diverso punto di vista, simile a quello di cui s'è detto nella precedente nota: allorché il consenso al trattamento è necessario per ottenere un bene o un servizio essenziale, ecco che viene a mancare la necessaria libertà. Escluderei, però, che nel caso di accesso a un sito qualunque si possa parlare di un bene o di un servizio essenziale: sicché la garanzia di libertà deve, in tali casi, essere riletta nel senso di cui al testo. Inoltre, un'analoga patologia potrebbe presentarsi ogni qual volta un soggetto non è in condizione di decidere serenamente sull'autorizzazione al trattamento: non tanto perché non ne ha il tempo o non è in grado di comprendere i valori alla base, ma perché, per la specifica situazione in cui opera, non può scegliere in modo libero. Conseguentemente, anche questi casi in effetti possono comportare un problema di libertà (si tratta, in particolare, delle già menzionate ipotesi in cui tra le parti vi è un rapporto asimmetrico e di dipendenza, come quello tra privato e autorità pubblica o tra dipendente e datore di lavoro).

31 Sulla valutazione d'impatto preventiva v. per tutti E. BATTELLI e G. D'IPPOLITO, *Art. 35 RGPD*, in *Comm. Gabrielli*, Milano, 2019, p. 661 ss.

apertura[32]. Tuttavia, forse essi non sono ancora sufficienti ad assicurare il pieno funzionamento del sistema del consenso.

Il punto richiederebbe indagini d'ordine psicologico e comportamentale[33]: nondimeno, già in via di prima approssimazione, e sulla base della comune esperienza, si può notare come, nonostante una consapevolezza generale che aumenta e che sempre più conduce le persone a ritenere "importanti" i loro dati[34], i paradossi cui si è fatto riferimento – il paradosso dell'attenzione e quello della valutazione – aleggiano ancora sul consenso al trattamento, con tutto ciò che ne consegue.

Pensiamo, anzitutto, al caso dei *cookie*.

È evidente che, là dove la scelta proposta dal gestore di un sito è tra accettare tutti i *cookie* o selezionare quelli davvero voluti, essa diviene di fatto irreale, poiché nessuno o quasi nessuno avrà il tempo per scegliere, per ciascun sito, i *cookie* ammessi[35]. Là dove, invece, è presente anche un pulsante di rigetto di tutti i *cookie* (o comunque, in assenza di scelta, il gestore del sito non installa altri *cookie* se non quelli tecnici), i problemi diminuiscono ma non sono del tutto evitati, giacché – di nuovo – è ovvio che nella normalità dei casi l'utente accetterà o rifiuterà tutto, in blocco; e lo farà sulla base per lo più di una personale posizione generale circa il tema della protezione dei dati (indifferenza o preoccupazione per i propri dati[36]), tutt'al più ammorbidita a se-

---

32 Seguendo un'opinione già sostenuta da Simitis, B. Buchner e J. Kühling, *Art. 7 DS-GVO*, in *DS-GVO - BDSG Kommentar*², München, 2018, p. 289 s., sostengono che in passato il consenso spesso non era che una "bloße Fiktion"; oggi il GDPR, secondo i due autori, cerca di circoscrivere l'ammissibilità del consenso proprio nei casi in cui esso ridonda in una finzione.

33 Indagini che, del tutto opportunamente, iniziano a venire compiute: v., a proposito uno studio condotto presso l'Università Suor Orsola Benincasa, I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica studi comportamentali*, in *ODCC*, 2018, p. 67 ss.

34 La diffusione di una "cultura dei dati" è uno degli obiettivi del GDPR, che probabilmente verrà raggiunto, e in parte è stato già conseguito, anche grazie all'insistenza sui diritti del singolo e sulla rigida regolazione del consenso al trattamento.

35 Come si sul dire, utilizzando un'espressione emblematica, la scelta è eccessivamente *time-consuming*.

36 Peraltro, l'utente indifferente, al solo fine di togliere dalla vista il *banner* dei *cookie*, potrebbe cliccare su "accetta" solo per un riflesso incondizionato (perché "accettare"

conda dei connotati apparenti del sito (ad esempio, se il gestore sembra affidabile e il sito interessante, si potrà pensare di accettare l'installazione dei *cookie*).

Ma anche al di fuori dei *cookie* si presentano numerosi problemi: un soggetto normale, mediamente diligente, spesso non è in condizione di compiere una scelta reale, mancando di tempo o comunque di facoltà cognitive sufficienti per porre in essere singole decisioni ponderate[37].

Ad esempio, a fronte di varie caselle relative al trattamento dei dati, non preselezionate, la prima delle quali riguarda un trattamento necessario per l'esecuzione di un contratto (rispetto a cui però il titolare chiede il consenso, non accontentandosi della diversa e apposita base legale) e le altre invece si riferiscano a trattamenti per finalità in senso lato pubblicitarie, avviene spesso che l'utente le rifiuti tutte o, al contrario, le accetti tutte, fermandosi a leggere solo la prima e poi compiendo istintivamente una medesima selezione per tutte le caselle o ipotizzando che sia necessario acconsentire per poter ottenere il bene o il servizio che, poniamo, in quel momento si sta acquistando.

E questa situazione è comune – e quindi, per così dire, "patologicamente fisiologica" – anche là dove i singoli trattamenti sono indicati in modo semplice, con frasi concise e con rimando (secondo una struttura "a più livelli") ad altri documenti per i necessari approfondimenti: anzi, in tal caso si pongono ulteriori problemi, ogni qual volta la richiesta di primo livello, nella sua necessaria brevità, non dà conto esattamente del trattamento e non permette, quindi, di compiere una decisione veloce e al tempo stesso sufficientemente consapevole.

---

a prima vista pare più positivo e sbrigativo di "rifiutare", anche se poi in realtà il "rifiuto" sarebbe equivalente). Lo stesso utente indifferente potrebbe acconsentire al trattamento ritenendo tendenzialmente preferibile, in termini generali, l'utilizzo dei suoi dati, piuttosto che il mancato utilizzo. L'utente preoccupato per l'uso dei suoi dati potrebbe compiere una scelta opposta, ma sempre non riflettuta. Del resto, anche un utente particolarmente attento difficilmente perderebbe tempo per scegliere i *cookie* che trova davvero utili, selezionandoli uno ad uno; piuttosto, deciderebbe se acconsentire o meno sulla base di una scelta semplicistica (favorevole, se uno o più *cookie* sono probabilmente utili; sfavorevole, in caso contrario).

37 In linea generale, si è notato che, mentre per i dati sensibili il consenso spesso è davvero informato e libero, per gli altri dati esso si riduce di regola a una veloce spunta di una casella. Cfr. B.-J. Koops, *The Trouble with European Data Protection Law*, in *International Data Privacy Law*, 2014, p. 251 ss.

E i problemi non derivano solo dalla scarsità di tempo e facoltà cognitive dell'interessato: talvolta, infatti, essi si collegano all'impossibilità, per un soggetto medio, di valutare i rischi e i benefici per le parti connessi al trattamento.

Ad esempio, una società sviluppatrice di *software*, che chiedesse semplicemente il consenso a inviare *report* dei *crash* di una sua applicazione, con tutta probabilità non chiarirebbe i menzionati rischi e benefici: ossia, per il *data subject*, il rischio di un *data breach* o comunque di un uso illecito dei suoi dati e, all'opposto, per il *data controller*, il beneficio derivante dal trattamento.

In breve, accade ancora spesso che la decisione sul consenso non abbia fisiologicamente modo di essere davvero consapevole e meditata: tra condizionamenti esterni (in particolare, la necessità di approvare per non perdere tempo o di rigettare per evitare rischi, così come l'impossibilità di prendere visione compiutamente di tutte le specifica finalità dei trattamenti) e difficoltà interne (soprattutto inerenti alla complessità che ogni valutazione dei rischi porta con sé), essa finisce per risultare inidonea a veicolare una normale volontà (ossia una volontà che, salvo fattori patologici, è presente).

E, di qui, una prima conseguenza: il disallineamento tra quello che sarebbe un consenso pieno e quello che invece è il consenso oggi rende ancora ipocrita questa base del trattamento, allorché essa è presente. Né si potrebbe invocare, in questi casi, l'autoresponsabilità del singolo: tale principio, come si è detto, può avere un valore per addebitare a ciascuno di noi le conseguenze negative delle sue azioni là dove sia normale e fisiologico che un soggetto mediamente diligente le eviti; non, invece, qualora sia inevitabile o comunque assai probabile che finanche l'uomo comune (un tempo si sarebbe detto: *bonus paterfamilias*) vi vada incontro. Per l'effetto, il modello di diligenza che si vuole adottare va plasmato sulle particolarità del contesto, tenendo peraltro in considerazione che, più lo si rafforza, più si finisce per lasciare senza tutela proprio i soggetti che ne sarebbero più bisognosi, mentre, più lo si indebolisce, più si tutela il contrario interesse di chi vorrebbe trattare i dati personali.

E non è tutto: le conseguenze, come già accennato, sono anche altre. Là dove manca il consenso, non è detto che sia compiuta una scelta (reale e ponderata): sì che l'assenza del consenso non è indice della mancanza di un interesse del *data subject* o, comunque, di un bilanciamento posto in essere, anziché dall'ordinamento, da quest'ultimo. E,

comunque, in tali casi si deve anche tenere in considerazione il disturbo inevitabilmente arrecato al titolare dei dati, ogni qual volta la richiesta interrompe la navigazione o comunque richiede la sua attenzione, anche solo per un istante e per negare – il più delle volte senza nemmeno leggere l'intero testo della richiesta, anche se sintetizzato in poche righe – il suo consenso.

A fronte di tutto questo, ci si deve chiedere se il consenso può essere reso maggiormente effettivo, senza con ciò comprimere eccessivamente gli interessi – legittimi – dei titolari del trattamento. E la risposta richiede, anzitutto, di domandarsi se un aiuto in questo senso può derivare dall'inquadramento dogmatico del consenso e, in senso luogo, di verificare se, indipendentemente da questo, una revisione ermeneutica o una riforma legislativa dei requisiti del consenso possa portare nella direzione divisata.

6.5. L'inquadramento dogmatico: una prima proposta (priva di effettiva utilità)

Come noto, l'inquadramento dogmatico del consenso al trattamento ha visto contrapporsi – in Italia come all'estero – opinioni anche assai distanti: in particolare, mentre taluni autori hanno accolto tesi negoziali (o addirittura contrattuali), altri hanno ridotto il consenso al trattamento ora (in Italia) a un atto giuridico in senso stretto, ora (in Germania, ossia nell'ordinamento dove maggiormente si è studiato l'inquadramento dogmatico dell'*Einwilligung*) a un atto pseudo-negoziale o a un atto reale[38].

Ciò che accomuna queste opinioni, come si sarà inteso, è il loro radicamento nell'ordinamento italiano: ossia, l'applicazione della dogmatica italiano all'atto di consenso. Nel vigore del GDPR, tuttavia, può per lo meno dubitarsi della correttezza di quest'operazione: sia perché esso è un Regolamento (e tende quindi all'uniformità del diritto), sia perché esso disciplina in modo pressoché compiuto l'atto di consenso,

---

[38] Per una sintesi delle diverse posizioni sostenute in Italia v. S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Ramagna, 2016, p. 2 ss. Per quelle tedesche v. invece P.M. ROGOSCH, *Die Einwilligung im Datenschutzrecht*, Baden-Baden, 2013, p. 36 ss.

sì che l'interpretazione (anche quella sistematica) dovrebbe essere condotta su un piano eurounitario, e non interno[39].

A fronte di ciò, però, è facile accorgersi che la mancanza di categorie eurounitarie rende assai difficile l'inquadramento dogmatico dell'atto di consenso: si tratta di un primo fattore che, già a livello generale, depone per l'inutilità dell'operazione di qualificazione, a fronte dell'assenza, a livello di diritto UE, di una teoria generale del negozio (e del contratto) e, viceversa, della presenza, nel GDPR, si una disciplina specifica per l'atto di consenso.

Tuttavia, possiamo provare a mettere da parte lo scetticismo e verificare se l'inquadramento dogmatico eurounitario può essere di una qualche utilità per risolvere i nostri problemi.

6.5.1. L'inquadramento generale

Possiamo definire – secondo una rivisitazione della dottrina pandettistica, che in vario modo ha influenzato l'intera tradizione di *civil law* – i meri atti quali dichiarazioni o comportamenti la cui regolazione coincide in tutto e per tutto con il loro significato socio-giuridico intrinseco e fattuale (venendo dunque disciplinati da una *regulative rule*) e i negozi quali atti che pongono una regola la quale, di per sé, non si riduce al significato socio-giuridico intrinseco e fattuale della dichiarazione o del comportamento, ma costituisce il frutto dell'attivazione concreta di una convenzione socio-giuridica direttamente volta ad approvare di una regola (il frutto dell'attivazione concreta di una *constitutive rule*)[40].

Quanto al consenso al trattamento, l'inquadramento come mero atto impone di ritenere che il permesso di utilizzare i dati crea una regola già immanente all'atto; quello, invece, come negozio richiede di

---

[39] A favore della necessità di un inquadramento eurounitario e autonomo v. F. Bravo, *Il consenso*, cit., p. 157 ss., e già G. Alpa, *La disciplina dei dati personali*, Roma, 1998, p. 90; nella letteratura tedesca v. A. Ingold, *Artikel 7*, in *Europäische Datenschutzgrundverordnung - Handkommentar*[2], Baden Baden, 2018, p. 450. Per la possibilità di utilizzare categorie interne, onde utilizzare per l'atto di consenso la disciplina interna quanto meno in via residuale (laddove la disciplina eurounitaria lasci aperti degli spazi), v. G. De Cristofaro, *Die datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens*, in T. Pertot (hrsg.), *Rechte an Daten*, Tübingen, 2020, p. 158 ss.

[40] Si consenta il rinvio ad A.M. Garofalo, *Le regole costitutive del contratto*, Napoli, 2018. La differenza tra atto e negozio giuridico è nota anche ai progetti di *soft law*: v. art. II.-1:101(2) DCFR.

rinvenirvi un atto che, già per il suo significato socio-giuridico, veicola qualcosa d'ulteriore, non immanente all'atto stesso. Un simile interrogativo, a sua volta, rappresenta una questione difficile (un *hard case*) da risolvere dall'interno dell'ordinamento giuridico (ossia, sulla base della sistemazione e della specificazione dei valori sociali propria dell'ordinamento giuridico).

Tra gli argomenti che possiamo valorizzare, e che dall'interno del sistema giuridico ci aiutano a giungere a una soluzione, il più importante attiene all'inquadramento dogmatico dei dati personali in sé e per sé. Senza dilungarsi sulla questione, mi pare necessario ammettere che oggi i dati personali – là dove rilevanti[41] – rappresentino dei valori, nel senso che essi incarnano e rappresentano l'oggetto degli interessi (diversi) del titolare dei dati e del potenziale titolare del trattamento. Come tali, essi possono anche venire reificati[42], se non come beni in senso proprio quanto meno come oggetto di diritti contrapposti: da un lato, quello dell'interessato a vedersi riconosciuto, per l'appunto, come titolare dei dati, a respingere ogni trattamento illecito e a controllare ogni trattamento lecito; da un altro lato, quello del titolare del trattamento, a utilizzare un bene personale altrui ogni qual volta è presente una base per il trattamento[43].

---

41 Ossia, entro l'ambito oggettivo di applicazione del GDPR: cfr. art. 2. Al di fuori, e al netto delle diverse discipline nazionali, i dati personali non sono rilevanti in sé e per sé; l'attenzione del sistema giuridico (dei singoli sistemi giuridici) si sposta di regola sui singoli diritti e interessi che stanno a valle, senza attribuire rilievo autonomo ai dati personali.

42 Su questo tema cfr., da ultimo, C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020. Sul dibattito, assai noto, circa l'ammissibilità di una "proprietà del dato", v. N. PURTOVA, *Property Rights in Personal Data: A European Perspective*, Alphen aan den Rijn, 2011; C. PRINS, *When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?*, in *Script-ed*, 2006, p. 270 ss.

43 Così ricostruito, il diritto del titolare del trattamento assomiglia a un diritto su cosa altrui, pur distinguendosene almeno sotto due profili: a) mentre i diritti reali su cosa altrui hanno consistenza prettamente patrimoniale, nel caso del diritto a utilizzare i dati le implicazioni per le due parti (interessato dal trattamento e titolare del trattamento) sono assai diverse e, soprattutto, sono differenti tra loro (v. *infra* nel testo); b) il diritto sui dati personali non è *erga omnes*, ma non è neppure un diritto relativo (è, piuttosto, un *pati* o, meglio ancora, l'attribuzione al titolare del trattamento di facoltà che, pur venendo ipostatizzate in uno specifico diritto, finiscono in realtà per ampliare le libertà generiche del titolare stesso). Sul dibattito, assai esteso in Italia, sui beni personali come beni immateriali oggetto di diritti v., da ultimo, la sintesi di

Ora, il consenso al trattamento, nel permettere l'utilizzo di questo bene, non è volto alla semplice rimozione di un limite e, soprattutto, non corrisponde a un'autorizzazione fattuale cui giuridicamente segue la disattivazione della di una certa disciplina (quella che proibisce il trattamento laddove difetti una base)[44]; piuttosto, il consenso al trattamento mira alla creazione, pur revocabile, di una situazione giuridica in capo a un altro soggetto[45]. E un simile effetto non è immanente alla fattualità della dichiarazione o del comportamento; esso, al contrario, deriva dall'attivazione di una convenzione socio-giuridica direttamente volta ad approvarlo. Di conseguenza, nell'atto di consenso deve rinvenirsi un negozio[46].

In replica non potrebbe sostenersi che tale inquadramento è disatteso dalla pratica sociale, in seno alla quale i dati personali ancora non

---

S. Thobani, *Diritti della personalità e contratto. Dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, p. 51 ss.

44 L'autorizzazione fattuale (e in particolare la tolleranza, ma anche il consenso dell'avente diritto e secondo taluno anche altre ipotesi autorizzatorie) si esaurisce di per sé nel suo significato, che non è quello di approvare una modificazione della realtà deontologica, ma semmai quello di decidere interlocutoriamente e fattualmente circa l'utilizzo di un proprio bene (sì che i riflessi giuridici sono di stampo regolativo e non costitutivo, ossia non sono socialmente, socio-giuridicamente e giuridicamente l'oggetto verso cui direttamente si indirizza la volontà). Nel diritto italiano v., proprio con riferimento al consenso dell'interessato e con posizioni diverse, S. Patti, sub *art. 23*, in C.M. Bianca e D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*, I, Padova, 2007, p. 553; G. Oppo, *Sul consenso dell'interessato*, in V. Cuffaro, V. Ricciuto e V. Zeno-Zencovich, *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 124.

45 Nella dottrina tedesca, v. M. Funke, *Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht*, Baden-Baden, 2017, p. 82 ss., e, in parte, anche G. von Zimmermann, *Die Einwilligung im Internet*, Berlin, 2014, p. 13 ss. (il quale sottolinea anche la congruità, rispetto agli interessi in gioco, della qualificazione nei termini di negozio).

46 Non mi sembra che, invece, aiuti a qualificare in un senso o nell'altro l'osservazione – pur corretta – secondo cui ogni inquadramento deve tenere a mente la fisiologica ammissibilità del trattamento dei dati, che non costituisce certo ipotesi eccezionale: e, ciò, sia perché tale considerazione non esclude la qualificazione come autorizzazione (seppur di tipo diverso dal consenso dell'avente diritto: cfr. F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e Impresa*, 2019, p. 42), sia perché a valle si ripropone il problema – assai arduo e acuito dalla prospettiva eurounitaria – della qualificazione dell'autorizzazione (cfr. G. Oppo, *«Trattamento» dei dati personali e consenso dell'interessato*, in, *Scritti giuridici*, VI, *Principi e problemi del diritto privato*, Padova, 2000, p. 112).

sono avvertiti come centri di interessi (autonomi e distinti rispetto agli interessi che si situano a valle rispetto al loro trattamento). La qualificazione giuridica, anche degli atti di autonomia, si basa sulla realtà socio-giuridica, ossia sul modo di intendere i valori in gioco in seno alla società (per come esso si proietta sull'ordinamento e si definisce all'interno dell'ordinamento). Se, poi, la percezione generale si discostasse dalla stessa realtà socio-giuridica, non si potrebbe comunque negare che solo quest'ultima è la base su cui compiere la qualificazione giuridica, pur dovendosi rilevare uno scarto con la percezione generale[47].

La qualificazione del consenso come negozio impone, più precisamente, di rinvenirvi un atto di disposizione: un negozio unilaterale volto al trasferimento costitutivo di un diritto. Questo diritto, a sua volta, ha ad oggetto un bene – in senso atecnico – personale; il diritto, tuttavia, sfugge alla distinzione tra personalità e patrimonialità[48], finendo per innestarsi nella specifica libertà o nello specifico diritto cui di volta in volta è più legato (ora alla libertà di espressione, ora alla potestà pubblica e così via). Solo nel caso in cui tale libertà altro non è che quella economica, come nei casi in cui il trattamento dei dati serve per finalità di *marketing* o simili, potrebbe ipotizzarsi che il diritto assuma dal lato del titolare del trattamento un valore patrimoniale e, di riflesso, che così si connoti (almeno in parte) pure il suo oggetto: ciò

---

47 Questo scarto, tra il piano dei valori effettivamente immanenti alla società (in sé e per sé e per come la costruzione sociale si proietta e si definisce sul piano dell'ordinamento giuridico) e la stessa percezione che la società ha dei valori (che condivide e che proietta sul sistema giuridico), è tipico della protezione dei dati e deriva dal "paradosso della valutazione" di cui si è già detto: sicché al tempo stesso certi valori sono inevitabilmente propri di un certo sistema socio-giuridico, ma di ciò spesso non se ne ha una generale e piena contezza. Sulla difficoltà di applicare i concetti di volontà e consenso a fronte degli atti di disposizione dei dati personali v. anche G. RESTA e V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 411 ss.

48 Considerazioni simili, pur declinate in modo diverso da quanto qui sostenuto e comunque con notevole varietà di accenti, sono diffuse nella dottrina italiana: di "duplicità di rilevanza giuridica" parla I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in *Annali dell'Università degli Studi Suor Orsola Benincasa*, 2016-2018, p. 24 (richiamando il noto scritto di G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 256 ss.); a favore di un superamento della tradizionale separazione tra patrimonialità e non patrimonialità si esprime R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e Impresa*, 2020, p. 760.

che, conseguentemente, imporrebbe di rinvenire nel negozio l'atto di disposizione di un bene (anche) patrimoniale.

Se tutto questo è vero, non può però nemmeno sottacersi che, a questo livello assai generale la qualificazione dogmatica non appare di alcuna utilità, giacché, da un lato, risulta assai difficile creare a livello interpretativo una disciplina generale del negozio eurounitaria e, da un altro lato, essa risulterebbe praticamente del tutto superata e disattivata da quella prevista dal GDPR per l'atto di consenso.

6.5.2. I riflessi specifici

Probabilmente, scendendo più nel dettaglio potrebbe in qualche modo recuperarsi una qualche precettività – una qualche utilità pratica e deontologica – anche per l'inquadramento dogmatico. Sennonché, altri problemi finirebbero per emergere: da un lato, questi tratti specifici di disciplina risulterebbero ancora meno attingibili in via di interpretazione del diritto eurounitario di quanto non avvenga per il generico inquadramento del consenso nella categoria del negozio (e ciò sarebbe vero, anche se ci si basasse unicamente sulle tradizioni nazionali e sugli strumenti di *soft law*); da un altro lato, a ben vedere anche tali tratti di disciplina mancherebbero di un'effettiva precettività, perché di fatto sarebbero legati a profili non di particolare rilievo o comunque assorbiti dalla disciplina prevista dal GDPR per l'atto di consenso.

Vediamo, a titolo di esempio, tre profili che appaiono di interesse. Premetto sin d'ora che escluderò dall'ambito dell'indagine ogni profilo inerente ai vizi del consenso, che appaiono strumenti inidonei a risolvere i nostri problemi, sia per il loro funzionamento operativo, sia per la loro connessione con situazioni di patologia (mentre, come si è visto, il punto dolente del consenso al trattamento deriva dalla fisiologica assenza di una volontà reale e realmente ponderata).

Anzitutto, va ricordato che in numerosi ordinamenti europei i contratti che non sono sostenuti da uno scambio o quanto meno da un interesse patrimoniale del disponente (secondo il lessico italiano) debbano venire ricondotti alla donazione, la quale sarebbe soggetta a un particolare onere di forma (solo in alcuni sistemi superabile in virtù dell'esecuzione del contratto). Ci si potrebbe allora chiedere se, quando il dato assurge a bene patrimoniale, la disposizione dello

stesso debba avvenire per forza di cose a titolo di scambio (anche solo empirico o interno), onde evitare la qualificazione di donazione.

Un simile esito, pur apparentemente controintuitivo, in realtà potrebbe apparire opportuno da un punto di vista di disciplina. In tal modo, infatti, non si escluderebbe che la disposizione del bene personale sia e resti un atto dominato da profili personali[49]; semplicemente, si introdurrebbe una ulteriore qualificazione, tale da richiedere, al fine di rendere valida la disposizione, di rinvenire uno scambio (come detto, anche solo empirico o interno)[50]. Ove così non fosse, la disposizione sarebbe nulla – perché priva della forma donativa – e, parimenti, il consenso non sarebbe validamente prestato, con tutto ciò che ne consegue. Il dibattito, ormai assai noto, circa l'ammissibilità che i dati divengano *consideration* dovrebbe allora risolversi nel senso che, ogni qual volta i dati costituiscono anche beni patrimoniali, il negozio – in tal caso presumibilmente un contratto – non solo può, ma addirittura deve prevedere una controprestazione o comunque un interesse patrimoniale in capo al disponente, soddisfatto mediante la stessa disposizione.

Nei fatti, però, questa conclusione non è persuasiva. Da un lato, così come è difficile applicare il diritto interno al negozio di consenso, così

---

[49] Nel caso di concessione del diritto di sfruttare economicamente l'immagine il contesto patrimoniale supera, in qualche parte, quello personale, che pur continua a deformare la disciplina del contratto (dal lato del disponente). Nel caso di dati personali, invece, le due dimensioni rimangono per forza di cose indipendenti e contemporaneamente esistenti, poiché la dimensione patrimoniale non rende in alcun modo meno pressante l'esigenza di tutela legata alla personalità del bene: prova ne sia che, per il GDPR, in tutti i casi il consenso è sempre revocabile (senza che l'affidamento di controparte abbia mai un ruolo, diversamente da quanto sosteneva la dottrina nel vigore della precedente Direttiva: cfr. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, 2006, p. 1053 s.); e ulteriore conferma si può trarre dal fatto che, in questi casi, la patrimonialità non diminuisce le note legate all'esigenza di protezione dell'individuo (come invece può avvenire in tutti i casi in cui l'immagine viene "venduta"). Più in generale, a proposito del fatto che "il richiamo all'idea di mercato" non "potrebbero essere inteso come indebolimento del grado di tutela rispetto al trattamento dei dati personali", cfr. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e Impresa*, 2018, p. 1117.

[50] Di conseguenza, nell'atto dovrebbe rinvenirsi anche un solo contratto, e non già – come da taluno proposto – il collegamento tra due atti o un atto complesso (rispettivamente G. DE CRISTOFARO, *Die datenschutzrechtliche Einwilligung*, cit., p. 169 ss.; R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2020, in corso di pubblicazione).

è arduo ritenere che il diritto eurounitario si allarghi sino a disciplinare profili ulteriori e che da questi faccia discendere delle conseguenze di disciplina per lo stesso consenso[51]. Da un altro lato, da un punto di vista pratico il profilo non appare di grande importanza: non è difficile accorgersi che la disposizione di dati personali, in campo patrimoniale, può di regola essere fatta afferire all'interesse del disponente di ricevere una pubblicità targettizzata.

In secondo luogo ci si può domandare se, in virtù del moto di tutto il diritto privato contrattuale europeo verso una pregnante funzionalizzazione e un forte solidarismo, l'inquadramento non possa condurre a perimetrare l'ambito di validità del consenso al trattamento[52].

Una tale materializzazione potrebbe indurre a normalizzare fortemente l'interesse di cui ipoteticamente, e ragionevolmente, è portatore

---

51 Di conseguenza, appare preferibile ritenere di trovarsi di fronte a un negozio di consenso, collegato a un contratto e inserito in uno schema di sinallagma condizionale (v. Ph. Hacker, *Daten als Gegenleistung. Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht*, in *die Zeitschrift für die gesamte Privatrechtswissenschaft*, 2019, p. 148 ss.; sul sinallagma condizionale in Italia v. per tutti G. Amadio, *Controllo sull'esecuzione ed efficacia negoziale (note intorno al concetto di onere)*, in *Letture sull'autonomia privata*, Padova, 2005, p. 220 ss.; in senso contrario, ossia ipotizzando l'esistenza di un'obbligazione di fornire i dati, si esprime A. Metzger, *Dienst gegen Daten: Ein synallagmatischer Vertrag*, in *Archiv für die civilistische Praxis*, 2016, p. 833 ss.). Venuto meno il consenso, cadrebbe quindi il rapporto contrattuale (ma non viceversa, per quanto patologie del contratto o del rapporto possano essere valutate per verificare la validità dell'atto di consenso o l'eventualità di una revoca); né questo potrebbe rappresentare un pregiudizio illegittimo per il *data subject*, giacché un simile *detriment* corrisponderebbe in tutto e per tutto al vantaggio – giocoforza legittimo – ottenuto dallo stesso *data subject* concedendo il suo consenso (ritiene invece che la revoca del consenso non faccia venire meno il contratto principale, ma consenta alla controparte di recedere, G. De Cristofaro, *Die datenschutzrechtliche Einwilligung*, cit., p. 169 ss., il quale in tal modo si propone di evitare la scure del principio per cui la revoca del consenso non può comportare un pregiudizio per il titolare dei dati).

52 Sulla diffusa "materializzazione" del diritto privato europeo (inteso, qui, come diritto privato dei singoli stati europei, anche esterni all'Unione), v. C.-W. Canaris, *Wandlungen des Schuldvertragsrechts - Tendenzen zu seiner „Materialisierung"*, in *Archiv für die civilistische Praxis*, 2000, p. 273 ss.; A. di Majo, *Giustizia e "materializzazione" nel diritto delle obbligazioni e dei contratti tra (regole di) fattispecie e (regole di) procedura*, in *Eur. dir. priv.*, 2013, p. 797 ss.; Cass. com., 22 octobre 1996, in Bull. civ., IV, n. 261, e il conseguente art. 1170 Code civil, per come modificato dall'ampia riforma del 2016. Un simile moto è rilevabile – e già da tempi – finanche nel *common law* inglese, pregno di formalismo: v. la *red hand rule* di J Spurling Ltd v Bradshaw [1956] EWCA 3, poi applicata nel più recente Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd [1987] EWCA Civ 6.

il *data subject*, valutando in relazione a esso la validità dell'atto di consenso. Si potrebbe, in particolare, ritenere che, là dove un negozio di consenso ingloba un interesse opposto a quello ragionevole, esso è nullo o comunque invalido[53].

Tuttavia, a parte gli evidenti problemi di ricostruire un'effettiva disciplina eurounitaria di questo stampo, comunque non si potrebbe esasperare questo controllo, poiché altrimenti si negherebbe la stessa scelta autonoma del *data subject* e si finirebbe per far ridondare la base del "consenso" in quella del "legittimo interesse" (svuotando del tutto la prima[54]).

Di fatto, questa via, pur in qualche modo percorribile, finirebbe per permettere un sindacato sull'*an* solo in casi estremi e, per il resto, un sindacato sul *quomodo*: il quale, però, riguarderebbe ipotesi abbastanza limitate. Si pensi, ad esempio, al caso in cui un soggetto chieda a una società che gestisce un sito di intermediazione immobiliare di venire contattato da eventuali venditori per avere informazioni circa l'acquisto di un bene. Ora, a ben vedere, tale acquisto corrisponde a un interesse normalmente e fisiologicamente limitato nel tempo: sì che estendere eccessivamente l'ambito del consenso valido (ad esempio, ipotizzando che esso possa giustificare anche un trattamento senza durata temporale) parrebbe un'operazione illegittima proprio per il contrasto tra l'interesse normale del *data subject* e quello irragionevole che altrimenti sarebbe introiettato nell'atto di consenso.

Solo entro questi risicati limiti l'inquadramento eurounitario, unitamente a una forte solidarizzazione dell'autonomia privata, potrebbe risultare di una qualche utilità. E, a dire il vero, perfino entro questo perimetro esso, a ben vedere, non apporta nulla di nuovo: già oggi un'interpretazione fedelmente orientata ai principi di correttezza e di minimizzazione, insiti nel GDPR, dovrebbe consentire di giungere a risultati corrispondenti. Sì che, ancora una volta, sembra che la qualificazione dell'atto di consenso non sia di alcuna utilità.

---

53 Clausole generali e categorie analoghe alla "meritevolezza" di cui all'art. 1322, comma 2, c.c. verrebbe così piegate a sindacare l'effettiva presenza di un interesse conforme a quello di cui è ipoteticamente portatore il *data subject* in quella situazione.

54 Di fatto, si assisterebbe a un bilanciamento secondo normalità e ragionevolezza, volto a svuotare anche la facoltà per il titolare dei dati di scegliere l'*an* (a questi sarebbe lasciata solo la scelta di negare il trattamento, ma non di consentirvi; di fatto, il diritto di autorizzarlo si tradurrebbe in una richiesta di *opt-out* anticipata).

Un terzo, e ultimo, profilo da considerare riguarda quell'inquadramento eurounitario che deriva non già dall'applicazione di principi derivanti dalle varie tradizioni nazionali e dagli strumenti di *soft law*, ma semmai dal resto della disciplina eurounitaria: e, in particolare, da quella in tema di contratto del consumo e di pratiche commerciali scorrette[55].

In effetti, questa via è stata già proposta in varie sedi: ci si è chiesti, ad esempio, se nella richiesta di consenso si può rinvenire un contratto del consumo e, quindi, vi si può applicare il controllo legale e giudiziale sulle clausole vessatorie[56]. La risposta più persuasiva, tuttavia, è stata negativa, anzitutto perché, in effetti, è difficile che un atto di consenso presenti uno squilibrio tra diritti e obblighi[57].

Dal punto di vista, invece, delle pratiche commerciali scorretti, si è effettivamente ammesso che l'offerta di un servizio, indicato come "gratuito" là dove invece esso è prestato a fronte della corresponsione di dati, può costituire una pratica commerciale scorretta[58]. E, tuttavia, anche questo esito non sembra del tutto utile ai nostri fini, non solo perché intercetta un profilo assai specifico, ma anche e soprattutto perché il servizio in questione, indicato come gratuito e in realtà pagato tramite i dati, non richiede affatto un consenso per trattare questi dati,

---

55 V., in linea generale, G. De Cristofaro, *Die datenschutzrechtliche Einwilligung*, cit., p. 173 ss.

56 Interrogativo, peraltro, stimolato anche dal considerando 42 del GDPR, secondo il quale, in conformità alla Direttiva 93/13/CEE, la dichiarazione di consenso non dovrebbe contenere "clausole abusive".

57 Cfr. del resto l'art. 4, par. 2, Direttiva 93/13/CEE, secondo cui "la valutazione del carattere abusivo delle clausole non verte né sulla definizione dell'oggetto principale del contratto, né sulla perequazione tra il prezzo e la remunerazione, da un lato, e i servizi o i beni che devono essere forniti in cambio, dall'altro, purché tali clausole siano formulate in modo chiaro e comprensibile". In questo senso v. S. Thobani, *Processing Personal Data and the Role of Consent*, in *European Journal of Privacy Law & Technologies*, 2020, p. 100; cfr. anche Th. Pfeiffer, *Datenschutz und AGB-Recht: Die Inhaltskontrolle vorformulierter Einwilligungserklärungen*, in M. Weller e M. Wendland (hrsg.), *Digital Single Market. Bausteine eines Digitalen Binnenmarkts*, Tübingen, 2019, p. 60 ss.

58 V. da ultimo T.A.R. Lazio, Sez. I, 10 gennaio 2020, n. 260, in *Foro Amm. - TAR*, 2020, p. 99, a proposito della quale v. anche B. Parenzo, *Dati personali come "moneta". Note a margine della sentenza TAR Lazio n. 260/2020*, in *juscivile*, 2020, p. 1364 ss.

ma li processa sulla base dell'interesse legittimo (sì che, dal punto di vista italiano, il contratto appare piuttosto gratuito e atipico)[59].

A tal riguardo, l'intervento di un altro corpo normativo, ossia il diritto della concorrenza, potrebbe sortire un migliore effetto: a fronte, infatti, dell'impossibilità per l'utente di scegliere se accettare o meno pubblicità targettizzate, la giurisprudenza (questa volta, tedesca) ha affermato che, sebbene non costituisca un illecito (civile e amministrativo) in base alla disciplina del GDPR, la mancata richiesta di un consenso per il trattamento dei dati o comunque l'assenza di una scelta a tal riguardo può rappresentare un illecito anticoncorrenziale[60]. Tuttavia, anche questa prospettiva non ci aiuta a risolvere le disfunzioni del consenso in sé considerato: anzi, ampliandone il ruolo (e in un certo modo quindi invertendo il percorso intrapreso dalla regolamentazione della protezione dei dati personali), le rende ancora più preoccupanti.

La soluzione ai problemi già messi sul tavolo va cercata, evidentemente, altrove.

6.6. La disciplina: una seconda proposta (priva di appiglio normativo)

Escluso che la via dell'inquadramento dogmatico possa aiutarci a trovare le risposte che cerchiamo, non resta che chiedersi se, da un punto di vista funzionale, si possa immaginare di perimetrare in modo diverso e forse ancora più rigido il consenso al fine di renderne effettivo il sistema, al tempo stesso evitando di limitare eccessivamente la liceità del trattamento dei dati[61]. Vale la pena di porsi questa domanda prima in astratto, per poi verificare se un'eventuale risposta richieda un cambiamento di legislazione o semplicemente un adattamento della sua interpretazione.

---

59 V. l'informativa di Facebook all'url *https://www.facebook.com/about/privacy/legal_bases* (controllato per l'ultima volta il 30 novembre 2020). Qui la base del trattamento è costituita dal legittimo interesse perché, in effetti, non viene garantito un servizio a fronte della processabilità di un dato, che costituisce al tempo stesso la remunerazione del servizio (come avviene finanche nel caso di iscrizione a una *newsletter*); piuttosto, si offre un servizio a fronte di ulteriori utilizzi dei dati già validamente raccolti (utilizzi per lo più pubblicitari e comunque intrinseci allo stesso servizio che viene offerto).

60 Così, da ultimo, BGH, 23 giugno 2020 - KVR 69/19.

61 Sulla libera circolazione dei dati v. già l'art. 1 GDPR, oltre ai considerando 3 e 9.

6.6.1. Alla ricerca del consenso effettivo

Anzitutto, ogni riflessione dovrebbe ammettere che la disciplina del consenso non può essere identica per casi eccessivamente diversi. Ovviamente, ciò non potrebbe risolversi in un approccio atomistico al problema del consenso: tuttavia, bisognerebbe quanto meno riconoscere che talune ipotesi – e qui il riferimento va soprattutto al consenso ai *cookie* – sono assai diverse da altre.

E, difatti, il consenso ai *cookie* per sua natura è molto particolare: esso presenta, per di più, problemi di regolazione peculiari, dovuti alla natura della navigazione sul *web* (alla sua velocità e alla sua complessità tecnica[62]). Ritenere che il consenso ai *cookie* debba e possa venire disciplinato come ogni altro consenso vorrebbe dire rinunciare, in ogni situazione, all'effettività di questa base e della connessa dichiarazione negoziale. E un simile risultato, per quanto possibile, va scongiurato: anche, per l'appunto, distinguendo il consenso generale da quella sua sottospecie tipica che è il consenso ai *cookie*, che richiede una regolazione autonoma.

Prendiamo allora a riferimento la fattispecie generale e proviamo a indagare come, in questa sede, il consenso possa essere reso più effettivo (nella convinzione che, là dove sufficientemente effettivo, il consenso deve restare accessibile come base, sia perché è utile, sia per evitare un eccessivo paternalismo).

La direzione da intraprendere, in linea di massima, dovrebbe essere quella già percorsa dal legislatore eurounitario: quella, cioè, per cui il consenso è valido solo in presenza di una scelta che, in sé e per sé, riveli una normale attività decisionale e, quindi, un utilizzo normalmente idoneo e sufficiente delle proprie capacità cognitive (attenzione, concentrazione, ponderazione).

Alcuni esempi possono essere utili. Talune ipotesi sono abbastanza eclatanti: si pensi al caso in cui un soggetto chieda, in modo formalmente conforme al dettato del GDPR, il consenso a trattare i dati per una finalità inaspettata (una biblioteca chiede di pubblicare sul proprio sito *web* la fotografia personale contestualmente caricata dall'utente per ottenere una tessera di entrata). Il fatto che tale finalità sia anomala,

---

[62] Le quali rendono inevitabile, a tacer d'altro, la mancanza di una decisione analitica circa gli specifici scopi di trattamento dei *cookie*: il *data subject* di fatto accetterà tutto o, se e quando potrà farlo in blocco, rifiuterà tutto.

rispetto a quanto di norma avviene nel mercato o comunque nel settore di riferimento, induce a ritenere che la semplice spunta di una casella sia inidonea a rivelare il consenso. Una soluzione diversa potrebbe imporsi se, per fornire il consenso, l'utente dovesse cliccare su un apposito *link*, identificato dalla finalità in parola ("se vuoi che la tua immagine sia pubblicata, clicca qui"), e una volta reindirizzato dovesse decidere se accettare o meno il trattamento.

L'esito divisato potrebbe già ora imporsi sulla base di un'interpretazione funzionale del GDPR. Del resto, tutto il Regolamento è percorso dall'idea per cui più inaspettato è un trattamento, ossia meno usuale, normale e finanche necessario, più si ammorbidiscono i requisiti di liceità del trattamento (cfr., ad esempio, gli artt. 6, par. 4, e 9): il che, tradotto nei termini del consenso, parrebbe ammettere un livello di trasparenza e informazione minore, tutte le volte in cui il trattamento è di natura tale per cui l'interessato può aspettarsi che gli sia richiesto, in quella data situazione, il consenso per porlo in essere.

Altri esempi, invece, sono meno vistosi, ma comunque richiedono di venire (ri)considerati[63]. Si pensi, in generale, a tutte le *boxes*, anche non preselezionate, che appaiono durante la fase di conclusione di un contratto *online*: un utente che voglia assicurarsi un certo servizio potrebbe, in modo disattento, selezionarle tutte (magari supponendo che le ipotesi di consenso facoltative si riferiscano, come avviene per la prima, solo a una *newsletter*; oppure ipotizzando, nella rapidità della lettura, che si tratti in ogni caso di un consenso necessario per l'esecuzione del servizio). Allo stesso modo, nel caso di un *banner* pubblicitario di un sito internet che nasconde momentaneamente la pagina e chiede all'utente se voglia ricevere notifiche di aggiornamento, la presenza di un tasto "accetta" e di uno "rifiuta" non esclude che un soggetto sia portato ad acconsentire senza rendersi effettivamente conto – nella velocità della navigazione – della scelta chiamato a compiere (a maggior ragione se lo specifico oggetto, la provenienza e la frequenza delle notifiche fossero analiticamente specificate solo in una diversa pagina)[64]. La ragionevole certezza di un vero e proprio consenso richiederebbe, al contrario, di ottenere lo stesso consenso in modo ben

---

63 Si tratta di esempi in parte già citati al § 4.

64 Qualcosa di simile, ma legato alla particolare natura dei *cookie*, è previsto per i *cookie walls* nelle linee guida sul consenso dell'EDPB, su cui ci siamo soffermati nel § 3.

diverso: ad esempio, ospitando in pagine *web* recanti anche altri contenuti e diverse da quelle menzionate (e in particolare da quelle di conclusione di un contratto) spazi e *link* appositi, cliccando i quali il titolare dei dati possa *sua sponte* lasciare i suoi dati e acconsentire al trattamento stesso. In tal modo si eviterebbe un'eccessiva aggressività e si collegherebbe l'iniziativa volta a concedere il consenso a una scelta autonoma del *data subject*[65].

Ovviamente, si tratta di indicazioni specifiche, corrispondenti a principi generali da declinare a seconda delle specificità del caso: se la selezione dell'unica *box* oppure l'apposizione della firma per il consenso, anche in sede di conclusione del contratto, richiedesse al tempo stesso di inserire il proprio *account email* (non detenuto dal futuro titolare del trattamento), l'attenzione dell'interessato sarebbe attirata in modo maggiore e di ciò si dovrebbe inevitabilmente tenere conto[66]; parimenti, la richiesta di impostare il consenso in una *app* si abbina normalmente (proprio perché avviene *una tantum*) a un'attenzione maggiore dell'utente di quanto non accada con riferimento alle continue richieste che compaiono sulle pagine *web*.

E, ancora, in tutti i casi si dovrebbe presumibilmente indicare il trattamento non solo identificandone la finalità, ma anche rivelandone rischi e benefici e magari anche fornendone un'esemplificazione: questo, al primo livello in modo sufficientemente breve da non stancare il lettore (e da non indurlo a concedere il consenso senza aver finito di leggere) e, invece, in modo più analitico ai livelli ulteriori. Ad esempio, una società di sviluppo di *software*, nel chiedere il consenso a utilizzare

---

65 Il riferimento va soprattutto ad appositi spazi di pagine, come quelle di apertura, ove si preveda la possibilità di aprire altre pagine (ad esempio, di iscrizione a *newsletter*). In tal modo sarebbe assicurato un sufficiente livello di attenzione dell'interessato, che non capiterebbe di certo per caso sulla seconda pagina; e sarebbero evitate anche quelle richieste che, comparendo nell'ambito di pagine di transizione, spesso conducono a lasciare il proprio consenso solo e soltanto perché, nella rapidità del momento, non si ha il tempo per leggerle compiutamente e meno che meno per compiere una valutazione.

66 Anche la possibilità di scaricare una *app* a fronte del pagamento di un prezzo oppure gratuitamente, ma con necessità di prestare un consenso al trattamento, può rappresentare una modalità sufficientemente chiara per descrivere e far comprendere il "valore" dei dati che vengono ceduti (purché la *app* in questione non dia modo di usufruire di un servizio essenziale, nel qual caso il pagamento tramite dati comunque non sarebbe ammesso).

i dati relativi ad eventuali *crash* di una applicazione, dovrebbe evidenziare quali sono i rischi per il *data subject*, quali sono i benefici per il titolare del trattamento, quali sono i vantaggi per il *data subject* (normalmente, nessuno, se non genericamente quello di aiutare lo sviluppatore nella sua attività)[67]. Parimenti, la richiesta di consenso dovrebbe ben chiarire eventuali effetti collaterali: ad esempio, nel caso di pubblicazione di dati, il rischio – se esistente – di una futura impossibilità pratica e quindi inesigibilità giuridica per il primo titolare del trattamento di comunicare a tutti i terzi il venir meno sopravvenuto della base per il trattamento[68].

Ovviamente, più si volesse percorrere questa strada, più il consenso verrebbe limitato. Addirittura, in talune situazioni esso non sarebbe di fatto ammesso, proprio per l'impossibilità sostanziale di rispettare questi requisiti stringenti. Si tratta, però, di un esito che non è abnorme: già ora, in effetti, si ritiene inadatto il consenso in situazioni connotate da un rapporto asimmetrico tra le parti; per di più, il GDPR contiene numerose altre basi che, venendo debitamente estese[69], impedirebbero uno stallo e, per l'effetto, un'eccessiva compressione del principio di libera circolazione dei dati anche personali.

Anzi, rendere il consenso più effettivo può evitare che a esso ricorrano i titolari del trattamento di fatto per deresponsabilizzarsi, così non domandandosi – come invece sarebbe richiesto – se il singolo trattamento sia o meno autorizzato dalle altre basi del GDPR. Rendere il consenso "difficile", unitamente ad altri approdi ermeneutici cui è già

---

67 Anche qui, la previsione di un piccolo corrispettivo a favore di chi fornisce i suoi dati può costituire uno strumento idoneo a far comprendere che gli stessi dati hanno un "valore" instrinseco.

68 Cfr. art. 17, par. 2, GDPR.

69 Del resto, come si è detto, il legittimo interesse che preveda un *opt-out* non è altro che un consenso interamente materializzato. E, a tal riguardo, deve anche considerarsi che un *opt-out* di fatto si ha tutte le volte in cui le impostazioni di base di un apparecchio non consentano la raccolta di certi dati (ad esempio, quando si impedisce di *default* la raccolta di dati di geolocalizzazione alle *app* installate su uno *smartphone*). Peraltro, in tal caso deve ritenersi che la richiesta di ottenere i dati, giacché di fatto equivalente a un consenso, debba seguirne il più possibile il regime: se una *app* volta a memorizzare gli itinerari percorsi chiede di essere autorizzata ad accedere a quei dati, deve prima aver descritto la funzionalità in parola (così garantendo che l'utente sia attento) e poi, domandando il consenso, evidenziarne rischi e benefici, in forma sia sintetica che analitica (e sempre anche tramite esempi del trattamento).

in parte giunto l'EDPB – quello per cui, scopertasi l'inidoneità di una base, non la si può sostituire con un'altra a piacimento del titolare del trattamento[70] e quello per cui, chiesto e non ottenuto il consenso, non si potrebbe fondare il trattamento su un'altra base[71] –, vuol dire scongiurare questo risultato e superare questa prassi, oggi molto diffusa[72].

Al tempo stesso, un consenso reso più effettivo imporrebbe in numerose occasioni di ottenerlo non già formulando una di quelle richieste che, ai più, appare come una fastidiosa interruzione della navigazione: onde evitare che le circostanze risultino inidonee o che la richiesta al primo livello non risulti sufficientemente chiara e al tempo stesso breve, il potenziale titolare dovrebbe ottenere il consenso in altri modi[73]. Questo esito gioverebbe indirettamente anche ad altre finalità, permettendo di conseguire ulteriori risultati positivi che, di per sé, costituirebbero altrettanti argomenti a favore della revisione divisata.

In particolare, da un lato si eviterebbe il continuo disturbo recato dalle richieste di trattamento di dati (rispetto alle quali finanche il GDPR auspica che non interrompano continuamente la navigazione[74]); da un altro lato si stimolerebbe la creazione di una consapevolezza della concessione del consenso e, quindi, la formazione di una

---

70 § 123 delle menzionate linee guida sul consenso.

71 A tanto non arriva l'EDPB (e, peraltro, un tale esito non sarebbe probabilmente consentito dall'attuale testo del GDPR). Al contrario, le citate linee guida, al § 120, prevedono la possibilità per il titolare del trattamento di cambiare base (passando dal consenso a un'altra condizione di liceità), purché di ciò sia fornita l'informativa all'interessato ai sensi degli artt. 13 e 14 GDPR.

72 Peraltro, deve tenersi in considerazione anche l'ulteriore principio per cui non si può subordinare l'accesso a beni e servizi alla prestazione del consenso (in nessun caso, là dove beni e servizi sono essenziali; soltanto là dove sia preservata la libertà del consenso – ad esempio, consentendo di ottenere uno sconto tramite la concessione dei dati –, negli altri casi). Esso, a rigore, dovrebbe valere ed essere fatto valere anche là dove il consenso è necessario per l'adempimento di un'obbligazione, proprio perché nel momento in cui è chiesto il consenso non si dovrebbero far valere considerazioni che di per sé potrebbero fondare una diversa base.

73 Ad esempio: inserendo un *link* nella pagina di apertura, da cliccare per iscriversi a una *newsletter*. Il *link* dovrebbe poi rimandare a una pagina con una breve descrizione esemplificativa del trattamento e dei rischi e dei benefici per le parti.

74 Cfr. il considerando 32, su cui anche *infra*.

cultura dei dati e, in fondo, in quell'auspicato mutamento antropologico, che renda non solo conosciuti, ma anzitutto riconosciuti i valori insiti nella protezione dei dati personali[75].

6.6.2. Necessità di riforme legislative

La direzione che si è indicata richiederebbe di reinterpretare svariate disposizioni del GDPR: il che, oltre a costituire di per sé un'operazione difficile e forse nemmeno ammissibile[76], si scontra apertamente con il tenore testuale di alcune disposizioni che, pur non riguardando specificamente la disciplina generale del consenso, impediscono una revisione ermeneutica.

In effetti, di primo acchito potrebbe sembrare che il percorso indicato – volto a restringere alquanto l'ambito del consenso al trattamento – sia in qualche modo suggerito dallo stesso GDPR: sia perché, come si è visto, è la strada su cui si sta muovendo l'EDPB (e così pure la Corte di Giustizia), sia perché, com'è stato a suo tempo accennato, sussistono talune disposizioni su cui far leva per proseguire su questa strada.

Tra queste, vale la pena di considerare quella parte del considerando 32, in cui il legislatore eurounitario richiede che l'atto di consenso non disturbi immotivamente la navigazione: previsione che potrebbe essere letta non solo a garanzia del *free flow of data*, ma anche, al contrario, come restrizione del consenso legittimo, tutte le volte in cui esso venisse "richiesto" dal titolare del trattamento tramite una do-

---

75 In realtà, è possibile che la stessa cultura dei dati sia altrove più diffusa di quanto non avvenga in Italia; e che, oltretutto, sia maggiore l'attenzione che, a costo di impiegare più tempo e più concentrazione, l'utente medio pone allorché deve dare il suo consenso (e, qui, mi riferisco soprattutto a quanto avviene in Germania, dove effettivamente la consapevolezza e l'attenzione verso i dati sono assai alte). Tuttavia, l'esistenza stessa di differenze culturali tra gli Stati membri dev'essere una preoccupazione del legislatore eurounitario, che deve farsene carico e deve adattare la figura dell'utente medio, non potendo fare esclusivo riferimento a quanto avviene entro i confini di uno Stato (e della sua corrispondente società).

76 Quanto meno perché, rispetto al sistema su cui è intervenuto il GDPR, la scelta del legislatore europeo appare abbastanza nitida nel senso su cui oggi si è assestata l'interpretazione prevalente, di cui si è detto nel § 3. Ad oggi, quindi, non appaiono mature le condizioni per rendere ammissibile una nuova lettura delle disposizioni, che richiederebbe per lo meno una certa distanza temporale dalla scelta politica compiuta a livello legislativo.

manda che interrompe la navigazione (e che, quindi, richiede una risposta, anziché essere prodromica a una solo eventuale iniziativa dell'utente, volta a consentirgli di fornire spontaneamente i suoi dati personali)[77].

Quanto, poi, all'art. 7, par. 3, GDPR, il quale prevede che la revoca del consenso debba essere possibile con modalità tanto semplici quanto la concessione dello stesso, esso, a ben vedere, potrebbe anche venire letto *a contrario*: non solo, cioè, come volto a potenziare e facilitare la revoca, ma anche come diretto a limitare il consenso. Se la revoca richiede – e questo è inevitabile – un atto di iniziativa del *data subject*, così dovrebbe essere anche per il consenso, che, per realizzare l'accennata simmetria, dovrebbe presupporre un atto di iniziativa dello stesso *data subject*[78].

Tuttavia, per quanto convincenti siano queste argomentazioni, esse non appaiono del tutto persuasive; soprattutto, poi, resta innegabile che il GDPR ammette pacificamente talune modalità di ottenimento del consenso che, nella prospettiva in cui ci siamo posti, dovrebbero risultare inammissibili.

Si pensi, in particolare, all'enfasi con cui il GDPR richiama la "richiesta" al trattamento dei dati: la centralità che essa assume (ad esempio, al considerando 32 o all'art. 7, par. 2) lasciano trasparire che l'accettazione di una simile richiesta può costituire valido atto di consenso, benché in un sistema volto a rendere più effettivo il consenso essa dovrebbe essere considerata quasi sempre sarebbe insufficiente (proprio perché il consenso, per essere validamente prestato, dovrebbe abbinarsi a una scelta e soprattutto a una iniziativa in qualche misura spontanea del *data subject*).

E si pensi anche al consenso in ambito sanitario o legale, previsto dal sistema del Regolamento finanche dove i dati sensibili debbono essere trattati per finalità contrattuali (legate, cioè, all'adempimento di

---

77 In altri termini, se la richiesta di consenso non può interrompere la navigazione immotivamente, allora dovrebbero a rigore non essere ammesse richieste che colgono di sorpresa l'utente e in questo modo strappano un veloce consenso; proseguendo per questa via, la legittimità stessa di una richiesta – ossia di un atto la cui iniziativa proviene dal futuro titolare del trattamento – potrebbe venire posta in dubbio.

78 Ovviamente, non ci si riferisce a un'iniziativa del tutto spontanea, ma semmai incanalata dal titolare del trattamento, che potrebbe nelle sue pagine *web* indicare, in appositi spazi, la possibilità di conferire i propri dati personali per finalità specifiche (ad esempio, per l'iscrizione a una *newsletter* o per l'ottenimento di uno sconto).

un contratto). Qui davvero sarebbe difficile richiedere qualcosa in più di un semplice consenso a una richiesta altrui: sicché l'interpretazione che si è proposta risulterebbe inidonea a tenere in considerazione questi casi, per come attualmente regolati, finendo per risultare inattendibile e infondata in un'ottica *de iure condito*.

Ciò non toglie che, per mezzo di una riforma legislativa[79], si potrebbe rendere il consenso più effettivo: si tratta, del resto, di una strada che già il GDPR ha percorso, riconoscendo l'importanza di basi legali quali il legittimo interesse e irrigidendo i requisiti che il consenso deve presentare per essere valido; una strada che, però, non è ancora giunta alla metà, giacché il legislatore eurounitario ha, evidentemente, preferito accogliere soluzioni di compromesso.

Una futura revisione legislativa dovrebbe, in particolare, intervenire sulla disciplina generale del consenso, prevedendo – oltre a quanto già disposto – che il consenso non sia ammissibile quando, per le sue circostanze[80] o per il suo contenuto[81], l'attenzione che un soggetto normalmente vi dedicherebbe non è sufficiente a ritenerlo espressione di una volontà vera o veramente ponderata (ora perché l'attenzione è scarsa, ora perché, anche se profonda, non è di per sé tale da permettere una piena comprensione). Ciò che richiederebbe, ovviamente e come già ora accade, l'elaborazione di una tassonomia volta a riempire di significato questa indicazione generale.

Al tempo stesso, si dovrebbero conseguentemente ampliare le altre basi. Ciò che avverrebbe non solo in via interpretativa, ma anche legislativa: ad esempio, introducendo l'adempimento quale base anche

---

79 In quella che sarà la "sesta" generazione di regolazione della protezione dei dati. Sulle prime quattro generazioni cfr. V. MAYER-SCHÖNBERGER, *Generational Development of Data Protection in Europe*, in P.E. AGRE e M. ROTENBERG (eds), *Technology and Privacy: The New Landscape*, Cambridge (Massachusetts), p. 219 ss.; sulla quinta generazione v. N. KATZ, *Could GDPR Introduce The Fifth Generation Of Data Security?*, in *Informationsecuritybuzz*, 5 giugno 2018.

80 Ad esempio, in sede di conclusione di un contratto o comunque interrompendo la navigazione. Sarebbe ammesso invece chiedere di fornire il consenso all'interno di una pagina *web* con altri contenuti, prevedendo che l'utente che voglia – ad esempio – iscriversi a una *newsletter* debba cliccare su un *link* e, lì, sottoscriverla.

81 Ad esempio, perché eclatantemente disassato rispetto a quanto avviene in situazioni analoghe oppure perché ragionevolmente non frutto di una ponderazione sufficiente di rischi e benefici. Sarebbe permesso invece domandare il consenso se si spiegassero, in forma concisa e chiara, rischi e benefici, esemplificando il tipo di trattamento.

per il trattamento dei dati sensibili, tutt'al più previa ulteriore "conferma" dell'interessato[82]; oppure estendendo l'ambito in cui è possibile un *opt-out* del *data subject*[83].

Una riforma, peraltro, potrebbe e dovrebbe accompagnarsi a una separazione del consenso al trattamento dal più specifico consenso nel caso di *cookie*: il quale, come si è detto, ne rappresenta un ambito speciale, che non può fungere da modello, a pena di rendere sempre il consenso ineffettivo.

A sua volta, il consenso ai *cookie* richiede, per vedersi migliorato nella sua disciplina, un intervento che elimini quella strutturale e fisiologica asimmetria, per cui gli utenti, nel fornire il consenso, non hanno a disposizione che pochi secondi (al fine di non rendere eccessivamente lenta la navigazione in internet), a fronte di una moltitudine di *cookie* rispetto a cui compiere scelte specifiche. La soluzione, che tra l'altro consentirebbe di rendere meno "disturbante" la richiesta di consenso per i *cookie*, potrebbe passare attraverso l'agglutinazione di queste singole e specifiche scelte, da compiere *ex novo* per ogni sito, in un'unica decisione prodromica alla navigazione e differente a seconda di macro-categorie di *cookie*, differenziati per la finalità dello specifico trattamento; una decisione che avverrebbe modificando le impostazioni del *browser* (e, tutt'al più, consentendo all'utente di cambiarle per siti specifici[84]).

In un senso per lo meno simile si muoverà, presumibilmente, il legislatore europeo, che nel progetto di Regolamento *ePrivacy*[85], volto a

---

82 Essa rappresenterebbe, più che un atto di consenso, una sorta di "informativa rafforzata" (ovviamente, lo dico in senso atecnico, e nella consapevolezza che si richiederebbe un'attenta qualificazione dogmatica di questa "conferma"). Una simile "conferma" potrebbe essere regolata in modo analogo a quel particolarissimo "consenso" (che in realtà consenso non è) di cui si è parlato alla nt. 69.

83 Attualmente il legittimo interesse è ritenuto base sufficiente per il *soft spam*, ossia per la pubblicità proveniente da soggetti con cui è già in essere un rapporto contrattuale (e sempre salvo, comunque, l'*opt-out*). Cfr., per quanto riguarda l'ordinamento italiano, l'art. 130, comma 4, d.lgs. 196/2003.

84 Si pensi ai siti che vendono prodotti desiderati dall'utente, che vuole quindi ricevere una pubblicità targettizzata.

85 Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (Regolamento sulla vita privata e le comunicazioni elettroniche).

sostituire la Direttiva 2002/58/CE, ha previsto tra l'altro che "[i] programmi immessi sul mercato che consentono le comunicazioni elettroniche, compreso il recupero e la presentazione di informazioni in rete, offrono l'opzione di impedire che terzi conservino informazioni sull'apparecchiatura terminale di un utente finale o trattino le informazioni già conservate su detta apparecchiatura. All'installazione il programma informa l'utente finale delle impostazioni relative alla vita privata e per proseguire nell'installazione richiede il consenso dell'utente per una data impostazione" (così all'art. 10[86]).

Resta poi l'esigenza, che in altra sede si era già rilevata[87], di non chiedere alla disciplina della protezione dei dati troppo o comunque qualcosa che essa non può dare. Probabilmente il consenso ai dati dovrà restare per sempre quale base; nondimeno, anche se particolarmente ristretto, esso finirà per nascondere in sé per sempre delle disfunzioni che lo allontano dal modello volontaristico contrattuale, rendendolo in buona parte ineffettivo.

Ciò non toglie, però, che per lo meno i riflessi negativi del consenso concesso potrebbero essere, se non eliminati, per lo meno ridotti per mezzo di una disciplina volta a ristabilire i diritti e gli interessi del titolare dei dati, di per sé compressi dallo stesso trattamento. E, infatti, se è vero che di regola il consenso al trattamento riguarda finalità in senso lato pubblicitarie, connesse al *direct marketing*, giocoforza è anche vero che una disciplina dello stesso *direct marketing* potrebbe restituire al *data subject* quella libertà di autodeterminazione commerciale che un consenso poco ponderato comprime (e, soprattutto, comprime senza che vi sia stata una scelta reale dello stesso *data subject*)[88].

Tutto questo, peraltro, assume importanza anche da un altro punto di vista. Il consenso al trattamento, anche se mai fosse totalmente effettivo, rischia di risultare distruttivo rispetto al sistema del GDPR an-

---

[86] Ma a tal riguardo v. anche il considerando 32 del GDPR, ove menziona – quale strumento per dare il consenso – "la scelta di impostazioni tecniche per servizi della società dell'informazione". Tale previsione, oggi, rischia di condurre a risultati assurdi (basterebbe non navigare "in privato" per acconsentire a tutti i *cookie*): sicché proprio il suo completamento nel Regolamento *ePrivacy* appare vieppiù necessario.

[87] Cfr. A.M. GAROFALO, *Protection*, cit.

[88] Ad esempio, si potrebbe prevedere – a livello di diritto del consumo – che le pubblicità profilate debbano dichiarare di esserlo e che, tramite una richiesta specifica, l'utente possa venire a conoscere i dati da cui deriva la sua profilazione.

che in un ulteriore senso, su cui finora non mi sono soffermato: la protezione dei dati ha un riflesso non solo individuale, ma anche – e forse soprattutto – sociale. Problemi come quello della *filter bubble* pongono pericoli, soprattutto per la tenuta sociale (e finanche istituzionale), che superano sicuramente la dimensione del singolo; problemi rispetto a cui un atto di consenso pone ovviamente dei rischi (quanto meno di *free riding*), che sicuramente non sono evitati solo perché il consenso è più effettivo e che, invece, richiedono di intervenire a valle, restituendo ai singoli quella capacità di giudizio altrimenti compromessa[89].

Insomma: se il consenso al trattamento resta irregolabile, ossia difficile o impossibile da regolare, forse è necessario spostare l'attenzione e disciplinare altri aspetti legati alla compressione degli interessi e dei diritti del singolo: altri aspetti, cioè, di un fenomeno che in fin dei conti da un punto di vista sostanziale rimane unitario.

[89] Ad esempio, inserendo una quota minima e necessaria di pubblicità e di notizie o opinioni giornalistiche non profilata, affinché nella libertà del caso si recuperi anche la libertà dei singoli v. S. Rodotà, Privacy *e costruzione della sfera privata*, in *Tecnologie e diritti*, Bologna, 1995, p. 121.

7. Note sulla regolazione dell'IA

Daniele Imbruglia

7.1. Introduzione

In un suo recente scritto, Pasquale Femia ha notato come gli algoritmi rischino di essere poco più di una moda culturale, ossia di essere l'ennesimo "tema" che "sale all'attenzione generale" su cui scrivono i "professori che occupano il campo simbolico" della materia sino a che la discussione "si aggroviglia, stanca di sé stessa" per poi "all'improvviso" spegnersi[1]. Avuto riguardo alla mole di contributi che accompagnano la riflessione sul tema, connesso, dell'intelligenza artificiale (nel prosieguo, anche, IA) non vi è dubbio che il timore così autorevolmente avanzato sia fondato. Non vi è, infatti, rivista giuridica che non contenga uno scritto dedicato al tema e il numero di convegni che si propongono di affrontare la questione è in continua crescita. Non solo, le stesse autorità regolative intervengono con report, studi, *white papers* ed altra documentazione grigia che tenta di delineare delle regole e delle discipline. Peraltro, a differenza di quanto avviene per altre mode culturali giuridiche dove la discussione spesso si spegne in occasione dell'intervento legislativo[2], la riflessione sull'IA sembra resistere anche alle prime manifestazioni normative. In questo articolo[3], darò, in modo parziale e sicuramente imperfetto, conto dell'attuale stato dell'arte, mettendo in risalto le varie contrapposizioni che l'odierna discussione

---

1 P. Femia, *Introduzione. Soggetti responsabili. Algoritmi e diritto civile*, in G. Teubner, *Soggetti giuridici digitali, Sullo* status *privatistico degli agenti* software *autonomi*, Napoli, 2019, 7.

2 Ibid., 7.

3 Comparso con il titolo *L'intelligenza artificiale* (IA) *e le regole. Appunti*, in *Media Laws*, 2020, 18.

sull'intelligenza artificiale (IA) ha generato[4]. Innanzitutto, esaminerò le posizioni che affrontano il tema della regolazione della realtà digitale, distinguendo tra la tesi conservatrice e quella, adeguatrice, più sensibile alle ricadute giuridiche delle diverse applicazioni dell'intelligenza artificiale. In un secondo momento, mi soffermerò sul dibattito relativo al come regolare tali nuovi fenomeni, richiamando le analisi della migliore dottrina civilistica. Poi, affronterò la questione di quale sia l'attuale applicazione dell'intelligenza artificiale che interroga il giurista, ponendo in luce come spesso questa discussione sia viziata dal credere i progressi della intelligenza artificiale maggiori di quanto siano e, quindi, concentrandomi sulle caratteristiche più critiche delle attuali applicazione dell'IA, anche richiamando la Risoluzione del Parlamento Europeo relativa alle norme di diritto civile sulla robotica del 16 febbraio 2017 (nel prosieguo, anche *Risoluzione*)[5]. In conclusione, darò conto dei possibili principi idonei a regolare il nuovo, consapevole che il discorso sia lungi dall'essere definito.

7.2. Regole e rivoluzioni scientifiche

Il tradizionale porsi come oracolo della legge vigente spiega perché davanti ad ogni mutamento proveniente dalla realtà regolata vi sia, tra i giuristi, una più o meno ampia comunità di interpreti che si attesta su posizioni conservatrici, sostenendo la sufficienza del dato normativo esistente a risolvere i conflitti che queste innovazioni portano con sé e che non vi sia, pertanto, bisogno di uno studio specifico di tali

---

[4] In questo lavoro si impiegherà indifferentemente il vocabolo robot, algoritmo, macchine intelligenti etc.: d'altra parte nella letteratura che si occupa del fenomeno dell'Intelligenza Artificiale, divenuta estremamente ampia negli ultimi anni, è ricorrente il rilievo circa l'incertezza del vocabolo da utilizzare con riferimento all'ente che svolge questo genere di applicazioni: talvolta si discute di robot, talaltra di algoritmo o, ancora, di agente elettronico o digitale, umanoide, etc.: in luogo di tanti, si v. G. Teubner, *Soggetti giuridici digitali?*, cit., 19-20; A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *Riv. Biodir.*, 2019, 8.

[5] Parlamento europeo, *Norme di diritto civile sulla robotica. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, (2015/2103(INL), 17 febbraio 2017, in *eur-lex.europa.eu.* Sulla risoluzione si vedano i commenti di G. Taddei Elmi e F. Romano, *Il robot tra* ius condendum *e* ius conditum, in *Inf. Dir.*, 2016, 115; S. Oriti, *Brevi note sulla risoluzione del parlamento europeo del 16 febbraio 2017 concernente le norme di diritto civile sulla robotica*, in *ratioiuris*, 2017, N. Busto, *La personalità elettronica dei robot: logiche di gestione del rischio tra trasparenza e fiducia*, in *Ciberspazio e dir.*, 2017, 499 e G. Passagnoli, *Regolamento giuridico e tutele nell'intelligenza artificiale*, in *Pers. merc.*, 2019, 79.

conflitti. Tale argomento è comunemente richiamato con la formula, *Law of the orse* , utilizzata a metà anni Novanta per negare dignità scientifica al *cyberlaw*, il quale, al pari appunto di un ipotetico corso di diritto dei cavalli, non presenterebbe un tratto di organicità e, per la comprensione delle regole sugli scambi o sulla responsabilità, nulla aggiungerebbe alla conoscenza delle «*general rules*» capaci di «*illuminate the entire law*"[6]. Oltre che su questo argomento, la posizione conservatrice, peraltro, sostiene anche che sarebbe inopportuno intervenire normativamente su di una realtà quale la tecnologia che, per definizione, presenta un elevato tasso di dinamicità[7]. Simile osservazione poggia infine su quella tradizionale e ricorrente illusione che vuole la tecnica come un qualcosa di neutrale, che presenta vantaggi per tutti e non determina conflitti, ma, al più, li risolve in modo inedito[8].

A differenza di quanto generalmente accade con le rivoluzioni politiche, tale posizione conservatrice, però, non esaurisce il panorama della letteratura scientifica, abitato anche da chi si sforza di discutere le ricadute giuridiche delle innovazioni tecniche[9]. Senza necessariamente propendere per la tesi che afferma la necessità di una legge per ogni nuova scoperta (c.d. eccezionalismo), tale secondo atteggiamento sostiene che l'esame e lo studio delle concrete implicazioni giuridiche delle innovazioni possa portare all'estensione di certe norme o alla rivisitazione di altri istituti, la cui *ratio* sottostante mal si adatta al nuovo mondo[10]. A tal proposito si deve ben ribadire come tali risultati siano solamente eventuali: essi non sono una automatica conseguenza della novità scientifica, ma dipendono dal concreto manifestarsi di una

---

6 F.. Easterbrook, *Cyberspace and the Law of the orse* , in *Univ. Chi. Legal. Forum*, 1996, 207.

7 Con riferimento all'intelligenza artificiale, un saggio di tale secondo argomento è offerto da A. Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom, Arlington, 2016* e da D. Castro – M. McLaughlin, *Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence*, 2019, in itif.org.

8 Sul tema si veda la discussione svolta in G. Mobilio, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *Riv. Biodir*., 2020, 406.

9 Alla tesi di Easterbrook, si oppongono almeno due non meno famose repliche L. Lessig, *The Law of the orse: What Cyberlaw Might Teach* , in *arv. Law Rev*., 1999, 501 e, più di recente, R. Calo, *Robotics and the Lessons of Cyberlaw,* in *Cal. Law Rev*., 2015, 513.

10 U. Ruffolo, *Intelligenza Artificiale,* machine learning *e responsabilità da algoritmo*, in *Giur. it*., 2019, 1690 e 1696.

lacuna (es. *responsability gap*)[11]. Ad esempio, è noto come, davanti ai mutamenti propri della rivoluzione industriale, il ceto dei giuristi abbia lavorato affinché le regole della responsabilità civile – tradizionalmente imperniate sul criterio della colpa – mutassero così da rendere più effettiva la possibilità per il lavoratore infortunato di ottenere una tutela[12].

Tra le due posizioni – quella conservatrice e quella adeguatrice – sembra essere preferibile la seconda. In tal senso, a ben vedere, milita l'esigenza propria del diritto quale prodotto della società di assicurare una elevata sintonia tra regola e regolato[13]. Come scrisse uno dei massimi civilisti del secolo scorso, la ragione del notevole interrogarsi da parte dei giuristi circa le rivoluzioni tecnologiche idonee ad alterare la materia regolata si spiega, infatti, con la consapevolezza circa il fatto che il diritto conosce il suo più grande rischio di svalutazione nella perdita della «effettiva capacità regolativa"[14]. Da ciò, allora, una prima ragione per sostenere la verifica del rapporto tra regola e regolato. Non solo. Sempre nel senso della preferenza dell'atteggiamento che ricerca una adeguatezza tra la norma e la realtà milita anche il rilievo per cui «l'estensione delle regole già stabilite, con i rafforzamenti e gli adattamenti necessari» è necessario per assicurare che anche nel nuovo contesto i valori fondamentali della nostra società – es. i diritti umani, la libertà e la dignità dell'individuo – siano rispettati[15].

---

11 Il punto è sostanzialmente pacifico in dottrina. Per tutti si veda, A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto: una prima ricognizione*, in *Nuova giur. civ. comm.*, 2012, 497: «Solo qualora non si dovesse riscontrare una soluzione adeguata, si potrà considerare la possibilità di introdurre nuove regole o di modificare quelle esistenti. In altre parole, si intende evitare un approccio eccezionalista, che è tipico di chi considera a priori le norme attuali inadeguate a disciplinare le questioni che emergono dagli sviluppi tecnologici, ritenendo, quindi, sempre necessario creare nuove regolamentazioni ad hoc».

12 P. Rosanvallon, *L'état en France. De 1789 a nos jours*, Paris, 1990, 175. Per la più generale osservazione per cui «*a technology is exceptional when its introduction into the mainstream requires a systematic change to the law or legal institutions in order to reproduce, or if necessary displace, an existing balance of values*", si veda *R. Calo, Robotics and the Lessons, cit., 552-553*.

13 In argomento, imprescindibile è la lettura di N. Irti – E. Severino, *Dialogo su diritto e tecnica*, Roma-Bari, 2001.

14 S. Rodotà, *La vita e le regole*, Milano, 2018, 202.

15 S. Rodotà, *La vita e le regole*, cit., 87. Come vedremo, una prima eco di questa impostazione si ha già nella *Risoluzione*, cit., lett. O e a cui *adde*, lett. U e V.

7.3. La lezione di Rodotà: afferrare il nuovo per darvi la giusta forma

Una volta convenuto sulle opportunità di studiare il nuovo contesto determinato dalle innovazioni tecniche dal punto di vista giuridico occorre, però, prestare particolare attenzione al come procedere. A tal riguardo, si può muovere proprio da quella compianta dottrina sopra richiamata a proposito del rischio di svalutazione e della necessità del diritto per il rispetto, anche nel nuovo contesto, dei valori fondamentali.

Rodotà svolgeva quella riflessione sull'esigenza di evitare una perdita dell'effettiva capacità regolativa del diritto e sulla impossibilità per il diritto di "distogliere lo sguardo" a margine dell'avvenuta riproduzione di una pecora per clonazione (il "caso" *Dolly*, 1997). D'altra parte, la possibilità aperta dalla tecnica di una riproduzione agamica dell'uomo interroga il diritto e, ciò, in quanto essa segna il superamento di un ordine segnato dal monopolio della natura sulla creazione della vita umana e animale[16]. Nella soddisfazione di questa domanda di regole che diano forma al mondo nuovo (perché non più dominato dalle sole leggi della natura), il diritto (privato) commette un grave errore, sia quando non vi provvede sia quando, secondo la convincente impostazione critica di Rodotà, procede al solo fine di rassicurare la società turbata dalla scienza, mimando, peraltro artificialmente, il limite che questa ha superato[17]. Nel momento in cui i giuristi rifiutano

---

[16] Sul punto si veda, almeno, S. Rodotà, *Sul buon uso del diritto e i dilemmi della clonazione*, in *Riv. crit. dir. privato*, 1999, 561; . Atlan, *Possibilità biologiche, impossibilità sociali*, in *ivi*, 571; M. Salvi, *Biotecnologie e bioetica, un ritorno alla metafisica? Terapia genica in utero, clonazione umana e lo statuto morale dell'embrione*, in *ivi*, 587; C.R. Sunstein, *La Costituzione e la clonazione*, in *ivi*, 599; S. Stammati, *Costituzione, clonazione umana, identità genetica*, in *Giur. costit.*, 1999, 4067; F.D. Busnelli, *Il problema della clonazione riproduttiva*, in *Riv. dir. civ.*, 2000, I, 175; P. Donadoni, *La disciplina biogiuridica della clonazione umana – Rassegna di materiali nazionali e sovranazionali*, in *Mat. storia cultura giur.*, 2000, 247.

[17] S. Rodotà, *La vita e le regole*, cit., 16; Id., *Il diritto di avere diritti*, Roma-Bari, 2017, 351-352. Per ciò che concerne la clonazione, è noto, sul piano normativo, la risposta fu quella di prevedere un divieto, assoluto, per ogni ipotesi di intervento tecnico il cui scopo fosse quello di creare – *rectius*, riprodurre – un essere umano geneticamente identico a un altro essere umano vivo o morto (così, l'art. 1 del *Protocollo addizionale alla Convenzione per la protezione dei diritti dell'uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina, sul divieto di clonazione di esseri*

di confrontarsi con la nuova realtà e non «afferrano» il nuovo, evitando di «dare corpo ai principi che a quel mondo nuovo possono dare forma» e limitandosi a ripetere principi di riferimento propri di altri sistemi regolativi (religione, economia, scienza, etc.), il diritto si espone al rischio di una sua svalutazione, rappresentata, appunto, da una perdita di effettiva e autonoma capacità regolativa, oltre che della scomparsa dei diritti fondamentali[18].

Orbene e come già detto (*supra*, §1), anche le innovazioni della tecnologia digitale che più caratterizzano questa età della storia umana interrogano il diritto: esse sono tali da porre in discussione il rapporto tra le regole tradizionali e ciò che di quel regolato è più interessato dal digitale, nonché la tenuta dei diritti civili, politici e sociali. Peraltro, anche queste innovazioni si pongono in termini di sfida[19]: le novità insite nei progressi costringono il giurista a rivisitare il dato normativo esistente e a costruire distinte discipline di effettivo governo del "mondo nuovo" in cui siamo entrati da più di un qualche decennio, così da «indirizzare l'intelligenza artificiale verso il bene degli individui e della società»[20]. Si tratta, inoltre, di una sfida decisiva, epocale[21]: attesa la centralità di queste innovazioni nella nostra società (basti pensare che il digitale è stato una delle poche costanti tra il mondo pre-Covid19 e il mondo pandemico), il diritto – si dice – non può sottrarsi e scegliere di non combatterla, rinunziando a disciplinare i conflitti caratterizzati e caratterizzanti il digitale[22]. A ben vedere, come davanti ai progressi della bioetica, anche davanti alle innovazioni proprie dell'IA serve

umani, sottoscritto a Parigi il 12 gennaio 1998 nell'ambito del Consiglio d'Europa; nella stessa direzione, si veda poi l'art. 3, EUCFR, nonché la risoluzione non vincolante dell'Assemblea generale delle Nazioni Unite sull'*uman Cloning* (UN GAOR, 59th Session, UN Doc., A/280 (2005)).

18 S. Rodotà, *Il diritto di avere diritti*, cit, 352-353.

19 Il Parlamento Europeo parla espressamente di "sfide" poste dall'apprendimento automatico ai principi di non discriminazione, giusto processo, trasparenza e comprensibilità dei processi decisionali: *Risoluzione*, cit., lett. . In dottrina, si v., in luogo di tanti, U. Pagallo, *Algoritmi e conoscibilità, Riv. fil. Dir*., 2020, 94, 101.

20 G. Sartor, *Introduzione*, in *Riv. fil. dir*., 2020, 69.

21 G. Pascuzzi, *Il diritto nell'era digitale*, Bologna, 2020, 24.

22 *Ex multis*, A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto*, cit., 495; E. Palmerini, *Robotica e diritto: Suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. prev*., 2016, 1815; U. Pagallo, I*ntelligenza artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sist. Intell*., 2017, 617; G. Teubner, *Soggetti giuridici digitali?*, cit., 26; A. D'Aloia, *Il diritto verso "il mondo nuovo"*, cit., 9. Sulla centralità del fenomeno e connessa inevitabilità della regolazione, si. v. anche *Risoluzione*, cit., lett. B, E, G, I.

evitare uno scollamento tra la regola e il regolato. Occorre quindi ricostruire, ora con interpretazioni ora con interventi del legislatore, un quadro normativo adatto alla verità effettuale della cosa e in grado di governare il nuovo mondo, fuggendo lacune e vuoti e assicurando la continuità dei valori fondamentali della nostra società23. Insomma, "afferrare il nuovo" e "dare corpo ai principi che a quel mondo nuovo possono dare forma".

7.4. Afferrare il nuovo e il mito del robot intelligente

Il compito di "afferrare il nuovo" non risulta facile e ciò, in particolare, per una rivoluzione, quale quella digitale, che presenta un notevole ambiguità. Per un verso, molte delle applicazioni tecnologiche che caratterizzano il nostro quotidiano non erano pensabili e pensate dalle generazioni precedenti. Per altro verso, l'idea di una cosa (perché non persona) evoluta (perché animata) alberga nel pensiero umano da tempo immemore[24].

Gran parte dei contributi giuridici aventi ad oggetto la ricerca di una disciplina del robot intelligente fanno ricorso ad immagini con le quali, nel corso della storia, l'uomo ha provato a descrivere la macchina animata. Talvolta, si cita l'etimologia del termine, il cui esordio si vuole risalente al 1923, quale traduzione del vocabolo ceco '*robotnik*' (lavoratore forzato), impiegato dallo scrittore Karel Capek nel suo dramma fantascientifico *Rossum's Universal Robots*, talaltra si richiama il mito di Pigmalione o il personaggio di Frankenstein. Ancora più diffuso è il richiamo alle tre leggi di Asimov, tratte da *Runaround* (1942), e la cui formulazione originaria così si sviluppa: «*A robot may not injure a human being or, through inaction, allow a human being to come to harm; A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law; A robot must protect its own existence as long as such protection does not conflict with the First or Second Law*». Tale tributo artisitico-letterario non è un vizio esclusivo della dottrina giuridica: la stessa famosa *Risoluzione* si apre rilevando come «gli

---

23 Uno sviluppo dei principi di IA in parallelo con quelli della bioetica è proposto da L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, E. Vayena, *AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, 689.

24 G. Wood, *Edison's Eve. A Magical istory of the Quest for Mechanical Life*, New York, 2002.

essere umani» abbiano «fantasticato sulla possibilità di costruire macchine intelligenti, spesso androidi con caratteristiche umane»[25].

L'idea che l'innovazione attuale non sia che una tappa verso il prossimo e certo momento in cui non vi sarà differenza tra uomo e macchina è poi anche alimentata dalla più diffusa narrazione dei progressi dell'intelligenza artificiale: quante volte, infatti, ci si è imbattuti in quella parabola che, continuamente arricchita di riferimenti (o personaggi?: *DeepBlue* che sconfigge Kasparov a scacchi[26], *AlphaGo* che trionfa contro Lee Sedol a Go[27], *Vital* che partecipa al *board* di una società[28], *Sophia* e il suo passaporto[29], *GPT-3* che scrive un articolo per il maggior quotidiano britannico30) e di applicazioni (militari31, finanziarie[32], giudiziali[33], occupazionali[34], etc.), racconta di una macchina lanciata in modo inarrestabile verso (e oltre) l'uomo?

A ben vedere, proprio la circostanza che vuole il mondo nuovo dell'intelligenza artificiale come una rivoluzione il cui esito era già stato anticipato e immaginato (la macchina\persona e il robot intelligente) incide sul perché, anche tra coloro i quali condividono la necessità di verificare la tenuta delle regole rispetto al nuovo mondo, sia tanto difficile convenire su ciò che va afferrato e sia facile imbattersi nella discussione di scenari non attuali[35]. Si pensi, in particolare, alla

---

25 *Risoluzione*, cit., lett. T.

26 https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/.

27 M. Tegmark, *Vita 3.0. Essere umani nell'era dell'intelligenza artificiale*, Milano, 2018, 121.

28 M.L. Montagnani, *Flussi informativi e doveri degli amministratori di società per azione ai tempi dell'intelligenza artificiale*, in *Pers. Merc.*, 2020, 86.

29 U. Pagallo, *Vital, Sophia, and Co. - The Quest for the Legal Personhood of Robots*, in *Information*, 2018, 230.

30 GPT-3, *A robot wrote this entire article. Are you scared yet, human?*, in *Guardian*, 8 settembre 2020.

31 Per una prima discussione in proposito, G. Tamburrini, *Autonomia delle macchine e filosofia dell'intelligenza artificiale*, in *Riv. filos.*, 2017, 263.

32 F. Pistelli, *Algoritmi e contratti nel sistema finanziario*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, 249.

33 Si pensi al *software* Compas, utilizzato da diverse corti statunitensi per valutare la probabilità di recidiva. In argomento, Aziz Z. uq, *Racial Equity in Algorithmic Criminal Justice*, in *Duke Law Journal, 2019,* 1043; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Riv. Biodir.*, 2019, 71; G. Pascuzzi, *Il diritto nell'era digitale*, cit., 293; più in generale sul tema, si veda: M. Luciani, *La decisione robotica*, in *Riv. AIC*, 2018, 872.

34 C. Casadei, *Per Esselunga primo job day di massa interamente virtuale*, in *Il Sole 24-ore*, 10 settembre 2020 (*www.ilsole24ore.com*).

35 Per tutti, K. Kurzweil, *The Singularity is Near: When umans Transcend Biology* , New York, 2005 e N. Bostrom, *Superintelligenza, Tendenza. Pericoli. Strategia*, Torino, 2018.

ampia e vivace discussione circa la personalità elettronica e della piena soggettività dei robot. Come noto, infatti, a fronte di chi nega alle presenti tecniche digitali la capacità di innovare il discorso giuridico e ritiene le *general rules* una disciplina sufficiente, vi è chi esagera la portata effettiva delle scoperte attuali. Come se convinti che le recenti innovazioni digitali siano una tappa del percorso che dal sogno della macchina intelligente inevitabilmente conduce al robot completamente autonomo, tali giuristi accettano, ancorché - giova ripeterlo - in anticipo sui tempi, di discutere l'attribuzione di diritti e doveri a tali enti immaginando di essere già davanti alla macchina completamente autonoma[36]. Più che sulla realtà del regolato, questa apertura alla c.d. piena personalità elettronica poggia sulla capacità che i continui progressi dell'attuale contesto (la realtà) hanno di illudere l'uomo di essere vicino alla fine della storia della macchina come prodotto e alla realizzazione del, già tante volte immaginato, sogno del robot intelligente e pienamente autonomo[37].

Orbene, invece di indugiare nella contrapposizione tra *Singularitarians* e *Aitheists* 38 o in altri assolutismi (persona o *res*)[39] che, come

---

[36] Tale atteggiamento, peraltro, non si ritrova solo in chi auspica il pieno riconoscimento della personalità giuridica alle macchine (più o meno) intelligenti, ma, curiosamente anche in chi nega *in toto* la discussione. Come è stato di recente osservato, infatti, «la vera ragione della resistenza a riconoscere la soggettivazione (parziale) quale unisca strategia dogmatica per la comprensione dell'intelligenza artificiale nel diritto civile non è la troppa distanza tra intelligenza artificiale e umana, ma l'eccesso di prossimità» (P. Femia, *Introduzione. Soggetti responsabili Algoritm e diritto civile*, in G. Teubner, *Soggetti giuridici digitali?*, cit., 10).

[37] D'altra parte, in qualche modo sintomatico di quanto si dice nel testo circa il tratto non attuale della discussione sulla piena personalità dell'IA, è la circostanza per cui l'articolo più citato che ne sostiene l'attribuzione all'IA risalga a un contesto (1992) in cui il quotidiano era certamente lontano dagli attuali progressi delle macchine (es. privo di internet!): L.B. Solum, *Legal Personhood for Artificial Intelligences*, in *North Carol. L. Rev*., 1992, 1231.

[38] L. Floridi, *Should we be afraid of AI?*, in *Aeon*, 2016 (aeon.co).

[39] Centrale nella esperienza giuridica occidentale, come noto, è la dicotomia che divide ogni entità che sia diversa dalla *actio* in persona o cosa (*D*., 1.5.1.), così che «cosa è la *non*-persona e persona la *non*-cosa» (R. Esposito, *Le persone e le cose*, Torino, 2014, 3). I due termini sono posti dalla tradizione in una relazione di strumentalità (Aristotele, *Pol*. I, 4, 1253b 25 – 1254a 18), dove «il ruolo delle cose è quello di servire, o comunque di appartenere, alle persone» e quello della persona è l'esercitare «una padronanza» sulle cose) e sono caratterizzati da una notevole flessibilità: attesa l'artificialità del diritto, infatti, sono numerose le entità che, in certi momenti e in certi luoghi, rivestono una qualifica differente da quella assunta in precedenza o ricoperta altrove (a tal proposito, l'esempio più diffuso è il riconoscimento della personalità giuridica a fiumi (Te Awa Tupua Act 2017, s. 14: *Te Awa Tupua is a legal entity, and has all the*

recentemente osservato rispetto ad analoghi discorsi di espansione della soggettività giuridica, sono eccessivamente ideologici40, è necessario afferrare la realtà per quello che è. Per un verso, occorre riconoscere che, allo stato, la possibilità di una macchina pienamente autonoma non è attuale, né tanto meno prossima: nessuna delle diverse applicazioni che compongono la parabola fa a meno dall'apporto umano (che, ora come programmatore ora come utilizzatore, resta pur sempre il soggetto partecipe delle diverse azioni) e nessuna macchina ha mai raggiunto i diversi tratti che vengono comunemente riconnessi all'intelligenza umana[41]. In questo contesto, allora, l'attribuzione della piena personalità elettronica non può che sollevare dubbi e preoccupazioni circa un suo possibile carattere abusivo, traducendosi in un ostacolo formale all'individuazione dell'effettivo responsabile[42]. Per altro verso, invece di trincerarsi dietro l'impossibilità della macchina di provare emozioni, di mimare l'intelligenza umana o comunque di raggiungere quell'indice che, in modo arbitrario e a-tecnico, si ritiene idoneo a giustificare l'equiparazione alla persona[43], si deve riconoscere che una discussione sulla soggettività si renda già oggi necessaria[44]. In effetti, non si può negare che molte delle odierne applicazioni

rights, powers, duties and liabilites of a legal person), foreste (es. Te Urewera Act 2014, s. 12: *Te Urewera is a legal entity, and has all the rights, powers, duties and liabilites of a legal person*) operato dal legislatore neozelandese nonché il (lento) processo di emersione dei diritti degli animali (da ultimo definiti come «esseri senzienti», ex art. 13, TFUE).

40 Per una intelligente critica di quella tendenza a sviluppare il discorso giuridico della natura in termini di passaggio da *res* a *persona*, si veda M. Spanò, *Perché non rendi poi quel che prometti allor? Tecniche e ideologia della giuridificazione della natura*, in Y. Thomas – J. Chiffoleau, *L'istituzione della natura*, Macerata, 2020, 104.

41 In questo senso, G. Teubner, *Soggetti giuridici digitali?*, cit., 30, nonché l'*Open Letter to the European Commission Artificial Intelligence and Robotics*, in http://www.robotics-openletter.eu/. Si tratta della lettera con cui centinaia di scienziati hanno criticato la proposta contenuta all'art. 59, *f*) *Risoluzione*, cit., di istituire la personalità elettronica. Come noto, la Commissione non ha accettato quella proposta del Parlamento.

42 Sul rischio dei «*robots as liability shields*» si v., per tutti, J.J. Bryson, M.E. Diamantis, T.D. Grant, *Of, for, and by the people: the legal lacuna of synthetic persons,* in *Artif. Int. Law*, 2017, 285.

43 U. Ruffolo, *Intelligenza Artificiale,* machine learning, cit., 1702-1703.

44 Si v., ad esempio, le diverse ricostruzioni circa una capacità e una soggettività parziale operate da U. Pagallo, *The Law of Robots. Crime, Contracts and Torts*, Dodrecht-eidelberg -New York-London, 2013, 103 e da G. Teubner, *Soggetti giuridici digitali?*, cit., nonché la tesi, allo stato isolata, per cui già l'attuale contesto normativo statunitense consentirebbe l'attribuzione di diritti e doveri all'IA avanzata da S. Bayern, *The Implications of Modern Business-Entity Law fot the Regulation of Autonomous Systems*, in *Stan. Tech. Law Rev*., 2015, 93.

presentano elementi di tensione con la tradizionale categoria di strumenti[45]. A ben vedere, più che nel (mito del) robot intelligente, il nuovo da afferrare risiede proprio in queste tensioni ed è a queste a cui occorre dare la giusta forma.

7.5. Afferrare il nuovo: l'IA, oggi

Uno dei pochi punti fermi e condivisi nella letteratura giuridica attiene alla inesistenza di una definizione di intelligenza artificiale[46]. Estranea al testo del *seminal work* di Turing[47], la formula dell'IA ricorre per la prima volta a metà degli anni Cinquanta del secolo scorso, con l'intento di indicare un «*attempt*» per «*to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves*»[48]. A questa prima fase, è seguito un periodo in cui l'obiettivo perseguito dalla comunità nella costruzione della macchina non è più rappresentato dalla sua idoneità a riprodurre il cervello dell'uomo (*Artificial General Intelligence*, AGI), ma piuttosto nella soluzione di specifici problemi.

Oggi vi è chi definisce la IA come «*the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable*»[49]. Altri, invece, la definiscono come «la scienza della produzione di macchine e sistemi volti all'esecuzione di compiti che, qualora realizzati da essere umani, richiederebbero l'uso dell'intelligenza per risolvere problemi di apprendimento e conoscenza, di ragionamento e pianificazione»[50]. Ancora, di recente, si è sostenuto che per IA si debba intendere il «*field that studies the synthesis and analysis of computational*

---

45 Per tutti, *Risoluzione*, cit., lett. AB.

46 In tal senso, tra gli altri, G. Pascuzzi, *Il diritto nell'era digitale*, cit., 289; A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto*, cit., 497 e A. D'Aloia, *Il diritto verso "il mondo nuovo"*, cit., 8.

47 A. Turing, *Computing machinery and intelligence*, in *Mind*, 1950, 433.

48 J. McCarthy, M.L. Minsky, N. Rochester, C.E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955, 1.

49 J. McCarthy, *What is Artificial Intelligence?*, 2007, 1 in http://www-formal.stanford.edu/jmc/.

50 U. Pagallo, I*ntelligenza artificiale e diritto*, cit., 615. In senso analogo, già, M.L. Minsky, *Semantic information processing*, Cambridge, 1969.

agents that act intelligently»[51]. Anche con riferimento al piano normativo e para-normativo, è dato registrare una notevole pluralità di soluzioni. Tra queste, particolare attenzione ha ricevuto quella proposta a livello europeo lo scorso anno e che così recita: «*Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analyzing how the environment is affected by their previous actions*»[52]. Orbene la mancanza di un consenso attorno a una determinata definizione è spiegata con la difficoltà di affermare «*a bright-line distinction between what constitutes AI and what does not*»[53] ed è impiegata per suggerire ai legislatori di «*to find specific definitions which could prove useful to address narrowly identified problems posed by AI applications*»[54].

Per quanto nella letteratura sull'IA sia ugualmente dibattuto il riferimento all'ente che svolge le applicazioni, ai fini del presente lavoro si può muovere dalla diffusa distinzione del robot in tre distinte categorie: i robot tele-operati, le cui azioni sono completamente controllate dall'uomo e che configurano più o meno semplici strumenti dell'operatore; i robot autonomi, che hanno l'abilità di svolgere un compito senza alcun intervento umano, ma seguendo un programma che gli fornisce regole di comportamento; i robot cognitivi, dotati di un sistema per auto programmarsi, pianificare e apprendere dalla propria esperienza, grazie ad algoritmi evolutivi[55]. All'interno di questa classificazione, poi, si possono isolare i due tratti più rilevanti e centrali: il concetto di autonomia e quello di auto-apprendimento. La prima è

---

51 D. Poole, A. Mackworth, *Artificial Intelligence*, Cambridge, 2017 (consultabile anche in *artint.info*).

52 European Commission's igh -Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* , 2019, 36.

53 National Science and Technology Council Committee, *Preparing for the future of Artificial Intelligence*, 2016, 7 (in www.whitehouse.gov).

54 A. Bertolini, *Artificial Intelligence and Civil Liability*, 2020, 31.

55 La classificazione, che si deve al progetto EUROP (European Robotics Technology Platform) ed è consultabile in www.eu-robotics.net, è ripresa, tra gli altri, da: G. Taddei Elmi e F. Romano, *Il robot*, cit., 124; L. Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Pol. Dir.*, 2018, 716 e, prima, A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto*, cit., 498.

definita dalla *Risoluzione* come quella «capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna». Si tratta di una capacità di «natura puramente tecnologica e il suo livello dipende dal grado di complessità con cui è stata progettata l'interazione di un robot con l'ambiente». Il secondo tratto caratterizzante l'IA odierna è rappresentato dalla sua capacità cognitiva, con ciò intendendo «la capacità di apprendere dall'esperienza e di prendere decisioni quasi indipendenti»[56].

Così individuato l'insieme di applicazioni a cui prestare attenzione, occorre porre in evidenza come, allo stato attuale, le funzioni prevalenti dell'IA concernono i processi di assunzione delle decisioni e si distinguono prevalentemente in sistemi decisionali automatici interamente basati su IA (es. auto senza conducenti) e in sistemi di supporto delle decisioni altrui (es: algoritmi di valutazione del cliente nella formazione del contratto)[57].

7.6. Afferrare il nuovo: rischi e criticità dell'IA oggi

Questo complesso utilizzo dell'IA è idoneo a determinare dei risultati che pongono in crisi gli ordinari criteri di imputabilità della responsabilità e che comportano inedite forme di lesione di diritti fondamentali, richiedendo al diritto uno sforzo interpretativo e, in subordine, legislativo.

Per quanto concerne il profilo della responsabilità, tale tensione è evidente nel confronto tra le applicazioni dell'IA, caratterizzata da autonomia e autoapprendimento, e il contesto normativo di diritto privato europeo, rappresentato dalla fondamentale direttiva sui prodotti difettosi, che compie quest'anno trentacinque anni[58], e dalle più recenti normative in materia di dispositivi medici[59], di sicurezza generale dei

---

56 Cons. Z e AA, *Risoluzione*.

57 A. Mantelero, *Come regolamentare l'intelligenza artificiale*, 2019, in www.agendadigitale.eu. Sul primo aspetto, si v. per tutti, F.P. Patti, *The European Road to Autonomous Vehicles*, in *Ford. Int. Law Journ*., 2019, 125. Sul secondo, invece, F. Pistelli, *Algoritmi e contratti*, cit., 256, nonché A. Davola, *La valutazione del merito di credito del consumatore*, in (a cura di) E. Pellecchia, L. Modica, *La riforma del sovraindebitamento nel codice della crisi d'impresa e dell'insolvenza*, Pisa, 2020, 146.

58 Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, in *OJ L 210, 7.8.1985, 29.*

59 Direttiva 93/42/CEE del Consiglio, del 14 giugno 1993 concernente i dispositivi medici, in *GU* L 169 del 12.7.1993, 1.

prodotti[60], di macchine[61], di giocattoli[62], di strumenti di misura[63] e di apparecchiature radio[64]. Come è stato notato anche di recente, questo *corpus* normativo – creato «in larga parte fra gli anni '70 e '80 del secolo passato, quando si usava il Commodore 64 e nelle case il robot era l'aspirapolvere»[65] – lascia aperte diverse questioni in merito ai danni causati dai robot autonomi e dotati di capacità di adattamento e quindi capaci di azioni imprevedibili per il produttore, programmatore, proprietario e per l'utente66. Innanzitutto, ci si domanda se la direttiva sui prodotti difettosi (archetipo di questo *corpus*) ricomprenda i sistemi di IA e riguardi i soli consumatori. In secondo luogo, si osserva quanto risulti complicato, attesa l'opacità e complessità dei sistemi dell'IA, consentire, sulla base dell'attuale contesto normativo euro-unitario, l'individuazione del soggetto effettivamente responsabile e come l'onere probatorio dalla stessa richiesta non sia facilmente assolvibile[67].

Tale incertezza è particolarmente critica e rischiosa per la tenuta dei diritti fondamentali. Difatti, anche maliziosamente opponendo la pretesa neutralità dell'IA al cervello dell'uomo, le cui decisioni sappiamo essere influenzate da una serie notevole di pregiudizi, si assiste sempre più spesso a un impiego dell'IA quale sistema di supporto di decisioni altrui concernenti aspetti centrali della vita delle persone e che, come tali, sono protetti quali diritti fondamentali[68]. Orbene, la cronaca

---

60 Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti, in *OJ L 11, 15.1.2002, 4.*

61 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 (rifusione), in *GU L 157 del 9.6.2006, 24.*

62 Direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli, in *GU L 170 del 30.6.2009, 1.*

63 Direttiva 2014/32/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014 , concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di strumenti di misura (rifusione), in *GU L 96 del 29.3.2014, 149.*

64 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/C, in *GU L 153 del 22.5.2014, 62.*

65 A. Mantelero, *Come regolamentare l'intelligenza artificiale*, cit.

66 *Risoluzione*, cit., lett. AE, AG, A, AI.

67 *Ex multis*, G. Teubner, *Soggetti giuridici digitali?*, cit., 25 e A. Bertolini, *Artificial Intelligence and Civil Liability*, cit., 57-59.

68 Si pensi alla posizione recente e autorevole che giustifica il ricorso all'IA proprio evidenziando come, a differenza di quelli che caratterizzano l'uomo, i bias dell'algoritmo possono essere corretti ed eliminati, una volta individuati: J. Kleinberg, J.

recente smentisce questo assunto (neutralità dell'IA) ed è piena di denunce circa il c.d. *bias in machine learning* o *AI bias*. L'effetto di questi errori di valutazione è spesso penalizzante per minoranze, razziali e non, e, a seconda dell'ambito in cui si manifesta, può rilevare anche come lesione di un diritto fondamentale[69].

7.7. Principi con cui dare forma al nuovo

Davanti a queste criticità e tensioni, lo si è detto, parte della comunità giuridica si sforza di trovare soluzioni, per un verso, adeguate alla materia, e, per l'altro, idonee ad assicurare la continuità dei principi fondamentali del nostro ordinamento. Come riconosciuto dalla stessa *Risoluzione*, è necessario che «gli sviluppi nel campo della robotica e dell'intelligenza artificiale siano pensati in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui»[70]. Per raggiungere questo obiettivo, l'interprete e il legislatore possono ricorrere a diversi principi, che appunto diano al nuovo una forma giusta perché conforme ai nostri valori fondanti.

Ad esempio, con riferimento alla responsabilità aquiliana e fermo restando la possibilità di rinvenire nel disciplina nazionale una base giuridica per una interpretazione che sappia fornire regole adeguate sull'illecito determinato da algoritmo[71], è noto che l'opinione maggioritaria propende per l'adozione di regole uniformi, quanto meno per lo spazio europeo, sottolineando come solo in tal modo si può provare a offrire una effettiva regolazione del fenomeno che presenta una dimensione globale[72]. Rispetto a questa ipotesi legislativa, il Parlamento Europeo ha suggerito l'adozione di una disciplina improntata al principio di effettività della tutela, di guisa che il futuro strumento legislativo «non dovrebbe in alcun modo limitare il tipo o l'entità dei danni che possono essere risarciti, né dovrebbe limitare le forme di risarcimento che possono essere offerte alla parte lesa per il semplice fatto che il danno è provocato da un soggetto non umano», e a quello di

---

Ludwig, S. Mullainathan, C. R. Sunstein, *Discrimination in the Age of Algorithms*, in *Jour. Legal Anal.*, 2018, 113.

69 *Per degli esempi si veda la ricerca di V.* Eubanks, *Automating Inequality: ow igh -Tech Tools Profile, Police and Punish the Poor*, New York, 2018.

70 *Risoluzione*, cit., lett. O.

71 U. Ruffolo, *Intelligenza Artificiale*, cit., 1689.

72 G. Passagnoli, *Regolamento giuridico e tutele*, cit., 81. Considerazioni più prettamente politiche sono invece rappresentate in *Risoluzione*, cit., lett. R e S.

proporzionalità, cosi che «una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere proporzionale all'effettivo livello di istruzioni impartite al robot e al grado di autonomia di quest'ultimo»[73]. A livello dottrinale, invece, si è auspicato che la disciplina della responsabilità civile dell'IA passi per regolamenti *ad hoc*, così da assicurare la massima uniformità possibile e, al contempo, da evitare norme vaghe e troppo generali in favore di soluzioni tagliate il più possibile sulla singola e specifica innovazione[74].

Invece, nel discorrere della responsabilità contrattuale connessa all'impiego di IA – es. inadempimento del robot nell'esecuzione del contratto - merita di essere segnalata la proposta di riconoscere ai robot una soggettività giuridica parziale avanzata da Gunther Teubner, la quale fa perno sul principio di eguaglianza, ossia su quell'imperativo «che – per gli eventi dannosi e per gli altri conflitti sociali pervenuti al cospetto del diritto – anche nello spazio digitale l'eguale sia trattato in modo eguale e il diseguale in modo diseguale»[75]. Dinnanzi al rischio di autonomia, ossia quello che «scaturisce dalla condotta, in linea di principio imprevedibile, degli algoritmi con autoapprendimento»[76], il grande giurista tedesco propone di considerare ciò che lui chiama «agente software» - e definisce come delle unità individue di interazione con gli uomini nei cui interessi prendono le decisioni – nei termini di un ausiliario del *dominus* \ principale, di guisa che questi, anche quando a lui non si imputabile alcuna negligenza, risponderà degli inadempimenti della macchina *ex* art. 278 BGB[77]. Il fondamento di questa interpretazione analogica che consente di attribuire la responsabilità per l'inadempimento della macchina la cui condotta non è prevedibile risiede, lo si è detto, nel principio di eguaglianza: è questo che «reclama la responsabilità» del *dominus*. Difatti, rileva Teubner, se per l'esecuzione del contratto fosse impegnato, in luogo del robot intelligente, un uomo, non vi è dubbio che il suo principale risponda

---

73 *Risoluzione*, cit., 52 e 56.

74 A. Bertolini, *Artificial Intelligence and Civil Liability*, cit., 88.

75 G. Teubner, *Soggetti giuridici digitali?*, cit., 127. Sull'eguaglianza nella costruzione della soggettività parziale dei robot operata da T., si v. anche la bella pagina di P. Femia, *Introduzione*, cit. 15.

76 G. Teubner, *Soggetti giuridici digitali?*, cit., 38.

77 G. Teubner, *Soggetti giuridici digitali?*, cit., 82.

dell'inadempimento altrui, non si può ammettere che il dominus sia liberato solo perché l'esecuzione sia affidata a un robot intelligente[78].

Connesso alle questioni attinenti la responsabilità, aquiliana e contrattuale, è poi la proposta di esportare nel «governo della società algoritmica» il principio di spiegabilità che, sotteso al diritto di contestazione ex art. 22 GDPR, si sostanzia sia nel diritto a comprendere come la tecnologia funzioni sia nel definire chi debba dar conto per come essa funziona[79]. Dall'estensione di tale diritto alle applicazioni IA potrebbe discendere un obbligo di rendere disponibili, secondo una modalità «sufficientemente comprensiva», i dati che spiegano come abbia funzionato l'algoritmo e chi ne sia il responsabile. L'effetto di questa estensione del principio di spiegabilità dalla disciplina sul trattamento dei dati personali all'IA sarebbe notevole. Qualora il titolare del trattamento sostenga che, in ragione della complessità e inconoscibilità dell'algoritmo, egli non può fornire spiegazioni sul funzionamento lesivo della sfera altrui, egli sarà comunque responsabile. In alternativa, qualora quel titolare adempia all'obbligo di spiegazione, il soggetto leso dal funzionamento dell'algoritmo sarà posto nelle condizioni di proteggersi e tutelarsi[80].

Per quanto attiene alla lesione dei diritti fondamentali, infine, è noto come il nostro sistema di tutela non ritenga sufficiente la sola risposta *ex post*. Orbene, proprio muovendo dalla consapevolezza che un approccio incentrato unicamente sulla responsabilità – e quindi successivamente alla lesione della sfera giuridica – sia incompatibile con il livello di protezione dei diritti fondamentali, nella dottrina più avvertita si propone l'estensione alla dinamica dell'IA del principio di precauzione (art. 191, co. 2, TFUE)[81]. In altri termini, al fine di fondare una «regolazione effettiva, di livello sovra-nazionale e sovra-legislativo, riguardante le tecnologie, vòlta ad evitare il verificarsi di violazioni delle libertà fondamentali non più (o molto difficilmente)

---

78 G. Teubner, *Soggetti giuridici digitali?*, cit., 84. Sulla distinzione tra *legal agenthood* e *legal personhood*, si v., per tutti, U. Pagallo, *Vital, Sophia,* cit., 236.

79 U. Pagallo, *Algoritmi e conoscibilità*, cit., 101.

80 U. Pagallo, *Algoritmi e conoscibilità*, cit., 103.

81 Alla previsione eurounitaria, si aggiunga, sempre sul piano normativo internazionale, il principio 15, *Dichiarazione di Rio de Janeiro sull'ambiente e lo sviluppo* (1992): «Al fine di proteggere l'ambiente, gli Stati applicheranno largamente, secondo le loro capacità, il Principio di precauzione. In caso di rischio di danno grave o irreversibile, l'assenza di certezza scientifica assoluta non deve servire da pretesto per differire l'adozione di misure adeguate ed effettive, anche in rapporto ai costi, dirette a prevenire il degrado ambientale».

rimediabili una volta che esse sono state diffuse»[82], si suggerisce di ricorrere al principio di precauzione[83], quale base giuridica idonea ad affermare la necessaria priorità della tutela dei diritti dell'uomo sulla tecnica[84].

In conclusione, contratti, responsabilità e diritti si confrontano con l'IA. Tale confronto agita la comunità degli interpreti che si sforza di definire principi – di effettività, di proporzionalità, di eguaglianza, di spiegabilità e di precauzione, etc. – con cui lottare per diventare una società giusta[85]: d'altra parte, ogni scienza ha i suoi tempi.

---

82 A. Simoncini, *L'algoritmo incostituzionale*, cit., 86.

83 Più in generale, è la stessa Commissione ad avere riconosciuto come il principio trova «applicazione in tutti i casi in cui una preliminare valutazione scientifica obiettiva indica che vi sono ragionevoli motivi di temere che i possibili effetti nocivi sull'ambiente e sulla salute degli esseri umani, degli animali e delle piante possano essere incompatibili con l'elevato livello di protezione prescelto dalla Comunità» (*Comunicazione della Commissione sul principio di precauzione*, 2000, (COM(2000)1 *final*, §3).

84 G. Passagnoli, *Regolamento giuridico e tutele*, cit., 83.

85 E. Garin, *La giustizia*, Napoli, 1968, 83.

8. «*Initial Coin Offering*» ed il mercato delle cripto-attività: riflessioni sugli «*utility token*»

Enzo Maria Incutti

8.1. Rivoluzione digitale e trasformazione tecnologica del settore finanziario

Il settore finanziario è da sempre attento all'innovazione tecnologica e pronto a recepire i cambiamenti radicali che essa determina[1]. Assistiamo, oggi, ad una profonda e rapida ristrutturazione dell'intero mercato finanziario, delle modalità di offerta dei nuovi servizi e delle dinamiche di relazione tra gli operatori ed i consumatori-investitori[2].

Il fenomeno di interazione tra nuove tecnologie e finanza ha condotto ad una sostanziale ridefinizione dei confini tradizionali e dei consolidati modelli di business, conducendo verso un fenomeno ampio e trasversale: quello che, ad oggi, assume il termine identificativo di «*Fintech*»[3].

---

1 «Sebbene l'innovazione nel settore finanziario non sia una novità, gli investimenti nella tecnologia sono aumentati notevolmente e il ritmo dell'innovazione ha subito una considerevole accelerazione», come ha sottolineato la Commissione Europea nel suo *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, COM (2018) 109 def., 2018, spec. p. 2.

2 «Le tecnologie finanziarie (fintech), ossia l'innovazione nel settore dei servizi finanziari resa possibile dalla tecnologia, si sono sviluppate notevolmente negli ultimi anni e stanno influenzando il modo in cui tali servizi sono prodotti e forniti. Le tecnologie finanziarie rappresentano il punto di incontro dei servizi finanziari e del mercato unico digitale. Il settore finanziario è il principale utilizzatore delle tecnologie digitali e un importante motore della trasformazione digitale dell'economia e della società», così Commissione Europea, *cit.*, spec. p. 2.

3 La locuzione *Fintech* è frutto della contrazione tra *finance* e *technology* e trova il corrispettivo nella lingua italiana nel neologismo «*tecnofinanza*». Questa locuzione è entrata a far parte del panorama economico-giuridico dei nostri giorni e si riferisce proprio alla interazione tra le nuove tecnologie e la finanza. Sebbene non vi sia una

Nel mondo finanziario le nuove tecnologie sono orientate ad operare su un piano bifronte. Difatti, si potrebbe sostenere che, da un lato, stia avvenendo una effettiva e totale disintermediazione delle attività e dei servizi e, dall'altro, una parallela e nuova intermediazione[4].

Risulta opportuno (ri)considerare differentemente le attività tradizionali oggi semplificate attraverso i servizi digitalizzati, rispetto ad attività del tutto nuove[5], che impiegano i più moderni strumenti tecnologici, quali sistemi dotati di Intelligenza Artificiale, *smart contract,* algoritmi sempre più sofisticati, *devices* connessi alla rete. Tali distinzioni sul piano empirico, impongono inevitabilmente un approccio differente sul piano regolatorio.

Uno dei principali problemi connessi alla regolamentazione del «*Fintech*» attiene proprio ad una diffusa "opacità regolatoria"[6], dettata

uniforme definizione di tale termine, con esso si potrebbe intendere «un'attività finanziaria alimentata dalle nuove tecnologie e che include l'intera gamma di servizi, prodotti e infrastrutture finanziari», così Commissione per i problemi economici e monetari del Parlamento Europeo, *Relazione sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario* (2016/2243(INI)), 2017, spec. p. 18. Come si sottolinea nello stesso documento, esso riguarda «l'intero settore finanziario in tutte le sue componenti, dal settore bancario a quello assicurativo, i fondi pensione, la consulenza in materia di investimenti, i servizi di pagamento e le infrastrutture di mercato», spec. p. 4. Per un inquadramento generale del fenomeno, *ex multis* v. G. Alpa, *Fintech: un laboratorio per giuristi,* in *Contratto e impresa,* vol. 2, 2019, p. 377 ss.; Aa. Vv., *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale,* in *Quaderni Fintech Consob,* n. 1, 2018.

4 Sulla sottile linea di demarcazione tra nuove attività finanziarie e nuove modalità di servizi tradizionali, v. G. P. La Sala, *Intermediazione, disintermediazione, nuova intermediazione: i problemi regolatori*, in M. Cian, C. Sandei (a cura di), *Diritto del Fintech,* Cedam, Padova, 2020, p. 4 ss. L'Autore, inoltre, sostiene che al fianco di questa flessibile e mutevole distinzione, si affiancano servizi mediani che corrispondono alla «ipotesi in cui il servizio è nuovo, ma non è autosufficiente, in quando deve necessariamente affiancarsi ad uno tradizionale di cui rappresenta un momento operativo innovativo», spec. p. 5.

5 Si pensi alle nuove attività di consulenza finanziaria automatizzata. Sul tema, si rimanda a M.T. Paracampo, *La consulenza finanziaria automatizzata,* in M.T. Paracampo (a cura di), *FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, Torino, 2017, p. 127-146; Aa. Vv., *Valore della consulenza finanziaria e robo advice nella percezione degli investitori. Evidenze da un'analisi qualitativa,* n. 6, 2019, R. Lener, *La «digitalizzazione» della consulenza finanziaria. Appunti sul c.d. robo-advice,* in Id. (a cura di), *Fintech: diritto, tecnologia e finanza,* Quaderni di Minerva Bancaria, 2, 2018; P. Maume**,** *Regulating Robo-Advisory,* in *Texas International Law Journal,* vol. 51, 2019, pp. 50-87.

6 Sulle difficoltà connesse ad una uniforme e trasversale regolazione del fenomeno, v. W. Magnuson, *Regulating Fintech*, in *Vanderbilt Law Review,* vol. 71, 2019, spec. p. 1204 ss.

dalle difficoltà di individuare specificatamente operatori, attività o servizi da loro svolti. La sfida attuale, pertanto, ruota attorno all'esigenza di calibrare le esigenze di regolazione giuridica con le necessità di evoluzione fisiologica del mercato finanziario.

Oramai, le nuove tecnologie appartengono al presente di cui tutti noi tutti siamo attori e spettatori: "attori" in qualità di soggetti coinvolti direttamente nel processo evolutivo tecnologico e "spettatori" quali destinatari degli effetti che le grandi innovazioni determinano.

8.2. «*Initial Coin Offering*»: un innovativo meccanismo di raccolta di finanziamenti

Un fenomeno nuovo del complesso e vivace mondo *Fintech* è quello che prende il nome di «*Initial Coin Offering*» (ICO), operazione finanziaria che sta assumendo una crescente rilevanza economica[7] e, di riflesso, sta attirando una sempre maggiore attenzione sul piano regolatorio in Italia ed all'estero.

Il presente studio mira a compiere un inquadramento del funzionamento tecnico delle «*Initial Coin Offering*» e del mercato delle cripto-attività nei ranghi del diritto, vagliando la possibilità di ricondurre le complesse dinamiche del fenomeno all'interno di preesistenti categorie giuridiche o, alternativamente, di sondare l'opportunità di una regolazione *ad hoc* capace di recepire appieno le novità tecnico-giuridiche. Inoltre, lo studio intende approfondire ed interrogarsi sulla natura degli «*utility token*» ibridi, in quanto questi, più di altre fattispecie, pongono consistenti dubbi sul piano della loro qualificazione giuridica a causa di una complessa struttura funzionale.

L'«*Initial Coin Offering*»[8] può essere intesa come un innovativo meccanismo di raccolta di finanziamento per progetti imprenditoriali che

---

[7] Per una valutazione dell'impatto economico sul mercato finanziario, si rimanda allo studio condotto dal «*Securities and Markets Stakeholder Group*», che mette in evidenza come, a fronte di un numero elevato di *Initial Coin Offering* non andate a buon fine, la rilevanza economica di quelle correttamente concluse è notevole, interessando decina di milioni in termini di investimenti raccolti. Interessante anche l'approfondimento sulla distribuzione territoriale di queste iniziative economiche, che riflette l'assenza di una regolazione uniforme su scala globale. Cfr. Securities and Markets Stakeholder Group, *Own Initiative Report on Initial Coin Offerings and Crypto-Assets*, Advice to ESMA, 19 ottobre 2018.

[8] Risulta opportuno sottolineare, in via preliminare, che si riconducono a questo fenomeno modalità di "offerta" alquanto diversificate tra loro. Il termine "*coin*" non deve, pertanto, condurre ad improprie riduzioni del tema sulla base di ragionamenti

sfrutta le trame della disintermediazione tipica della tecnologia *blockchain*[9].

L'emittente pubblica sul proprio sito internet un prospetto, il c.d. «*white paper*», contenente la descrizione del proprio progetto imprenditoriale.

La presenza di un prospetto informativo[10] è necessaria ai fini della delimitazione della tipologia del progetto imprenditoriale che si vuole intraprendere e dei *token* che si vorranno immettere sul mercato[11].

L'offerta è rivolta ad un numero indefinito di destinatari ed è diretta a finanziare il progetto attraverso l'acquisto in rete con moneta

analogici fondati su preesistenti categorie giuridiche e/o istituti. L'eterogeneità dei *token* determina una inevitabile frammentazione anche sul piano fenomenologico. Dunque, il richiamo alla moneta non deve essere fuorviante in quanto ricomprende al suo interno cripto-attività ben distanti dalla semplice moneta virtuale. Si noti che la più recente tendenza evidenzia il sempre maggiore ricorso a «*Security Token Offering*» (STO), vale a dire modelli di offerta di *token* che si identificano principalmente in prodotti e strumenti finanziari. Volendo, quindi, generalizzare si potrebbe parlare più correttamente di «*Initial Token Offering*». Sul punto, v. Deloitte, *Are token assets the securities of tomorrow?*, Whitepaper, 2019, p. 7 ss.

9 L'*European Market and Securities Authority* (ESMA) definisce l'*ICO* come «an operation through which companies, entrepreneurs, developers or other promoters raise capital for their projects in exchange for crypto-assets (often referred to as 'digital *token*s' or 'coins'), that they create». Cfr. ESMA, *Initial Coin Offerings and Crypto-Assets,* Advice, 9 gennaio 2019, spec. p. 43.

10 Il «*white paper*» richiama inevitabilmente il prospetto da pubblicare per l'offerta al pubblico di sottoscrizione o vendita e anche per l'ammissione alla negoziazione dei servizi finanziari, come disciplinato dal Regolamento (UE) 2017/1129, che ha abrogato la Direttiva 2003/71/CE. Si noti, però, che il contenuto dei «*white paper*» non è spesso dettagliatamente definito e può risultare poco comprensibile agli investitori, facendo riferimento agli standard tecnici che l'offerta dovrà assumere. Pertanto, esso, seppur astrattamente assimilabile, presenta delle notevoli differenze dal prospetto richiesto dalla normativa europea e dalla disciplina nazionale all'art. 94 del T.U.F., essendo richiesta, invece, una struttura estremamente precisa che possa rappresentare un presidio di sicurezza per i soggetti coinvolti nelle operazioni finanziarie. Sul punto, la recente «*Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività*» (art.5) stabilisce in dettaglio il contenuto del *white paper*, introducendo, di fatto, una disciplina che si avvicina profondamente a quella del Regolamento (UE) 2017/1129. Il passo compiuto in sede europea, seppur non definitivo, rappresenta, però, uno *input* determinante nella corretta regolamentazione del fenomeno.

11 Talvolta il prospetto è arricchito da un documento che sintetizza le caratteristiche che assumeranno i futuri *token* immessi sul mercato. Il documento prende il nome di «*Simple Agreement for Future Tokens*».

avente corso legale o con cripto-valuta[12] di un certo numero di *token*. L'emittente che può essere una persona fisica o giuridica, nonché una *start-up* in fase di lancio, sfrutta appieno tutte le potenzialità della rete, compiendo ampie campagne pubblicitarie, anche attraverso i vari canali dei s*ocial network* con l'obiettivo di rivolgersi ad un pubblico sempre più vasto.

Solitamente vengono predeterminati un ammontare minimo[13] di finanziamenti, il c.d. «*min cap*», ed una precisa data di scadenza dell'offerta. Prima dell'apertura dell'offerta, la *ICO* può essere preceduta da una fase preliminare di vendita (c.d. «*Pre-ICO*»), durante la quale viene venduto sul mercato un numero ristretto di *token* ad un prezzo nettamente inferiore rispetto a quello di vera e propria vendita[14].

Se al momento della scadenza, infatti, non si è raggiunto l'ammontare minimo, i fondi raccolti verranno restituiti automaticamente agli investitori attraverso l'attivazione degli *smart contract* [15] connessi

---

12 Le cripto-valute maggiormente utilizzate per questo tipo di investimenti sono *Bitcoin* ed *Ether*. Proprio le criptovalute, ed in particolare i *Bitcoin*, costituiscono la primissima applicazione della *blockchain*. Sul tema, oltre agli autori che verranno citati nel prosieguo si vedano, nella dottrina italiana, i seguenti contributi: M. CIAN, *La criptovaluta – Alle radici dell'idea giuridica di danaro attraverso la tecnologia: spunti preliminari*, in *Banca, borsa e tit. cred*., 2019, I, p. 315 ss.; M. RUBINO DE RITIS, *Obbligazioni pecuniarie in criptomoneta*, in *Giustiziacivile.com*, 2018; V. DE STASIO, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca borsa tit. cred*., 2018, p. 747 ss.; R. BOCCHINI, *Sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inf*., 2017, p. 27 ss.; G. LEMME - S. PELUSO, *Criptomoneta e distacco dalla moneta legale*, in *Rivista di diritto bancario*, 2016; G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. inf*., 2015, p. 415 ss.; N. VARDI, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin*, in *Dir. inf*., 2015, p. 443 ss. Sul rapporto con i sistemi *blockchain*, v. D. FAUCEGLIA, *La tecnologia blockchain: bitcoin e smart contract*, in G. Bruno (a cura di), *Diritto delle comunicazioni*, Giappichelli, Torino, 2019, p. 249 ss.

13 Può accadere, molto più raramente, che sia fissato un ammontare massimo di raccolta, legato al numero di *token* che si vorranno immettere sul mercato (il c.d. *hard cap)*.

14 Sul punto, v. P. P. PIRANI, *Gli strumenti della finanza disintermediata: Initial Coin Offering e blockchain*, in *Analisi Giuridica dell'Economia*, 1, 2019, spec. p. 334.

15 Il legislatore italiano con il d.l. n. 135 del 2018 (convertito con modificazioni dalla l. n. 12 dell'11 febbraio 2019), all'art. 8-*ter*, co. 2, afferma che «si definisce "*smart contract*" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli *smart contracts* 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

all'offerta. Se, viceversa, si sarà raggiunto il termine minimo prefissato, i *token* oggetto dell'offerta verranno attribuiti ai singoli sottoscrittori attraverso il medesimo processo automatizzato garantito dagli *smart contract* [16].

Innanzitutto, va da subito notata la stretta correlazione tra queste nuove forme di appello al pubblico risparmio e la tecnologia *blockchain*, che le rende, di fatto, non solo possibili ma anche efficienti in termini di costi e fattibilità tecnica.

Senza entrare nel merito della discussione riguardante questa nuova tecnologia, la *blockchain* va intesa come «una modalità particolarmente trasparente e decentralizzata per la registrazione di elenchi di transazioni» [17], attraverso un protocollo di comunicazione che si basa su un *database* distribuito, in cui i dati vengono memorizzati su diverse ed autonome macchine, i c.d. nodi, connesse in un rapporto assimilabile, per certi versi, alle reti *peer-to-peer.* Esse sono, letteralmente, delle catene di blocchi che presentano il carattere tipico della disintermediazione, differenziandosi dai tradizionali registri informatici, di natura centralizzata o decentralizzata [18].

Per le caratteristiche tecnico-funzionali che essa presenta, la *blockchain* [19] garantisce immodificabilità dei dati inseriti, trasparenza

---

adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto». Sull'applicazione degli *smart contract* nel contermine settore bancario, sia consentito rimandare a E. Battelli, E. M. Incutti, *Gli "smart contracts" nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contratto e impresa*, 3, 2019, p. 925 ss.

16 Per una corretta disamina del funzionamento tecnico delle *ICO,* v. C. Sandei, Initial Coin Offering *e appello al pubblico risparmio,* in *Diritto del Fintech*, cit., spec. p. 277 e ss.

17 P. Boucher, *Come la tecnologia blockchain può cambiarci la vita*, Servizio di ricerca del Parlamento Europeo, Febbraio 2017, spec. p. 4.

18 La *blockchain*, *species* tecnologica del più ampio *genus* della «*Distribuited Ledger Technology*», è un sistema distribuito in cui ogni nodo può svolere una doppia funzione, comportandosi sia come un operatore *client* e sia quale *server,* detentore di una copia del registro in cui è inserito. Questo garantisce una notevole resistenza ad attacchi esterni, in quanto per poter modificare una singola parte della catena, sarebbe necessario ottenere il "consenso" di tutti gli altri nodi o della maggioranza degli stessi, a seconda delle tipologie funzionali prescelte. (cfr. M. Iansiti e K.R. Lakhani, *The truth about Blockchain,* in *Harvard Business Review*, January – February Issue, 2017).

19 Nell'ordinamento italiano, il primo comma dell'art. 8-*ter* del d.l. n. 135 del 2018 definisce le tecnologie basate su registri distribuiti, 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

delle informazioni concernenti le transazioni compiute lungo la catena e tracciabilità delle operazioni compiute.

Ai fini del presente discorso e anticipando questioni che verranno successivamente analizzate con maggiore accuratezza, è opportuno ricordare che tali sistemi si distinguono in catene *«permissionless»*, prive di sistemi centrali di autorizzazione o di preventiva identificazione e *«permissioned»*, in cui opera una sorta di filtro centrale che funge da "blocco" di validazione dell'accesso al sistema. Inoltre, va aggiunto che per la realizzazione di una *ICO* si ricorre indistintamente a *blockchain* già esistenti o sistemi nativi, cioè creati appositamente per tali operazioni[20].

8.3. Le diverse tipologie di *token*

Alla base di ogni singola *ICO* risiede il processo di «*tokenizzazione*», il quale consiste nella conversione tramite criteri crittografici di diritti di diversa natura in un *token* digitale registrato su un sistema dotato di tecnologia *blockchain*[21]. Il collegamento tra il mondo reale (quindi, il bene o il diritto "*tokenizzato*") ed il mondo virtuale è rappresentato da uno *smart contract*[22].

Sul piano del processo tecnico impiegato, la «*tokenizzazione*» presenta similitudini con il metodo di "creazione" delle *securities* nella sua

---

sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili». Inoltre, il terzo comma sancisce che le validazioni temporali effettuanti mediante tali tecnologie producono i medesimi effetti giuridici della validazione temporale elettronica prevista dall'art. 41 del Regolamento (UE) n. 910/2014.

20 Un fenomeno simile ad alternativo è quello delle «*Initial Exchange Offering*» (IEO), attraverso cui l'emittente-offerente raccoglie capitali presso il pubblico offrendo i token in vendita direttamente su un'unica piattaforma di «*exchange*», senza ricorrere ad una preventiva offerta. In questo caso, quindi, i due mercati (primario e secondario) dei token si fondono in un unico momento di emissione ed ammissione ai mercati di *trading*.

21 «*Tokenisation* is a method that converts rights to an asset into a digital *token*», ESMA, *op. cit.*, spec. p. 18.

22 In tema si vedano: T. PELLEGRINI, *Prestazioni auto-esecutive. Smart contract e dintorni*, in *Comparazione e diritto civile*, 3, 2019, spec. p. 847-848; N. GUGGENBERGER, *The Potential of Blockchain Technology for the Conclusion of Contracts*, in *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps*, Aa. Vv., Nomos/Hart ed., 2017, p. 85 ss. E da ultimo per tutti si veda lo studio di M. MAUGERI, *Smart Contracts e disciplina dei contratti*, Il Mulino, Bologna, 2020.

funzione di incorporazione dei diritti all'interno di un singolo certificato[23]. In via generale, dunque, il *token* costituisce una rappresentazione digitale e crittografica di specifici rapporti giuridici[24]. Come si può notare dalle trame del funzionamento tecnico, a monte del pagamento di un corrispettivo, sussiste l'impegno del soggetto emittente di realizzare dei *token*, o più correttamente cripto-attività («*crypto-assets*» nella versione inglese), quali forme digitali rappresentative di diritti connessi ad investimenti in specifici progetti imprenditoriali.

A livello nazionale e sovranazionale, manca una definizione univoca delle cripto-attività a causa della frenetica velocità a cui l'innovazione tecnologica propone prospettive nuove, proprio come sottolineato sia dalla EBA sia dall'ESMA nei loro studi sul tema[25].

Sembra, però, condivisibile (e diffusamente condivisa[26]) la catalogazione proposta dall'Autorità federale di vigilanza sui mercati finanziari (FINMA) della Svizzera[27], sulla base della funzione economica svolta dal *token*. Apprezzabile è stato, infatti, il tentativo di ridurre a grandi categorie il *genus* ampio ed eterogeneo delle cripto-attività, con

---

23 È quanto sostenuto anche dalla Consob che afferma che la *tokenizzazione* «presenta profili di analogia con il meccanismo di "creazione" di securities, ovvero l'incorporazione dei diritti del sottoscrittore in un certificato, che costituisce titolo di legittimazione per il loro esercizio ma anche uno strumento per la più agevole trasferibilità dei medesimi», così Consob, *Le offerte iniziali e gli scambi di cripto-attività*, Documento per la Discussione, 19 marzo 2019, spec. p. 2.

24 In questi termini si è espresso anche il Trib. di Firenze, sentenza n. 18 del 21 gennaio 2019, in *Dir. Internet*, 2019, p. 337.

25 «Crypto-assets are a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT). There are a wide variety of crypto-assets», così ESMA, *op.cit.*, spec. p. 2. In relazione ai *token* che si sostanziano in strumenti finanziari, l'ESMA propone due approcci differenti: da un lato, introdurre una disciplina speciale che possa tutelare al meglio il consumatore-investitore e dell'altro, l'approccio c.d. di "*Do Nothing*", vale a dire lasciare che il fenomeno si evolva liberamente (cfr. ESMA, *op. cit.*, p. 40 ss.). Si sottolinea, inoltre, anche la fonte "disintermediata" delle crypto-attività, le quali sono generate diffusamente sulla rete senza l'intervento di una autorità centrale. Questo elemento è fortemente sottolineato dall'EBA. Sul punto, si legge che «crypto-asset […] is neither issued nor guaranteed by a central bank or public authority and can be used as a means of exchange and/or for investment purposes and/or to access a good or service», EBA, *Report with advice for the European Commission on crypto-assets*, 9 gennaio 2019, spec. p. 11).

26 La presente tassonomia è ripresa dalle autorità europee negli studi *supra* citati e, tra gli altri, dalla *Financial Conduct Autority* (FCA) del Regno Unito. (cfr. FCA, *Guidance on Cryptoassets*, Policy Statement, luglio 2019).

27 FINMA, *Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle Initial coin offering (ICO)*, 16 febbraio 2018 (disponibile anche in lingua italiana).

la consapevolezza di un aggiornamento - facilmente ipotizzabile - dell'elencazione suggerita, senza alcuna pretesa di tassatività[28].

I *token* sono, così, suddivisi in tre categorie: a) i *token* di pagamento (*payment token*), vale a dire le cripto-valute o monete virtuali; b) i «*token* di utilizzo» (*utility token*), ossia quei *token* che attribuiscono al titolare il diritto di utilizzare o di godere di un bene o di un servizio (fisico o digitale) presente o futuro; ed infine, c) i «*token* d'investimento» (*asset* od *investment token*), che «possono rappresentare, in particolare, un credito ai sensi del diritto delle obbligazioni nei confronti dell'emittente oppure un diritto sociale ai sensi del diritto societario»[29]. A questa tripartizione[30] si affianca la fattispecie aperta dei *token* ibridi, i quali possono combinare al proprio interno funzioni ed elementi tipici delle singole cripto-attività[31].

La tripartizione qui considerata è confermata anche dalla «*Proposta di Regolamento relativo ai mercati delle cripto-attività*»[32]. Le tre categorie, anch'esse fondate sulla funzione economica svolta dai *token*, prendono il nome di a) *token* di moneta elettronica[33], b) *utility token* e c) *token* collegati ad attività. Quest'ultima formulazione, più "ampia" sul piano strettamente terminologico, sembrerebbe corrispondere a tutte quelle attività finanziare che possano essere rese attraverso un processo di

---

28 Cfr. G. Gitti, M. Maugeri e C. Ferrari, *Offerte iniziali e scambi di cripto-attività,* in *Osservatorio del diritto civile e commerciale*, 1, 2019, spec. p. 97.

29 Così, FINMA, *op.cit.,* spec. p. 3.

30 Come ritenuto dall'Autorità svizzera se i «*payment token*» e gli «*utility token*» puri non possono considerarsi come strumenti finanziari, gli «*asset token*» sono, invece, assimilabili ai valori mobiliari, in quanto costituiscono un valore negoziabile sul mercato, come stabilito dall'art. dell'art. 2, lett. b), della legge svizzera sull'infrastruttura finanziaria. Per una analisi approfondita dell'impostazione seguita dall'Autorità svizzera, v. P. P. Pirani, *op.cit.,* spec. p. 337 ss.

31 G. Gitti (a cura di), *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca, borsa e tit. cred.*, 1, 2020, p. 13 ss.

32 *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937,* Bruxelles, 24.9.2020, COM (2020) 593 def., spec. p. 19 ss.). Questa tassonomia è anticipata con nettezza anche dal *considerando* 9 della Proposta. Senza entrare nel merito dell'analisi del testo, è opportuno, però, sottolineare che la Proposta in esame abbia un campo applicativo definito in "negativo" dall'art. 2 par. 2, applicandosi, difatti, alle sole cripto-attività che non trovino già una cornice legislativa di riferimento in ambito europeo.

33 Il riferimento sembrerebbe essere orientato maggiormente verso i c.d. «*stable coins*» di recente emersione che presentano minori rischi sotto il profilo della volatilità dei mercati, in quanto fondano il loro prezzo su un mezzo di scambio stabile, come, ad esempio, una moneta fiat.

tokenizzazione[34], che abbiano un valore stabile e che presentino profili di evidente finanziarietà.

In linea più generale, l'art. 3 della Proposta propone una definizione di «cripto-attività» fortemente descrittiva, quale «una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga»[35].

Il problema passa dalla mera classificazione fenomenologica dei *token* alla loro, ben più complessa, qualificazione giuridica. Ulteriore profilo di rischio è quello relativo alla sempre più diffusa ibridazione dei *token* che determina una sempre maggiore complessità di qualificazione giuridica del fenomeno[36]. Infatti, come si analizzerà in dettaglio successivamente, gli «*utility token*» oltre a concedere il diritto di godimento di un bene o di un servizio, talvolta, possono offrire rendimenti di natura finanziaria che li pongono in una zona di confine tra diversi insiemi di indagine: da un lato, quello, empiricamente più immediato, che li riconduce al loro ambito "consumeristico" di appartenenza e, dall'altro, quello che mira, invece, a verificare la prevalenza della concreta funzione di queste cripto-attività. Nel prosieguo di questo studio, si cercherà di percorrere la prospettiva delineata dal secondo di questi insiemi di indagine.

In considerazione di ciò, al fianco dell'apprezzabile tentativo di ricondurre le varie tipologie di *token* a confini più facilmente adattabili, basandosi sulla loro funzione economica[37], resta sempre da chiarire l'aspetto "dinamico" di questi «*crypto-assets*». Infatti, i *token* vivono (spesso, ma non sempre) di due fasi: quella della loro emissione e la

---

34 Art. 3 n. 3, *Proposta di Regolamento relativo ai mercati delle cripto-attività,* cit.: «un tipo di cripto-attività che intende mantenere un valore stabile facendo riferimento al valore di diverse monete fiduciarie aventi corso legale, di una o più merci o di una o più cripto-attività, oppure di una combinazione di tali attività».

35 Art. 3 n. 2.

36 Per tutti, G. Benedetti, *Sull'in-certezza del diritto. Dal dogma della certezza a un'ermeneutica critica*, in Id., *Oltre l'incertezza. Un cammino di ermeneutica del diritto*, Bologna 2020, p. 137 ss.

37 Si potrebbe parlare in tal senso di un approccio «*bottom-up*» che si focalizza sulla natura *ex se* dei *token*. Sarebbe, però, preferibile affiancare a questa prospettiva, un metodo di analisi «*top-down*», muovendo dallo studio dei *token* e delle loro funzioni nel mercato secondario di *trading* per poi risalire alla fase iniziale di emissione. A favore di questa impostazione, v. F. Annunziata, *La disciplina delle* trading venues *nell'era delle rivoluzioni tecnologiche: dalle criptovalute alla* distributed ledger technology, in *Orizzonti dir. comm.*, 2018, p. 3 ss.

successiva fase della loro circolazione e, quindi, della loro negoziabilità su appositi mercati di *exchange*[38]. Ed allora, appare chiaro che né l'approccio statico né quello dinamico siano sufficienti da soli, ma necessitino inevitabilmente della loro reciproca integrazione per poter offrire una chiave interpretativa "universale" che sappia cogliere le molteplici sfaccettature dei *token*[39].

8.4. La posizione della Consob e le questioni aperte

Emerge con evidenza, nella disamina di questo nuovo e scivoloso processo tecnologico, la necessità di risolvere la questione definitoria sul piano, prima, fenomenologico e, poi, giuridico.

Nel nostro ordinamento, il primo tentativo di affrontare il problema qualificatorio delle cripto-attività connesse ad un ICO è riconducibile all'attività compiuta dalla Consob[40] attraverso la pubblicazione di un iniziale documento per la discussione[41] a cui ha fatto seguito il Rapporto finale del 2 gennaio 2020.

Il punto di vista assunto dalla Consob è stato quello di qualificare le «cripto-attività» come attività diverse dagli strumenti finanziari di cui all'art. 1, co. 2 del TUF e dai prodotti di investimento di cui al co. 1, lettere w-*bis*.1, w-*bis*.2 e w-*bis*.3 e consistenti nella rappresentazione

---

38 Sul punto, v. G. GITTI, M. MAUGERI e C. FERRARI, *op.cit.*, p. 99.

39 In questa direzione, v. C. SANDEI, *op.cit.*, spec. p. 290 ss.

40 L'autorità italiana, in realtà, aveva già affrontato indirettamente il problema delle ICO in alcuni precedenti provvedimenti volti alla sospensione in via cautelare delle offerte di cripto-attività. Si vedano, in particolare, Delibera Consob n. 20660 del 31 ottobre 2018 (*Togatoken*), Delibere nn. 20740 e 20741 del 12 dicembre 2018 (*Green Earth e Bitsurgetoken*).

41 Consob, «*Le offerte iniziali e gli scambi di cripto-attività*», *Documento per la discussione*, 19 marzo 2019.

crittografica di diritti connessi ad investimenti in specifici progetti imprenditoriali[42]. Questi *token* devono essere, da un lato, emessi, conservati e trasferiti attraverso sistemi DLT[43] e, dall'altro, devono essere negoziati o destinati alla negoziazione in una o più piattaforme di scambio [44].

Sono, pertanto, esclusi i «*payment token*» e i «*token* di investimento»: i primi per la loro funzione di moneta virtuale; i secondi, invece, per le peculiari caratteristiche che vanno ad integrare le fattispecie degli strumenti finanziari o dei prodotti finanziari[45].

I *token* delineati dalla Consob rappresentano, quindi, una categoria *ad hoc* e prospettano, così, «la previsione di una disciplina speciale delle cripto-attività»[46] capace di affrontare al meglio le particolarità del fenomeno.

A dire il vero, i *token* così descritti possono presentare dei profili di analogia con i prodotti finanziari *ex.* art. 1, co. 1 lett. u del T.U.F.[47], «in quanto comunque caratterizzati dall'investimento di un capitale finanziario, dall'assunzione del relativo rischio e da un'aspettativa di rendimento»[48]. Non viene chiarito, però, se in questi casi vada applicata la disciplina "speciale" prospettata o se sia preferibile ricondurre queste ipotesi a categorie preesistenti, applicando, quindi, la disciplina

---

42 Sul punto, nel Rapporto finale si chiarisce che, onde evitare indebite e preventive esclusioni di *token* non direttamente connessi con specifici progetti imprenditoriali, «si ribadisce la preferibilità di non vincolarsi a definizioni precostituite, potendo trattarsi di progetti in uno stato embrionale così come di attività in uno stato di maggiore avanzamento», Consob, *Rapporto finale,* p.

43 Ciò indica l'esclusività dell'infrastruttura tecnologica di supporto a questo tipo di processi crittografici, diventando elemento costitutivo della stessa fattispecie fornita all'interno del Documento. Il richiamo è generico ed è a tutte le tecnologie dotate di registri distribuiti. Mancano, però, riferimenti tecnici che possano maggiormente specificare le caratteristiche strutturali che questi sistemi di emissione-scambio devono avere. Il rischio, a tal riguardo, è quello di non comprendere nello sforzo regolatorio fenomeni che rispecchiano peculiarità tecnico-informatiche diverse dal disegno regolatorio proposto ma che, invece, coincidono sul piano delle funzioni con gli obiettivi di disciplina perseguiti.

44 Cfr. Consob, *Documento per la discussione*, cit., spec. p. 6.

45 In questi casi si applicherà la disciplina nazionale ed europea prevista per le fattispecie ad essi riconducibili.

46 Consob, *Documento per la discussione*, cit., p. 7.

47 Diversa, chiaramente, è l'ipotesi dei *token* che siano totalmente riconducibili ai prodotti finanziari.

48 Consob, *Documento per la discussione*, cit., p. 7

"tradizionale" di riferimento. Sembrerebbe, piuttosto, che venga definita una sorta di «intersezione tra due insiemi»[49], potendo rientrare nell'ampia definizione fornita sia i *token* sussumibili anche all'interno della disciplina dei prodotti finanziari sia i *token* che non sono in alcun modo ad essi riconducibili.

Ciò che è certo, invece, è che elemento costitutivo delle cripto-attività sia la loro negoziabilità. Esse, infatti, devono essere destinate alla negoziazione su sistemi di scambio appositamente predisposti, le c.d. piattaforme *«exchange».*

Il limite della negoziabilità dei *token* (attuale o futura) pone delle zone d'ombra all'interno del programma di chiarificazione della Consob. Difatti, come sembra emergere dalle osservazioni compiute in sede di Rapporto finale, non è necessario che il *token* sia già pronto per la negoziazione ma è indispensabile che al momento della sua emissione, all'interno del *white paper*, sia indicata la futura destinazione alla negoziazione[50].

Aderendo a questa prospettiva, si devono necessariamente escludere dallo schema di regolazione speciale tutti quei *token* che, seppur connessi ad un progetto imprenditoriali, non siano in alcun modo destinati allo scambio.

Un aspetto meritevole di apprezzamento consiste nel tentativo di far rientrare all'interno del paradigma definitorio delineato dalla Consob anche quegli «*utility token*» che siano dotati di prospettive di rendimento finanziario. La Consob ricorda, infatti, che gli investimenti di natura finanziaria riconducibili alla categoria dei prodotti finanziari sono tutte quelle proposte di investimento che implichino la compresenza di tre elementi: (i) l'impiego di un capitale, (ii) la promessa o l'aspettativa di un rendimento di natura finanziaria[51] e, (iii) l'assunzione di un rischio direttamente connesso e correlato all'impiego di capitale.

---

[49] G. Gitti, M. Maugeri e C. Ferrari, *op. cit.,* spec. p. 103.

[50] Rimane il dubbio circa quei *token* che, sebbene non inizialmente previsti come *token* destinati alla negoziazione, siano successivamente immessi all'interno di sistemi di scambio (cfr. Consob, *Rapporto Finale,* spec. 5-6).

[51] La prospettiva di rendimento deve essere intesa quale eventuale accrescimento della somma investita, senza alcuna prestazione ulteriore se non quella della dazione della somma di danaro. Sul tema, v. Cass. Civ., Sez. II, n. 2736 del 2013 in *Contratti*, 2013, 1105; secondo cui «la causa negoziale è finanziaria [allorquando] la ragione giustificativa del contratto, e non il suo semplice motivo interno privo di rilevanza qualificante, consiste proprio nell'investimento del capitale (il "blocco" dei risparmi)

In altri suoi provvedimenti, la stessa Consob aveva già ulteriormente affinato questi criteri valutativi, stabilendo che una operazione presenta gli elementi distintivi di un investimento di natura finanziaria se «l'atteso incremento di valore del capitale impiegato (ed il rischio ad esso correlato) sia elemento intrinseco all'operazione stessa»[52].

Proprio da quest'ultimo orientamento è possibile ricavare un prezioso corollario che ben si adatta al mercato delle cripto-attività: la causa in concreto[53] del contratto può rappresentare una nuova prospettiva di analisi e di qualificazione di questi *token*[54].

La Consob non si è, però, limitata allo spazio definitorio delle cripto-attività, ma ha voluto inquadrare il fenomeno anche dal lato degli operatori coinvolti. A questo riguardo, si forniscono due distinte definizioni: da un lato, quella della piattaforma coinvolta nella fase di emissione e dall'altro, quella del sistema di scambio adoperato nella successiva fase di negoziazione.

La piattaforma per le offerte di cripto-attività deve essere considerata come «una piattaforma on line che abbia come finalità esclusiva la

con la prospettiva dell'accrescimento delle disponibilità investite, senza l'apporto di prestazioni da parte dell'investitore diverse da quella di dare una somma di denaro».

52 Cfr. Consob, comunicazione n. DTC/13038246 del 6 maggio 2013.

53 Sull'adesione giurisprudenziale a questo nuovo filone interpretativo della causa del contratto, v., *ex multis*, Cass., III sez. civ., sentenza del 08 maggio 2006 n. 104, in *Corriere giur*., 2006, 1718. La Suprema Corte sostiene, infatti, una ridefinizione della nozione di causa fin ad allora intesa, affermando che «lo scopo pratico del negozio, la sintesi, cioè, degli interessi che lo stesso è concretamente diretto a realizzare (c.d. causa concreta), quale funzione individuale della singola e specifica negoziazione, al di là del modello astratto utilizzato».

54 In questo senso, «indispensabile capire quale sia il rapporto negoziale sottostante che giustifica l'emissione del *token* (: la causa negoziale), tenendo presente l'ulteriore (ed eventuale) circostanza, per così dire "estrinseca" al *token*, che questo sia negoziato o destinato alla negoziazione su uno o più sistemi di scambio», M. De Mari, *Prime ipotesi per una disciplina italiana delle Initial Token Offerings (ITOs): token crowdfunding e sistemi di scambio di crypto-asset*, in *Orizzonti del Diritto Commerciale*, 2, 2019, spec. p. 288.

promozione e realizzazione di offerte di cripto-attività di nuova emissione»[55]. I sistemi di scambio dei *token*[56], invece, si possono definire come un «insieme di regole e di strutture automatizzate, che consente di raccogliere e diffondere proposte di negoziazione di cripto-attività e di dare esecuzione a dette proposte, anche attraverso tecnologie basate su registri distribuiti»[57].

In merito al funzionamento delle piattaforme dedicate alle offerte di cripto-attività, viene prospettata l'estensione della normativa prevista per i gestori di portali per la raccolta di capitali di rischio (c.d. piattaforme di *crowdfunding)*[58], la cui attività è definita dal regolamento Consob n. 18592 del 26 giugno 2013[59].

La proposta di regolamentazione in esame è orientata all'introduzione di un regime di «*opt-in*»[60] che lascia al singolo emittente-offerente la scelta di ricorrere, per l'emissione di *token*, a quelle piattaforme così come definite dall'Autorità o, alternativamente, di agire al di fuori di questi confini. L'applicazione della disciplina su base volontaria rischia di offrire un quadro frammentato e pericoloso per l'investitore[61].

---

55 Consob, *Documento per la discussione,* cit., p. 8. In relazione a ciò, va sottolineato che la Consob sembrerebbe prendere in considerazione i soli *token* che siano stati, prima, emessi attraverso una ICO e, poi, successivamente negoziati sui sistemi di scambio. Questo approccio lo si può evincere dallo stesso titolo («*Le offerte iniziali e gli scambi di cripto-attività*») del documento iniziale della Consob che mette in evidenza la due fasi di emissione e negoziazione quali elementi "costitutivi" del fenomeno.

56 Questi sistemi si dividono, a loro volta, in due principali categorie: le piattaforme «*with order book*», cioè sistemi dotati di un *book* di negoziazione, che provvede al *matching* tra gli ordini e le piattaforme di «*direct trading*», che, invece, consentono una negoziazione diretta tra le parti (una sorta di sistema *peer-to-peer).*

57 *Ivi,* p. 12.

58 Questi soggetti devono rispettare i requisiti indicati all' art. 50-*quinquies* del d. lgs. n. 58 del 1998 (TUF), necessari ai fini della autorizzazione allo svolgimento di questo tipo di attività.

59 In ambito europeo, si ricorda il *Regolamento (UE) 2020/1503 del Parlamento Europeo e del Consiglio del 7 Ottobre 2020 relativo ai fornitori europei di servizi di crowdfunding per le imprese,* che modifica il regolamento (UE) 2017/1129 e la direttiva (UE) 2019/1937.

60 Sorge spontaneo domandarsi se quei *token* tagliati fuori dalla definizione di cripto-attività vista, possano comunque usufruire di questa disciplina speciale e volontaria per la loro emissione nel mercato primario.

61 «[…] una disciplina derogabile che mal si accorda con la tutela dell'investitore e che può disorientare e risultare frammentata. Può disorientare tanto gli investitori nella percezione dell'effettiva disciplina applicabile quanto gli stessi enti emittenti i *token*», così M. De Mari, *op.cit*., spec. p. 307.

In questo, forse, il documento mostra la sua "debolezza"[62]: ad un corretto inquadramento fenomenologico e ad un apprezzabile sforzo definitorio non segue un adeguata prospettazione di disciplina che sappia cogliere le evoluzioni del mercato attraverso maglie regolatorie elastiche ma chiare.

È il mercato stesso a richiedere regole ben definite per poter procedere liberamente senza la preoccupazione di incorrere in zone grigie all'interno della cornice normativa[63]. Allo stesso tempo, sarebbe opportuno non sfociare in un frenetico processo di regolazione che, nel tentativo di anticipare i fenomeni tecnologici, si affatica nel predisporre argini inidonei ai cambiamenti in atto[64].

---

62 «[…] la proposta regolamentare dell'Autorità di vigilanza appare troppo timida», C. Sandei, *Le Initial Coin Offering nel prisma dell'ordinamento finanziario,* in *Rivista di dir. civ.*, 2, 2020 spec. p. 415.

63 Altro tema non adeguatamente approfondito è quello attinente alle caratteristiche strutturali e tecniche che i sistemi di DLT impiegati in queste operazioni devono avere. Come si evince dal documento e dalla consultazione pubblica, si auspica l'impiego di sistemi c.d. «*permissioned*» che garantiscono una maggiore sicurezza e tracciabilità delle operazioni. Se è vero che questa soluzione si muove in controtendenza rispetto alle scelte attuali del mercato (le maggiori piattaforme utilizzano reti «*permissionless*») e del principio di neutralità tecnologica, va, parimenti, considerato che soltanto sistemi «*permissioned*» possano garantire sicurezza e trasparenza nelle operazioni. A tal riguardo, a favore di un impianto regolatorio che privilegi sistemi dotati di filtri di controllo, v. A. Caponera, C. Gola, *Aspetti economici e regolamentari delle «cripto-attività»,* Questioni di Economia e Finanza, marzo 2019, spec. p. 35 ss.

64 Si sarebbe potuto ipotizzare l'introduzione di un regime di «*regulatory sandbox*», attraverso cui si concede spazio di manovra e di sviluppo agli operatori economici, che si possono avvantaggiare anche di alcune deroghe normative. Questo approccio è diretto a facilitare lo sviluppo di nuovi modelli di business nel settore finanziario, come peraltro già avvenuto con il Decreto-Legge convertito con modificazioni dalla L. 28 giugno 2019, n. 58, che all'art. 36-*bis,* co. 2-*bis* ha previsto un regime autorizzativo favorevole con una durata temporale limitata a diciotto mesi. Per una ricostruzione favorevole a questo approccio regolatorio, v. M. De Mari, *op.cit.*, spec. p. 308 ss.

L'incertezza delle regole[65], per la loro molteplicità, variabilità e per l'intrinseca ambiguità dei testi anche di *soft law* proposti, rischia di limitare molto l'efficacia di questi strumenti[66], proprio a causa della mancanza di un approccio sistematico e della frammentarietà dei modelli propri delle diverse tradizioni nazionali. In misura tutt'altro che marginale, a ciò si associa anche l'incertezza di una politica legislativa oscillante fra la tutela dell'efficienza del mercato (unica finalità del tempo in cui l'Europa era solo una comunità economica) e la necessità di una politica sociale, orientata alla sostenibilità dei nuovi paradigmi e modelli di business (sempre più avvertita nell'attuale contesto socioeconomico)[67].

Il ripensamento del capitalismo come sino ad ora concepito, passa proprio dall'accettazione del superamento del modello della massimizzazione, senza scrupoli, dei profitti[68] a favore della promozione di un «valore condiviso»[69], ovvero di nuovi paradigmi economici che siano sostenibili e sani.

---

65 Per un inquadramento teorico L. GIANFORMAGGIO, *Certezza del diritto*, in *Dig. Disc. Priv. sez. Civ.*, II, Torino, 1988, p. 274 ss. e A. PIZZORUSSO, *Certezza (II. Profili applicativi)*, in *Enc. giur.*, VI, Roma, 1988. Cfr. anche la critica di N. BOBBIO, *La certezza del diritto è un mito?*, in *Riv. int. fil. dir.*, 28, 1951, p. 146 ss. e la sintesi delle "manifestazioni della certezza" operata da M. CORSALE, *Certezza del diritto*, in *Enc. giur.*, 1988, Roma, p. 1203 ss. *Ex multis* si segnalano: F. LOPEZ DE OÑATE, *La certezza del diritto*, Roma, 1942, poi ripetutamente ripubblicato; in particolare, nell'edizione del 1968 (a cura di G. Astuti) si dà conto di alcuni dei saggi che vi fecero seguito, quali quelli (di notevole rilievo) di F. CARNELUTTI, *Nuove riflessioni intorno alla certezza del diritto*, in *Riv. dir. proc.*, 1950, p. 115 ss. A seguire si veda G. LONGO, *Certezza del diritto*, in *Nov. Dig. It.*, III, Torino, 1958, p. 125 ss. Di recente, si veda l'analisi di N. IRTI, *Un diritto incalcolabile*, Giappichelli, Torino, 2016, in specie sul rapporto tra decisione, ambiguità interpretative, schema normativo e fatto concreto, spec. p. 107 ss.

66 G. BENEDETTI, *«Ritorno al diritto» ed ermeneutica dell'effettività*, in ID., *Oltre l'incertezza. Un cammino di ermeneutica del diritto*, cit.

67 Rimangono preziose riflessioni quelle contenute in P. BARCELLONA, *Diritto privato e processo economico*, 2ª ed., Jovene, Napoli, 1977, p. 259 ss.

68 Il rimando è agli studi di Milton Friedman ed alla sua teoria, da molti poi successivamente condivisa e ripresa, sulla massimizzazione del valore dell'azionista come unica obiettivo e responsabilità di ogni azienda (cfr. M. FRIEDMAN, *The Social Responsibility Of Business Is to Increase Its Profits,* in *New York Times,* 13 settembre 1970).

69 Cfr. R. HENDERSON, *Nel mondo che brucia. Ripensare il capitalismo per la sopravvivenza del pianeta,* Sustain, Luiss University Press, 2020, spec. p. 47 e ss. L'Autrice sostiene l'esigenza di calibrare il nuovo capitalismo verso orizzonti più equi, sostenibili, innovativi ed etici perseguendo il "valore condiviso", ovvero impostare un modello di business che sia al tempo stesso redditizio e giusto per l'ambiente e per la collettività. Sia consentito rimandare anche a R.A. POSNER, *La crisi della democrazia capitalistica*, Milano, Egea, 2010, spec p. 124 ss., il quale invita a ripensare all'impresa e ad

Il mercato delle cripto-attività, nella sua specificità, rappresenta un ripensamento delle tradizionali forme di investimento e di finanziamento, nonché di circolazione dei prodotti finanziari. E dinanzi ad un simile cambiamento, è necessario predisporre un sentiero economicamente e giuridicamente sostenibile.

8.5. Un punto di vista comparato tra primi interventi legislativi e prospettive "caso per caso"

Uno dei primi interventi legislativi volti ad inquadrare il fenomeno e ad offrire una cornice normativa chiara sia per gli operatori che per i singoli investitori, è stato il «*Virtual Financial Asset Act*»[70] del 1° novembre 2018. La legge in esame disciplina le «*Initial Virtual Financial Asset Offering*», qualificandole come innovativi strumenti di raccolta di risorse attraverso l'acquisto di «*virtual financial asset*» emessi dall'offerente.

La qualifica di «*virtual financial asset*» è subordinata all'approvazione di un'autorità appositamente creata e con specifiche competenza in materia, la «*Malta Digital Innovation Authority*». Si deve, inoltre, notare che sono esclusi da questa disciplina i *token* non negoziati dalle piattaforme di scambio.

I profili di maggiore interesse di questo ambizioso tentativo legislativo sono sostanzialmente due. Il primo riguarda, il c.d. «*white paper*», il quale deve contenere informazioni precise e dettagliate e deve essere preventivamente validato dall'Autorità maltese. L'emittente è, infatti, responsabile dei danni patrimoniali subiti dagli investitori a causa di informazioni fuorvianti od imprecise. L'altro elemento di rilevanza at-

---

eliminare tutti i corollari "dell'imbroglio contrattualista" e della ricerca esclusiva del "valore per gli azionisti". Sul tema, ed in particolare sulle deviazioni e sulla crisi del modello societario, per profili più generali ma non del tutto estranei, si veda A. Mingardi, *La verità, vi prego, sul neoliberismo*, II ed., Milano, Marsilio, 2019. Nel nostro ordinamento, la prospettiva "proprietaria" ed individualista, che il Codice Civile aveva inteso tutelare e valorizzare, d'altronde, come è noto, ha già conosciuto per altri versi una evidente abrasione nell'affermarsi di un «capitalismo senza capitale» (cfr. J. Haskel, S. Westlak, *Capitalismo senza capitale,* Milano, Franco Angeli, 2018), a seguito dell'impatto sulla disciplina della società azionaria del mercato finanziario e delle conseguenti "alterazioni" dei principi caratterizzanti l'esperienza storica della società.

70 L. n. 43/2018 della Repubblica di Malta.

tiene alla istituzione del c.d. «*VFA agent*» che svolge funzioni sia di *advisory* preventiva che di controllo operativo sull'offerta e l'intera campagna finanziaria, cooperando con l'Autorità competente.

È questo senza dubbio «un tentativo coraggioso che mostra però i suoi limiti»[71], legati ad uno schema normativo eccessivamente rigido e non facilmente adattabile ai costanti mutamenti del mercato delle cripto-attività.

Successivamente, anche la Repubblica di San Marino si è orientata a disciplinare queste complesse operazioni finanziarie, pubblicando il 27 febbraio 2019 il decreto delegato n. 37[72].

Si disciplinano sia gli «*utility token*»[73] sia i «*security token*» che, come ricorda l'art. 9, sono rappresentativi di «a) azioni; b) strumenti finanziari partecipativi; c) titoli di debito dell'emittente».

Al fianco di questi primi tentativi propriamente legislativi, si può diffusamente notare che le varie Autorità europee abbiano assunto un approccio "*soft*" simile a quello adottato dalla Consob, privilegiando una prospettiva casistica.

È, ad esempio, il caso del Regno Unito in cui la «*Financial Conduct Authority*» (FCA) con le sue «*Guidance on crypto-assets*» del luglio 2019 ha proposto un approccio "*case-by-case*" che non esclude la possibilità di qualificare anche gli «*utility token*» quali prodotti finanziari laddove dotati dei caratteri tipici dell'investimento finanziario.

Lo stesso discorso vale anche per l'«*Autorité des Marchés Financiers*» (AMF) francese, che dopo aver avviato una prima consultazione pubblica sul tema nel 2017, è risultata sempre favorevole ad un'analisi basata sul caso specifico per cogliere le sottili differenze tra le tante tipologie di *token*[74].

L'Autorità di vigilanza tedesca (*BAfin*)[75] è apparsa meno timida nell'approccio qualificatorio, sancendo con chiarezza che i *token* di investimento che presentino i caratteri degli strumenti di capitale o di debito possono rientrare nella nozione di strumento finanziario, a

---

71 P. P. PIRANI, *op. cit.,* spec. p. 348.

72 Decreto Delegato 27 febbraio 2019, n. 37 del 2019, «*Norme sulla tecnologia Blockchain per le imprese*».

73 All'art. 8, co. 2 del citato decreto si definiscono dettagliatamente le caratteristiche tecnico-funzionali che i *token* di utilità devono assumere.

74 Per un inquadramento degli sviluppi regolatori in Francia, v. G. GITTI, M. MAUGERI e C. FERRARI, *op. cit.,* p. 109 ss.

75 Cfr. Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN), *Initial Coin Offerings: Hinweisschreiben zur Einordnung als Finanzinstrumente,* circolare del 20 febbraio 2018.

patto che essi siano trasferibili, negoziabili sul mercato di capitali e devono incorporare un diritto di natura partecipativa. Inoltre, compiendo un ulteriore passo in avanti, l'Autorità tedesca sembra equiparare le piattaforme di «*exchange*» ai sistemi multilaterali di negoziazione[76].

Volgendo, infine, lo sguardo oltreoceano, la «*Security and Exchange Commission*»[77] statunitense adopera il c.d. «*Howey Test*»[78] al fine di verificare se una *ICO* possa considerarsi come l'offerta di un contratto di investimento, con conseguente applicazione della disciplina prevista per le *securities.* Una valutazione che guarda alla "sostanza" dell'operazione e che verifica, caso per caso, la sussistenza di una ragionevole aspettativa di profitto derivante dall'investimento compiuto.

Alla luce delle presenti considerazioni ed in relazione alla transnazionalità del mercato delle cripto-attività, il quadro complessivo appare eccessivamente frammentato e privo di una matrice comune di disciplina. È, forse, proprio questo lo scopo primario da perseguire a livello sovranazionale: superare interventi a macchia di leopardo e orientarsi verso un orizzonte condiviso di regole, che faciliti l'emersione legittima di questi nuovi fenomeni e che offra sponde di tutela efficaci per gli investitori

8.6. L'ambiguità degli «*utility token*». Prospettive di analisi

Si è potuto notare che a livello sia nazionale che sovranazionale si sia cercato di compiere uno sforzo definitorio volto ad inquadrare il complesso fenomeno all'interno di categorie che in alcuni aspetti ricalcano gli antecedenti "tradizionali" ed in altri da essi se ne distaccano[79].

---

76 Per una analisi dettagliata dell'approccio seguito in Germania, v. E. Rulli, *Incorporazione senza res e dematerializzazione senza accentratore: appunti sui token,* in *Orizzonti del diritto commerciale,* 1, 2019, p. 136 ss.

77 Il 3 aprile 2019, la SEC ha pubblicato un documento che sintetizza i parametri per qualificare le operazioni legate ad una ICO quali contratti di investimento finanziario (cfr. SEC, *Framework for "Investment Contract" Analysis of digital asset,* Strategic Hub for Innovation and Financial Technology).

78 *SEC v. W.J. Howey Co.,* 328 U.S. 293, 1946. (Cfr. «a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party»).

79 Sulla necessità di ricondurre queste nuove dinamiche finanziarie entro i confini delle "tradizionali" categorie giuridiche, v. P. Carrière, *Le "criptovalute" sotto la luce delle*

È sfuggito, però, dai primari obiettivi di regolazione il tema degli «*utility token*» ibridi, e, in particolare, di quelli dotati di (diretta od indiretta) finanziarietà.

Anche la recente «*Proposta di Regolamento relativo ai mercati delle cripto-attività*» sembrerebbe (ad ora) aver mancato l'occasione di affrontare questo aspetto secondo l'angolo visuale della potenziale funzione finanziaria dei *token* di utilità, dettata, nella prassi, dalla sempre più frequente ibridazione delle loro caratteristiche funzionali[80]. Nella recente Proposta europea, infatti, la prospettiva di indagine rimane altamente descrittiva, non entrando mai nel merito del problema qualificatorio connesso alla combinazione, sul piano pratico, di suddette funzioni.

Appare chiaro, quindi, che se gli *utility token* puri «soddisfano esigenze di consumo del sottoscrittore, senza che l'apporto finanziario sia funzionale alla partecipazione all'iniziativa imprenditoriale dell'emittente o ad operazioni di prestito con obbligo di rimborso a carico dell'emittente stesso»[81], le difficoltà classificatorie si moltiplicano nel caso di *token* di utilità ibridi.

A tal proposito, sorge spontaneo domandarsi se quest'ultimi mantengano la prevalente funzione consumeristica di accesso ad un bene od un servizio anche laddove essi siano negoziati (o destinati al *trading)* sulle piattaforme di scambio e, soprattutto, nell'ipotesi in cui essi siano immessi sul mercato con lo scopo di procurare un incremento di valore nel patrimonio investito dal singolo sottoscrittore.

---

nostrane categorie giuridiche di *"'strumenti finanziari", "valori mobiliari" e "prodotti finanziari"; tra tradizione e innovazione,* in *Riv. dir. banc.*, 2, 2019, p. 3 ss.

80 Volendo esemplificare questi nuovi flussi, si pensi al caso in cui il *token* oltre al tipico diritto di godimento o di uso, attribuisce una forma di rendimento finanziario, quale la partecipazione ai profitti derivanti dal progetto imprenditoriale sostenuto o la previsione di un obbligo di riacquisto che comporti un incremento di valore patrimoniale. Un caso emblematico in questa direzione è rappresentato dai *token* emessi sulla piattaforma *Ethereum,* i c.d. «*Crypto-kitties*». Lanciati nel 2017, avevano la funzione di offrire l'accesso ad un gioco virtuale in cui ogni singolo utente poteva crescere un piccolo gatto "virtuale" (dotato di caratteristiche tali da differenziarlo da qualsiasi altro gatto). Il prezzo iniziale di vendita del singolo *token* si aggirava intorno ai 25 dollari, ma immediatamente dopo la loro prima immissione sulle piattaforme di scambio, il prezzo medio è cresciuto in modo esponenziale (toccando dei picchi di oltre 115mila dollari per ogni singolo "gattino" acquistato). Risulta, pertanto, evidente che nel caso di specie, come in altre ipotesi simili, la funzione di godimento ha ceduto il passo al carattere indirettamente finanziario della operazione.

81 M. De Mari, *op.cit.*, spec. p. 293.

Il problema, dunque, si pone proprio con gli «*utility token*» ibridi che, combinando tra loro più funzioni operative, lasciano aperte differenti ipotesi interpretative. Restano, pertanto, operazioni di natura consumeristica o assumono il rango di investimenti finanziari veri e propri[82]?

In via generale e nell'ottica di un possibile inquadramento degli elementi che vanno a comporre il substrato normativo delle operazioni qui in esame, si è prospettata l'applicazione della disciplina prevista per i contratti conclusi a distanza, così come prevista, nel nostro ordinamento, dal d.lgs. n. 70/2003[83]. La *ratio* di questa estensione risiede nella circostanza che il contratto di vendita di *token* avvenga in un contesto virtuale, dematerializzato e disintermediato[84].

Tenendo conto dell'alto tasso di ibridazione che questi *token* possono assumere, è, a maggior ragione, necessario indagare attentamente la causa in concreto dell'operazione finanziaria, verificando l'ulteriore e sempre più ricorrente, elemento della negoziabilità all'interno dei sistemi di scambio[85].

Infatti, come si è notato, spesso questi *token* dopo essere stati immessi nel mercato "primario" attraverso una ICO, vengono, poi, ammessi all'interno del mercato c.d. "secondario", composto da apposite piattaforme di *trading*.

Emerge nuovamente l'esigenza di inquadrare il fenomeno nella sua matrice dinamica, ovvero quella legata allo scambio dei *token* al fine di

---

82 «[…] il problema di vertice che da più parti si è posto è se la tokenizzazione valga ad attribuire carattere finanziario alla relazione (di per sé di consumo) che si instaura tra il sottoscrittore e l'emittente», così C. Sandei, Initial Coin Offering *e appello al pubblico risparmio,* cit., spec. p. 286.

83 Cfr. C. Sandei, *Le* Initial Coin Offering *nel prisma dell'ordinamento finanziario,* cit. p. 401 e ss. L'Autrice propone, in aggiunta, l'applicazione anche della disciplina consumeristica dettata dagli artt. 49-59 cod. cons. in relazione ai contratti a distanza, laddove, chiaramente, il sottoscrittore possa considerarsi come un "consumatore" ai sensi della disciplina nazionale ed europea.

84 Appare più forzata, invece, l'estensione applicativa della *Direttiva (UE) 2019/770/UE «relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali»,* sulla base di una distanza fenomenologica tra i contenuti digitali («i dati prodotti e forniti in formato digitale»; art. 2 n. 1 della recente direttiva), i servizi digitali (« *a)* un servizio che consente al consumatore di creare, trasformare, archiviare i dati o di accedervi in formato digitale; oppure *b)* un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore e da altri utenti di tale servizio o qualsiasi altra interazione con tali dati»; art. 2 n. 2) e i *token* di utilità dotati di una indiretta forma di investimento finanziario.

85 Favorevole a questa impostazione, v. M. De Mari, *op.cit.*, p. 288 ss.

poter comprendere l'effettiva funzione svolta, non limitandola ad una visione parziale e monca di un aspetto operativo determinante[86].

Sembrerebbe, infatti, da escludersi l'ipotesi per cui gli «*utility token*» dotati di finanziarietà possano essere considerati al pari di semplici *voucher*[87] che conferiscono al detentore il diritto di godere di determinati beni o servizi. Questa impostazione che ben si adatta alle forme c.d. pure, troverebbe anche una sponda argomentativa nella Direttiva UE 2016/1065[88] ma difetta di una analisi "sostanziale" utile a cogliere le effettive e concrete potenzialità finanziarie di questi *token*.

Se è vero che l'operazione finanziaria vada considerata nel suo complesso, allora, ci si domanda se la semplice indicazione all'interno del «*white paper*» della negoziabilità (certa o potenziale che sia) dei *token* emessi basti a considerare queste cripto-attività al pari dei prodotti finanziari[89].

---

[86] È, pertanto, auspicabile il riavvicinamento dell'approccio "statico", legato alla funzione economica, con quello "dinamico", connesso alla naturale inclinazione alla negoziabilità di questi nuovi strumenti. A sostegno di un approccio "*top-down*", specialmente nell'ipotesi di analisi dei *token* di utilità ibridi, v. F. ANNUNZIATA, *Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings*, in *European Company and Financial Review*, 2, 2020, spec. p. 142 ss.

[87] È questo l'approccio adottato dalla Agenzia delle Entrate, per cui l'emissione e la circolazione di *token* di utilità non assumono rilevanza ai fini dell'applicazione dell'IVA. Sul punto, si rimanda alla Risposta n.14/2018 dell'Agenzia delle Entrate. Per un ulteriore inquadramento della disciplina fiscale applicabile, F. ANTONACCHIO, *Initial Coin Offering: riflessi fiscali, antiriciclaggio e di tutela dei mercati finanziari, connessi all'emissione di criptovalute* (o *cripto-asset)*, in *Riv. dir. tributario*, I, 2019, p. 245 ss.

[88] Direttiva (UE) 2016/1065 del Consiglio, del 27 giugno 2016, recante modifica della direttiva 2006/112/CE per quanto riguarda il trattamento dei buoni. La direttiva qualifica i cd. *voucher* come strumenti validi ad essere impiegati come corrispettivo per la prestazione di un servizio o la cessione di un bene.

[89] L'art. 1, co. 1 lett. u del T.U.F stabilisce che debbono considerarsi come prodotti finanziari, «gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria; non costituiscono prodotti finanziari i depositi bancari o postali non rappresentati da strumenti finanziari». Come si può osservare, la definizione fornita risulta essere una nozione ampia, elastica, adattabile a fenomeni tra loro differenti ed altamente funzionale. Anche la giurisprudenza nazionale ha qualificato come operazioni aventi natura finanziaria ipotesi apparentemente molto lontane. È il caso, a titolo esemplificativo, delle opere d'arte vendute ad un prezzo scontato con la facoltà attribuita all'acquirente di rivenderle ad un prezzo maggiorato. In questa ipotesi, si è dato rilievo al carattere marcatamente finanziario dell'operazione, imponendo, pertanto, l'applicazione della disciplina finanziaria prevista in sede nazionale ed europea (cfr. Cass. civ., sez. II, n. 5911/18, in *ilcaso.it*).

La ragione di questo interrogativo risiede nella possibilità che nel documento iniziale di offerta venga prevista l'amissione dei *token* alla negoziazione all'interno delle piattaforme di «*exchange*», avvicinando queste cripto-attività alla categoria "aperta" dei prodotti finanziari, anche nella prospettiva visuale del singolo investitore[90].

Di conseguenza, se si dovesse ritenere accertata la natura finanziaria dell'operazione[91], il problema ulteriore sarebbe quello di inquadrare correttamente il *token* all'interno dei «microinsiemi che compongono l'arcipelago disegnato dal TUF»[92].

Pertanto, è necessario comprendere in dettaglio il funzionamento tecnico di queste operazioni finanziarie, per poter ricavare gli elementi rilevanti ai fini della collocazione giuridica di questi *token.*

Va osservato che questi «*utility token*» ibridi sono solitamente emessi in massa, in forme e modalità standardizzate e sono destinati alla negoziazione sui sistemi di «*exchange*»[93]. Sono queste caratteristiche che avvicinerebbero significativamente tali cripto-attività alla categoria dei valori mobiliari[94] *ex* art. 1, co. l-*bis*, TUF[95].

---

90 È quanto sostentuto anche dall'ESMA che, nel suo studio sul fenomeno, afferma: «also, while certain crypto-assets are outside of the scope of EU financial regulation, they may still be perceived as security-like investments by retail investors, e.g., due to the possibility of trading them on secondary markets»; cfr. ESMA, *op.cit.,* spec. p. 13.

91 Chiaramente la qualificazione dei *token* ibridi (emessi tramite una apposita ICO) come prodotti finanziari dovrebbe comportare l'applicazione della disciplina prevista dagli artt. 93-*bis* e ss. del TUF in tema di offerta al pubblico di sottoscrizione e di vendita.

92 C. Sandei, Initial Coin Offering *e appello al pubblico risparmio,* cit., spec. p. 294.

93 Per un inquadramento (scettico) di questi *token* ibridi e della disciplina europea, v. P. Hacker e C. Thomale, *The Crypto- Security. Initial Coin Offerings and EU Securities Regulation*, in Aa. Vv., *Regulating Blockchain: Techno-Social and Legal Challenges,* p. 241 ss.

94 Anche l'ESMA sembra non escludere questa ipotesi, rimarcando la forte standardizzazione dei *token* e la loro connaturata funzione di negoziabilità all'interno dei mercati di *trading* (cfr. ESMA, *op. cit.,* p. 19 ss.). In questo senso v., E. Rulli, *op. cit.,* spec. p. 150. L'Autore sostiene, infatti, che «sia lecito sostenere che i *token* di investimento standardizzati, trasferibili, negoziabili su di un mercato digitale la cui esistenza non può essere negata, siano potenzialmente riconducibili alla fattispecie dei valori mobiliari e, per il tramite di questa, rientrare nella nozione di strumento finanziario».

95 «Per "valori mobiliari" si intendono categorie di valori che possono essere negoziati nel mercato dei capitali, quali ad esempio: *a*) azioni di società e altri titoli equivalenti ad azioni di società, di partnership o di altri soggetti e ricevute di deposito azionario; *b)* obbligazioni e altri titoli di debito, comprese le ricevute di deposito relative a tali titoli; *c*) qualsiasi altro valore mobiliare che permetta di acquisire o di vendere i va-

Come si evince dalla norma, la negoziabilità dei valori mobiliari deve avvenire all'interno di specifici "mercati di capitali". Il corollario di interrogativi che discende dalla potenziale applicazione della suddetta disciplina, abbraccia il tema della qualificazione delle piattaforme di «*exchange*» e della loro riconducibilità al dettato regolatorio derivante dalla MIFID II e, in particolare, dal titolo II della direttiva[96].

Si deve osservare, da subito, che queste piattaforme possono essere sia "decentralizzate"[97] sia "centralizzate", ovvero sistemi che operano sia come piattaforme di *trading* sia come fornitori di servizi di custodia (c.d. servizi di *wallet*). Se le piattaforme "decentralizzate" non possono considerarsi, ad oggi, come sedi di negoziazione legittime[98], le piattaforme "centralizzate", invece, potrebbero considerarsi assimilabili ai "sistemi multilaterali di negoziazione"[99] od ai "sistemi organizzati di negoziazione"[100] per le loro peculiarità tecniche.

---

lori mobiliari indicati alle lettere a) e b) o che comporti un regolamento a pronti determinato con riferimento a valori mobiliari, valute, tassi di interesse o rendimenti, merci o altri indici o misure».

96 Sembrerebbe da escludersi, infatti, l'estensione della disciplina prevista per i c.d. "mercati regolamentati" (art. 1, co. 1, lett. w-*ter*, TUF), non presentando le caratteristiche richieste anche dal titolo III della direttiva MIFID II.

97 Le piattaforme "decentralizzate" agiscono come meri strumenti di *matching* per le offerte di acquisto di *token,* non conservano dati delle transazioni e non svolgono attività di custodia per i singoli investitori.

98 Cfr. F. ANNUNZIATA, *La disciplina delle* trading venues *nell'era delle rivoluzioni tecnologiche: dalle criptovalute alla* distributed ledger technology, in *Orizzonti del diritto commerciale,* 3, 2018, p. 21 ss.

99 «"sistema multilaterale di negoziazione": un sistema multilaterale gestito da un'impresa di investimento o da un gestore del mercato che consente l'incontro, al suo interno e in base a regole non discrezionali, di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, in modo da dare luogo a contratti conformemente alla parte II e alla parte III»; art. 1, co. 5-*octies,* lett. a), TUF.

100 «"sistema organizzato di negoziazione": un sistema multilaterale diverso da un mercato regolamentato o da un sistema multilaterale di negoziazione che consente l'interazione tra interessi multipli di acquisto e di vendita di terzi relativi a obbligazioni, strumenti finanziari strutturati, quote di emissioni e strumenti derivati, in modo da dare luogo a contratti conformemente alla parte II e alla parte III», art. 1, co. 5-*octies,* lett. b), TUF.

Questa impostazione sembra essere avallata anche dall'ESMA[101] e permetterebbe di conciliare (o quantomeno mitigare) anche l'obbligo di gestione accentrata dettato dalla sezione II del titolo II-*bis* del TUF[102].

Rimanendo focalizzati sugli aspetti pratico-funzionali, si potrebbe, infine, sostenere che questi *token* ibridi che, oltre alla funzione consumeristica di godimento del bene o servizio, offrono anche un rendimento di natura finanziaria, talvolta sotto forma di diritto di partecipazione, possano essere accostati agli strumenti finanziari partecipativi *ex* art. 2346 c.c., ult.co[103].

Tale accostamento potrebbe svincolare, di fatto, il problema qualificatorio degli «*utility token*» ibridi dalle maglie rigide delle classificazioni precedentemente analizzate, verso un inquadramento maggiormente flessibile e più aderente alla reale funzione economica di questi strumenti. In tal modo, ci si distaccherebbe anche dal vincolo "interpretativo" costituito della negoziabilità dei *token* all'interno delle apposite piattaforme, concentrando, invece, l'attenzione sulla natura dei diritti che vengono attribuiti tramite tali operazioni.

La giustificazione a una siffatta ricostruzione, difatti, potrebbe risiedere non soltanto sulla indiretta finanziarietà di queste cripto-attività ibride, ma anche sulla loro caratteristica di poter attribuire fasci di diritti (specialmente patrimoniali, ma anche amministrativi) connessi

---

101 ESMA, *op. cit.,* p. 25 ss. Per un confronto tra piattaforme centralizzate e decentralizzate, *ivi,* p. 44 ss.

102 Bisogna considerare la necessità di ridefinire le regole preesistenti adattandole alle mutate esigenze del mercato finanziario. In questo senso, probabilmente, molto significative saranno le implicazioni che deriveranno dall'implementazione e dai successivi passaggi evolutivi della «*Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito*» COM (2020) 594 def. Sul punto, l'art. 2(3), propone una definizione di «sistema multilaterale di negoziazione DLT (MTF DLT)», quale un «sistema multilaterale di negoziazione, gestito da un'impresa di investimento o da un gestore del mercato, che ammette alla negoziazione solo valori mobiliari DLT e che può essere autorizzato, sulla base di regole e procedure trasparenti, non discrezionali e uniformi, a: *(a)* assicurare la registrazione iniziale dei valori mobiliari DLT; (*b*) regolare le operazioni in valori mobiliari DLT contro pagamento; e (*c*) prestare servizi di custodia in relazione ai valori mobiliari DLT o, se del caso, ai relativi pagamenti e garanzie reali, utilizzando il sistema multilaterale di negoziazione DLT».

103 «Resta salva la possibilità che la società, a seguito dell'apporto da parte dei soci o di terzi anche di opera o servizi, emetta strumenti finanziari forniti di diritti patrimoniali o anche di diritti amministrativi, escluso il voto nell'assemblea generale degli azionisti. In tal caso lo statuto ne disciplina le modalità e condizioni di emissione, i diritti che conferiscono, le sanzioni in caso di inadempimento delle prestazioni e, se ammessa, la legge di circolazione».

ad uno specifico progetto imprenditoriale. In tal senso, sarà utile verificare se la prassi di mercato vada a confermare questo profilo di indagine, il quale potrebbe offrire ulteriori spunti di delucidazione sul consequenziale problema della circolazione di questi *token*[104].

Alla luce di queste considerazioni, in assenza di un dettagliato ed esaustivo intervento legislativo a livello nazionale ed internazionale data la trasversalità del fenomeno in esame, la prospettiva di analisi non potrà che seguire un approccio caso per caso che miri a verificare nell'ambito degli «*utility token*» ibridi la prevalenza della funzione finanziaria rispetto all'elemento meramente consumeristico di godimento del bene o servizio, tenendo conto del complesso dell'operazione effettuata, privilegiando, dunque, un criterio "sostanziale" che superi la mera "forma" della terminologia impiegata.

8.7. Riflessioni conclusive: quale futuro per il mercato delle cripto-attività?

È indubbio che queste innovative iniziative finanziarie possano presentare considerevoli vantaggi per gli operatori economici, costituendo una valida e reale alternativa alle tradizionali forme di finanziamento e permettendo una raccolta di risorse finanziarie rapida, disintermediata, ed efficiente.

Elemento centrale delle «*Initial Coin Offering*» ed in generale dell'intero mercato delle cripto-attività, è la tecnologia impiegata. Si è detto in apertura che senza il ricorso ai sistemi dotati di tecnologia DLT, tra cui la "celebre" *blockchain*, simili operazioni sarebbero non solo estremamente onerose e complesse, ma anche e soprattutto, impossibili. L'infrastruttura tecnologica utilizzata riduce notevolmente i costi di intermediazione, tipici di siffatte operazioni finanziarie e rende facili ed immediate queste transazioni.

Ulteriore aspetto da dover considerare è la sempre maggiore liquidità del mercato delle cripto-attività, specialmente nella fase secondaria di negoziazione all'interno di specifici sistemi di *trading* e negoziazione.

---

[104] L'art. 2346, ult.co. lascia, infatti, notevole autonomia allo statuto in merito alle modalità di emissione di questi strumenti partecipativi, alla natura dei diritti concessi e alle condizioni della loro circolazione, rendendoli, di fatto, strumenti molto flessibili che ben si adattano alle mutevoli necessità economico-aziendali.

Al fianco degli evidenti aspetti positivi, si nascondono, però innegabili criticità. Sorvolando sulla natura fraudolenta delle prime *ICOs* [105], bisogna, innanzitutto, sottolineare che queste siano solitamente operazioni caratterizzate da una forte asimmetria informativa [106] che gioca a favore dell'emittente/offerente, a discapito dell'esigenza di sicurezza e trasparenza [107], imprescindibile in un settore delicato come quello degli investimenti finanziari.

Dunque, l'assenza di un quadro giuridico esaustivo ed uniforme impedisce di fornire una «efficace tutela legale e/o contrattuale degli interessi degli investitori» [108], lasciando tutt'oggi il fenomeno in una zona d'ombra.

In considerazione dei primi interventi legislativi adottati a livello europeo ed internazionale ed alla luce delle osservazioni compiute, le linee direttive da poter seguire sembrano essere principalmente tre: i) riadattare le regole preesistenti, facendo rientrare questi fenomeni nella legislazione in materia finanziaria; ii) adottare una prospettiva casistica, che valuti la singola operazione nel suo complesso al fine del più corretto inquadramento giuridico, ed, infine, iii) predisporre una regolamentazione *ad hoc,* sul modello della Proposta di regolamento citata.

In conclusione, al di là di quello che sarà l'approccio adottato, è sempre utile rimarcare l'opportunità di conoscere prima il fenomeno

---

105 Infatti, la possibilità di compiere queste operazioni in via del tutto anonima, ricorrendo a sistemi «*permissionless*», privi di qualsiasi forma di controllo, facilita il perseguimento di finalità fraudolente.

106 I prospetti informativi, infatti, non sono sempre dettagliatamente definiti e lasciano spesso dubbi interpretativi riguardo la natura dei *token* emessi ed in merito alle (eventuali) modalità di negoziazione. A tal riguardo, l'art. 7 della citata Proposta di Regolamento sul mercato delle cripto-attività, non impone una preventiva approvazione del «*white paper*» da parte delle autorità competenti, ma la semplice comunicazione venti giorni prima della pubblicazione. Sarebbe stato, forse, più opportuno allineare questi aspetti ai ben più rigidi schemi in tema di prospetto ed offerta al pubblico di prodotti finanziari per evitare inefficaci discrasie.

107 «Non sono previsti meccanismi di tutela degli investitori o dei creditori dell'organizzazione», così P. P. Pirani, *op.cit.,* spec. p. 344.

108 S. Comellini, M. Vasapollo, *Blockchain, Criptovalute, I.C.O. e Smart Contract,* Soluzioni di Diritto, Maggioli ed., 2019, spec. p. 55. Non va, inoltre, dimenticata l'esigenza di tutela del consumatore, il quale, specialmente nel caso di *token* di utilità, assume la veste "ibrida" di acquirente-investitore. Sul punto, v., EBA, *op. cit.*, p. 15 ss.

sul piano tecnico-operativo per poi operare in sede legislativa le desiderate trasformazioni. Come d'altronde ricordava Catone il Censore, «*rem tene, verba sequentur*»[109].

[109] G. G. VITTORE, *De inventione*, in *Ars rhetorica*, p. 374.

9. Protezione dei dati personali e *antitrust*. L'incidenza dell'uso secondario dei *big data* sulla concorrenza

Laura Mancini

9.1. *Big data* e mercato

I *big data*[1] sono «*ingenti quantità di dati disponibili all'interno del nuovo ecosistema digitale, prodotti ad alta velocità e provenienti da una moltitudine di fonti, la cui gestione richiede potenti processori e algoritmi*»[2].

Si tratta di informazioni di vario contenuto[3] raccolte in modo massivo mediante i sistemi di Intelligenza Artificiale, anche per essere cedute ad altri operatori economici allo stato "grezzo" o previa trasformazione, mediante gli algoritmi, in informazioni utilizzabili.

L'interesse giuridico per i *big data* deriva dall'incidenza che l'utilizzazione e la riutilizzazione delle informazioni con essi veicolate può

---

1 Tra i più recenti contributi sul tema si vedano FINOCCHIARO, *Intelligenza artificiale e diritto - intelligenza artificiale e protezione dei dati personali,* in *Giur. it.*, 2019, 7, 1657; STAZI, CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inf. e informatica*, 2019, 2, 442 e ss.; OLIVI, *Big data, metadati e intelligenza artificiale: i confini tra i diversi diritti,* in *Dir. ind.*, 2020, 2, 181; D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf. e informatica*, 2020, 3, 634 e ss.; VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, in *Giur. comm.*, 2018, 6, 1064 e ss.; *Big data, competition and privacy: a look from the Antitrust perspective*, in DI PORTO (a cura di), *Big data e concorrenza*, in *Concorrenza e mercato*, 2016, 15 ss.

2 Definizione elaborata nello studio su *L'economia dei dati. Tendenze di mercato e prospettive di policy*, Roma, gennaio 2018, condotto dalla IT Media Consulting in collaborazione con l'Università Bocconi.

3 I dati identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e conoscibili le sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica.

esplicare, oltre che sulla protezione dei dati personali, sul funzionamento della concorrenza, ben potendo la circolazione dei dati personali interferire con l'efficienza del mercato.

Tale fenomeno sta assumendo in tempi recenti dimensioni ragguardevoli in ragione della sempre più marcata tendenza dei titolari delle maggiori *digital platforms* ad estendere la propria attività di impresa in settori economici diversi da quello digitale[4] e ad utilizzarvi i *data set* detenuti.

L'impiego *secondario* o *alternativo* dei *big data analytics* genera, infatti, un vantaggio competitivo perché la possibilità di raccogliere, immagazzinare, analizzare, aggregare dati e di produrre *metadati* [5] pone gli operatori digitali nella condizione di offrire ai clienti dei nuovi settori economici servizi migliori, personalizzati e a prezzi più bassi.

L'osservazione empirica dell'ecosistema digitale dimostra, invero, gli utenti trasmettono i propri dati agli operatori al fine di fruire gratuitamente di prodotti o servizi digitali o di condividere contenuti (foto, messaggistica, video, come accade con i *socialnetwork*), o, comunque, li rilasciano - più o meno consapevolmente - nel *web* attraverso i *cookies*[6].

Una parte della dottrina ritiene che nel mercato digitale i dati rappresentano un *asset* essenziale controllato da imprese in posizione dominante che impediscono ai concorrenti di entrare nel relativo mercato, giacché il possesso di *data set* (collezioni di dati) attribuisce

---

4 Come, ad esempio, i settori bancario, finanziario e assicurativo. Osservano, in proposito, STAZI, CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inf. e informatica*, 2019, 2, cit., che «*Tra gli altri, l'esempio più chiaro di industria data driven è forse rappresentato dal settore finanziario-assicurativo, in cui gli istituti creditizi, attraverso lo sfruttamento dei dati dei clienti sono in grado di trasformare il loro business, realizzare nuove opportunità di ricavi, gestire al meglio i rischi e rafforzare il rapporto fiduciario con i clienti stessi. Le imprese dei media guardano al paradigma Data Driven Innovation per decidere su quali prodotti investire e per modellare le proprie offerte al fine di attrarre e soddisfare al meglio la domanda dei fruitori dei propri servizi in un mercato che è sempre più competitivo. Non è più sufficiente pubblicare una rivista o mandare in onda nuovi programmi televisivi, bensì gli operatori devono estrarre valore dai propri assets rispetto a ciascuna fase del ciclo di vita dei dati*».

5 I metadati sono dati ottenuti per mezzo di altri dati.

6 Si tratta di *files* in grado di catturare e memorizzare i siti visitati, la geolocalizzazione dell'utente e informazioni su abitudini, preferenze, bisogni dei consumatori.

all'operatore un vantaggio competitivo non replicabile[7].

Per altra tesi i dati personali costituiscono, invece, beni liberamente accessibili da parte di chiunque[8].

Alla stregua della prima impostazione, la scorretta gestione delle informazioni fornite dagli interessati può generare, oltre che condotte in contrasto con le norme sul trattamento dei dati personali, comportamenti anticompetitivi (operazioni di concentrazione e acquisizione, condotte escludenti derivanti dal rifiuto di accesso o accesso discriminatorio ai dati, contratti di esclusiva, vendite vincolate, utilizzo incrociato di *data set*, nell'uso di dati per realizzare attività di *price discrimination*) e ipotesi di abuso di posizione dominante.

Per tale ragione le particolarità del mercato digitale, della natura dei dati personali e della loro circolazione impongono un'opera di adattamento della vigente disciplina *antitrust* che tenga conto dell'inscindibile commistione tra l'interesse al governo del mercato e le esigenze di *data protection*.

Occorre, in particolare, rivisitare la nozione di *mercato rilevante* e istituti come il *test* del monopolista ipotetico per la valutazione della sostituibilità dal lato della domanda e il parametro delle soglie di fatturato per il calcolo delle quote di mercato ai fini del giudizio sulla posizione di dominanza o sulla rilevanza delle concentrazioni[9].

È, inoltre, avvertita l'esigenza di indagare sugli eventuali profili di interferenza e di interessenza tra i distinti sistemi disciplinari della protezione dei dati personali e della normativa sulla concorrenza.

---

[7] EZRACHI, STUCKE, *Virtual Competition. The promise and perils of the algorithm-driven economy*, in *Harvard University Press*, 2016; PITRUZZELLA, *Big Data, competition and privacy: a look from the antitrust perspective*, cit., 15 ss., richiamati da D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, cit., 634 e ss., spec. nota 17.

[8] SOKOL, COMERFORD, *Does antitrust have a role to play in regulating Big Data?*, in *Cambridge handbook of Antitrust, Intellectual Property and High Tech, Cambridge University Press*, 2016; LAMBRECHT, TUCKER, *Can Big Data protect a firm from competition?*, *Working paper*, 18 dicembre 2015, richiamati da D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, cit., 634 e ss., spec. nota 18.

[9] *L'esigenza di rivisitazione della disciplina* antitrust *trova conferma nella riforma del diritto antitrust (GBW) tedesco intervenuta con legge del 9 marzo 2017.*

L'approccio degli interpreti a tale operazione ermeneutica si è mostrato sinora altalenante[10] poiché, a fronte di un'iniziale considerazione in termini di autonomia[11], si è passati ad un apprezzamento dei diversi aspetti (analisi *antitrust* e protezione dei dati personali) del fenomeno in termini sinergici e congiunti[12].

9.2. Dati personali e autonomia privata

La propensione degli utenti a concedere con disinvoltura i propri dati personali al fine di fruire di contenuti e servizi digitali costituisce ormai un fenomeno imponente, al quale si correla la tendenza altrettanto marcata degli operatori a fare della raccolta, dell'elaborazione e dello sfruttamento delle informazioni così acquisite il proprio *business model*, tanto che si parla di economia *data-driven*.

Osservata *sub specie iuris*, la circolazione dei dati personali pone una serie di questioni di rilevante portata sistematica, tutte riconducibili alla natura giuridica dei dati personali e alla loro attitudine a formare oggetto di contratti di scambio.

È appena il caso di ricordare la ritrosia del pensiero giuridico tradizionale ad accogliere l'idea della contrattualizzazione degli attributi della personalità dell'individuo, tra i quali vanno inclusi, secondo un'opzione ermeneutica ampiamente condivisa, anche i dati personali[13].

Tale atteggiamento riluttante si radica sull'idea per la quale l'autonomia privata, di cui il contratto costituisce la più significativa

---

10 Per un'esaustiva ricostruzione del dibattito, si veda ancora VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., spec. note 80-83 e 86-91 e i riferimenti bibliografici ivi indicati qui di seguito parzialmente riportati (note 10 e 11).

11 In tal senso Commissione europea, Microsoft/LinkedIn (COMP/M. 8124 del 6 dicembre 2016). In dottrina si veda ROSSI, *Social network e diritto antitrust*, in *AIDA*, 2011, 84 e ss.; opta per tale approccio anche Corte giust., 23/11/2006, Asnef-Equifax, C-238/05.

12 Aderisce a tale opzione interpretativa MERIANI, *Digital platforms and spectrum of data protection in competition law analyses*, in *ECLR*, 2017, 38, 2, 89.

13 In generale, sul rapporto tra autonomia privata e diritti della personalità, v. RESTA, *Contratto e diritti della personalità,* in *Trattato del contratto* diretto da ROPPO, VI, *Interferenze,* Milano, 2006; THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali,* Milano, 2018.

estrinsecazione, implicando la nozione di disposizione, ossia di passaggio di una situazione soggettiva da un compendio ad un altro, si palesa incompatibile con i diritti della persona, i quali sono tradizionalmente contraddistinti da intrasmissibilità, indisponibilità e irrinunciabilità[14].

In questa prospettiva si è sostenuto che il consenso del titolare del diritto all'ingerenza del terzo nella propria sfera personale (come il consenso al trattamento dei dati personali) è estraneo al paradigma concettuale dell'atto dispositivo ed ha natura di esimente rispetto ad un'attività altrimenti illecita e lesiva. E tale ricostruzione sarebbe avvalorata dalla naturale revocabilità del consenso autorizzatorio e della sua incapacità a trasferire in capo alla controparte situazioni soggettive se non in termini di precarietà[15].

Un diverso approccio ermeneutico suggerisce di operare un distinguo tra beni-fine e beni-presupposto[16]. I primi sono considerati disponibili dal titolare, sia pure nei limiti di una disposizione temporanea o parziale o comunque reversibile, inerendo l'atto con il quale viene autorizzata l'ingerenza nella sfera del titolare all'esercizio e non anche alla titolarità del diritto fondamentale.

La medesima concezione predica, invece, l'intangibilità dei beni-presupposto (come la vita e l'integrità psicofisica) dalla cui sussistenza dipende lo stesso potere di godere e disporre di ogni altra situazione giuridica soggettiva.

In tale contesto si iscrive il dibattito sulla contrattualizzazione dei dati personali che vede contrapposta alla tesi che riduce il consenso al trattamento dei dati ad esimente da responsabilità[17], l'opinione che,

---

14 NICOLUSSI, *Autonomia privata e diritti della persona,* in *Enc. del dir., Annali,* IV, Milano, 2011, 133 e ss.

15 In tal senso Cass. Sez. I, 17/2/2004, n. 3014; Cass. Sez. I, 29/1/2016, n. 1748, in *Danno e resp.,* 2017, 1, 47 e ss., con nota di BARNI, *Cassazione e diritto all'immagine: divulgazione del ritratto per scopi pubblicitari, revocabilità del consenso, tutela risarcitoria.*

16 NICOLUSSI, *Autonomia privata e diritti della persona,* cit., 134, il quale richiama CASTRONOVO, *Autodeterminazione e diritto privato*, in *Eur. dir. priv*., 2010, 1046.

17 A tale impostazione ha aderito il Garante europeo della protezione dei dati, il quale nel parere del 17 marzo 2017 ha sottolineato la pericolosità dell'accostamento alla controprestazione pecuniaria della fornitura di dati personali, essendo questi ultimi oggetto di un diritto fondamentale, come tale non paragonabile ad una merce. In conseguenza di tale indicazione, dal testo dell'art. 3 della dir. UE 2019/770 è stato

valorizzando le direttrici ermeneutiche provenienti dal diritto dell'Unione europea, vi intravede una manifestazione di volontà negoziale che compendia in sé non solo la funzione di strumento di controllo sui dati, ma anche quella di elemento essenziale di un contratto che comporta uno spostamento patrimoniale e, quindi, la circolazione della ricchezza secondo le regole del mercato[18].

Il fenomeno circolatorio costituisce, invero, il *telos* della disciplina dettata dal Regolamento UE 2016/679, il quale all'art. 1 precisa che la circolazione dei dati non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali[19].

La tesi propensa ad ammettere la contrattualizzazione dei dati personali trae, inoltre, elementi di conferma dalla direttiva 2019/770 UE del 20 maggio 2019, relativa ai contratti digitali, il cui art. 3, par. 1, considera, accanto ai contratti con i quali un operatore si impegna a fornire un bene o un servizio digitale dietro il corrispettivo di un prezzo, anche i contratti con i quali lo stesso operatore economico si impegna a fornire un contenuto o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali[20].

Sebbene nelle fonti unionali non risulti chiarito se il contratto predetto trasferisca un diritto di natura dominicale o un diritto di uso del dato, è innegabile, secondo l'impostazione in esame, che esso realizzi una funzione di scambio tra la fruizione di contenuti e servizi digitali e lo sfruttamento i dati personali dell'interessato, intesi quale specifica ricchezza patrimonialmente valutabile[21].

Altri intravedono nella fattispecie delineata dall'art. 3 della dir. UE 2019/770 due manifestazioni di consenso parallele, la prima delle quali

---

espunto il riferimento al "corrispettivo" originariamente previsto. In dottrina v. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 350 e ss..

18 RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf. e informatica*, 2018, 4, 689 e ss.

19 V., *infra*, § 7.

20 Sulla quale v. DE FRANCESCHI, *Il "pagamento" mediante dati personali,* in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO, RICCIUTO, Torino, 2019, 1384.

21 Così RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 689 e ss.

diretta a disporre, solo apparentemente in forma gratuita, la fornitura di contenuti o servizi digitali, e la seconda volta ad autorizzare il trattamento dei dati personali.

Tale soluzione riposa sull'assunto per il quale il dato personale è estrinsecazione dell'identità personale e della personalità dell'individuo. Di conseguenza, il diritto alla protezione dei dati è considerato assoluto, indisponibile, intrasmissibile, imprescrittibile e insuscettibile di commercializzazione. Esso rientra nel sistema di tutela della riservatezza e tra i diritti fondamentali della persona, come si ricava dall'art. 8 della CEDU, dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 16 TFUE[22].

La validità di tale ricostruzione è stata, tuttavia, posta in dubbio da coloro che valorizzano il vincolo funzionale che avvince le due manifestazioni di consenso per attribuire all'operazione economica un'effettiva corrispettività. In questa linea ermeneutica i dati personali vengono, invero, concepiti come beni, sia pure immateriali, di cui può essere concesso il godimento non esclusivo o il diritto allo sfruttamento economico ovvero alla trasformazione finalizzata alla creazione di dati ulteriori, sul presupposto che tali informazioni possono formare oggetto di fruizione contemporanea da parte di più soggetti senza essere consumate.

Secondo la concezione contrattualistica, l'opposta tesi che esclude che i dati possano essere assimilati ai beni-merce, trascura il fatto indiscutibile dell'attitudine di tali informazioni alla circolazione, la quale postula, a propria volta, operazioni di scambio.

In definitiva, la circolazione rende il dato personale una risorsa economicamente apprezzabile[23] collocandolo in una dimensione patrimonialistica che, peraltro, non è affatto estranea all'esperienza giuridica dei sistemi di *civil law*[24], non ravvisandosi ostacoli sistematici alla

---

[22] Tra i più autorevoli sostenitori di tale tesi si ricorda RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 397 ss.; Id., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583. Per un'ampia disamina sul tema, v. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, cit., 634 e ss.

[23] In questi termini SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali,* in *Contratto e impr.*, 2020, 2, 760 e ss.

[24] Paradigmatiche, al riguardo, sono le fattispecie della sponsorizzazione e lo stesso contratto di lavoro.

deducibilità dei diritti della personalità in un negozio giuridico[25]. Infatti, la circolazione immette i dati personali nel mercato, il quale attribuisce loro un valore d'uso e un valore di scambio[26].

Va, infine, evidenziato che l'approccio *market oriented* è incline ad attribuire al mercato il compito di assicurare la protezione dei dati personali attraverso la concorrenza o la *self regulation*[27].

9.3. Il mercato rilevante dei *big data*

Tra le questioni interpretative suscitate dall'innesto della circolazione dei dati nell'assetto del mercato particolare criticità presenta quella concernente la possibilità di identificare autonomamente un mercato rilevante dei dati personali[28].

Occorre, innanzitutto, considerare che i *big data* possono assolvere ad una funzione diversa a seconda dell'oggetto dell'attività economica svolta dall'operatore economico che se ne avvalga.

Infatti, se per talune imprese, come quelle operanti nei settori assicurativo, bancario e finanziario, essi costituiscono un *input* della produzione, ovvero uno dei molteplici fattori che concorrono alla creazione ed implementazione del *business*, per altri operatori i dati personali costituiscono il risultato dell'attività economica (*output*), avendo l'attività di impresa ad oggetto proprio la raccolta e la rivendita di dati stoccati in maniera grezza o raffinati attraverso l'algoritmo (cd. *metadati*).

Non va, inoltre, trascurato che il mercato digitale si impernia sull'utilizzo delle piattaforme, le quali possono essere anche a doppio versante o multiversante, in relazione alla possibilità per i gestori di

---

25 PERLINGIERI, *L'informazione come bene giuridico,* in *Rass. dir. civ.*, 1990, 339; più in generale si rinvia al fondamentale contributo di PUGLIATTI, voce *Beni (teoria generale),* in *Enc. del dir.*, Milano 1959, 173.

26 Così SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali,* cit., 760 e ss.

27 A tale ricostruzione accede HERMSTRÜVER, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data,* in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2017, 9.

28 Su cui si veda, MINUTO RIZZO, *I profili antitrust del nuovo web e della nuova economia digitale*, in *Dir. ind*., 2019, 2, 113 e ss.

motori di ricerca, i *socialnetwork* e le piattaforme di *e-commerce* di rivendere i dati memorizzati e collezionati agli inserzionisti che intendono acquistare gli spazi pubblicitari[29].

Al fine di tratteggiare la nozione di mercato rilevante nell'economia digitale occorre, inoltre, considerare:

a) gli effetti di rete (o *esternalità di rete*), ovvero il dato empirico per il quale il beneficio che un individuo trae dall'utilizzo di un bene si accresce all'aumentare del numero di utilizzatori di quel bene. Questo tipo di situazione assume particolare rilevanza nei mercati in cui predomina la proprietà intellettuale, come il *software* e le innovazioni tecnologiche.

b) La natura dei dati e, in particolare, la loro assimilabilità alla moneta di scambio (*currency*) del servizio. Infatti, secondo una prima ricostruzione, cui ha prestato adesione il legislatore tedesco, la piattaforma è un mercato perché i dati sono il corrispettivo del servizio. Altra tesi sostiene, invece, che i dati non hanno natura patrimoniale e la piattaforma non integra un mercato.

c) La distinzione tra piattaforma "di contrattazione" e non[30].

Ancora, nella determinazione del perimetro merceologico del mercato rilevante dei dati occorre stabilire se e in che misura i dati sono beni sostituibili al fine di valutare l'esistenza di fonti alternative di approvvigionamento effettive[31].

Tanto premesso, secondo l'opinione prevalente in dottrina, alla quale ha mostrato di accedere la stessa Commissione europea, con riferimento ai *big data* non è configurabile un unico mercato rilevante, ma una pluralità di mercati rilevanti, specie nell'ipotesi in cui i dati

---

29 V. il provvedimento dell'AGCM del 30 maggio 2017, n. 26620 che individua un mercato per ciascuna piattaforma.

30 Valorizza tali presupposti VESSIA, op. cit., spec. note 22-26.

31 VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., 1070, individua i parametri di sostituibilità negli effetti di rete diretti e indiretti, unilaterali e bilaterali, nell'ubiquità, ossia nella possibilità di raccoglierli ovunque nel *cyber space*; nella non rivalità; nella velocità di raccolta e aggiornamento (per ciò che concerne il profilo temporale, questo è a tal punto rilevante che qualcuno ha ritenuto di aggiungere alle tradizionali categorie del mercato merceologico e di quello geografico, anche il criterio dell'orizzonte temporale); nella rilevanza degli algoritmi utilizzati per l'analisi dei dati e l'estrazione dei metadati.

costituiscono l'*output* di un'attività di impresa e siano oggetto di scambio attraverso la licenza d'uso[32].

Secondo tale prospettiva, si distinguono, quindi, tanti mercati quanti sono i segmenti del ciclo dei dati, da identificarsi nella raccolta (*big data capture*), nell'immagazzinamento di dati grezzi (*big data storage*), nell'analisi dei dati ed estrazione dei metadati (*big data analytics*), nel riutilizzo (*big data utilisation*) [33].

9.4. Intese e pratiche collusive

Nella *digital economy* si assiste ad un fenomeno di concentrazione del potere di mercato in capo a pochi operatori dotati di grandi quote di mercato, da cui sorge il rischio di creazione di barriere di ingresso per altri operatori (*foreclosure effect).*

È stato, infatti, evidenziato come tale assetto generi un circolo vizioso, dal momento che gli utenti - i quali ambiscono a fruire di contenuti e servizi sempre più sofisticati - tendono a cedere i loro dati personali ai colossi del digitale [34] sostenendone gli investimenti pubblicitari e la creazione di servizi sempre migliori a scapito delle imprese minori, il cui *gap* quantitativo e qualitativo conosce un costante incremento[35].

Una simile tendenza assume rilevanza non solo con riguardo alla fattispecie dell'abuso di posizione dominante, ma anche con riferimento alle intese e alle pratiche collusive[36] e al rischio di allineamento dei prezzi.

---

32 Evidenzia VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., 1071, spec. nota 28, che tale approccio interpretativo è stato seguito dalla Commissione europea nelle operazioni di fusione Google/DoubleClick (COMP/M.4731 del 22/7/2008), Microsoft/Yahoo!SearchBusiness (COMP/M.5727 del 18/2/2010), Microsoft/Skype (COMP/M. 6281 del 7/10/2011), Facebook/WhatsApp (COMP/M.7217 del 3/10/2014), Microsoft/LinkedIn (COMP/M. 8124 del 6/12/2016).

33 Così, ancora, VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., 1072.

34 Si ricorre all'acronimo GAFAM per indicare i maggiori operatori dell'economia digitale, Google, Apple, Facebook, Amazon, Microsoft.

35 VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., 1073-1074.

36 Si vedano, al riguardo, Commissione Europea (2019), "AT.40411 Google Search (AdSense)"; Commissione Europea (2018), "AT.40099 Google Android".

Tale ultima anomalia di mercato risulta, invero, sicuramente favorita dall'uso, da parte degli operatori del mercato digitale, di algoritmi predittivi delle scelte di consumo, oltre che dalla trasparenza e dall'agevole accessibilità ai prezzi praticati, di guisa che, a differenza che nel mercato tradizionale, lo scambio di informazioni non necessita neanche di un'apposita, preventiva intesa.

9.5. Abuso di posizione dominante e *big data*

Tra gli effetti distorsivi del mercato provocati dall'economia *data-driven* particolare attenzione desta l'ipotesi dello sfruttamento abusivo della posizione di dominanza economica acquisita attraverso i *big data* e i *data set*, siano essi *input* o *output* della produzione, ai danni degli operatori che non sono in grado di acquisire autonomamente i dati necessari per competere sul mercato[37].

Occorre soffermarsi, in particolare, sulla questione della riconducibilità dei dati nel paradigma concettuale dell'*essential facilities* cui si ricollegano le condotte consistenti in pratiche escludenti e nel rifiuto di licenza.

In linea di principio, all'impresa che investe nella raccolta di *big data* al fine di rendere competitiva la propria attività sul mercato non dovrebbe imporsi la condivisione di tali informazioni con i propri concorrenti, dal momento che i dati personali e le loro aggregazioni costituiscono un importante fattore del proprio avviamento commerciale e, precisamente, il principale *asset* competitivo del proprio *business*. In altre parole, l'impresa che disponga di *big data*, al pari di quella titolare di brevetti, modelli industriali, *software* e altri diritti di privativa, dovrebbe poter sfruttare in via esclusiva i propri beni immateriali.

È stato, non di meno, osservato che la tenuta di tale assunto deve

---

[37] Per un'ampia trattazione del tema si rinvia a D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data,* in *Dir. inf. e dell'informatica,* 6, 2018, 943 e ss., il quale richiama MUSCOLO, *Big data e concorrenza. Quale rapporto*?, in FALCE, GHIDINI, OLIVIERI, (a cura di*), Informazione e big data tra innovazione e concorrenza,* Milano, 2017, 178 e ss.; EZRACHI, STUCKE, *Artificial Intelligence & Collusion: When Computers Inhibit Competition, University of Illinois Law Review,* 2017, Oxford Legal Studies Research Paper No. 18/2015, University of Tennessee Legal Studies Research Paper No. 267; MAGGIOLINO, *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, 1, 1 gennaio 2016, 95-138.

essere verificata alla luce della teoria dell'EFD (*essential facility doctrine*)[38], secondo la quale le grandi strutture materiali irreplicabili o difficilmente replicabili - ma il discorso è stato esteso anche al settore della *information technology*[39] - devono essere equiparate ai diritti di privativa al ricorrere di tre condizioni: l'*input* controllato dall'impresa deve essere insostituibile; l'impresa che chiede l'*input* deve essere intenzionata ad utilizzarlo in un mercato diverso; non vi devono essere cause che possano giustificare il rifiuto[40].

Invero, nel caso in cui si optasse per la tesi della trasponibilità della teoria dell'*essential facilities* nel mercato dei *big data,* dovrebbe ammettersi che il rifiuto di effettuare forniture possa essere inquadrato nella fattispecie dell'abuso di posizione dominante.

Più di una voce dottrinale ha, tuttavia, rifiutato tale identificazione in ragione dei caratteri dell'ubiquità, non rivalità, facilità di acquisizione, velocità di raccolta e aggiornamento dei dati personali, aprendosi all'applicazione analogica dell'EFD soltanto in casi eccezionali[41].

Secondo altra opinione, nell'ipotesi in esame potrebbe trovare applicazione la disciplina dell'abuso di dipendenza economica ai sensi dell'art. 9 della legge n. 192 del 1998[42], sul presupposto che, come più volte confermato dalla giurisprudenza di legittimità, si è al cospetto di una disciplina transtipica applicabile a tutti i rapporti verticali tra imprese che si trovino in posizione di disequilibrio economico e giuridico.

---

38 Secondo la dottrina dell'*essential facility*, un'impresa detentrice di un'infrastruttura essenziale, il cui accesso da parte di operatori terzi è imprescindibile per lo svolgimento di attività economiche in un mercato a valle, può porre in essere una condotta abusiva nel caso in cui neghi, ovvero imponga ai suoi concorrenti su detto mercato a valle, condizioni di accesso all'infrastruttura inique (FATTORI, TODINO, *La disciplina della concorrenza in Italia,* Bologna, 2010, 185).

39 Si veda, al riguardo, Corte di giustizia UE, C-241/91 P e C-242/91, Radio Telefis Eireann (RTE) e Independent Television Publications (ITP)/ Commission (Magill).

40 SIRAGUSA, *L'abuso di posizione dominante*, in AA.VV., *Codice commentato della concorrenza e del mercato*, Torino, 2010, 1125.

41 PITRUZZELLA, *Big data, competition and privacy: a look from the Antitrust perspective*, in DI PORTO (a cura di), *Big data e concorrenza*, cit., 15 ss., richiamato da VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., 1064 e ss., spec. note 2 e 63.

42 VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., 1078 e ss.

Un elemento sintomatico dal quale desumere la fattispecie in questione viene individuato nella possibilità di reperire alternative sul mercato soddisfacenti, ma l'abuso può consistere anche nel rifiuto di vendere e di comprare; nella imposizione di condizioni contrattuali ingiustificatamente gravose o discriminatorie; nella interruzione arbitraria delle relazioni commerciali in atto.

L'elemento sintomatico dell'"eccessivo squilibrio" viene, infine, ravvisato nella detenzione, da parte dei *majors*, dei dati essenziali di cui hanno bisogno le piccole imprese che hanno difficoltà a sostenere i costi di ricerca e sviluppo se l'impresa che ha la disponibilità di *big data* si rifiuta di contrarre ovvero di rilasciare la licenza per l'uso dei dati e sia la depositaria dei *data set* più aggiornati, così che possono ritenersi insoddisfacenti le alternative reperibili sul mercato; oppure se non pratica condizioni paritarie; ovvero se pone in essere pratiche leganti (cd. *tyings contracts*), consistenti nell'imporre l'acquisto di dati in abbinamento ai servizi di *data analytics*[43].

9.6. La pratica dei prezzi personalizzati e l'illecito discriminatorio

Un altro profilo di potenziale incidenza dei *big data* sull'analisi *antitrust* è quello della pratica dei prezzi personalizzati.

Dalle prime riflessioni della dottrina emerge la considerazione dell'ambivalenza di tale fenomeno, capace di sortire effetti positivi e negativi ad un tempo[44].

Invero, se, per un verso, alla personalizzazione dei prezzi si associa una tendenza all'aumento e alla massimizzazione del benessere generale dei consumatori (*consumer welfare*), intesi nella loro totalità (*social welfare*), così da rendere «*più poveri i più ricchi e meno poveri i meno ricchi*»[45], nonché una maggiore rivalità tra le imprese; per altro verso si

---

[43] Per un'analisi *antitrust* del mercato digitale v. ZENO ZENCOVICH, *Internet e concorrenza,* in *Dir. inf.,* 2010, 697 e ss.

[44] Si rinvia ancora una volta a VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, cit., 1064 e ss. e agli ampi riferimenti bibliografici ivi riportati, tra cui MAGGIOLINO, *Big data e prezzi personalizzati*, in *Concorrenza e mercato,* 2016, 1, 95 ss., spec. 110; COLANGELO, *Big data, piattaforme digitali e antitrust*, in *Merc. conc. reg.*, 2016, 3, 429-430.

[45] Così MAGGIOLINO, op. ult. cit., 98, spec. nota 55.

registra una perdita di benessere individuale per alcuni consumatori (quelli disposti a pagare prezzi più alti per avere determinati beni) a fronte del risparmio di spesa riservato soltanto ad alcuni consumatori (quelli disposti a pagare prezzi più bassi per fruire di determinati beni) [46].

Per quel che riguarda più specificamente l'analisi *antitrust*, si pone il fondamentale problema se la prassi di personalizzazione dei prezzi possa violare il principio di parità di trattamento e dare luogo ad abuso di posizione dominante ovvero ad una pratica commerciale scorretta.

La discriminazione dei prezzi praticata da un'impresa in posizione dominante o da due o più imprese all'esito di un accordo (intesa restrittiva della concorrenza) se rivolta nei confronti – e dunque a danno – di altre imprese sul mercato costituisce indubbiamente un illecito *antitrust* sia comunitario, ai sensi degli artt. 101 e 102 TFUE, sia nazionale, in applicazione degli artt. 2 e 3 della legge n. 287 del 1990.

Se, invece, la condotta è ascrivibile ad un operatore economico che non riveste la posizione di dominanza ovvero ad imprese che non si siano tra loro accordate per praticare la discriminazione dei prezzi, deve necessariamente escludersi la configurabilità di un illecito *antitrust sub specie* di abuso di posizione dominante o di intesa restrittiva della concorrenza.

La dottrina si è, tuttavia, interrogata sulla possibilità che una condotta siffatta possa assumere rilevanza quale pratica commerciale scorretta in quanto lesiva del principio di parità di trattamento, ovvero per la modalità occulta con la quale venga praticata.

La prima ipotesi non trova un addentellato nel diritto positivo, giacché, come confermato da autorevole dottrina, nei rapporti contrattuali tra privati non è configurabile un dovere generale di parità di trattamento che non trovi giustificazione in una situazione di disparità, come quella creata dal monopolio[47]. La garanzia di parità di condizioni contrattuali è, infatti, imposta al monopolista legale ai sensi degli artt. 2597 e 1679 c.c., sicché deve escludersi l'operatività di un

---

46 MAGGIOLINO, op. cit., 98.

47 Sottolinea SACCO, voce *Parità di trattamento (nel diritto dei contratti)*, in *Dig. disc. priv., sez. civ.*, VII agg., Torino, 2012, 738, che «nessuna norma esplicita prevede o contiene la regola di cui parliamo». V. anche PASETTI, voce *Parità di trattamento (diritto civile*), in *Enc. giur.*, XXII, Roma, 1990, 1.

generale divieto per le imprese di praticare prezzi diversi per prestazioni equivalenti, ove le condizioni di concorrenza sul mercato siano tali da garantire ai consumatori un'adeguata varietà di scelta[48].

È stato, invece, sostenuto che la pratica della personalizzazione dei prezzi potrebbe essere qualificata come omissione ingannevole ai sensi dell'art. 22, primo comma, c.c., ove l'offerta personalizzata di beni o servizi non sia accompagnata dalla chiara manifestazione della sua natura personalizzata e pertanto discriminatoria[49].

La fattispecie – chiarisce la dottrina in esame – pur non rientrando tra le ipotesi tipiche considerate «in ogni caso ingannevoli» dall'art. 23, cod. cons., presenta i requisiti imposti alternativamente dall'art. 22 cod. cons., posto che la discriminazione dei prezzi operata all'insaputa del consumatore integra una condotta non trasparente e contraria alla correttezza professionale in quanto risulta idonea a ledere la libertà di scelta del contraente che, ove informato sulla natura personalizzata e

---

[48] Il divieto di disparità opera, dunque, solo in relazione a specifici obblighi a contrarre e in funzione di riequilibrio di una situazione di disparità contrattuale scaturente dalla presenza di una situazione monopolistica. Oltre all'obbligo a contrarre imposto al monopolista legale dall'art. 2597 c.c. e a quello previsto a carico del concessionario di un pubblico servizio di linea per il trasporto di persone o cose, ai sensi dell'art. 1679 c.c., si ricordano l'obbligo a contrarre ex art. 1706, secondo comma, c.c.; l'obbligo a contrarre ex art. 1032 c.c. in materia di costituzione di servitù coattiva; l'obbligo di alienare le proprie azioni illegittimamente acquistate, ai sensi dell'art. 2357, quarto comma, c.c.; l'obbligo ex art. 2359-ter c.c. di cedere le azioni della società controllante illegittimamente acquistate dalla società controllata. Nell'ambito della legislazione speciale particolare rilevanza assumono gli obblighi a contrarre previsti nei settori soggetti a regolazione, come l'obbligo di accesso che, ai sensi dell'art. 45 del codice delle comunicazioni elettroniche (d.lgs. n. 259 del 2003), può essere imposto dall'autorità competente a tutte le imprese detentrici di un significativo potere di mercato in un mercato specifico. Va, infine, menzionato l'obbligo di vendita imposto dall'art. 3 del d.lgs. n. 114 del 1998. Occorre, altresì, rilevare che l'art. 1679 c.c. associa all'obbligo legale a contrarre l'obbligo di non discriminazione che si esprime: a) nella fissazione legale dei criteri di soluzione di eventuali conflitti tra più richiedenti la prestazione (criterio dell'ordine cronologico; criterio del percorso maggiore); b) nell'imposizione all'erogatore dell'obbligo di osservare la parità di trattamento nel praticare speciali concessioni previste dalle condizioni generali; c) nel sanzionare con la nullità e con il meccanismo della sostituzione automatica l'eventuale clausola difforme dalle condizioni generali stabilite o autorizzate nell'atto di concessione o fissate con legge o con atto amministrativo. Su tale ultimo dovere si vedano, *ex aliis*, NIVARRA, *L'obbligo a contrarre e il mercato*, Padova, 1989, 67; VISALLI, *Il contratto imposto,* in *Riv. dir. civ.*, 1999, 193 ss.

[49] VESSIA, *Dai vantaggi competitivi alle pratiche abusive*, 1090-1091.

discriminatoria del prodotto o del servizio, sarebbe stato indotto ad assumere maggiori informazioni su offerte analoghe al fine di comparare ed assumere una decisione maggiormente ponderata.

9.7. Uso secondario dei *big data* e protezione dei dati personali

La tendenza dei maggiori operatori del mercato digitale all'uso cd. secondario o alternativo dei *big data,* ossia ad entrare in settori economici diversi dal proprio e ad avvalersi dei poderosi e aggiornatissimi *data set* ottenuti attraverso l'attività economica svolta nel mercato di provenienza, comporta, come già evidenziato, significativi risvolti anche sul versante del sistema di *data protection*.

Sembra, infatti, raccogliere ampio consenso l'orientamento interpretativo che considera unitariamente e sinergicamente la disciplina *antitrust* e la normativa sulla protezione dei dati personali, prediligendo, quindi, un approccio convergente e non una considerazione autonomistica dei due settori disciplinari, con l'obiettivo di promuovere l'innovazione e l'efficienza dei mercati digitali[50].

Anche nella dottrina italiana è stato posto in evidenza come alcuni istituti rimediali di *data protection* possano essere d'ausilio nell'ambito di valutazioni *antitrust*[51].

Tale opzione ermeneutica si pone in linea con le direttrici della normativa di derivazione europea in materia di dati personali, imponendo il Regolamento generale sulla protezione dei dati personali UE, n. 679 del 2016 (GDPR) non certo il divieto dell'uso di dati personali, ma il bilanciamento tra la protezione dei diritti e della libertà fondamentali delle persone fisiche, con particolare riferimento alla protezione dei dati personali, e la tutela del mercato, la libera circolazione di dati nell'ottica dell'incentivazione all'innovazione tecnologica nell'attività di impresa.

È appena il caso di evidenziare che il Regolamento europeo solo apparentemente si riduce ad una sorta di *restatement* della previgente disciplina eurounitaria e nazionale sui dati personali e della correlata

---

50 V., *supra,* nota 7.

51 D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data,* cit., 943 e ss.

elaborazione giurisprudenziale stratificatasi nel tempo.

L'opera di risistemazione messa a punto dal legislatore europeo non ha, invero, portata meramente ricognitiva, ma innovativa, implicando significative scelte di politica del diritto, la più evidente delle quali viene individuata proprio nell'enfasi attribuita al momento circolatorio dei dati personali rispetto al profilo personalistico che risulta, invece, fortemente ridimensionato[52].

Se ne trae conferma, oltre che dalla minuziosa attenzione riservata alle condizioni di liceità del trattamento, da precisi dati positivi, tra i quali i più significativi sono rappresentati dal considerando n. 4, secondo il quale «*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità*» e dall'art. 1, par. 3, a mente del quale «*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*».

9.8. Il principio di limitazione della finalità del trattamento

L'orientamento interpretativo che predilige l'approccio sinergico intravede nel principio di limitazione della finalità del trattamento dei dati personali[53] un valido strumento di prevenzione degli effetti distorsivi che l'uso secondario dei *big data* può provocare sul funzionamento del mercato[54].

---

[52] Così RAMACCIONI, *La protezione dei dati personali e il danno non patrimoniale*, Napoli, 2017.

[53] L'originaria enunciazione di tale fondamentale regola si rinviene nell'art. 5 della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108, siglata a Strasburgo il 28 gennaio 1981, a mente del quale «*I dati di carattere personale oggetto di elaborazione automatica devono essere registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini*», ma l'antecedente storico più prossimo alla sua attuale formulazione è rappresentato dall'art. 8 della Carta dei diritti fondamentali dell'UE, il cui secondo comma dispone che i dati personali devono essere trattati «*per finalità determinate*».

[54] D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data*, in *Dir. inf. e dell'informatica*, cit., 951 e ss.

Il divieto di trattamento dei dati per finalità diverse e incompatibili rispetto a quelle per le quali erano stati originariamente raccolti, è recepito nell'art. 5, paragrafo 1, lett. b), del Regolamento n. 679 del 2016, secondo il quale i dati personali devono essere «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»)*».

Un principio contiguo e rafforzativo di detta regola è quello, enunciato all'art. 5, par. 1, lett. c), del GDPR, cd. di minimizzazione dei dati, a mente del quale i dati raccolti devono essere «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)*».

Dalle predette disposizioni si traggono il criterio di specificazione delle finalità e il criterio dell'uso compatibile. Infatti, il principio di limitazione della finalità impone al titolare del trattamento di definire *ex ante* e in modo specifico le finalità del trattamento, mentre l'uso dei dati per finalità aggiuntive è possibile solo se si tratta di finalità compatibili con quelle originarie.

Entrambi i parametri sono tesi a garantire la prevedibilità del trattamento proteggendo l'interessato dall'uso inaspettato, inappropriato e altrimenti discutibile dei dati, così garantendo, in una prospettiva più vasta, la certezza del diritto e la fiducia nell'operato dei titolari del trattamento.

I principi di limitazione e di minimizzazione sono stati, infatti, concepiti secondo una logica preventiva, nell'intento di scongiurare o, per lo meno, di limitare la tendenza degli operatori ad accumulare quanti più dati possibili anche se non strettamente necessari, in ragione della mera possibilità della loro utilità futura.

Orbene, ad avviso della dottrina in esame, il principio di limitazione delle finalità può trascendere l'ambito del *data protection* e trascorrere in quello dell'*antitrust* intervenendo efficacemente nella situazione in cui il titolare del trattamento sia un'azienda dominante che abusi della propria posizione anche a scapito dei consumatori interessati agendo in settori terzi rispetto al proprio, alterando la concorrenza

nei mercati e sfruttando dati e *asset* strategici già in suo possesso e preclusi ai concorrenti[55].

La valutazione della compatibilità dello scopo ulteriore con quello originario va condotta sulla base dei criteri individuati nel considerando n. 50 e nell'art. 6, par. 4, del GDPR, il quale impone di tener conto di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; del contesto in cui i dati personali sono stati raccolti; della natura dei dati personali; delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

In particolare, la valutazione della compatibilità deve essere condotta sulla base di un duplice *test*, formale e sostanziale, il primo dei quali è diretto a verificare se le finalità ulteriori siano già rintracciabili in modo esplicito o implicito nelle finalità iniziali, mentre il secondo è volto ad indagare l'effetto delle ulteriori finalità sull'interesse, ossia come vengono recepite dall'interessato tenendo conto del contesto e degli altri elementi che caratterizzano la fattispecie concreta.

Il concetto di compatibilità deve essere valutato anche alla luce della nozione di sostituibilità, ossia del criterio impiegato nel diritto della concorrenza per individuare quali prodotti possano essere considerati concorrenti nello stesso mercato.

Invero, affinché una finalità possa essere considerata compatibile con quella del trattamento originario occorre verificare anche se il trattamento secondario sia diretto o meno a una finalità sostitutiva di quella originaria.

Ne deriva, secondo l'impostazione in esame[56], che, se l'impresa rielabora i dati in suo possesso per fornire un nuovo servizio in un mercato del tutto separato, ancorché non concorrente con quello originario, si è sicuramente al cospetto di una finalità non sostituibile e quindi incompatibile e quindi non utilizzabile[57].

---

55 D'IPPOLITO, op. ult. cit., 954.

56 Si rimanda ancora a D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data,* in *Dir. inf. e dell'informatica,* cit., 956-957 e ss.

57 È stato evidenziato che, alla stregua dei richiamati principi, dovrebbe essere precluso l'uso di dati raccolti, per esempio, per un *social network* o una piattaforma attiva

Pertanto, il titolare del trattamento originario, per poter superare il principio di limitazione deve dare una nuova base giuridica al trattamento secondario, altrimenti vietato.

Le basi giuridiche del trattamento previste dal GDPR sono il consenso dell'interessato[58] e il legittimo interesse.

Naturalmente, il consenso dell'interessato all'uso secondario dei propri dati, se validamente prestato per una finalità ulteriore indicata in modo specifico ed esplicito, fa venire meno l'esigenza di verificare la compatibilità tra le finalità originarie e le nuove perché contribuisce concretamente e fattivamente ad evitare il fenomeno del *function creep* ovvero dello slittamento dell'uso del dato verso una finalità non prevista dall'interessato.

Quanto al legittimo interesse, proprio o di terzi, previsto dall'art. 6, par. 1, lett. f, del GDPR – a mente del quale «*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. (C47-C50)*» – il titolare del trattamento che intenda far valere questa base giuridica si espone alla ben più pervasiva verifica di prevalenza dell'interesse invocato rispetto agli interessi, diritti e libertà fondamentali dell'interessato.

In definitiva, il trattamento secondario per essere lecito deve essere connotato da finalità non incompatibili con quelle originarie, ovvero deve essere supportato da una nuova manifestazione di consenso informato dell'interessato o giustificato da un legittimo interesse proprio o di terzi prevalente sui diritti e sule libertà fondamentali dell'interessato medesimo.

Occorre, tuttavia, evidenziare che la chiave di lettura della nuova disciplina sul trattamento dei dati non vieta in assoluto l'uso secondario, ma fornisce gli strumenti per far fronte ad abusi compiuti dal titolare del trattamento, nell'ottica del bilanciamento tra le opposte istanze.

---

nel commercio elettronico al fine di offrire servizi finanziari, bancari o assicurativi, nonché i servizi di pagamento previsti dalla direttiva 2366/2015 (cd. PSD2).

[58] Il consenso è previsto dall'art. 6, par. 1, lett. a), del GDPR ed è lo strumento che attribuisce all'interessato il maggiore controllo sui propri dati, tenuto conto del potere di revoca previsto dall'art. 7, comma 3.

Tale approccio interpretativo è in linea con il principio di bilanciamento fra protezione delle persone fisiche e libera circolazione dei dati sancito dall'art. 1 del GDPR[59].

9.9. I rimedi preventivi e successivi

La tutela contro l'uso abusivo dei dati già raccolti e poi elaborati in ulteriori mercati per finalità diverse si esplica in rimedi preventivi e successivi.

Tra i primi vanno annoverati i dispositivi riconducibili alla nozione di *privacy-enhancing services* (servizio di miglioramento della *privacy*), rappresentati da tutte quelle tecnologie, tecniche e servizi che tutelano la *privacy* delle persone limitando, riducendo, eliminando o impedendo di raccogliere ed elaborare i dati non necessari al trattamento. Si tratta di congegni preventivi, intesi a limitare la possibilità di usi distorti e rischiosi dei dati personali.

Particolare interesse destano gli istituti della "*protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*" di cui all'art. 25 del GDPR e il diritto alla portabilità dei dati di cui all'art. 20 del GDPR.

Con riferimento ai primi, l'art. 25, par. 1, del GDPR dispone che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per attuare in modo efficace i principi di protezione dei dati quali la minimizzazione[60].

Il secondo paragrafo del medesimo art. 25 impone, invece, al titolare del trattamento di adottare misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. È questo il principio della data *protection by default* che impone al titolare di impostare il trattamento in modo da raccogliere solo i dati pertinenti e limitati a quanto necessario per le finalità del trattamento (principio di minimizzazione).

Nella prospettiva della prevenzione degli effetti distorsivi dell'uso

---

[59] Per un'ipotesi applicativa dei principi richiamati, paradigmatico è il caso Facebook/WhatsApp deciso dalla Commissione europea nel 2014, case M7217.

[60] Il concetto a cui la norma fa riferimento è comunemente conosciuto come *data protection by design* (protezione dei dati sin dalla progettazione).

secondario dei *big data* sulla concorrenza, particolare rilevanza viene, poi, attribuita al diritto alla portabilità dei dati previsto dall'art. 20 del GDPR, ossia al diritto dell'interessato di ricevere i dati personali che lo riguardano e da lui forniti a un titolare del trattamento, «*in un formato strutturato, di uso comune e leggibile da dispositivo automatico*», e il conseguente diritto di trasmettere tali dati ad altro titolare del trattamento, anche direttamente, ossia attraverso un passaggio dal precedente al nuovo titolare.

È stato osservato che l'attitudine del diritto alla portabilità dei dati ad incidere positivamente sulla concorrenza deriva dal fatto che per suo tramite vengono abbassate le barriere all'entrata per i nuovi operatori e gli operatori già presenti sul mercato sono indotti ad implementare e migliorare i propri servizi, nonché a ridurre i cd. *switching cost*, ovvero i costi da sostenere in caso di cambiamento del fornitore.

È stato, inoltre, notato che attraverso l'esercizio del diritto alla portabilità dei dati, potrebbero essere gli stessi utenti a decidere a quale operatore fornire i propri dati, determinando uno spostamento di risorse fondamentali per l'economia *data-driven*.

L'impostazione in esame intravede nel diritto alla portabilità dei dati uno strumento di prevenzione dei fenomeni di abuso di posizione dominante «*che sfruttino il fatto che i consumatori si trovino bloccati in determinati servizi a causa di condizionamenti tecnologici o di altra natura. Inoltre, la portabilità dei dati potrebbe consentire ai consumatori di usufruire dei servizi a valore aggiunto di imprese terze facilitando l'accesso al mercato da parte di concorrenti, ampliando le sue possibilità di scelta e tutelando la concorrenza*»[61].

Per quanto concerne, invece, la tutela successiva, tra le prerogative in cui questa si esplica, merita attenzione il diritto di opposizione ex art. 21 del GDPR, quale contraltare dell'utilizzo, da parte del titolare, del legittimo interesse (*legitimate interest*) come base giuridica del trattamento secondario dei dati, in relazione al quale, non venendo in rilievo il consenso dell'interessato, questi non può avvalersi del diritto di revoca ex art. 7, par. 3, del GDPR.

Tale rimedio assume significativa rilevanza soprattutto quando l'ulteriore trattamento dei dati sia effettuato per finalità di *marketing*,

---

61 Così D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data,* cit., 976.

avuto riguardo alla previsione del Considerando n. 47 secondo la quale «*Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto*».

Infatti, l'art. 21, par. 2 e 3, del GDPR prevede che «*Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità*».

9.10. La tutela risarcitoria

Per quel che riguarda, infine, la tutela risarcitoria da illecito trattamento dei dati personali[62], il GDPR non sembra, *prima facie*, avere apportato significative modifiche alle nozioni di responsabilità da illecito trattamento dei dati e di danno da lesione del diritto sugli stessi delineati dal regime previgente, risultando l'art. 82 del Regolamento in linea di massima sovrapponibile all'art. 15 del d.lgs. n. 196 del 2003.

La lineare formulazione dell'art. 82 è riassumibile nell'enunciato per il quale è riconosciuto il diritto di ottenere il risarcimento del danno patrimoniale e non patrimoniale da chiunque subito a causa della violazione del regolamento.

Dalla lettura combinata di tale disposizione con il considerando n. 146 -secondo il quale «*il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento*» - si trae una nozione di danno risarcibile coerente con la connotazione del di-

---

62 Sulla quale si vedano, *ex aliis*, CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus civile*, 2020, 3, 786 e ss; MANTELERO, *Responsabilità e rischio nel Regolamento UE 2016/679*, in *Nuov. leggi civ. comm.*, 2017, 1, 144 e ss.; TOSI, *Il trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno e Resp.*, 2020, 4, 433 e ss.; INFANTINO, *La responsabilità per danni algoritmici: prospettive europeo-continentali*, in *Resp. civ. e prev.*, 2019, 5, 1762 e ss.; DE PAMPHILIS, *Risarcimento del danno per illegittimo trattamento dei dati personali dopo il reg. ue 2016/679*, in *Giustiziacivile.com*, Approfondimento del 19 febbraio 2019.

ritto sui dati personali delineato dal GDPR in termini di situazione giuridica soggettiva strumentale e procedimentale e non finale.

L'ancoraggio, nel testo dell'art. 82 del GDPR, del rimedio risarcitorio alla sola violazione delle norme sul trattamento dei dati personali ha fatto dubitare della necessità, ai fini del riconoscimento del risarcimento, di una verifica della reale consistenza del pregiudizio lamentato, ravvisandosi nella disposizione predetta una fattispecie di danno *in re ipsa*[63], nella quale il rimedio risarcitorio risulta connotato da una spiccata finalità sanzionatoria e preventiva rispetto alla tipica funzione compensativa propria della responsabilità civile disciplinata dall'ordinamento nazionale.

Secondo una recente ricostruzione[64], che si rifà alla teoria del danno giuridico[65], il regolamento europeo introduce una trasformazione notevole della struttura dell'illecito in quanto oggettivizza il pregiudizio risarcibile sino ad identificarlo con la stessa antigiuridicità della condotta. Si sarebbe, in altre parole, al cospetto di un danno *tecnico* o in senso oggettivo, diretta scaturigine delle nuove tecnologie informatiche capaci di archiviare, incrociare, scambiare, selezionare, modificare, aggiornare e diffondere un numero immenso di dati personali. D'altronde, di fronte al rischio di aggressione provocato da condotte altamente sofisticate – quali sono, all'evidenza, la raccolta, l'immagazzinamento, l'elaborazione, l'aggregazione e il riuso dei dati personali da parte dei colossi del digitale – la prova della colpa e del danno-conseguenza diviene ardua, così che, al fine di scongiurare il rischio di frustrazione della tutela, l'azione risarcitoria deve poter prescindere dall'allegazione e dalla dimostrazione degli elementi strutturali dell'illecito, per essere ancorata sulla sola antigiuridicità della condotta del titolare del trattamento.

---

63 La nozione di *danno in re ipsa* è coerente con la teoria normativa, elaborata dalla dottrina tedesca (NEUNER, *Interesse und Vermögensschaden,* in *Arch. civ. pr.,* CXXXIII, 1931, 277 e ss.), ma recepita anche da alcuni autori italiani (DE CUPIS, *Danno,* in *Enc. del dir.,* XI, Milano, 1962; ALPA, *Trattato di diritto civile*, IV, Milano, 1999), secondo la quale l'oggetto del danno si identifica con l'oggetto della tutela giuridica e, quindi, coincide con l'interesse protetto dall'ordinamento.

64 RAMACCIONI, *La protezione dei dati personali e il danno non patrimoniale*, cit.

65 MESSINETTI, *Danno giuridico*, in *Enc. dir., agg.*, I, Milano, 1997.

A giudizio della dottrina in esame, l'orientamento in senso preventivo e sanzionatorio di simile esegesi trova conforto in un *trend* generalizzato, sia a livello europeo, che nazionale, sempre più ispirato alla funzione deterrente della responsabilità civile.

A conclusioni diverse è, invece, giunta la giurisprudenza di legittimità che, sia pure con riferimento alla disciplina dettata dal d.lgs. n. 196 del 2003, ha ricostruito il danno non patrimoniale da lesione della *privacy* e, in particolare, del pregiudizio da illecito trattamento dei dati personali in coerenza con i consolidati principi elaborati in materia di responsabilità.

Paradigmatica, al riguardo, è la sentenza della Terza Sezione civile n. 16133 del 15 luglio 2014, secondo la quale il danno non patrimoniale risarcibile ai sensi dell'art. 15 del codice della *privacy*, pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della gravità della lesione e della serietà del danno - quale perdita di natura personale effettivamente patita dall'interessato -, in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., di cui il principio di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della *privacy*, ma solo quella che ne offenda in modo sensibile la sua portata effettiva. Il relativo accertamento di fatto è rimesso al giudice di merito e resta ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale ed al suo essere maturata in un dato contesto temporale e sociale[66].

La Corte di cassazione muove dalla premessa secondo la quale il danno risarcibile non si identifica con la lesione dell'interesse tutelato dall'ordinamento, ma con le conseguenze di tale lesione, evidenziando come sia stata superata dalla giurisprudenza di legittimità la teorica del c.d. danno evento elaborata dalla sentenza n. 184 del 1986 della Corte Costituzionale in materia di danno biologico, posto che la stessa Consulta, con la nota sentenza n. 372 del 1994, ripresa dalla sentenza

---

[66] In applicazione di tale principio la Suprema Corte ha cassato la decisione di merito che, sulla base del mero disagio, aveva ritenuto risarcibile il danno alla privacy, caratterizzato dalla possibilità, per gli utenti del *web*, di rinvenire agevolmente su *internet* - attraverso l'uso di un comune motore di ricerca - generalità, codice fiscale, attività di studio, posizione lavorativa e retributiva della parte attrice.

n. 26972 dell'11 novembre 2008 delle Sezioni Unite, ha aderito alla ricostruzione dottrinaria secondo la quale tra gli elementi costitutivi dell'illecito aquiliano che si ricavano dal testo dell'art. 2043 c.c. va incluso, insieme alla condotta, al nesso causale tra la condotta e l'evento di danno, connotato dall'ingiustizia determinata dalla lesione non giustificata di interessi meritevoli di tutela secondo l'ordinamento giuridico, anche il danno che ne consegue (danno-conseguenza)[67].

La sentenza n. 16133 del 2014 ha, inoltre, precisato che nel predetto schema deve essere ricondotto anche il danno non patrimoniale di cui all'art. 2059 c.c., posto che tale disposizione non disciplina un'autonoma fattispecie di illecito produttiva di danno non patrimoniale, distinta da quella di cui all'art. 2043 c.c., ma regola le condizioni e i limiti di risarcibilità del danno non patrimoniale intesa come categoria comprensiva, nell'ambito della quale non è possibile individuare, se non a fini descrittivi, ulteriori sottocategorie, ove sussistano tutti i presupposti di cui all'art. 2043 c.c.

La Corte ha, altresì, evidenziato che la gravità della lesione attiene al momento determinativo dell'evento dannoso quale incidenza pregiudizievole sul diritto interesse selezionato dal legislatore come meritevole di tutela aquiliana e la sua portata è destinata a riflettersi sull'ingiustizia del danno che non potrà più predicarsi tale in presenza di una minima offensività.

In particolare, la gravità dell'offesa è funzione plastica del requisito dell'ingiustizia del danno, mentre la serietà del danno attiene al piano delle conseguenze della lesione e, quindi, all'area dell'obbligazione risarcitoria che si appunta sulla effettività della perdita subita (cd. danno-conseguenza).

Tale ricostruzione si pone in continuità con l'orientamento, prevalente nella giurisprudenza di legittimità, che nega la configurabilità del *danno in re ipsa*, sul presupposto che, in linea di principio, deve escludersi che la responsabilità civile assolva ad una funzione punitiva e

---

[67] Si tratta della nota teoria di GORLA, *Sulla cosiddetta causalità giuridica: «fatto dannoso e conseguenze»*, in *Riv. dir. comm.*, 1951, I, 405, la quale, muovendo dall'interpretazione sistematica degli artt. 1223 c.c. e 2043 c.c., propone una scomposizione dell'accertamento del danno risarcibile in due autonomi e consecutivi segmenti, il primo dei quali volto a identificare il nesso di causalità materiale che avvince la condotta all'evento di danno, e il secondo diretto a verificare il nesso di causalità giuridica che lega tale evento alle conseguenze dannose.

sanzionatoria, ancorché, come chiarito dalle Sezioni Unite nella sentenza n. 16601 del 5 luglio 2017, nel vigente ordinamento, alla responsabilità civile non è assegnato solo il compito di restaurare la sfera patrimoniale del soggetto che ha subito la lesione, poiché sono interne al sistema la funzione di deterrenza e quella sanzionatoria del responsabile civile, sicché non è ontologicamente incompatibile con l'ordinamento italiano l'istituto, di origine statunitense, dei risarcimenti punitivi.

Difatti, pur ammettendo, in linea con la giurisprudenza costituzionale, che, accanto alla preponderante e primaria funzione compensativo-riparatoria della responsabilità civile, dal sistema normativo che è venuto componendosi nel corso degli anni è emersa una natura polifunzionale e, quindi, anche preventiva, o deterrente o dissuasiva, e sanzionatorio-punitiva, le Sezioni Unite hanno avvertito che tale rinnovato approccio non consente una generalizzata facoltà di modulazione giudiziale del risarcimento avulsa dal concreto pregiudizio accertato, dal momento che ogni imposizione di prestazione personale esige un'intermediazione legislativa in forza del principio di cui all'art. 23 Cost., correlato agli artt. 24 e 25 Cost., con la conseguenza che il risarcimento punitivo può ritenersi configurabile soltanto a condizione che sia supportato da un'apposita previsione normativa.

Nello stesso senso si è espressa più di recente la Sezione VI-I che, nell'ordinanza n. 17383 del 20 agosto 2020, ha ribadito che il danno non patrimoniale risarcibile ai sensi dell'art. 15 del d.lgs. n. 196 del 2003, pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della gravità della lesione e della serietà del danno, in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., di cui quello di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della *privacy*, ma solo quella che ne offenda in modo sensibile la sua portata effettiva, restando comunque il relativo accertamento di fatto rimesso al giudice di merito.

La mera inclusione da parte del legislatore di un determinato interesse nell'alveo del rimedio risarcitorio del danno non patrimoniale – precisa la Cassazione – non si risolve nell'affermazione stessa di gravità della lesione del diritto-interesse stesso e di serietà del danno che

ne consegue**.**

La Suprema Corte ha, inoltre, posto in luce come nel disegno del codice della *privacy*, al rimedio risarcitorio si accompagni una tutela composita che rende, pertanto, suscettibile di graduare la risposta in funzione delle concrete esigenze di salvaguardia dell'interessato. In tale solco si colloca la tutela inibitoria che può essere esperita in caso di trattamento contrario ai presupposti di liceità da cui deriva l'inutilizzabilità dei dati ai sensi dell'art. 7 del codice.

Nella medesima prospettiva, l'ordinanza della Sezione VI-III n. 18812 del 5 settembre 2014 ha precisato che l'illecito trattamento di dati personali giustifica l'accoglimento della pretesa risarcitoria azionata ai sensi dell'art. 15 del d.lgs. 30 giugno 2003, n. 196, solo a condizione che sia dimostrata dall'interessato l'esistenza di un pregiudizio di natura non patrimoniale sofferto in conseguenza di esso.

Ancora, la sentenza della Sezione III n. 15240 del 3 luglio 2014, ha ribadito che l'illegittimo trattamento di dati sensibili ex art. 4 del d.lgs. 30 giugno 2003, n. 193, configurabile come illecito ai sensi dell'art. 2043 c.c. non determina un'automatica risarcibilità del danno poiché il pregiudizio (morale o patrimoniale) deve essere provato secondo le regole ordinarie, quale ne sia l'entità e la difficoltà di assolvere l'onere probatorio, trattandosi di un danno-conseguenza e non di un danno-evento, senza che rilevi in senso contrario il suo eventuale inquadramento quale pregiudizio non patrimoniale da lesione di diritti costituzionalmente garantiti.

La tensione tra logica compensativa ed effettività della tutela risarcitoria che emerge dal confronto tra la riflessione dottrinale e l'elaborazione giurisprudenziale origina, per un verso, dalla complessità della prova del danno derivante dalla violazione delle regole sulla circolazione dei dati personali – la quale, in difetto di meccanismi legali di sgravio probatorio, può tradursi in un ostacolo insuperabile all'accesso alla tutela risarcitoria – e, per altro verso, dalla spiccata funzionalizzazione di tale ultimo rimedio all'obiettivo ultimo del corretto ed efficiente funzionamento del mercato.

Non può non rilevarsi che, specie nella prospettiva della tesi che auspica un impiego sinergico delle tutele offerte dalla disciplina *antitrust* e dalla normativa di protezione dei dati personali, la semplificazione probatoria che è alla base della ricostruzione del pregiudizio da

illecito trattamento dei dati in termini di danno *in re ipsa*, pur risultando distonica rispetto all'impostazione sistematica adottata dalla giurisprudenza nazionale in materia di responsabilità civile, risponde pienamente al fine ultimo del *private enforcement* di derivazione eurounitaria rappresentato dalla garanzia dell'efficacia regolatoria in senso deterrente dei presidi privatistici, i quali, al pari degli istituti di natura pubblicistica (funzione di controllo e sanzionatoria delle autorità garanti), risultano, in definitiva, concepiti in funzione della tutela della concorrenza.

10. Gli *smart contracts* come prodotti *software*

Salvatore Orlando

10.1. Premessa

Come noto, nel linguaggio dei programmatori, di *smart contracts* si parla tanto relativamente a rapporti contrattuali che fuori dall'ambito dei rapporti contrattuali[1].

Nel primo contesto, che – come vedremo meglio più avanti – è quello che ha attratto maggiormente l'attenzione della dottrina[2] e che

---

[1] Proprio per distinguere gli *smart contracts* inerenti a rapporti contrattuali dai programmi per elaboratori che pur non inerendo a rapporti contrattuali sono indicati nel linguaggio dei programmatori come "*smart contracts*", si è proposto di utilizzare l'espressione «*smart legal contracts*» per i primi e l'espressione «*smart contract code*» per gli altri (cfr. J. STARK, *Making Sense of Blockchain Smart Contracts*, 2016, accessibile su http://www.coindesk.com/making-sense-smart-contracts/; C.D. CLACK, V.A. BAKSHI, L. BRAINE, *Smart contract templates: foundations, design landscape and research directions*, 4 agosto 2016, accessibile su https://arxiv.org/pdf/1608.00771.pdf, p. 2 ss.; *Smart contracts. Legal framework and proposed guidelines for lawmakers,* pubblicato online sul sito https://www.ebrd.com dalla *European Bank for Recontruction and Development* e *Clifford Chance* nell'ottobre 2018, p. 6).

[2] Senza pretesa di completezza: M. MAUGERI, *Smart Contracts e disciplina dei contratti. Smart Contracts and Contract Law*, Bologna, 2021; ID., *Smart Contracts*, in *Enc. dir. – I tematici I*, Milano, 2021, p. 1132 ss.; E. BATTELLI, *IA e* smart contract *nel diritto bancario e assicurativo*, in *Internet, contratto e persona: quale futuro?* a cura di R. Clarizia, Milano, 2021, p. 55 ss.; S. ORLANDO, *Profili definitori degli* "smart contracts", in *Internet, contratto e persona: quale futuro?* cit., p. 41 ss.; A. ZOPPINI, *Considerazioni generali su contratto e nuove tecnologie,* in *Internet, contratto e persona: quale futuro?* cit., p. 29 ss.; F. DELFINI, *Forma digitale, contratto e commercio elettronico*, Torino, 2020; ID., Blockchain, Smart Contracts *e innovazione tecnologica: l'informatica e il diritto dei contratti*, in *Riv. dir. priv.*, 2019, p. 167 e ss.; N. DE LUCA, *Documentazione crittografica e circolazione della ricchezza assente*, in *Riv. dir. civ.*, 2020, p. 101 ss.; F. DI GIOVANNI, *Sui contratti delle macchine intelligenti*, in *Intelligenza artificiale - Il diritto, i diritti, l'etica* a cura di U. Ruffolo, Milano, 2020; G. FINOCCHIARO, C. BOMPREZZI, *A legal analysis of the use of*

blockchain technology for the formation of smart legal contracts, in *Medialaws*, 2020, p. 111 e ss.; G. Gitti, A. Sardini, *I conferimenti di criptoattività*, in *Contratto e impresa*, 2020, p. 1289 e ss.; A. Quarta, G. Smorto, *Diritto privato dei mercati digitali*, Firenze, 2020; S. Fidotti, *Nuove forme contrattuali nell'era della Blockchain e del Machine Learning. Profili di responsabilità*, in *Diritto e intelligenza artificiale* a cura di G. Alpa, Pisa, 2020, p. 325 ss.; G. Rinaldi, *Smart contract: meccanizzazione del contratto nel paradigma della* blockchain, in *Diritto e intelligenza artificiale*, cit., p. 343 ss.; *Legal Statement on Cryptoassets and Smart Contracts* del novembre 2019 elaborato dalla *UK Jurisdiction Taskforce* (https://technation.io/about-us/lawtech-panel); *AA.VV.*, Blockchain *e* Smart Contract, a cura di R. Battaglini e M.T. Giordano, Milano, 2019; R. Battaglini, *La normativa italiana sugli smart contract*, in Blockchain *e* Smart Contract cit.; T. Belardi, *Gli* Smart Contract*: storia e definizioni di un ibrido contratto/software*, in Blockchain *e* Smart Contract cit.; S.A. Cerrato, *Contratti tradizionali, diritto dei contratti e* smart contract, in *Blockchain e Smart Contract,* cit.; R. de Caria, Blockchain *e* smart contract*: questioni giuridiche e risposte regolatorie tra diritto pubblico e privato dell'economia*, in *Blockchain e Smart Contract,* cit.; C. Poncibò, *Smart contract: profili di legge applicabile e scelta del foro*, in *Blockchain e Smart Contract,* cit.; N. Travia, *Profili internazionali del diritto degli smart contract*, in *Blockchain e Smart Contract,* cit.; *AA.VV.*, *Decisione robotica*, a cura di A. Carleo, Bologna, 2019; *AA.VV.*, *Legal Tech, Smart Contracts and Blockchain*, a cura di M. Corrales, M. Fenwick, H. Haapio, Singapore, 2019; *AA.VV.*, *Privacy Digitale*, a cura di E. Tosi, Milano, 2019; E. Battelli, E.M. Incutti, *Gli* smart contracts *nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contratto e impresa*, 2019, p. 925 e ss.; F. Benatti, *Un nuevo paradigma contractual: el caso de los smart contracts*, in *Derecho y nuevas tecnologías. El impacto de una nueva era,* a cura di J. Chipana Catalán, Lima (Perù), 2019; *L. Casalini, Blockchain and smart contracts. What changes lie ahead for banking and financial law?, in Diritto del risparmio, 3, 2019*; A. Contaldo, F. Campara, *Blockchain, criptovalute, smart contract, industria 4.0*, *Registri digitali, accordi giuridici e nuove tecnologie*, Pisa, 2019; L. Di Donna, *Diritto e tecnologia. Il contratto ai tempi dell'intelligenza artificiale e la giustizia predittiva*, in *Liber amicorum Guido Alpa*, a cura di F. Capriglione, Padova, 2019; M. Giaccaglia, *Considerazioni su* blockchain *e* smart contracts *(oltre le criptovalute)*, in *Contratto e impresa*, 2019, p. 941 e ss.; G. Lemme, *Blockchain, smart contracts, privacy, o del nuovo manifestarsi della volontà contrattuale*, in *Privacy Digitale*, a cura di E. Tosi, Milano, 2019, p. 293 ss.; G. Lemme, *Gli smart contracts e le tre leggi della robotica*, in *Analisi giuridica dell'economia*, fasc. 1, giugno 2019, Bologna, p. 129 ss.; R. Pardolesi, A. Davola, «Smart contract»*: lusinghe ed equivoci dell'innovazione purchessia*, in *Foro it.*, 2019, V, p. 195 ss. e in *Liber amicorum Guido Alpa*, a cura di F. Capriglione, Padova, 2019; T. Pellegrini, *Prestazioni auto-esecutive. Smart contract e dintorni*, in *Comparazione e diritto civile*, 2019, p. 843 ss.; A. Stazi, *Automazione contrattuale e "contratti intelligenti". Gli* smart contracts *nel diritto comparato*, Torino, 2019; L. Piatti, *I contratti informatici e gli smart contract*, in *Tecnologia e diritto (Vol. II - Informatica Giuridica)*, a cura di G. Ziccardi e P. Pierluigi, Milano, 2019; F. Scutiero, Smart contract *e sistema di diritto, un connubio tutto da definire*, in *Foro napoletano*, 2019, p. 113 e ss.; I.A. Caggiano, *Il contratto nel mondo digitale*, in *Nuova giur. civ. comm.*, 2018, p. 1152 e ss.; G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, p. 441 e ss.; M. Orcutt, *States that are passing laws to govern 'smart contracts' have no idea what they're doing*, in *MIT Technology Review*, 2018: *https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-*what-theyre-doing*/*; S.

ha formato il centro delle definizioni fin qui rese dai vari legislatori che vi si sono cimentati (compreso il legislatore italiano)[3] non sembrano

---

ESPOSITO DE FALCO, N. CUCARI, *Una reinterpretazione della* Corporate Governance *alla luce della tecnologia* blockchain*: nuove prospettive*, in *Referred Electronic Conference Proceeding*, 2018, p. 379 e ss.; A. LAFARRE, C. VAN DER ELST, *Blockchain Technology for Corporate Governance and Shareholder Activism*, European Corporate Governance Institute (ECGI) - Law Working Paper, 2018, n. 390, *Tilburg Law School Research Paper*, 2018, n. 7, accessibile in pdf a https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135209; P. MATERA, *Note in tema di Blockchain e assemblee delle società quotate nell'età della disintermediazione*, 2018, consultabile su http://www.comparazionedirittocivile.it/prova/files/blockchaine_matera.pdf; L. PAROLA, P. MERATI, G. GAVOTTI, Blockchain *e* smart contract: *questioni giuridiche aperte*, in *Contratti*, 2018, p. 681 e ss.; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della Blockchain, intelligenza artificiale e IoT*, Milano, 2018; M. Durovic, A. Janssen, *The Formation of Smart Contracts and Beyond: Shaking the Fundamentals of Contract Law?*, 2018 consultabile sul sito https://www.researchgate.net; P. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in *Nuova giur. civ. comm.*, 2017, p. 107 e ss.; D. DI SABATO, Gli smart contracts: robot *che gestiscono il rischio contrattuale*, in *Contratto e impresa*, 2017, p. 378 e ss.; V. PASQUINO, Smart contracts*: caratteristiche, vantaggi e problematiche*, in *Diritto e processo*, 2017, p. 239 e ss.; J. SKLAROFF, *Smart Contracts and the Cost of Inflexibility*, in *University of Pennsylvania Law Review*, Vol. 166, 2017, p. 263 ss.; K. WERBACH, N. CORNELL, *Contracts* ex machina, in *Duke Law Journal*, 2017, vol. 67, p. 313 ss.; P. DE FILIPPI, *The interplay between decentralization and privacy: the case of blockchain technologies*, in *Journal of Peer Production*, 2016; J. STARK, *Making sense of blockchain smart contracts*, cit.; C.D. CLACK, V.A. BAKSHI, L. BRAINE, *Smart contract templates: foundations, design landscape and research directions*, cit.; L. PIATTI, *Dal Codice Civile al codice binario: blockchain e* smart contracts, in *Ciberspazio e diritto*, 2016, p. 325 e ss.; M. ATZORI, *Tecnologia blockchain e governance decentralizzata: lo Stato è ancora necessario?*, 2015, e in lingua inglese *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 2015 https://www.academia.edu/23719145/Tecnologia_blockchain_e_governance_decentralizzata_lo_Stato_%C3%A8_ancora_necessario, e in lingua inglese: http://ssrn.com/abstract=2709713; G. ZYSKIND, O. NATHAN, A. PENTLAND, *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, 2015 in *IEEE Security and Privacy Workshops*, San Jose, CA, 2015.

[3] Il comma 2 dell'art. 8-*ter* Decreto Semplificazioni 2019, così reca:

«2. *Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.*». L'espressione "tecnologie basate su registri distribuiti" fa riferimento alle tecnologie *blockchain*, ed è a sua volta oggetto di una definizione, contenuta nel comma precedente, il comma primo dell'art. 8-ter del Decreto Semplificazioni 2019, ossia: «1. *Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione,*

esserci dubbi sulla possibilità teorica di riferirsi allo *smart contract* in due modi, integranti due ben distinte nozioni giuridiche: come ad un programma per elaboratore utilizzato esclusivamente per dare esecuzione, in tutto o in parte, ad un contratto (prima nozione), e come ad un programma per elaboratore utilizzato anche per esprimere, in tutto o in parte, il contenuto del contratto che viene eseguito automaticamente, ossia come programma per elaboratore che esprime al contempo, in linguaggio informatico, in tutto o in parte il programma contrattuale vincolante (seconda nozione)[4].

Il problema è, piuttosto, quello di stabilire i limiti entro i quali il concetto di accordo in senso giuridico sia compatibile con la seconda nozione di *smart contract*.

Per la proposizione e la trattazione di tale problema è indifferente in linea di principio che il programma per elaboratore operi o meno su

---

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.». Chiudono l'art. 8-*ter* i commi 3 e 4, del seguente tenore: «3. *La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.* 4. *Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3.*».

4 Cfr. il *Legal Statement on Cryptoassets and Smart Contracts*, della *UK's Jurisdiction Taskforce*, cit., p. 8: «*The parties' contractual obligations may be defined by computer code […] or the code may merely implement an agreement whose meaning is to be found elsewhere (in which case the code is unimportant from the perspective of defining the agreement)*», e p. 32: «*The precise role played by the software in a smart contract can vary: Alice and Bob may contract on the basis that their obligations are defined by the code and that they abide by the behaviour of the code whatever it does; or they may contract on the basis that code will be used to implement their agreement but not to define it; or they may contract on some hybrid basis, where some obligations are defined by code, others merely implemented by code and perhaps others not involving code at all*» (p. 32); similmente, in sintesi : «*"Smart legal contract" […] refers to legal contracts which are partly or wholly represented and/or performed by software*», così nella pubblicazione *Smart contracts. Legal framework and proposed guidelines for lawmakers*, cit., p. 6; A. Zoppini, *Considerazioni generali su contratto e nuove tecnologie*, cit., p. 31; S. Orlando, *Profili definitori degli "*smart contracts*"*, cit., p. 48 ss.; E. Battelli, *IA e* smart contract *nel diritto bancario e assicurativo*, cit., p. 60 ss.; A. Stazi, *Automazione contrattuale e "contratti intelligenti". Gli* smart contracts *nel diritto comparato*, cit., p. 119-120; G. Rinaldi, *Smart contract: meccanizzazione del contratto nel paradigma della* blockchain, cit., p. 353; G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, cit., p. 441 ss.; D. Di Sabato, Gli smart contracts: robot *che gestiscono il rischio contrattuale*, cit., p. 378 ss.; P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, cit., p. 107 ss.

una tecnologia *blockchain*, e sono a maggior ragione indifferenti le specifiche caratteristiche tecnologiche della *blockchain* come previste – peraltro in modo diversificato[5] e in qualche caso incompleto[6] – dai vari legislatori che ne hanno fin qui offerto una definizione[7].

Per questo motivo, non ci soffermeremo in questo articolo sulle peculiarità delle DLT (acronimo dalla espressione in lingua inglese per tecnologie a registro distribuito *Distributed Ledger Technology*).

---

5 A proposito della connotazione tecnologica della previsione del legislatore italiano, contenuta nell'art. 8-ter del c.d. Decreto Semplificazioni 2019 (decreto-legge 14 dicembre 2018, n. 135 recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione, convertito in legge con modificazioni dalla Legge 11 febbraio 2019, n. 12), v. la critica espressa in F. DELFINI, *Forma digitale, contratto e commercio elettronico*, cit., p. 27: «*[la normativa] non si attiene al principio della neutralità tecnologica e dunque fotografa una situazione puntuale nel tempo, destinata ad evoluzione con conseguente prevedibile e celere obsolescenza della disciplina giuridica stessa*»; e cfr. anche R. PARDOLESI, A. DAVOLA, «Smart contract»*: lusinghe ed equivoci dell'innovazione purchessia*, cit., p. 195 e ss. Rilievi critici di carattere generale sono espressi in M. ORCUTT, *States that are passing laws to govern 'smart contracts' have no idea what they're doing*, cit.

6 Ad oggi, l'Agenzia per l'Italia Digitale (AgID) non ha ancora emanato né le linee guida di cui al comma 2 né gli standard tecnici di cui al comma 4 dell'art. 8-*ter* Decreto Semplificazioni 2019.

7 Si riportano qui di seguito alcune definizioni dei legislatori di alcuni Stati degli Stati Uniti d'America e di Malta. Come si può vedere, nella definizione del legislatore di Malta manca il riferimento alle tecnologie *blockchain*. Per l'Arizona viene in rilievo la seguente definizione (del 29 marzo 2017): «*"smart contract" means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger*». Per il legislatore del Nevada (20 marzo 2017): «*"Smart contract" means a contract stored as an electronic record pursuant to chapter 719 of NRS which is verified by the use of a blockchain*». Per il legislatore del Tennessee (22 marzo 2018): «*"Smart contract" means an event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: (A) Take custody over and instruct transfer of assets on that ledger; (B) Create and distribute electronic assets; (C) Synchronize information; or (D) Manage identity and user access to software applications*». Per il legislatore di Malta (24 aprile 2018): «*''smart contract'' means a form of innovative technology arrangement consisting of: (a) a computer protocol; and, or (b) an agreement concluded wholly or partly in an electronic form which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both*».

10.2. Gli *smart contracts* come prodotti *software*

Per i fini del presente studio, e occupandoci soltanto delle questioni inerenti ai rapporti contrattuali, abbiamo deciso di incominciare la nostra analisi prescindendo dal rapporto che lega le parti che utilizzano uno *smart contract*, e di prestare attenzione al fatto – di per sé indubitabile, e pur tuttavia comunemente non considerato con la dovuta attenzione – che lo *smart contract*, in quanto programma per elaboratore[8], prima ancora di essere impiegato dagli utilizzatori-contraenti (ossia dalle parti di un contratto parzialmente o totalmente eseguito attraverso uno *smart contract*) assume rilevanza in rapporti giuridici diversi e distinti da quello che lega i suoi utilizzatori.

Lo *smart contract*, in quanto programma per elaboratore, innanzitutto, avrà uno o più autori, che potranno averlo creato per sé stessi, oppure in costanza di un rapporto di lavoro subordinato o in esecuzione di un contratto d'appalto o d'opera. Colui che (autore, datore di lavoro, committente) può disporre del programma, potrà, a sua volta, alternativamente, o utilizzarlo direttamente, sicché – proseguendo nell'analisi degli *smart contracts* inerenti a rapporti contrattuali – tale soggetto diventerà parte di un contratto eseguito (parzialmente o totalmente) attraverso il programma per elaboratore da egli predisposto a tal fine; oppure disporne in vario modo, e così alienarlo o darlo in licenza a vario titolo.

Naturalmente, la numerosità delle combinazioni ottenibili unendo il titolo della creazione a quello della disposizione del programma per elaboratore in questione rendono ampia e diversificata la gamma dei modelli giuridici dei rapporti potenzialmente interessati e delle relative discipline. Ciò vale a sottolineare la possibilità di riguardare lo

---

8 Che lo *smart contract* sia nel mondo dei fatti un programma per elaboratore, non è contestato da alcuno, ed è l'unica certezza riscontrabile in materia. Ciò è riflesso anche nelle formule dei legislatori che hanno offerto una definizione. Come visto, la prima proposizione del secondo comma dell'art. 8-*ter* del già citato c.d. Decreto Semplificazioni 2019 così reca: «2. *Si definisce "smart contract" un programma per elaboratore […]*»; per il legislatore dell'Arizona: «*"smart contract" means an event-driven program, with state […]*», per quello del Tennessee: «*"Smart contract" means an event-driven computer program […]*», per quello di Malta: «*''smart contract'' means a form of innovative technology arrangement consisting of: (a) a computer protocol; and, or (b) an agreement concluded wholly or partly in an electronic form which is automatable and enforceable by execution of computer code […]*».

smart contract quale oggetto di rapporti giuridici distinti rispetto al rapporto giuridico che corre tra i suoi utilizzatori, a partire dai rapporti conseguenti alla protezione della proprietà intellettuale del *software*.

Relativamente agli obiettivi della nostra analisi, possiamo limitarci in questo contesto a riferirci allo *smart contract* come a un prodotto *software*, allo specifico fine di evidenziare certe peculiarità del processo di creazione del programma per elaboratore e certe caratteristiche del suo risultato.

Sulla base di queste premesse, non sarà difficile cogliere che lo *smart contract*, in quanto prodotto *software*, propone una serie di questioni che vanno indagate per il loro riverbero sul rapporto che lega i suoi utilizzatori. Intuitivamente, per incominciare, si comprende che, in quanto prodotto *software*, lo *smart contract* può essere scritto e funzionare "male", e che ogni eventuale errore di progettazione, malfunzionamento o difettosità dello *smart contract* può pertanto riverberarsi anche sul rapporto che lega i suoi utilizzatori e produrre effetti sfavorevoli per uno o entrambi gli utilizzatori.

Ma, come vedremo più avanti, la prospettiva adottata consente anche di assumere maggiore consapevolezza per affrontare - prima di questi problemi ed anzi in vista di una loro corretta impostazione - la questione fondamentale su cui si interroga la dottrina, ossia stabilire se lo *smart contract* sia o non sia un contratto.

Conviene pertanto cominciare la nostra indagine, provando a capire, innanzitutto, come uno *smart contract* viene creato, ossia quali attività vengono poste in essere, e da chi, per la scrittura di un programma per elaboratore che serve all'esecuzione di prestazioni contrattuali.

10.3. Il linguaggio di programmazione e le questioni traduttologiche inerenti al processo di creazione degli *smart contracts*

Nell'analisi degli *smart contracts* come prodotti *software* vengono in rilievo una serie di questioni traduttologiche[9] che non possono essere

[9] Per la necessità di un'apertura alla traduttologia da parte del giurista contemporaneo, v. il magistrale saggio di G. BENEDETTI, *L'interpretazione traducente e la traduttologia giuridica*¸ in *Id.*, *Oggettività esistenziale dell'interpretazione. Studi su ermeneutica e*

ignorate, in quanto si tratta di questioni necessariamente implicate nel processo di creazione di qualsiasi programma per elaboratore.

All'esposizione che segue sembra opportuno premettere alcune nozioni elementari sulle caratteristiche dei linguaggi implicati dal processo in questione, in particolare il linguaggio di programmazione e il linguaggio macchina.

Sono essi l'uno in funzione dell'altro: il primo (il linguaggio di programmazione), è un linguaggio che si esprime attraverso parole, numeri, simboli di puntuazione e altri simboli grafici[10]. Si manifesta in una pluralità (centinaia) di lingue e perfino di "dialetti" variamente diversificati in termini sintattici e semantici, ed è preordinato all'elaborazione di istruzioni da tradurre nel linguaggio macchina che serve a trasmetterle agli elaboratori per la loro esecuzione. Il linguaggio macchina è composto di bit convenzionalmente rappresentati con i numeri 0 e 1 (c.d. alfabeto o codice binario di *bit*)[11]. Anch'esso si manifesta in una pluralità di 'lingue' o codici o linguaggi, diversificati in funzione delle caratteristiche degli elaboratori (architettura *hardware*).

Come risaputo, le istruzioni fornite ad un elaboratore attraverso un programma (programma per elaboratore) sono tutte riducibili allo schema logico *se* → *allora*: il programma prevede certe condizioni, soddisfatte le quali si chiede all'elaboratore di compiere una o più operazioni. Sebbene il concetto di algoritmo non sia associato necessariamente ad istruzioni eseguibili da un computer, nel linguaggio comune si è ormai affermato l'uso per il quale le istruzioni impartite agli elaboratori vengono chiamate anche algoritmi, e si fa anzi comunemente riferimento a tale parola per indicare specificamente le istruzioni affidate all'elaborazione dei *computer*.

---

diritto, Torino, 2014, p. 189 ss.; già pubblicato con diverso titolo, *L'elogio dell'interpretazione traducente nell'orizzonte del diritto europeo*, in *Eur. dir. priv.*, 2010, p. 413 ss.; e in *Scritti in onore di Alessandro Pace*, I, Napoli, 2012, p. 21 ss. In termini problematici, si confronta con i problemi del linguaggio di programmazione a proposito degli *smart contracts*, sottolineando le "*criticità dello strumento*", G. Rinaldi, *op. loc. ult. cit*.

10 Il linguaggio di programmazione si distingue in linguaggio di programmazione c.d. di alto livello, che è normalmente il primo linguaggio di programmazione utilizzato dai programmatori, e linguaggio di programmazione c.d. di basso livello chiamato *assembly*, la cui sintassi e semantica si avvicinano di più al linguaggio macchina e per questo motivo è più difficile da utilizzare e da comprendere anche da parte dei programmatori.

11 Può essere rappresentato anche in codice esadecimale (0-9 A-F) per ridurne la lunghezza.

In questo modo viene creato e affidato agli elaboratori (*hardware*) qualunque istruzione di qualunque programma per elaboratore (*software*) quale che ne sia il contenuto e la funzione: le nozioni di cui sopra sono pertanto nozioni generali – ed anche molto elementari – che riguardano qualunque linguaggio di programmazione, qualunque linguaggio macchina, qualunque istruzione contenuta in qualunque programma per elaboratore (*software*), e cioè non si tratta di osservazioni particolari relative ai soli programmi per elaboratori chiamati *smart contracts*. Infine, aggiungiamo che, nel linguaggio corrente, il programma per elaboratore viene anche chiamato *code*, ossia ('codice'). Il programma scritto in linguaggio di programmazione[12] viene chiamato 'codice sorgente', mentre quello scritto in linguaggio macchina, che viene eseguito dal computer, viene chiamato 'codice macchina' (o anche 'codice oggetto').

Con valenza altrettanto generale (ossia non limitata agli *smart contracts*), bisogna ora osservare che le istruzioni impartite all'elaboratore sono il frutto di almeno due traduzioni, e, nella grande maggioranza dei casi, di tre traduzioni: poiché esse vengono originariamente concepite ed ordinariamente espresse nei termini di una determinata lingua del linguaggio c.d. naturale, per trasferirle ad un elaboratore sarà necessaria una prima traduzione da quella determinata lingua del linguaggio naturale ad una determinata lingua del linguaggio di programmazione; ed una seconda traduzione dalla lingua del linguaggio di programmazione ad una lingua del linguaggio macchina.

Mentre la prima traduzione (quella dal linguaggio naturale al linguaggio di programmazione) è operata da uomini, i "programmatori", la seconda traduzione è operata da elaboratori che lavorano a loro volta eseguendo automaticamente apposite istruzioni contenute in appositi programmi per elaboratore che servono proprio a questa funzione, in gergo chiamati *software* "compilatori"[13].

---

[12] Sia se scritto in una lingua di linguaggio di programmazione c.d. di alto livello, sia se scritto in una lingua del linguaggio *assembly* c.d. di basso livello.

[13] Seppure normalmente i programmatori scrivono il codice sorgente in una lingua di linguaggio di programmazione di alto livello, è possibile che lo facciano in una lingua del linguaggio *assembly* di basso livello (in passato era questo il linguaggio utilizzato dai programmatori per i primordiali videogiochi). Ad ogni modo, anche il linguaggio di programmazione di basso livello *assembly* deve essere tradotto in linguaggio macchina, e questa traduzione avviene attraverso un *software* c.d. *assembler*. In alcuni casi, infine, si dice che il linguaggio di programmazione viene direttamente

Nei fatti, e nella quasi totalità dei casi, le traduzioni sono tre, perché vengono utilizzati due livelli di linguaggio di programmazione prima di passare alla traduzione nel linguaggio macchina. In particolare, le istruzioni concepite ed espresse nel linguaggio naturale vengono dapprima versate dai programmatori in un primo linguaggio di programmazione c.d. di alto livello (prima traduzione), successivamente si ha una traduzione del programma per elaboratore espresso in questo linguaggio (codice sorgente) in un secondo linguaggio di programmazione di c.d. basso livello, l'*assembly* (seconda traduzione), ed infine si ha una traduzione di questo secondo codice espresso in linguaggio *assembly* in linguaggio macchina (terza traduzione).

Le traduzioni tra i linguaggi informatici sono a loro volta fatte da *software* "compilatori" (*compilers*). Quando si frappone il linguaggio *assembly*, tali *software* sono chiamati in gergo "assemblatori" (*assemblers*). In particolare, la traduzione dal linguaggio di alto livello al linguaggio *assembly* è fatta da software compilatori e la traduzione dal linguaggio *assembly* al linguaggio macchina è fatta da *software* assemblatori.

10.4. (Segue) le perdite e le trasformazioni dal linguaggio naturale al linguaggio di programmazione

Come si potrà ora ben intuire, la prima traduzione (dal linguaggio naturale al primo linguaggio di programmazione) è nei fatti il frutto, prima che di una traduzione, di un adattamento: i programmatori cercheranno di rendere al meglio in una specifica lingua di un linguaggio di programmazione quanto originariamente concepito ed espresso (nella maggior parte dei casi: da altri) in una specifica lingua del linguaggio c.d. naturale.

I programmatori dovranno dunque innanzitutto comprendere

eseguito dal computer (è il caso ad es. delle lingue di programmazione del vecchio *Basic*). In realtà, anche in questi casi vi è pur sempre una traduzione (in linguaggio macchina), solo che la traduzione è contestuale all'esecuzione ed è fatta di volta in volta (ossia allorquando il programma deve essere eseguito), con la vera differenza che in questi casi non viene prodotto un *file* in linguaggio macchina. In gergo informatico si parla in questi casi di "interpretazione" per distinguerla dalla "compilazione", perché quest'ultimo sostantivo esprime proprio il risultato della compilazione consistente nella creazione di un 'oggetto', ossia il *file* in linguaggio macchina che contiene un programma o codice (il 'codice macchina' o 'codice oggetto') che viene eseguito.

senza riserve (interpretandolo) il testo da tradurre, espresso in una lingua del linguaggio naturale, e, in secondo luogo, quale che sia la formulazione del testo da tradurre in linguaggio di programmazione (ed anche se esso non si esprime letteralmente con formule di istruzioni), ridurlo ad una serie di istruzioni rispondenti ineluttabilmente alla logica del *se* → *allora*; per applicarvi – infine – la sintassi e la semantica proprie della lingua di programmazione prescelta.

Nel far ciò, il programmatore dovrà scartare qualsiasi elemento del testo del linguaggio naturale da tradurre, che (secondo il suo giudizio) sia irriducibile alla predetta logica (*se* → *allora*). Allo stesso modo, il programmatore dovrà eliminare e non includere nel programma per elaboratore qualsiasi elemento che (secondo il suo giudizio) comporti ambiguità circa l'identificazione delle circostanze da soddisfare come condizioni ("se") o delle operazioni richieste al soddisfacimento delle medesime condizioni ("allora") o circa la necessaria consequenzialità tra le une e le altre ("→").

Come anche si potrà facilmente intuire, quest'opera di adattamento è interamente affidata a interpretazioni e giudizi di vario tipo, e dunque può ben dar luogo ad esiti opinabili, ad errori e a distorsioni volontarie, con la conseguenza che può verificarsi sia un'ingiustificata esclusione dal programma per elaboratore di alcune istruzioni implicitamente o esplicitamente contenute nel testo da tradurre (in quanto, ad esempio, alcune istruzioni non sono riconosciute come tali dal programmatore o sono da egli ritenute irriducibili alla logica del *se* → *allora*, oppure in quanto il programmatore, pur riconoscendo che un pezzo di testo contiene un'istruzione riducibile alla logica del *se* → *allora*, ritenga nondimeno che uno o più degli elementi di tale istruzione sia troppo ambiguo e non sia di conseguenza possibile – secondo il suo giudizio – procedere con sufficiente certezza alla sua individuazione) sia, naturalmente, una loro inesatta traduzione in linguaggio di programmazione per un colpevole fraintendimento o per una volontaria deviazione dal significato testualmente riconoscibile o comunque conosciuto dal programmatore e riconoscibile sulla base di elementi extra-testuali.

Infine, e abbastanza evidentemente, la possibilità delle perdite e delle trasformazioni di cui stiamo parlando sarà tanto più intensamente ricorrente quanto più il testo originario del linguaggio naturale

da tradurre in linguaggio di programmazione sarà tecnicamente connotato, perché, in questo caso, al programmatore verrà richiesto un supplemento di capacità, ossia di essere egli stesso sufficientemente competente per comprendere appieno il linguaggio tecnico (es. linguaggio medico, giuridico, artistico) impiegato nel testo di lingua naturale che egli deve tradurre, o di avere o fruire dei mezzi di un'organizzazione che abbia sufficienti risorse per assumere, gestire ed assimilare una consulenza che sia a sua volta qualificata in modo sufficiente a colmare pienamente la lacuna di conoscenza del programmatore per i fini dell'interpretazione del testo e della sua traduzione nella lingua di programmazione prescelta.

Dopo di ciò, il programma per elaboratore espresso in una lingua di programmazione, sarà affidato ad uno o più *software* "compilatori" per la sua traduzione in linguaggio macchina (previa eventuale traduzione intermedia in linguaggio di programmazione *assembly*, come accade il più delle volte); e anche l'esito di queste operazioni dipenderà dalle funzionalità degli specifici *software* "compilatori" impiegati, che sono soggetti (come tutti i *software*) a malfunzionamenti (in gergo, *bugs*).

A completamento di queste osservazioni, sembra opportuno aggiungere che la ricorrente affermazione per la quale il primo linguaggio di programmazione sarebbe immediatamente e facilmente comprensibile a differenza del linguaggio *assembly* e del linguaggio macchina – motivo per il quale si indica con l' espressione "linguaggio di alto livello" la famiglia dei linguaggi usualmente utilizzati dai programmatori per la scrittura del codice sorgente (*high level* in inglese è una espressione utilizzata per segnalare un discorso semplice ed immediatamente comprensibile) – è un'affermazione priva di senso se non soggettivamente contestualizzata, ossia se non riferita a capacità e conoscenze medie di classi di soggetti, quali i programmatori o altri soggetti che per motivi di studio o professionali abbiano significative esperienze del linguaggio di programmazione (e naturalmente in concreto, ossia con riferimento a specifiche lingue di programmazione).

Per rendersene conto, ossia per rendersi conto di quanto incomprensibili siano i linguaggi di programmazione di alto livello per le persone che non possiedano quelle specifiche conoscenze, indico qui di seguito il *link* a un breve *smart contract* che opera su *Ethereum*

espresso nella lingua di programmazione di alto livello *Solidity*[14] che, al soddisfacimento di certe condizioni, crea lo spazio per inserire una prova crittografica (una firma digitale) all'interno di una *blockchain* nell'ambito di un progetto di tracciabilità di filiere produttive[15]:

https://github.com/Devoleum/devoleum-eth-notarization-muninn/blob/main/contracts/Devoleum.sol

riportandolo per esteso qui di seguito:

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;

import "@openzeppelin/contracts/ownership/Ownable.sol";
import "@openzeppelin/contracts/math/SafeMath.sol";

/// @title Devoleum
/// @author Lorenzo Zaccagnini Elisa Romondia
/// @notice You can use this contract for your JSONs notarization
/// @dev All function calls are currently implemented without side effects
contract Devoleum is Ownable {
  using SafeMath for uint256;

  struct Step {
    uint256 createdAt;
    string hashOfJson;
  }

  //COUNTERS
  uint256 public stepsCounter = 0;
```

[14] *Solidity* è una lingua di linguaggio di programmazione di alto livello usata diffusamente per gli *smart contracts* che operano su *Ethereum*.

[15] Progetto *Devoleum*: https://www.devoleum.com/ su cui v. M. GULMINI, *Opportunità e criticità derivanti dall'applicazione delle tecnologie blockchain nella gestione della* supply chain*, con particolare riferimento al settore agroalimentare e all'esperienza di Devoleum*, tesi di laurea a.a. 2018/2019 disponibile *online* sul sito dell'Università Ca' Foscari di Venezia: http://dspace.unive.it/handle/10579/16576.

```
    //STRUCT MAPPINGS
    mapping(uint256 => Step) public stepIdToStepInfo;
    mapping(string => uint256) public hashToId;
    event StepProofCreated(uint256 _id, string _hash);

    //Modifiers
    modifier noDuplicate(string memory _hashOfJson) {
      require(hashToId[_hashOfJson] == 0, "duplicate");
      _;
    }

    /// @notice Notarizes a supply chain Step Proof
    /// @param _hashOfJson The hash proof of the JSON file
    /// @return The numeric ID of the Step proof
    function createStepProof(string calldata _hashOfJson)
      external
      onlyOwner
      noDuplicate(_hashOfJson)
      returns (uint256 stepID)
    {
      Step memory newStep = Step(now, _hashOfJson);
      stepsCounter = stepsCounter.add(1);
      stepIdToStepInfo[stepsCounter] = newStep;
      hashToId[_hashOfJson] = stepsCounter;
      emit StepProofCreated(stepsCounter, _hashOfJson);
      return stepsCounter;
    }
}
```

E per completezza indico qui di seguito il *link* per accedere ai corrispondenti programmi in linguaggio *assembly* e in linguaggio macchina[16]:

[16] Nella pagina che si apre con il *link* il programma in linguaggio macchina si trova nell'ultimo riquadro in fondo "*Contract Creation Code*" ed è rappresentato in codice esadecimale (0-9 A-F). Per vedere la versione *assembly* basta cliccare sul tasto in alto a destra del riquadro: "*Switch to Opcodes View*".

https://rinkeby.etherscan.io/address/0x64169a158089f879048738e944c5c930548c620f#code

10.5. Asimmetria informatica e accordo in senso giuridico

Le osservazioni svolte nei paragrafi precedenti permettono di vedere la fragilità dell'ipotesi per la quale sarebbe generalmente possibile ricostruire lo *smart contract* nei termini di un contratto, ossia di un programma per elaboratore che esprime esso stesso in linguaggio informatico il programma contrattuale giuridicamente vincolante.

Si tratta infatti di un'ipotesi ricostruttiva che sembra sottovalutare la complessità del processo di creazione del programma per elaboratore e le specificità dei linguaggi implicati in tale processo produttivo, manifestando di non considerare innegabili elementi di fatto che devono necessariamente sottoporsi all'analisi giuridica, ed in particolare al confronto con il concetto di accordo in senso giuridico.

La precisazione che sia rilevante sottoporre l'analisi degli *smart contracts* al confronto con il concetto di accordo "in senso giuridico", vale, naturalmente, ed in primo luogo, ad allontanare teorie che – ove mai siano state normativamente e storicamente giustificate – sono ormai largamente superate, e così, ad escludere concezioni per le quali la sequenza procedimentale per la conclusione del contratto debba necessariamente intendersi in termini dialogici[17].

Se tanto è sicuro, si tratta nondimeno (e diremmo per l'appunto) di stabilire quali dichiarazioni e comportamenti possano ritenersi idonei

---

[17] Quanto al procedimento di formazione del contratto, la specificazione che ci si debba rivolgere all'accordo "in senso giuridico", serve, naturalmente, a richiamare l'esito più consapevole del dibattito odierno, per cui la sequenza procedimentale che porta alla conclusione del contratto può, ben vero, configurarsi entro «*confini dialogici, ma può anche da essi prescindere, incentrandosi sulla pura e semplice conformità delle dichiarazioni negoziali rese dalle parti in tempi diversi o contestuali e persino nell'assenza di dichiarazioni, quando atti ad esse non riconducibili siano ciononostante considerati idonei dalla disciplina normativa*»: G. VETTORI, *Contratto e rimedi*, III ed., Milano, 2017, p. 262; cfr. R. SACCO, *Il problema della riforma (La conclusione del contratto)*, in *Il diritto delle obbligazioni e dei contratti verso una riforma? Le prospettive di una novellazione del Libro IV del Codice Civile nel momento storico attuale, Atti del Convegno per il cinquantenario della Rivista di diritto civile*, Treviso, Palazzo dell'Università, 23-24-25 marzo 2006, Padova, 2006, p. 200 s.; ID., voce *Scambio*, in *Dig. disc. priv., sez. civ., Aggiornamento* *******, II, Torino, 2012, p. 896 ss.; S. ORLANDO, *Fattispecie, comportamenti, rimedi. Per una teoria del fatto dovuto*, in *Riv. trim. dir. proc. civ.*, 2011, p. 1051.

secondo la legge a valutarsi in termini di accordo nell'ambito disciplinare oggetto di analisi e regolato nell'art. 8-*ter* co. 2 del Decreto Semplificazioni 2019, proponendo soluzioni realistiche, plausibili e coerenti al fenomeno indagato.

Ove ciò sia condiviso in termini di metodo, apparirà senz'altro necessario considerare le specifiche nozioni che servono a comprendere il processo di creazione dei programmi per elaboratori e i linguaggi *software*, quanto meno nei termini elementari riassunti ai precedenti paragrafi 10.2. e 10.3.

Ponendo mente a quelle nozioni, è possibile specificare e sviluppare alcune questioni conseguenti alla rilevazione di un dato di fatto di comune esperienza, che, pur frequentemente individuato in dottrina, non appare indagato in modo approfondito, e che consiste nell'oggettiva e ben riscontrabile ignoranza dei linguaggi dei programmi per elaboratori da parte della generalità dei consociati.

A questo riguardo, tenute presenti le caratteristiche dei linguaggi di programmazione e dei linguaggi macchina di cui abbiamo detto *supra*, ci sembra senz'altro corretto ritenere che, laddove si riscontri una situazione di carenza cognitiva consistente nell' ignoranza del linguaggio informatico di uno *smart contract* da parte di uno degli utilizzatori contraenti – situazione che abbiamo già proposto in altra sede di chiamare per brevità "asimmetria informatica" [18] – non possa farsi altro che ritenere tale situazione ostativa alla conclusione di un accordo in senso giuridico su un programma contrattuale espresso in linguaggio informatico, e dunque ostativa alla conclusione di *smart contracts* rispondenti alla seconda nozione di cui sopra.

In tutti i casi in cui si ravvisi un'asimmetria informatica, si dovrà ritenere inammissibile la conclusione di un accordo in senso giuridico e quindi di uno *smart contract* inteso come contratto auto-esecutivo, e lo *smart contract* eventualmente attivato tra due parti dovrà intendersi semplicemente come programma *software* inteso a dare esecuzione in tutto o in parte ad un contratto dichiarato altrove (prima nozione).

Poiché – nel tempo presente – la situazione soggettiva di generale ignoranza del linguaggio informatico e l'asimmetria informatica, nel senso sopra inteso, sono senz'altro riscontrabili nella generalità dei

---

[18] S. Orlando, *Profili definitori degli* smart contracts, cit., p. 51 ss.

casi, dovrà necessariamente ritenersi che la conclusione di *smart contracts* intesi come 'contratti' auto-esecutivi (seconda nozione) sia generalmente inammissibile, mentre dovrà ritenersi generalmente ammissibile la conclusione di contratti per l'esecuzione dei quali una delle parti abbia predisposto un dispositivo tecnologico governato da programmi per elaboratori (prima nozione).

La situazione soggettiva di generale ignoranza del linguaggio informatico da parte dei consociati – che possiamo qualificare come stato soggettivo generalmente rilevante – osta in particolare a che si possa ritenere generalmente sufficiente ad essere giudicato come espressivo di un accordo in senso giuridico ai fini della formazione di un contratto una qualunque manifestazione anche se esplicita ed inequivocabile di assenso e di adesione di un soggetto al contenuto di un programma per elaboratore; e osta a che possa generalmente ritenersi ammissibile ricavare il contenuto di un contratto dal contenuto di un programma per elaboratore.

Con ciò, naturalmente, non intendiamo anche negare generalmente la possibilità di conclusione di contratti la cui esecuzione sia affidata (parzialmente o totalmente) a *smart contracts*, ma vogliamo dire che, nella generalità dei casi, ove si riscontri che uno *smart contract* viene attivato tra due parti, esso dovrà intendersi semplicemente come programma per elaboratore inteso a dare esecuzione in tutto o in parte ad un contratto tra di esse eventualmente concluso secondo le regole ordinarie, ed espressivo di un contenuto da ricavarsi secondo le regole ordinarie.

Ciò sta anche a significare che il programma per elaboratore servirà nella generalità dei casi solo come dispositivo tecnologico di esecuzione di un contratto per la cui conclusione sarà tuttavia necessario che la parte aderente sia stata preventivamente messa a conoscenza di una offerta contrattuale espressa ed intellegibile alla stregua del linguaggio naturale. Pertanto, del contratto in questione (al quale lo *smart contract* può generalmente servire solo come dispositivo tecnologico di esecuzione) né la formazione potrà essere asseverata sulla base di contegni dichiarativi o esecutivi ricostruibili in termini di conformità o mera adesione al contenuto del programma per elaboratore, né il contenuto potrà dirsi coincidente, nemmeno parzialmente, con il contenuto del programma per elaboratore.

Si deve ora aggiungere che alle predette conclusioni sono in linea

di principio irrilevanti le tradizionali distinzioni e le più recenti subdistinzioni tra contratti B2C, B2B, B2b, così come non deve confondersi l'asimmetria informatica (nel senso sopra inteso) con l'asimmetria informativa.

L'asimmetria informatica, nel senso sopra delineato, è ben distinguibile dall'asimmetria informativa, perché mentre quest'ultima esprime la mancanza di conoscenza di informazioni rilevanti, secondo le circostanze, da parte di un contraente, a fronte della conoscenza delle medesime informazioni da parte di un altro contraente, l'asimmetria informatica, nel senso sopra inteso e riferito allo *smart contract*, esprime la mancanza di conoscenza da parte di un contraente del linguaggio nel quale un altro contraente pretenderebbe che fosse dichiarato il contenuto di un contratto, ossia il linguaggio in cui è espresso un programma per elaboratore.

Per tale motivo, laddove anche il programma per elaboratore di uno *smart contract* venga reso accessibile in *open source* (ciò che anche negli ecosistemi *blockchain* dipende sempre da una precisa scelta del predisponente)[19], non per questo solo potrà ritenersi che esso è stato reso conoscibile alla generalità dei potenziali contraenti secondo l'ordinaria diligenza, essendo viceversa ostativa a questa conclusione la carenza di intelligibilità (qui non coincidente con la conoscibilità) del medesimo programma, a cagione dell'ignoranza del linguaggio nel quale esso è espresso.

Ed invero sembra in proposito corretto osservarsi che, tutte le volte in cui la conoscibilità è intesa dalla legge come conseguenza ineluttabile sul piano cognitivo dell'accessibilità ad una informazione (es. art. 1341 co. 1 c.c., art. 1335 c.c.) ciò avviene nel presupposto della conoscenza del linguaggio nel quale è espressa l'informazione da parte di chi può accedervi. Da qui la distinzione tra intellegibilità e conoscibilità nel fenomeno di cui stiamo parlando, che contribuisce a spiegare il concetto di asimmetria informatica.

Su queste basi, si può prendere posizione su due questioni particolari, conseguendo da quanto sopra esposto sia una generale inammissibilità per gli *smart contracts* del procedimento di conclusione del contratto attraverso l'inizio di esecuzione (art. 1327 c.c.) sia una generale inconfigurabilità dello *smart contract* come offerta al pubblico (art. 1336

[19] Cfr. https://docs.soliditylang.org/en/v0.8.1/layout-of-source-files.html

c.c.).

Mentre, alla luce di quanto già illustrato, la conclusione relativa all'offerta al pubblico non sembra necessitare di ulteriori spiegazioni, sembra opportuno spendere qualche parola in più sulla questione dell'art. 1327 c.c., che appare più complicata e bisognevole di distinzioni chiarificatrici, anche per la necessità di interpretare la previsione dell'art. 8-*ter* del Decreto Semplificazioni 2019, una cui lettura superficiale potrebbe indurre a ritenere che per il nostro legislatore sia autorizzata o addirittura doverosa la conclusione opposta.

Deve in proposito specificarsi che, mentre ben potrà concludersi un contratto espresso in linguaggio naturale attraverso un'attività materiale consistente nell'avvio di esecuzione di un programma per elaboratore (*smart contract*), in quanto tale attività materiale potrà ben intendersi – ricorrendo tutti gli altri requisiti – come inizio di esecuzione del contratto ex art. 1327 c.c., non può invece ritenersi che si possa generalmente "concludere uno *smart contract*" in questo modo, perché una simile affermazione presuppone che ci si riferisca allo *smart contract* come a un contratto che si possa "concludere", ossia presuppone che ci si riferisca alla seconda nozione di *smart contract* sopra enunciata.

Alla luce di queste osservazioni, possiamo rivolgerci ora al dettato dell'art. 8-*ter* del Decreto Semplificazioni 2019, con la necessaria consapevolezza circa il modo in cui intendere il concetto di esecuzione colà impiegato, specificando con nettezza: che in quella norma l'«*esecuzione*» è l'esecuzione di un codice, intesa in senso tecnico-informatico, e dunque che tale sostantivo si riferisce propriamente al soggetto logico della frase che in quella frase è per l'appunto il «*programma per elaboratore*» (e non già il contratto), cosicché le parole «*la cui esecuzione*» devono leggersi come "l'esecuzione del programma per elaboratore"[20]; che «*effetti predefiniti*» sono da intendersi predefiniti tra le parti nel linguaggio naturale; e che l'espressione «*vincola automaticamente*» sta a significare, come detto, l'idoneità di un'attività meramente materiale, consistente nell'avvio di esecuzione di un programma per elaboratore, a concludere automaticamente un contratto (e di conseguenza

[20] Si osserva e si precisa infine che quando il legislatore dice «*la cui esecuzione*», esso si riferisce al codice macchina perché è solo questo il programma per elaboratore che può essere eseguito dall'elaboratore. Si tratta cioè del programma per elaboratore scritto in linguaggio macchina, che è praticamente incomprensibile anche per i più esperti programmatori.

a «vincolare automaticamente» le parti) il cui contenuto («*la base di effetti predefiniti*») è tuttavia espresso e ricostruibile in linguaggio naturale e previamente portato a conoscenza dell'utilizzatore-aderente secondo le regole ordinarie.

Alla luce delle considerazioni di cui sopra, si comprende perciò come si tratti di una previsione normativa assolutamente in linea con la regola generale di cui all'art. 1327 c.c. In altre parole, nulla di ciò che è scritto nell'art. 8-*ter* Decreto Semplificazioni autorizza a deviare in termini generali dal contesto dei principî sottesi all'art. 1327 c.c., tanto meno una simile deviazione è promuovibile in considerazione delle caratteristiche del fenomeno disciplinato.

Fermo restando quanto sopra, ed anzi a conferma del valore generale della superiore conclusione, dovrà riconoscersi anche che, se non può deviarsi in termini generali dalla medesima conclusione (per la valenza a sua volta generale dell'asimmetria informatica, nel senso illustrato), ciò non vale ad escludere anche l'ipotesi che una conclusione diversa, che ammetta la possibilità della conclusione di *smart contracts* intesi come contratti (seconda nozione), possa rinvenirsi in casi particolari, da asseverarsi di volta in volta. In particolare, laddove sia possibile riscontrare l'assenza di una asimmetria informatica e la volontà di entrambi i contraenti di vincolarsi esattamente al contenuto contrattuale come espresso da un programma per elaboratore. Simili accordi possono per il vero perseguire finalità di certezza, senz'altro meritevoli di tutela.

Ciò potrà riscontrarsi, con indagine da compiersi di volta in volta, quanto al primo requisito (carenza di asimmetria informatica) laddove risulti che il programma *software* sia stato congiuntamente elaborato o condiviso da entrambi i contraenti attraverso tecnici programmatori informatici; e, quanto al secondo requisito (volontà), laddove risulti una manifestazione di volontà inequivoca da parte di entrambi i contraenti di adottare una specifica lingua di programmazione quale lingua espressiva del programma contrattuale nella forma di un programma per elaboratore.

Solo in casi simili, e, allo stato non riscontrabili in casistiche note o significative, potrà ritenersi che lo *smart contract* esprima esso stesso il programma contrattuale vincolante tra le parti, e sia pertanto nominabile in termini di contratto.

Fuori di questi casi, viceversa, il concetto di accordo in senso giuridico impone di erigere, per così dire, una diga, e di promuovere la consapevolezza che l'area occupata dagli *smart contracts* è, per rimanere in metafora, un bacino artificiale, popolato da repliche per elaboratori di programmi contrattuali.

Sulla base di questa consapevolezza, si tratterà allora di individuare con rigore i rischi, non soltanto quelli che gli *smart contracts* intendono gestire[21], ma anche quelli creati dagli *smart contracts* per la loro consistenza o natura di programmi *software*.

Nel linguaggio corrente con l'espressione "rischio informatico" (in inglese "*cyber risk*") si fa genericamente riferimento a una serie di rischi derivanti da minacce alla sicurezza dei sistemi informatici e dei dati (c.d. *cyber attacks* e *data breach*), che possono presentarsi e propagarsi fino al punto da connotarsi come minacce di "sistema" ("*systemic cyber risk*")[22].

Seppure si tratti di tipi di rischi sicuramente rilevanti nell'ambito di un discorso sui nuovi ecosistemi digitali, non è su di essi che vogliamo qui soffermarci; e ciò, non tanto perché alcuni di quei rischi (non tutti) sono ridotti o assenti negli ecosistemi *blockchain* sui quali tipicamente operano gli *smart contracts*, ma perché il nostro discorso ha

---

21 Cfr. D. Di Sabato, *Gli* smart contracts: robot *che gestiscono il rischio contrattuale*, cit., p. 378 e ss. Sul rischio contrattuale, v. per tutti F. Delfini, *Autonomia e rischio contrattuale*, Milano, 1999; G. Alpa, *Rischio contrattuale*, in *Noviss. Dig. It., Appendice,* VI, Torino, 1986, p. 863 ss.; E. Gabrielli, *Alea e rischio nel contratto. Studi*, Napoli, 1997; Id., *Il rischio contrattuale*, in *I contratti in generale*, a cura di Alpa e Bessone, I, Torino, 1991, p. 635; Id., *Tipo negoziale, prevedibilità dell'evento e qualità della parte nella distribuzione del rischio contrattuale*, in *Giur. it.,* 1986, I, 1, c. 1713 ss.; Sargenti, voce «Rischio contrattuale (diritto romano)», in *Enc. dir.*, XL, Milano, 1989, p. 1126 ss.; Bessone, *Adempimento e rischio contrattuale*, Milano, 1968.

22 Cfr. la definizione di "*systemic cyber risk*" resa a p. 5 del *White Paper* del *World Economic Forum* dell'ottobre 2016 dal titolo *Understanding Systemic Cyber Risk*, disponibile su http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf: «*Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security. The adverse real economic, safety and security effects from realized systemic risk are generally seen as arising from significant disruptions to the trust in or certainty about services and/or critical data (i.e. the integrity of data), the disruption of operations and, potentially, the incapacitation or destruction of physical assets*.».

ad oggetto il rapporto tra programma contrattuale e programma per elaboratore: che presenta degli specifici rischi, diversi da quelli relativi alla sicurezza dei sistemi informatici e dei dati.

10.6. Il rischio dell'esecuzione e il rischio della dichiarazione

Avendo compreso che gli *smart contracts* sono generalmente definibili come codici *software* intesi a replicare programmi contrattuali o pezzi di programmi contrattuali in funzione della loro esecuzione automatica, e solo eccezionalmente idonei ad esprimere essi stessi in tutto o in parte programmi contrattuali, si comprenderà anche agevolmente che questo fenomeno propone una sua specifica rischiosità.

Seppure, naturalmente, non è possibile affrontare in questa sede questo tema nella sua interezza, sembra utile proporre un'indagine tipologica[23], volta all'individuazione di tipi di rischio a partire da tipi di accadimenti e da tipi di sacrifici minacciati dagli accadimenti, e, su questa base, individuare generalmente una tipologia di rischi con l'espressione "rischi della programmazione", che possiamo distinguere in due sotto-categorie, a seconda che si abbia a riferimento la prima nozione o la seconda nozione di *smart contract*, come sopra illustrate: la categoria del "rischio dell'esecuzione" e quella del "rischio della dichiarazione".

Tali categorie propongono altrettanti problemi, consistenti nello stabilire chi debba sopportare (o sopportare definitivamente)[24] le conseguenze sfavorevoli dell'accadimento genericamente individuato con l'espressione "rischi della programmazione", e che si tratterà a sua volta di specificare per affinare l'analisi.

Così, con il problema del 'rischio dell'esecuzione' intendiamo, nell'ambito degli *smart contracts* rispondenti alla prima nozione (meri

---

23 Per la proposta di individuazione tipologica dei rischi giuridicamente rilevanti cfr. E. Gabrielli, *Alea e rischio nel contratto. Studi*, cit., p. 115 ss.; Id., *Il rischio contrattuale*, cit., p. 635; S. Orlando, *Rischio e vendita internazionale*, cit., p. 15 ss.

24 La precisazione è necessaria in conseguenza dell'automaticità delle operazioni eseguite dall'elaboratore, sicché laddove un'operazione eseguita automaticamente dall'elaboratore, per errore di scrittura o altro malfunzionamento del software, comporti un sacrificio per un contraente, il problema di rischio consiste nello stabilire se tale sacrificio debba rimanere definitivamente in capo a tale contraente o possa essere ribaltato sulla controparte.

software in funzione di esecuzione di contratti dichiarati altrove), individuare una serie di sacrifici minacciati dalla non rispondenza di quanto impartito al sistema informatico attraverso il linguaggio *software* al contenuto del contratto. Sulla base del concetto di asimmetria informatica, sembra senz'altro coerente e rispondente al sistema di regole e principi di diritto contrattuale ritenere che in linea di principio i rischi rientranti in questa categoria (da individuarsi con maggiore precisione in relazione a specifici tipi di accadimenti e di sacrifici) debbano essere sopportati dalla parte che ha predisposto lo *smart contract*.

A differenza di quanto si potrebbe essere indotti intuitivamente a ritenere, tuttavia, i temi che si riallacciano a questo problema di rischio non si esauriscono tutti sul piano dell'inadempimento (del contraente predisponente) e del risarcimento (in favore del contraente aderente), posto che un errore di scrittura del *software* o malfunzionamenti aventi altre cause (es. interazione con oracoli che trasmettano informazioni false o incomplete) possono comportare effetti sfavorevoli anche per il contraente predisponente (ad es. provocando un pagamento da parte di quest'ultimo, non dovuto ai termini del contratto o di legge), cosicché – proseguendo lungo la linea dell'esempio – si propongono anche temi ascrivibili al piano dell'indebito, dell'ingiustificato arricchimento e dell'indennizzo genericamente inteso, che dovranno essere sviluppati criticamente e con coerenza rispetto alle caratteristiche del fenomeno in questione. Dovranno peraltro in quest'ambito proporsi e affrontarsi in maniera specifica ed adeguata al fenomeno (tenendo a mente le specificità dei linguaggi e delle questioni traduttologiche implicate) anche i temi dell'interpretazione, della traduzione (v. *supra* parr. 10.2. e 10.3.) e dell'integrazione del contratto. Ciò in quanto sembra corretto ritenere che lo *smart contract* deve prevedere o comunque essere scritto considerando non solo quello che le parti si sono dette, o hanno scritto, o hanno altrimenti concordato, secondo un significato ascrivibile al loro contegno negoziale ai sensi delle norme sull'interpretazione del contratto ex art. 1362 ss. c.c. (contenuto di cui, in caso di contestazione, si dovrà verificare l'idoneità ad essere adattato e tradotto in programma per elaboratore, per poi verificare e giudicare il risultato effettivo di tali operazioni) ma anche tutte le regole che vi si applicano per legge e per via di integrazione *ex* art. 1374 c.c. Riteniamo cioè che le repliche artificiali dei contratti propongano specifiche que-

stioni, assai interessanti, sia in tema di traduzione (dalle lingue del linguaggio naturale alle lingue dei linguaggi di programmazione) sia in tema di integrazione del contratto; che individuano altrettante aree di rischiosità ascrivibili alla categorie del rischio dell'esecuzione, nel senso sopra spiegato.

Infine, come si diceva, con l'espressione 'rischio della dichiarazione' si può proporre il problema di stabilire chi debba sopportare (o sopportare definitivamente) le conseguenze sfavorevoli di esecuzioni inaspettate del programma per elaboratore limitatamente alle ipotesi (eccezionali) in cui si possa riscontrare uno *smart contract* che risponde alla seconda nozione (*smart contract* come contratto). In questo caso, come potrà intuirsi, non può stabilirsi *a priori* e in linea di principio chi debba sopportare i rischi ascrivibili a questa categoria, proprio perché il programma per elaboratore è, in questo caso, per definizione, il risultato di una condivisione, ed i temi di approfondimento da svolgere (avendo a mente le particolarità del linguaggio di programmazione) sono pertanto i temi dell'interpretazione del contratto insieme ai collegati temi di traduzione e di integrazione. Ciò in quanto, a fronte di eventuali rimostranze di uno dei contraenti circa i risultati derivanti dall'esecuzione automatica dello *smart contract*, si tratterà di stabilire se tali risultati possano ritenersi o meno inaspettati, ossia, in termini giuridici, se essi rispondano o meno alla «*comune intenzione delle parti*» (art. 1362 c.c.), e al significato da attribuirsi al programma contrattuale, che va ricavato applicando, insieme al canone della comune intenzione, tutti gli altri criteri di interpretazione del contratto previsti dalla legge, nei limiti della compatibilità con la natura e le caratteristiche delle lingue del linguaggio di programmazione di volta in volta prescelte dai contraenti. Le questioni di interpretazione e di traduzione si presenteranno (e vanno affrontate) in modo diverso da come si presentano nelle ipotesi del 'rischio dell'esecuzione', proprio perché, in questo caso, il programma contrattuale dichiarato da entrambe le parti è espresso in un unico e condiviso documento scritto nella lingua del linguaggio informatico da esse prescelta. Naturalmente, in questo contesto, per ricostruire la comune intenzione, verificare il comportamento complessivo delle parti anche precedente alla conclusione del contratto, analizzare il materiale per l'interpretazione e applicare gli altri criteri ermeneutici, a partire da quello della buona fede, si dovrà

fare un percorso a ritroso e, se serve, una traduzione a ritroso, per recuperare, attraverso una prova storica o solo logica, l'ipotetico testo in linguaggio naturale che possa ragionevolmente ritenersi aver costituito la base per l'adattamento (con tutte le inevitabili perdite e le possibili trasformazioni: v. par. 10.3. *supra*) e la traduzione di quanto voluto dalle parti nel programma per elaboratore da esse individuato come testo vincolante. Anche in questo caso, infine, dopo che si sarà – con le particolarità appena riferite – ricostruito in linguaggio naturale il significato del programma contrattuale dichiarato dalle parti, avranno campo le questioni di integrazione del contratto.

11. Financial contracts and "the good algorithm"

Federico Pistelli

11.1. Humanization or mechanization: which path leads to financial inclusion?

In the midst of global financial crisis repercussions, Robert Shiller - Nobel Prize-winning economist – has theorized the pivotal role of finance in building the foundation of the "good society"[1]. In an atmosphere of general distrust towards the soundness and efficiency of financial capitalism, the Author glimpses the potential of financial innovation and information technology as key elements that should characterize an effectively inclusive and democratic system[2]. However, the American economist issues a warning in the last pages of his book, stressing out how the democratization of finance must proceed step by step with its humanizatio: to this end, it is essential for finance "to be human".

This lesson doesn't seem to perfectly fit in the current financial environment.

The automation and application of decision-making processes are

---

1 SHILLER, *Finance and the good society*, Princeton, 2012. The Author provides a description of the good society as the "*kind of society in which we should aspire to live; it is usually understood as an egualitarian society, one in which all people respect and appreciate each other*", SHILLER, cit., p. 1. The references in the book are clearly related to the philosophy of Plato, the social critique of Marx and to the liberal ideologies of Milton Friedman.

2 In the economist's view, "*democratization of finance* [...] *calls for an improvement in the nature and extend of participation in the financial system, including awareness of fundamental information about workings of the system. public needs to have reliable information, and that can only be provided by advisers, legal representatives, and educators who see their role as one of promoting enlightened stewardship*», SHILLER, op. cit., p. 235.

the fulcrum of a system that is mainly driven by machines. For instance, in 2015 66% of global stock exchanges have been managed entirely by robots, i.e. independently of any bidding inputs generated by a human being[3]. In addition, the most recent data show a further increase in the volume of exchanges conducted with automatized trade, which account for around 74% of the notional amount of the trades conducted by institutional intermediaries, with an annual increase of 24% on the use of algorithmic trade systems[4]. The architecture of markets is also experiencing a profound revolution for the advent and spreading of new economic players, such as FinTech companies[5].

At a first glance, those clues allow to predict that a further reliance to the machine will eventually kick out any human being input from the decision-making process.

An example could further clarify the effects of an uncontrolled misalignment of decision-making processes. One of the most serious collapses of the Dow Jones index on the Wall Street stock exchange (by

---

3 The data is reported on various sources, including Carlini, *Incontro ravvicinato con il robo-trader*, in *Il Sole 24 Ore*, 3 January 2016.

4 The data are made up of the researches conducted annually by the American investment bank JP Morgan, *Electronic Trading Survey for 2019*, available at the web address (https://www.jpmorgan.com/solutions/cib/markets/etrading-trends-2019).

5 The Financial Stability Board defines the FinTech process as "*technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material and effect on financial markets and institutions and the provision of financial services* ", Financial Stability Board, *Artificial Intelligence and machine learning in financial services*, 1 November 2017, available at the address (https://www.fsb.org/wp-content/uploads/P011117.pdf). The European Central Bank stresses the difficulties of providing a precise definition of FinTech, considering it as «*an umbrella term encompassing a wide variety of business models*», in European Central Bank, *Guide to Assessments of FinTech Credit Institution License Applications*, September 2017, available at (https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_ inst_licensing.en.pdf). In literature, FinTech is not defined as a new industry, but a new component of the financial industry, Schema, Tanda, Arlotta, Power, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in D'Agostino and Munafò, in *Quaderni FinTech Consob*, 1 March 2018.

more than 9% in a few minutes)[6] has been in fact caused by the interaction between high frequency trade software[7]. A single purchase order of a future contract has produced an uncontrolled reaction of simultaneous and automatized selling/buying inputs from algorithms, determining a deep collapse of assets value (this phenomenon is also known as "hot potato trade")[8].

The frame that has been roughly depicted clearly testifies the inappropriateness of an unconditional and passive reliance in the thaumaturgical effect of a "good algorithm", as a unitary response to a crisis of certainty. On the contrary, a system that primarily aim at promoting the financial inclusion has to acknowledge the fundamental role and interconnectedness of natural intelligence and artificial intelligence, thus contributing to a twilight of the "algorithm-objectivity" idol[9].

This paper will investigate the current role of the algorithm as a response to a generalized crisis of certainty and need for effectivity (§ 2). Then it will examine the various applications of algorithmic decision-making in financial contracts (§ 3) to demonstrate how contract's

---

6 For a particularly critical approach in the reconstruction of the events that led to the episode of the Flash Crash see LEWIS, *Flash Boys. On Wall Street Revolt* , New York, 2014.

7 The High Frequency Trade is defined by the MiFID II, recital 61, 2014/65/EU). In essence, it is a species of algorithmic negotiation, used for the purpose of market making or arbitraging, PERRONE, *Il diritto del mercato dei capitali*, Milano, 2016, p. 272. For a broader and more technical contribution to the phenomenon see, PUORRO, *High Frequency Trading: una panoramica*, in *Questioni di Economia e Finanza. Occasional Paper*, Banca d'Italia, 2013; ALVARO, VENTORUZZO, *"High Frequency Trading": note per una discussion*, in *Banca, Impresa e Società*, 2016, p. 416 ff.

8 The functioning of these systems is well described in ROMANO, *Intelligenza artificiale, decisioni e responsabilità in ambito finanziario: snodi problematici*, in FINOCCHIARO, FALCE, *Fintech: diritto, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019, p. 323.

9 According to the studies conducted with the report on gender discrimination on workplaces made by Johanna Bryson, University of Bath, "*people expected AI to be unbiased; that's just wrong. If the underlying data reflects stereotypes, or if you train AI from human culture, you will find these things*". This study is reported in BURANYI, *Rise of the racist robots - how AI is learning all our worst impulses*, in *the Guardian*, August 2017 (https: //www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses). For a review of the cases of the non-objectivity of algorithms in the various fields of application, see also O'NEIL, *Weapons of Math Destruction. How big data increases inequality and threatens democracy*, New York, 2016, and NOBLE, *Algorithms of oppression*, New York, 2018.

agreement (§ 3.1.), performances (§ 3.2) and execution (§ 3.3.), are getting independent from parties' consent. Finally, the last section is devoted to an analysis of the role of "freedom of contract" principle in light of the expansive capacity of machine learning (§ 4).

11.2. Algorithm decision-making: when math meets law

The algorithm can be essentially defined as a process deputed to solve a practical issue[10]. Its mechanism is articulated in a sub-sequence of basic instructions, which prescribe a finite number of actions or steps to be performed in order to achieve a specific result: in a nutshell, the algorithm "divides a problem into sub-problems, smaller in size and similar to the original"[11]. At a logical level, the codification of an algorithm moves from circumscribing a problem and identifying individual actions that are necessary to obtain a determined solution. Each step of an algorithm presents two essential features: *i*) the *predetermination* of the links that connect each step; *ii*) the *effectivity*, understood as a tension towards a concrete and useful result[12]. Input data are processed through predetermined instructions, to provide an effective response as output. Practically speaking, many actions of every-day life can be described using the language of algorithms[13].

A modern definition of algorithm rose in the context of the late 19th century as a solid ordering instrument to face the consequences of the

---

10 Zellini, La dittatura del calcolo, Milano, 2018; Domingos, The master algorithm, New York, 2015; Pagallo, The laws of robot. Crimes, contracts and torts, New York, 2013; Chopra, White, A legal theory for autonomous artificial intelligence, Michigan, 2011; Wellman, Autonomous Bidding Agent. Strategies and lessons from trading agent competition, New York, 2007.

11 Zellini, *cit.*, p. 29.

12 Post, *Recursively Enumerable Sets of Positive Integers and their Decision Problems*, in *Bulletin of the American Mathematical Society*, 50, 5, 1944.

13 An example of the application of the algorithmic process in everyday life is the preparation of a coffee. The process of making a coffee, which is achieved automatically by the human mind, is susceptible to be broken down into a series of sub-steps. Simplifying and assuming that the process should be implemented by a machine, it could be done in the following way: unscrew the coffin - fill the base with water up to the indicator - insert the filter - fill the filter with ground coffee - screw the two parts together - turn on the stove - place the "Moka" on the stove - wait for the coffee to come out - turn off the stove. Each of these instructions can work as an algorithm, as long as they lead to the concrete result of preparing the coffee, because they are characterized by concrete executability, unambiguousness and finiteness.

upcoming crisis of mathematics theoretical foundations[14]. The need of rationality and objectivity made the algorithm the most suitable instrument to describe and dominate the uncertainty of reality thorough its de-structuring in a mathematical formula. In other words, the algorithm has represented for scientists the key to provide a solution to the infinite sets theory's contradictions.

Given these reasons, it comes with no surprise that the legal reasoning has also been able to grasp the algorithm's value as a mean to face the uncertainty. To this end, legal and math lexicon shows the use of common terms: "certainty"[15] and "effectivity"[16].

It is well known that law, and especially contract regulation, is currently experiencing a moment of profound crisis of general and abstract rules, in favor of a judicial-oriented approach that frequently results in a lack of calculability of the decision. In a same way in which mathematics showed that reality can be expressed thorough formulas, the law aims at repossessing its power of dominating the unforeseeable, by prescribing provisions that guide individual through pre-determined and effective steps. It is therefore not so futuristic to glimpse the first signs of a new era of "coding the contract", understood as a

---

[14] The problem of the foundations of mathematics mainly deals with philosophical and epistemological issues. Under this aspect, mathematics has always played a role of certain science, until the moment in which the philosophical analysis has questioned certain assumptions, often linked to new discoveries (such as, for instance, irrational numbers, infinitesimals, the calculations of infinite series and, the study on infinite sets). The nineteenth century has been defined as the crises of mathematics foundations, because it led to a need for a reassertion of confidence in certain math principles. The end of the nineteenth century has come however characterized as a moment of real revolution in the nature of mathematics and, at the same time, as a phase of great progress of this science, on the belief that the use of logic was the correct procedure for finding of the fundamentals of mathematics. LOLLI, *La questione dei fondamenti tra matematica e filosofia*, in ALBEVERIO, MINAZZI, *Matematica e filosofia*, in *Note di Matematica, Storia, Cultura*, 2006, p. 17-35; ID., *Logica e ragionamento giuridico*, in COMANDÈ, PONZANELLI, *Scienza e diritto nel prisma del diritto comparato*, Bologna, 2004, p. 103-123. SHAPIRO, *Thinking about mathematics: the philosophy of mathematics*, Oxford, 2001; DEDEKIND, *Was sind und was sollen die Zahlen?*, 2018 (reprint 1888), published in Italy by Zanichelli,

[15] IRTI, *Un diritto incalcolabile*, Torino, 2016; DENOZZA, *In viaggio verso un mondo re-incantato? Il crepuscolo della razionalità formale nel diritto neoliberale*, in *Oss. dir. civ. comm.*, 2016, p. 419; NIVARRA, *Dalla crisi all'eclissi: ovvero da un paradigma all'altro*, in *Europa e Dir. Priv.*, 2017, 801. Lopez De Oñate, *La certezza del diritto*, posthumous, ASTUTI, Roma, 1950; WEBER, *Economics and Society*, II, Berkley, 1974.

[16] REICH, *General Principles of EU Civil Law*, Cambridge-Antwerp-Portland, 2014.

normativity expressed in the language of codes[17].

Against this background, the algorithm has been (and still is) a spontaneous response to a need of certainty that affects both law and math. The propositions in which the legal reasoning is structured can be in fact translated into the language of algorithm and into the "if…then" logic: "*da mihi factum, dabo tibi ius*"[18].

11.3. Code is contract

The negotiation of a contractual agreement has been described as the most genuine expression of economic rationality[19].

Theoretically, an action can be defined as "rational" when it's based on a previous calculation of hypothetical, either positive or negative, consequences, aiming at achieving the best and most efficient result. The human behavior in the marked has been for a long time described as "rational" to justify the capitalistic base of the economic system, which requires a legal system to be calculated in a way similar to a machine[20]. Max Weber's theory has been highly criticized by those who relegates the paradigm of the "rational agent" as a relic of the past[21], because it is based on the idea that reality can be traced down through cases and simple causal linkages. This idea wouldn't correspond to a system in which law and regulation are highly affected by the application of principles and general clauses that progressively ate away the dogma of contract agreement' intangibility, opening a wide judicial intervention on the content of parties' agreement.

However, the algorithmic decision-making could give rise to a rethinking of this assumption in which calculation and predictability

---

17 This principle is expressed by the well-known statement "code is law", Reidenberg, *Lex informatica: the formulation of information policy rules through technology*, in *Texas Law Review*, 1997-1998, 76, p. 553; Lessig, *Code and other laws of Cyberspace*, New York, 1999; Brown, Marsden, *Regulating code*, New York, 2013. For a broader perspective, see, Young, Lodge, *Algorithmic Regulation*, Oxford, 2019.

18 Finck, *Blockchain. Regulation and governance in Europe*, Cambridge, 2019, p. 66, according to which: «whereas code is increasingly assuming the function of law, law growingly takes the form of code ".

19 Weber, cit., p. 20.

20 This quote is attributed to Weber, *Economic history: lines of a universal history of the economy and society*, Roma, 1997, p. 298.

21 Irti, *op. cit.*, p. 109.

constitutes fundamental tools of economic rationality. Contracts in financial sector nowadays refuse the logic of the traditional negotiation, in favor of automation, sustainable allocation of resources and decision-making relied on "intelligent" systems, able to balance interests through broad-spectrum data analysis (so-called Big data).

Under this point of view, contracts in financial sector can be a privileged starting point for discussing the intersection between law and artificial intelligence, by analyzing how freedom of contract deals with the cognitive delegation towards machines. To these means, algorithms are instrument for governing the complexity of reality, by affecting each phase of the negotiation among parties.

11.3.1. Agreement

The impact of algorithmic decision-making can be appreciated from the very beginning of the negotiation, when parties have to reach an agreement. The pre-contractual phase is in fact broadly delegated to the algorithm, with a view of sparing the costs of negotiation and filling the information gap among the parties.

Amongst various applications, the advent of algorithms has radically changed the decision-making process of concluding credit agreements. The collection of data from multiple sources and their combination with information on an aggregate level provides a more accurate evaluation on the probability of default of the debtor and, consequently, an optimal allocation of surplus resources. In particular, such algorithms implement bank’s systems to assess the creditworthiness of debtors, in order to grade the capacity of the counterparty to bear the financial burden of the contract by regularly fulfilling the performance due [22]. Every potential contractor is thus involved in a pro-

[22] The first applications of these techniques took place through the model developed by the American thematic Earl Isaac and the engineer William Fair, named FICO (Fair Isaac Corporation), and aimed at quantifying the risk of default of the loan applicant. This model was introduced towards the end of the 1980s and is based almost exclusively on the debtor's credit history, therefore only take into account the fulfillment of debtor’s previous obligations and the use of credit cards. The model therefore has the advantage of transparency of the algorithm on which is based, explaining the methods through which the debtor can increase his/her credit access score. Likewise, the main limitation of the model is that is taking into consideration

filing activity, aimed at processing data related to his personal and financial sphere, for the purpose of deciding whether or not he/she meets the requirements for access to credit. Furthermore, the application of these models is becoming more complex due to the interaction between individual information and big data. Any information regarding the life of the individual is potentially capable of provide insights on his aptitude and ability to fulfill his obligation [23]: the web pages visited on search engines, the geo-localization of the user, the activities shared on social networks allow the software to process aggregate data, to learn from their comparison and give a result in term of counterparty's reliability[24].

A further step has been achieved through the use of scoring algorithms on the lending crowdfunding platforms[25]. The algorithm that governs the platform is in fact able to independently conduct the assessment of creditworthiness by accessing the information stored in the database and to assign each potential contractor to a specific risk class. Through this process, the parties are therefore able to conclude a perfectly valid loan agreement, while completely ignoring the identity and characteristics of the counterparty, on the mere basis of the matching operated by the algorithm.

11.3.2. Performances

The parties, especially in complex and structured agreements, are

only information related to previous financial experience, which might cause a discrimination of requests that come from startups. O'Neil, *cit.*, p. 142.

23 This process of transformation of credit scoring is fueled by start-ups which make use of machine learning and data cross-checking techniques, in order to obtain information on creditworthiness of the money takers (according to the famous motto of Douglas Merrill, founder of ZestFinance, "all data is credit data").

24 The problem of the cd. Black Box in the context of the algorithmic decision was summarized by Stuart Russel, theorist of artificial intelligence, in these terms: "*so, if I'm not mistaken, most, if not all of these deep learning approaches, or even more generally machine learning approaches are, essentially black boxes, in which you can't really inspect how the algorithm is accomplishing what it is accomplishing*".

25 Hacker, Lianos, Dimitropulos, Eich, Abramowicz, *Regulating Blockchain*: *techno-social and legal challenges*, Oxford, 2019; Alscher, Kolbeaker, *Ist Deutschlands Mittelstand bereit für FinTech und Online-Kredite? Eine Akzeptanzanalyse zu Peer-to-Business Lending für deutsche KMU*, in *ZBB/JBB*, 2018, 1, p. 43; Zwach, *Peer-to-Peer-Geschäftsmodelle zur Absicherung privater Risiken Eine Exploration am Beispiel Wildschaden*, Munich, 2016.

not always able to grasp in the detail the extent and the content of each other's performances. Their intentions are often based on general objectives that need to be translated into concrete contracts terms to form reciprocal obligations.

In this sense, the algorithmic decision-making plays an essential role to give shape and concreteness to the specific terms of the contract. This phenomenon is framed by international doctrine in the purely descriptive category of "self-driving contracts" or "smart contracts"[26]: once the parties have agreed on the general objectives that supported the impulse to the negotiation, «they can rely on the machine to set all other terms of performance»[27]. The coding of an algorithm allows the parties to overcome the obstacle of quantifying the performances by incorporating general instructions to generate a wide range of obligations, the content of which varies according to the specific contingencies existing at the time of its implementation.

These algorithmic decision techniques have a broad application in the context of InsurTech[28] and currently stands as the engine of a real revolution in pricing and in assessing risk of insurance contracts.

---

[26] On self-driving and smart contract, CASEY NIBLETT, *Self-Driving contracts*, 2017, available on SSRN: https://ssrn.com/abstract = 2927459; ID., *Death of Rules and Standards*, in *Indiana Law Journal*, 2017, 92, p. 4; RASKIN, *The law and legality of smart contracts*, in *L. Tech. Rev*., 2017, p. 305. The first definition of smart contract is traditionally attributed to SZABO, *Smart contract: building blocks for digital markets*, 1996 (accessible at http://www.fon.hum.uva.nl/ rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html), which identifies the smart contract in "*a set of promises, specified in digital form, including protocols within which the parties perform on these promises* ". According to someone «*artefacts are neither smart not contracts. Smart contracts are not smart in the AI sense, as they are unable to understand natural language (such as contractual terms) or to independently verify whether an execution-relevant event occurred […] Smart contracts also cannot be qualified as contracts in the legal sense […] As such, these technical artefacts are better defined as an autonomously executing piece of code whose inputs and outputs can include money* ", FINCK, cit., p. 24-25.

[27] CASEY NIBLETT, cit., p. 105.

[28] The Financial Stability Board simply defines the InsurTech phenomenon as an application of FinTech to the insurance sector (see FINANCIAL STABILITY BOARD, *Artificial intelligence and machine learning in financial services. Market developments and financial stability implications*, 1 November 2017). See also, NICOLETTI, *Future of FinTech Integrating Finance and Technology in Financial Services*, London, 2017; ID., *Digital Insurance: Business Innovation in the Post-Crisis Era*, London, 2014; MCFALL, MOOR, *Who, or what, is insurtech personalizing?: persons, prices and the historical classifications of risk*, in Journal of Social, 2018, 19, 2, p. 193.

The predictive analysis and the actuarial techniques are the main criteria used by insurance companies to classify risks and to calculate the corresponding value of policies and insurance premia in relation to the probabilistic impact of certain factors on the life of the individual (risks of accidents, injuries, p act of environmental actions). However, these analyses usually refer to large-scale aggregate data. The application of algorithmic process to the aforementioned phenomenon allows instead to design the concrete content of the policy on the specific profile of each customer (so-called "personalized policy"). The receptive capacity of the algorithm with respect to input data translates the general objectives of the guaranteed in micro-directives imparted to the machine, to determine the cost of the policy depending on a steadily risk monitoring.

For instance, these techniques are currently experiencing a widespread in the context of the digital health insurance. These contracts make use of devices and activity trackers able to capture data relating to health and physical activities of the insured person in order to automatically translate that information in contractual terms, to directly affect the price, renewal and content of performances[29]. The constant monitoring of vital functions produced two fundamental consequences. On the one hand, it fills the information gap existing between the insurer and the insured. On the other hand, it allows a constant updating of the policy price in relation to the reclassification of insured risk, on a customer-based approach.

11.3.3. Execution

Undoubtedly, the most frequent and widespread application of the algorithmic decision-making is related to contract execution[30]. Once

---

[29] The application of similar techniques is also widely used in the Motor TPL insurance sector, through the installation on the vehicle of a black box ("Black Box"), capable of monitor driving activity, taking into account habits, techniques and conduct by the driver, in order to reshape the policy premium, as a result of conduct aimed at avoiding risks in circulation.

[30] European Securities and Markets Authority, *Final Report*, 19 December 2014, ESMA/2014/1569: «*Algorithmic trading refers not only to the generation of orders but also to the optimization of order-execution processes by automated means once the buy-and-sell decisions have been made by automated means or not. algorithmic trading may still take place when the trading decision has been made by a person*".

the parties (or the machines) agreed on the contractual terms and obligations, the artificial intelligence also plays a fundamental role in the definition of methods, times, and techniques for the execution of contractual agreement. The main features of such use of algorithm is the wide range of machine's autonomous choices and the absence of any human intervention for the fulfillment of reciprocal obligations. On the purely basis of software programming, the algorithm is then able to process determinate inputs from external environment - "if something happen... " (e.g. the price of a share goes above a certain threshold), to produce a certain result in terms of parties obligations - "… then buy or sell" (e.g. buy 100 shares at that price). It is however worth pointing out that the application of algorithmic techniques to contract execution doesn't make the machine a mere tool for the purposes of human parties because the software is designed to have a wide decision-making discretion[31].

Evidence from the process of cognitive delegation to the machine

[31] An American doctrine of the early 1970s has introduced a well-known distinction among goods. This study has been focused on a first line distinction between ordinary goods, search goods and experience goods, depending on the different impact that information produces on consumer evaluation of qualities and characteristics of a good. As regards ordinary good, the price discloses sufficient information for the consumer on its quality and efficiency. This means that the consumer is perfectly capable to evaluate whether or not that good is suitable for him. The substantial difference that exists between the other categories lies on the availability of information before the purchase: in fact, there are products for which a simple search an comparison is sufficient to guide the consumer's choice, while for others the quality and efficiency can be tested only after their purchase (experience goods). In addition to that, further doctrine has introduced another type of goods for which, not even after the consumption is sufficient to fully assess product's quality and suitability to satisfy the interest of those who buy it. In this regard, the literature has defined "credence goods" products for which the provider "knows more about the type of good or service the consumer needs, than the consumer himself ". The main feature of this type of goods is that the consumer owns a specific need but is not aware of the most appropriate means for the satisfaction of his/her interest. In this context, the complete information on the price, on the structure and on the characteristics of the product may not be sufficient to make a conscious evaluation, thus making itself necessary to trust the evaluation of an expert who knows how to avoid undertreatment or overtreatment of the consumer's need. For a framework on the subject, DULLECK, KERSCHBAMER, SUTTER, Economics of Credence Goods: An Experiment on the Role of Liability, Verifiability, Reputation, and Competition, in American Economic Review, 2011, 101, p. 530.

can be found in the field of algorithmic trade[32]. In this context, technological innovation has produced a large impact on investing and trading in financial market, resulting in a large-scale use of algorithms in managing investment orders on the markets. The use of algorithms allows traders to pursue complex purchase and sale strategies through the analysis of an enormous amount of information on prices and volumes of transactions and to promptly re-set those strategies taking into account any change in market conditions.

The application of these mechanisms has experienced some intermediate step to evolve into the current shape. The earliest forms of trading thorough computer have been regulated by the supervisory authority on financial market already in the early 2000s, framing this phenomenon as a peculiar executive mode, not as a new investment service. According to a Consob opinion, trading machines are designed exclusively as a tool for transmitting the impulse to negotiation, because they cannot operate without an input that comes from a human being[33]. Over time and due to a progressive improvement of automation processes, the financial markets have however experienced a broader use of high-frequency trading systems, supported by some new provisions at European level which have favored its development (e.g. the removal of the obligation to centralized stock exchanges on regulated markets, the introduction of the best execution rule).

The process was then led to its most extreme consequences at the time in which the contract execution has been entirely subtracted from party's input, to become the mere outcome of a "dialogue" between machines. The step emerges from a well-known opinion from ESMA [34], that describes the complete automation as a structural element of algo-trade. To this extent, algorithmic trade is defined as a system that

---

[32] On this phenomenon, Mattli, *Global algorithmic Capital Markets: High Frequency Trading, Dark Pools, and Regulatory Challenges*, Oxford, 2018; Bush, *MiFID II: regulating high frequency trading, other forms of algorithmic trading and direct electronic market access*, in *Law and Financial Markets Review,* 2016, 10, II, p. 72.

[33] Ref. Consob, 21 April 2000, n. D/I 30396 on Online Trading and Rules of conduct (http://www.consob.it/documents/46180/46181/30396.pdf/0015 ff03-1 a- eb-4220-af22-9635feb4eade).

[34] European Securities and Markets Authority, Final Report, 19 December 2014, ESMA/2014/1569 (https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1569_final_report_-_esmas_technical_advice_to_the_commission_on_mifid_ii_and_mifir.pdf).

presents a complete decision-making autonomy in every phase of the negotiation, from sending, to transmitting and executing an investment order. In addition, EU delegated regulation have further identified the distinctive feature of the High Frequency Trade with respect to any other form of interaction between law and technology in the full ability of this mechanism to operate in absence of any human intervention[35].

11.4. Algorithm against contractual freedom: the risk of a "reverse engineering"

The various applications of algorithmic decision-making that have been taken into account in the paragraphs above highlight the fil-rouge of machines that, far from being mere tool for transmitting human's will, are living part in the formation of contractual consent. However, despite the fact that artificial intelligence intervenes in several phases of the negotiation process, it is worth pointing out that machines still operate in response of impulses to negotiation related to human being wiliness[36].

This assumption might suggest a further question: how the aforementioned scenario is likely to vary in light of an expansion of the learning component of machines, also known as "Machine learning"?[37].

---

35 Ref. EU Delegated Regulation 2017/589, 19 July 2016, European Commission, to integrate of Directive 2014/65 / EU, on regulatory technical standards to specify the requisites is the organizational structure of the investment firms that carry out the algorithmic trading, according to which "Investment decision algorithms make automated trading decisions determining which financial instruments to buy or sell. Optimized order execution algorithms manage the order execution process through the automated generation and transmission of orders or quotes to one or more trading venues once the investment decision is made was taken. Among the trading algorithms it is appropriate to distinguish the decision algorithms on investments by execution algorithms, given their respective potential impact on operation correct and orderly markets' (recital 5).

36 "*As everywhere, code is simply a human tool, used to express the objectives and beliefs of those who operate it.* [...] *Yet those trusting the system in question don't, ultimately, trust numbers and mathematics but, rather, the humans behind them* ", v. FINCK, cit., p. 182.

37 ALPAYDIN, *Machine learning*, New York, 2016; BALDI, BRUNAK, BACH, *Bioinformatics: the machine learning approach*, London, 2001; SUTTON, BARTO, *Reinforcement learning: an introduction*, London, 1998.

More and more frequently the sub-sequence of actions followed by the machine to solve a practical problem – according the definition of "algorithm" sub § 2. – not only works perfectly without any human intervention, but it is also able to learn from interactions with other algorithms. It is in fact defined as "deep learning" the phenomenon of communication and coexistence of algorithms on several levels, capable of create real neural structures of artificial neural networks and therefore able to formulate abstract concepts starting from experiential data. Though deep learning, the system is thus capable of making predictions on potential interests of the human being, as well as to act directly to adapt negotiating scheme that, from time to time, better achieve a synthesis between them.

This mechanism hides a subtle threat that deep learning, pushed to its maximum extremes, can invert the traceability of interests, making man a tool of the machine. Further arguments can be drawn along these lines.

Each kind of commercial transaction implies an interaction between human activity and artificial intelligence on a two-layered level. On the first layer, the user asks the machine to detect the good or the service that best suits him/her. On the side layer, the user discloses to the machine a parallel flow of information regarding his/her personal sphere, specific needs and preferences. On closer inspection, even the absence of any interaction with a machine is, for this very reason, source of an enormous amount of data on the needs and preferences of a person. If this is true, the use of the algorithmic process, combined with predictive and learning techniques, might facilitate the overturning in interest's traceability, allowing intelligence artificial to predict and, consequently, influence the hypothetical interest of the contractor. Following this argument, the product or service would suit not an actual and concrete interest of the individual, but a hypothetical interest that is obtained on the basis of predictive calculation, combining historical and experiential individual data with aggregate information. How much would be therefore easy in this regard, to draw a boundary line between machine interest (or better software provider interest) and human interest?

Along these lines, the algorithmic decision process has only a facade of an inclusion-oriented tool. On the one hand, the "good algo-

rithm" still needs a robust regulatory framework for contractual liability, data sharing and treatment[38]. On the other hand, the human being autonomy should not blindly rely on algorithm objectivity to achieve its goals.

As a matter of fact, the algorithm consists of a problem-solving process, capable of putting into discussion the antithesis between determinism and free will[39] and transmitting the appearance of man being able to dominate the infinite and reality. However, the algorithm still remains, in the end, a tool to which the human being must attribute a value. In fact, no algorithm is able to replace the importance of financial education, the value of risk management and the constitutional protection of savings. By reverse engineering this argument, it would be more accurate to discuss a mechanization of human willingness rather than a humanization of algorithms and finance.

---

38 An interesting perspective emerges from GOODMAN, FLAXMAN, *European Union regulations on algorithmic decision-making and a "right to explanation"*, in *AI Magazine Cornell University*, 38, 3, 2017.

39 GONSETH, *Déterminisme et libre arbitre*, Paris, 1947.

12. **The evolution of U.S. proxy voting: may blockchain help us out?**

Eugenio Prosperi

As M. Khan and E. Rock noted in an article dated 2007, "*Never has voting been more important in corporate law*".[1]

The proxy season from February to June 2019 saw 468 billion shares processed and voted in connection with 4,216 shareholders' meetings.[2] Those figures testify the huge amounts of votes cast by shareholders through proxies, the presently used voting system. Notwithstanding the significant role played by shareholders' voting in nowadays corporations, inaccuracies and concerns regarding the voting mechanism still exist.[3] Shareholders' contests often ended up with results showing tight margins, which made it difficult to ascertain to what extent the calculations were accurate. Similar problems occurred with respect to the votes' tabulation phase, where an entity is entrusted to double-check the results obtained with the calculations.[4]

---

1 Marcel Kahan & Edward B. Rock, *The Hanging Chads of Corporate Voting*, 96 Geo. L. J. 1227 (2008), at 1229. This milestone paper profusely addressed the problems arising out of corporate elections, including inexact voter lists, incomplete distribution of ballots, and chaotic vote tabulation.

2 BROADRIDGE, 2019 Proxy Season Key Statistics and Performance Rating, https://www.broadridge.com/_assets/pdf/broadridge-proxy-season-stats-final.pdf.

3 In *Re Appraisal of Dell Inc.*, Opinion No. C.A. 9322-VCL, 2016 (Del. Ch. May 11, 2016), in which T. Rowe (shareholder) instructed Institutional Shareholder Services to vote against the Dell merger but, because of an error made in the chain of intermediaries in proxy voting, his vote was cast in favor of the merger. As a result, T. Rowe was not able to benefit from the fair price ruling in the appraisal procedure.

4 Todd. S. Purdum, *Counting the Vote: the Overview; Bush is Declared Winner in Florida, but Gore Vows to Contest Results*, N.Y. Times, November 27, 2000, at A1, available at https://www.nytimes.com/2000/11/27/us/counting-vote-overview-bush-declared-

Meanwhile, blockchain technology has taken hold across different fields by showing its versatility and problem-solving capacity. Entrepreneurs have been looking at blockchain as both a cost-saving tool – getting rid of all the third parties needed to connect a company to a certain service – and a structure through which data quality may be guaranteed.

The abovementioned issues have given rise to the following main queries: to what extent can we still rely on the proxy voting system? Would blockchain technology represent the straightforward solution to address the current voting system's issues?

This paper aims at providing a response to those queries by endorsing the application of the blockchain technology to the voting, tabulation and clearing phases of the shareholders' voting process.

12.1. Blockchain Technology

Blockchain technology is to be credited to Haber and Stornetta, who in 1991 first suggested the implementation of the blockchain technology for time-stamping digital documents in the intellectual property field.[5] In their view, this new tool, aimed at certifying data contained in digital form documents, would make documents' backdating and forward-dating infeasible. Haber and Stornetta's model aimed to ensure the authenticity of each stamp by means of cryptographically secured collision-free hash functions.[6] Hash cryptography can turn data into a hexadecimal fixed-length code that cannot be changed to recover the original *input*.[7] This scheme enabled turning each entry in their sequence into a hash code, which would then be

winner-florida-but-gore-vows-contest.html. Although it occurred in a political election, it is worth noting how the 2000 presidential election Florida showed the ostensible limits of the punch card ballot machines, unable to figure out who the winner of the contest was.

5 Stuart Haber & Scott W. Stornetta S., *How to Time-Stamp a Digital Document*, Journal of Cryptology, 99-111 (1991).

6 *Id*., at 107.

7 For a broad understanding of the concept of cryptography see Chris Burniske & Jack Tatar, *Cryptoassets. The Innovative Investor's Guide to Bitcoin and Beyond*, (2017), where cryptography is defined as "the science of secure communication. It involves taking information and scrambling it in such a way that only the intended recipient can understand and use that information for its intended purpose."

combined with the raw data for the next entry and turned into another hash code, ad infinitum.

Yet unknown Satoshi Nakamoto, in his paper dated 2008, conceived the blockchain technology as a way of validating the new developed bitcoin currency. Currently, the bitcoin blockchain is probably the most known, and has specific features. In particular, as a distributed ledger, computers can access the bitcoin's blockchain without being subject to any kind of restriction.[8] Each transaction recorded in the blockchain must be cryptographically validated to demonstrate that people actually own the bitcoin they are trying to sell. Cryptography still involves adding new transactions, *rectius* blocks of transactions, to the blockchain by ensuring an automated system of mathematical trust.

Once the block has added to the blockchain by globally distributed computers, it becomes unmodifiable, giving rise to an immutable database.[9] What determines the addition of a new block to the chain is the Proof-of-Work (PoW) that works as consensus protocol.[10] Such a concept explains the functioning of the blockchain and blends together its other attributes: cryptography, immutability and distribution. The PoW addresses the question as to how blocks are chained together to form the blockchain.

Nakamoto's blockchain model presents the following four main

---

8 The bitcoins' blockchain designed by Nakamoto is public – i.e., everybody has access to the chain by adding new blocks, as opposed to the private blockchain. The latter, instead, is overseen by a trusted third party that can prevent users from accessing, impose fees, and/or limit users' access to data.

9 Marco Iansiti & K. Lakhani, *The truth about blockchain*. Harv. Bus. Rev. 95, no. 1, Jan-Feb. 2017, at 118–127, available at https://hbr.org/2017/01/the-truth-about-blockchain. Computers can add blocks in an *append only* fashion: the information can only be added without any possibility to delete it. Moreover, no central entity is empowered with altering the ledger, which could be modified only through consensus.

10 Still, an alternative to the proof-of-work protocol is the proof-of-stake protocol utilized by other cryptocurrencies. In the proof-of-stake system, the creator of a new block of transactions is chosen by an algorithm based on the total wealth of each network participant, i.e. their stake. In addition, unlike the proof-of-work protocol, the proof-of-stake enables for validation of transactions without relying on massive amounts of energy currently utilized through the proof-of-work process. See EOS.IO, *Technical White Paper*, (March 16, 2018), available at https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

features.

Decentralization: Its system is decentralized, meaning that transactions should not be validated through a central trusted agency (a third-party entity). Conversely, consensus algorithms in blockchain allow data to maintain their consistency in distributed networks.

Anonymity: Each user interacts with the blockchain anonymously, by using a generated address which does not disclose his/her real identity.

Persistency: Transactions on the blockchain can be quickly validated, and invalid transactions would not be admitted by honest miners. Blocks that contain invalid transactions could be discovered immediately.

Accountability: Any transaction should refer to some previous unspent transactions. Once the current transaction has been recorded in the blockchain, the state of those referred unspent transactions switch from *unspent* to *spent*. Therefore, transactions could be easily verified and tracked into the blockchain.

12.2. Typologies of blockchains

Although Nakamoto's blockchain model has been featured with public openness, other kinds of blockchain structures have been developed, known as private blockchains and permissioned blockchains. In private blockchains viewing, access is restricted to a designated list of approved users, and transactions can only occur through interfaces offered by the operator. Instead, in permissioned blockchains the power to add blocks to the blockchain is limited to a set of known entities that control the access by end-users.

As we noted, bitcoin blockchain is a public, permission-less blockchain. Still, its predicates are not mandatory for a blockchain structure to exist. For instance, in the context of clearing and settlement of securities, private and permissioned blockchains may offer several advantages as a blockchain design, varying either the levels of access to network participants or the permissions to write blocks to the blockchain.

12.3. The Voting Mechanism

12.3.1. The Proxy System

Since the enactment of the Securities & Exchange Act of 1934 (the Act), proxy mechanisms have been considered the only viable means to face the increasingly high volumes of traded shares. Thanks to a system of proxies, shareholders can delegate their voting power to an agent after receiving requests for voting instructions from the issuer.[11]

The Act requires that all shares held in "street name" be immobilized in a central depository, the Depository Trust and Clearing Corporation (DTCC),[12] which tracks who owns the securities.[13] The street-name system entails that securities bear the names of the financial intermediaries (record holders) that hold the securities on behalf of their clients, the beneficial owners of the shares themselves.[14] Given this fungible bulk system, the DTCC does not deal with the precise allocation of the traded shares among the individual shareholders (beneficial owners); instead, are the financial intermediaries tasked with discerning how to allot the shares they hold on behalf of their clients.

Record holders should cast votes according to beneficial owners' instructions. Indeed, the voting powers always rely on the record hold-

---

11 Once received all the voting materials from the issuer (proxy cards, proxy statement, annual report), record holders have five days to forward those materials to beneficial owners. Custodians frequently entrust Broadridge, the most prominent company in the investor communications sector, to deal with the whole proxy process – i.e., Broadridge receives the voting instructions, verifies receipt, ascertains that signatories hold voting power, signs the proxy on behalf of its clients (banks or brokers), and sends the collected proxies to the tabulator.

12 Khan and Rock, *supra* note 1, at 1237, where the authors point out that, prior to the adoption of the immobilization approach, shareholders used to hold share certificates registered with the issuer and transferred by the transfer agent upon delivery of the post-sale certificate.

13 Currently, most traded shares are held in street name by both financial intermediaries and broker-dealers. The other way to own shares is the direct ownership, where the record (registered) holders own the shares directly with the company.

14 Article 8 of the Uniform Commercial Code provides that the holder of the shares in "street name" has a "security entitlement" in a "financial asset", meaning that the shareholder legally owns only a pro-rata interest in a fungible bulk of securities held by the intermediary, and, consequently, holds only a pro-rata claim against the intermediary's holdings.

ers at the record date. As just noted, the shareholder-paradigm considered for the general corporate ownership structure does not apply to corporate voting: here those who are entitled to vote are not the actual shareholders.

The described burdensome voting system involving several layers of entities in between the beneficial owner and the issuer undoubtedly needs improving. That infrastructure creates higher costs to be borne by issuers' shareholders and contributes to obfuscating the ownership of real shareholders.

In light of these issues, as of 2018, Broadridge Financial Solutions has taken some steps forward by starting to use blockchain to revolutionize the way proxy votes are distributed, managed and tabulated. The Broadridge project is aimed at streamlining the process by generating an immutable share record of all the voting activity. As Broadridge representatives stated, "for the first time it is possible to conduct real time proxy voting reconciliation, to improve record-keeping, efficiency and cost-savings".[15]

The Broadridge system may be summed up as follows: the issuer imports meeting information – including but not limited to agenda items and event details – onto a distributed ledger. Meanwhile, the issuer defines specific rules related to the meeting which constitute the smart contract (the computer protocol that contains the process and logic for the shareholders' meeting). Only those shareholders entitled to vote as at the record date can use Broadridge Proxy Systems to cast their votes onto the distributed ledger. Each time a vote is imported onto the ledger, it creates cryptographically signed blocks, since each block is an immutable record in the chain. The blockchain architecture developed by Broadridge is also committed to ensuring data privacy and security, through the following procedure: 1) the smart contract manages data access based on ownership and assigned privileges; and 2) the distributed ledger ensures vote integrity: the blockchain is supposed to be tamper-proof.

Broadridge cutting-edge project has so far proved to be efficient.

---

[15] See Broadridge, *How Blockchain Transforms Proxy Voting*, available at https://www.broadridge.com/video/how-blockchain-transforms-proxy-voting.

Due to the presence of a unique immutable record-keeping system including information on the issuer components, entitlements to shareholders, and the actual voting record, there is no need to reconcile multiple databases or systems.[16]

12.3.2. The Calculation of Ballots

Both in political and corporate contexts, operators have always struggled to calculate ballots exactly – there are some practices that make votes' calculation even more troubling.

First, empty voting renders the ballots' calculation cumbersome. This is when "*an investor uses borrowed shares or certain combinations of derivative securities to acquire voting rights temporarily, without economic exposure to the cash flow rights connected to a share*."[17]

Even though the legitimacy of this practice is not at issue, its acceptance among market operators is still unclear. Its endorsers highlight that (i) it effectively enables pricing voting rights according to the marginal benefits attributed to the highest-valued voter; and (ii) it provides minority shareholders with an opportunity to maximize their profits by selling or temporarily renting their voting rights.

On the other side, empty voting may be rather undemocratic, leading to an extreme separation of ownership and voting rights, to the detriment of the real shareholders attempting to benefit from such a practice.[18] That happens when minority shareholders' interests are at odds with those of the majority and control shareholders. Indeed, selling or renting their voting rights to the controlling shareholders may result in the unconscious support and approval of a resolution not in line with their interest.

To sum up, establishing whether the empty voting practice is acceptable relies on what level of shareholder participation in corporate governance one deems appropriate.

---

[16] *Id*., available at https://www.broadridge.com/video/how-blockchain-transforms-proxy-voting.

[17] David Yermack, *Corporate Governance and Blockchains*, 21 Rev. Fin. 1, 2017, https://academic.oup.com/rof/article/21/1/7/2888422, at 24.

[18] *Id*. at 24.

12.3.3. Tabulation Systems

The tabulation of the votes stands at the end of the voting process. The tabulator – almost always Broadridge – is tasked with double-checking the voting outcomes. In particular, tabulators' tasks encompass verifying the validity of the collected proxies and focusing on whether the number of nominee shares voted corresponds to the number of shares the DTCC reports to be held by that precise nominee.

The work undertaken by tabulation service firms is extremely delicate, especially in relation to tight corporate contests. Moreover, those firms are often required to carry out their work in a narrow window of time, making the counting of ballots even more complex than expected.

Broadridge, acting as a de facto monopolist, has experienced more than one misattribution of votes so far, failing to include millions of votes in the final counting.[19] Those misattributions led to votes' recounts, eventually determining a more precise result.

What described newly testifies the inadequacy of the current voting system encompassing too many layers of players at each phase. As a result, besides massive human involvement, it is likely that voting results will eventually be inaccurate. Perhaps, tabulation is the most evident trait of inaccuracy and no-reliability of the old-fashioned proxy system.[20]

12.3.4. Clearing Process

In applying the blockchain technology to securities clearing and settlement systems, several factors must be considered, including settlement speeds, integration (delivery-versus-payment), security (resilience to hacking or other kinds of misbehaviors), operational resilience (avoiding operational failures), and the impact on costs required to run

---

19 Yi-Wyn Yen, Yahoo Recount Shows Large Protest: Yang's Approval At 66 Not 85 Percent, HUFFINGTON POST Aug. 6, 2008, available at https://www.huffpost.com/entry/yahoo-recount-shows-large_n_117195.

20 Kahan and Rock, *supra* note 1, at 1279. See also, Center on Executives Compensation, *A Call for Change in the Proxy Advisory Industry* Status Quo, at 50-61 (White Paper c11-07b, January 2011), available at https://online.wsj.com/public/resources/documents/ProxyAdvisoryWhitePaper02072011.pdf.

the system.

Currently, the DTCC and the National Securities Clearing Corporation are capable of processing 300 million shares per second over the peak trading period, often at the expense of the time of settlement. The average time to settle for most of the transactions amounts to two days as of the transaction date (T+2).[21] Notwithstanding the improved time of settlement, the DTCC has estimated that the current settlement period compels system participants to detain an average of USD 5 billion collectively in risk margin, to manage counterparty default risk.[22]

The introduction of the blockchain technology in this phase would improve the already developed ongoing system.[23]

First, introducing blockchain in this process would enable for real-time settlement, aimed at ensuring swifter times of settlement, reducing counterparty risk, freeing up capital, and making the financial system more dynamic, automated, and resilient.

On the other hand, blockchain could enhance assets ownership's transparency and verification, by reducing operational costs of trade.[24] Last, the distributed nature of blockchain would contribute to mitigating the single-point-of-failure problems experienced by centralized

---

21 See George S. Geis, *Traceable Shares and Corporate Law*, 113 NW. U. L. REV. 227 (2018); Spencer J. Nord, *Blockchain Plumbing: a Potential Solution For Shareholder Voting?*, 21 J. Bus. L. 706 (2019), available at https://scholarship.law.upenn.edu/jbl/vol21/iss3/4/. Data report the T+5 standard was applicable until 1995 the, and the T+3 standard from 1995 to 2017, respectively.

22 See DTCC, *Modernizing the US Equity Markets Post-Trade Infrastructure A White Paper to the Industry, DTCC,* (January 2018), available at http://perspectives.dtcc.com/assets/img/equities-structure-whitepaper-jan2018-(1).pdf.

23 In 2017, DTCC announced a pilot project with IBM to clear and settle credit derivatives through a customized distributed ledger system. See Michael del Castillo, *$11 Trillion Bet: DTCC to Process Derivatives with Blockchain Tech* (January 9, 2017, 12:59 pm), available at http://www.coindesk.com/11-trillion-betdtcc-clear-derivatives-blockchain-tech/.

24 See Anquan, Deloitte, MAS, Nasdaq, and SGX, *Delivery versus Payment on Distributed Ledger Technologies* (November 11, 2018, 5pm), available at https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-DvP-on-Distributed-Ledger-Technologies.pdf. See Anquan, Deloitte, MAS, Nasdaq, and SGX, *Delivery versus Payment on Distributed Ledger Technologies* (November 11, 2018, 5pm), available at https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-DvP-on-Distributed-Ledger-Technologies.pdf.

systems.

Unlike Nakamoto's model, featured with decentralization and no need for counterparties to trust each other, with respect to the clearing and settlement, blockchain would improve the speed and efficiency of the settlement process.

As intermediaries often slow down or endanger the settlement process, a private permissioned blockchain, rather than a public one, would better fit this process, enabling for appropriate balance among the benefits provided by the distributed nature of the blockchain, meanwhile assuring that transactions could be added to the blockchain only by known, entrusted entities.[25] Therefore, the permissioned feature of the blockchain would avoid the need for proof-of-work validation or any other inefficient consensus protocol.[26]

However, the main concerns arising from the application of private permissioned blockchain to clearing and settlement are (i) delivery versus payment, and (ii) immutability.

According to the delivery-versus-payment settlement procedure (DvP), the buyer must carry out the payment for securities when the latter are delivered by the seller. In order for securities to be transferred on a blockchain, while ensuring that cash payments are made simultaneously, both the securities and cash legs of a transaction need to be validated by the network. Accordingly, either of them should be on the same blockchain system, such that transactions can account for

---

25 The most appropriate blockchain design would encompass a private permissioned blockchain with the permissioned parties (nodes) consisting of a known consortium of financial institutions. These institutions, tasked with validating the securities transactions, would be highly motivated to ensure that the integrity of the blockchain is not compromised. Moreover, reputational concerns for each financial institution and the threat of legal liability would also ensure that only valid transactions are verified and manipulation of the blockchain is avoided.

26 This way blockchain would be able to handle the high volumes of transactions inherent in securities markets. See DTCC, *DTCC Announces Study Results Demonstrating that DLT Can Support Trading Volumes in the US Equity Markets, DTCC Press Release,* (October 16, 2018), available at http://www.dtcc.com/news/2018/october/16/dtcc-unveils-groundbreaking-study-on-dlt.

both simultaneously.[27] This goal may be undertaken through digitalization and tokenization of the currency used for payment, such as through *stablecoins*.[28] In such a way, the transaction written in the block would consist of both transfers which would lead to real-time settlements of the securities leg.[29]

The Bank of Canada, the Toronto Stock Exchange operator TMX Group and the non-profit organization Payments Canada have recently developed an integrated securities and payment settlement proving that blockchain technology could be used for automating instantaneous securities settlements. This settlement structure provides that cash and assets be tokenized to complete an instant settlement. Despite the creation of this model, some representatives of the concerned entities have been skeptical as to whether the implementation of blockchain to the securities clearing and settlement would lead to cost savings.[30]

The European Central Bank (ECB) raised analogous concerns on the speed and costs of blockchain's implementation. In particular, the ECB suggested that the objectives achieved through the blockchain

---

27 See Andrea Pinna & Weibe Ruttenberg, *Distributed Ledger Technologies in Securities Post-Trading: Revolution or evolution?*, ECB Occasional Paper Series, no. 172, (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770340.

28 For further background on stablecoins, see CB Insights, *What Are Stablecoins?*, available at https://www.cbinsights.com/research/report/what-arestablecoins/.

29 See Finextra, *MAS and SGX apply blockchain tech for settlement of tokenized assets*, (November 12, 2018), available at https://www.finextra.com/newsarticle/32937/mas-and-sgx-apply-blockchain-tech-for-settlement-of-tokenised-assets. A joint project by the Monetary Authority of Singapore and the Singapore Exchange successfully demonstrated the use of smart contracts to automate the DvP settlement process. In particular, automated DvP was successfully achieved in the trading of Singapore government securities (securities leg) for central bank-issued cash-depository receipts or CDR (cash leg), each of which were represented on separate distributed ledgers.

30 See Reuters, *Bank of Canada, TMX say blockchain feasible for securities settlement*, (May 11, 2018, 6:25 am), available at https://www.reuters.com/article/us-canada-tech-blockchain/bank-of-canada-tmx-say-blockchain-feasible-for-securities-settlement-idUSKBN1IC18G. In this article, Scott Hendry, Bank Canada's Senior Special Director, stated "*it's not clear that all the participant dealers and banks are going to get a significant benefit out of this settlement system*."

could rather be reached through the Target Instant Payment Settlement (TIPS) system, recently implemented by the ECB itself,[31] which deems TIPS systems would offer faster transaction speeds at lower costs.[32]

Still, blockchain endorsers maintain that TIPS systems lack a level of security as high as the distributed ledgers technology's.[33] Indeed, unlike distributed ledger technology, TIPS systems have a single point of failure, making it more vulnerable than decentralized blockchain systems in this respect.

The other main issue lies in dealing with blockchain records immutability. In Nakamoto's Bitcoin blockchain no third-party was entrusted with voiding or reversing a transaction; in that context, investors would be willing to stick to the consensus mechanism to validate transactions. In connection with the securities settlement, the need to reverse or void "clearly erroneous" transactions is evident, because of an obvious error in price, number of shares, or identification of the security.[34]

Even in this case, immutability concerns may be mooted through implementing a permissioned blockchain structure in which the trusted nodes can void or reverse trades under clearly defined rules. Reputational and legal liability concerns can again help discipline the permissioned entities to enforce rules appropriately.

The transaction revision process through permissioned nodes must be carefully considered. Some financial market participants would

---

31 See European Central Bank, *The new Target Instant Payment Settlement (TIPS) service*, (June 2017), available at https://www.ecb.europa.eu/paym/intro/mip-online/2017/html/201706_article_tips.en.html.

32 Carolynn Look & Piotr Skolimowski, *ECB's Mersch Says His Payment System Is Better Than Blockchain*, Bloomberg, (February 8, 2018, 11pm), available at https://www.bloomberg.com/news/articles/2018-02-08/ecb-s-mersch-says-his-payment-system-is-better-than-blockchain.

33 Simon Chandler, *No, Yves Mersch, the ECB's System is Not 'Better' than the Blockchain*, Cryptonews, (February 12, 2018), available at https://cryptonews.com/exclusives/no-yves-mersch-the-ecb-s-system-is-not-better-than-theblock-1195.htm.

34 See Nasdaq, *Clearly Erroneous Transactions Policy*, available at https://www.nasdaqtrader.com/Trader.aspx?id=ClearlyErroneous.

prefer a more immutable blockchain structure, giving transacting parties more certainty that a validated trade is permanent. While others may prefer more leeway for subsequent revisions. Therefore, striking the appropriate balance on immutability is a key concern for an effective clearing and settlement system.

12.4. Blockchain-based Application to the Voting System

12.4.1. Current Blockchain Initiatives

(1) The Table below illustrates the state of the art of the blockchain initiatives carried out by market participants – mainly, issuers, corporate service companies, stock exchanges, and CSDs – in connection with AGM, tabulation, and clearing and settlement of securities.[35]

Entity	Date of initiative	Initiative	Technology used?	Launched in practice?	Updates / comments
Australian Securities Exchange ASX), Digital Asset, and MWare[36]	2016	Three-party MOU to build a replacement platform for the existing clearing system (CHESS).	Unknown	No. The platform should run from March/April 2021. Due to concerns over the coronavirus pandemic, the new go-live	30-40% of the platform is already available to replace the CHESS.

[35] See Anne Lafarre & Cristoph Van der Elst, *Blockchain Technology for Corporate Governance and Shareholder Activism*, EUR. CORP.GOVERNANCE INST., Working Paper No. 390/2018, at 17 (March 2018).

[36] See Coindesk, Australian Securities Exchange Building New Blockchain Platform With VMWare, Digital Asset, (August 26, 2019, 5.30 pm), available at https://www.coindesk.com/australian-securities-exchange-building-new-blockchain-platform-with-vmware-digital-asset; see also ASX, *ASX, Digital Asset and VMware join forces on DLT VMware adds support and scale to ASX offering*, (August 26, 2019), available at https://www.asx.com.au/documents/about/MediaRelease-ASX-DigitalAsset-and-VMware-join-forces-on-DLT.pdf

				date will be April 2022, 12 months beyond the original go-live target.[37]	
Bundesbank and Deutsche Börse	2016	Trial project for transferring and settling securities and cash.	Browser-based software on a private blockchain, no white-paper.	No	No, Germany's Central Bank President said it would be more costly and less speedy than traditional means.[38]
Euroclear (Belgian, Dutch, Finnish, French, Irish, Swedish, UK CSD)[39]	2019	Pilot blockchain-based platform for issuing and set-	End-to-end blockchain platform.	No	Proof of value completed with Banco Santander and EY.

[37] Australian Securities Exchange, ASX consults on CHESS replacement implementation timetable, Target go-live of April 2022 subject to user feedback (June 30, 2022), available at file:///C:/Users/eugen/Downloads/chess-replacement-consultation-paper-revised-implementation-timetable.pdf

[38] See Bloomberg, *Blockchain Settlement Was Slow, Costly in Trial, Weidmann Says* (May 29, 2019), available at https://www.bloomberg.com/news/articles/2019-05-29/blockchain-settlement-was-slow-costly-in-trial-weidmann-says?utm_source=twitter&utm_content=business&cmpid=socialflow-twitter-business&utm_medium=social&utm_campaign=socialflow-organic.

[39] See Reuters, *Euroclear to Press Ahead with Blockchain Pilot for Commercial Paper*, (June 19, 2019, 12.23 pm), available at https://www.reuters.com/article/us-euroclear-blockchain/euroclear-to-press-ahead-with-blockchain-pilot-for-commercial-paper-idUSKCN1TK0D8.

		tling commercial paper transactions.			Intention to move onto a pilot phase.
Deutsche Börse, Swisscom, Falcon Private Bank, Vontobel, and Zürcher Kantonalbank	2019	DLT Proof of Concept (PoC) on settling securities transactions with tokenized shares.	Protocols Corda and Hyperledger Fabric are used for processing cash and security tokens. Parties use cross-chain secure settlement to ensure no one had to make an advanced payment throughout the settlement process.	No	"This proof of concept is an excellent example of successful collaboration and innovative strength across company boundaries."[40]
Nasdaq and Estonian	2016	E-voting blockchain platform.	Nasdaq cooperated with Chain and made	Different AGMs in Estonia, including the	Nasdaq announced the pilot was successful

[40] Deutsche Börse Group, *Deutsche Börse, Swisscom and Partners Successfully Settle Securities Transactions via Tokens in Switzerland*, (November 19, 2019), available at https://www.deutsche-boerse.com/dbg-en/media/press-releases/Deutsche-B-rse-Swisscom-and-partners-successfully-settle-securities-transactions-via-tok ens-in-Switzerland-1631516.

Government[41]			use of the e-Residency platform of the Estonian government.	AGM of LHV Group.	and they established a PoC.
NSD (Russian CSD)	2019	Full Delivery versus Payment settlement model for transferring bonds and funds.	Publication of white paper.[42] Hyperledger Fabric 1.1. NXT platform and use of ISO 20022 international standard for messaging.	Issuance of a bond on NSD blockchain from MTS. Redemption of the bond from Sberbank.	
	2016	Prototype for managing AGM.	NXT platform using ISO 20022 solutions.	The prototype was tested in bondholder meetings.	Confidentiality and transparency issues addressed

41 See Anna Irrera, *Nasdaq successfully completes blockchain test in Estonia*, Reuters, (January 23, 2017, 7:01 am), available at https://www.reuters.com/article/nasdaq-blockchain-idUSL1N1FA1XK.

42 Ledger Insights, *Russia's NSD publishes whitepaper on blockchain in finance*, (November 2019), available at https://www.ledgerinsights.com/nsd-whitepaper-blockchain-in-finance/.

					along with DataArt.[43]
SWIFT, SLIB, SGX (Singaporean Securities Exchange), Deutsche Bank, DBS, HSBC and Standard Chartered Bank	2019	DLT PoC on e-Voting relating to AGMs and proxy voting.[44]	ISO 20022 based solutions and Hyperledger Fabric technology.	No.	
ADX (Abu Dhabi Securities Exchange)	2016	E-voting for AGMs.[45]	Sahmi digital platform.	Yes, six AGMs of listed companies.[46]	(ADX) announced it will be managing remote e-voting for Annual General Meetings (AGMs) of

43 National Settlement Depository, NSD makes it possible to maintain financial privacy in blockchain use (October 17, 2017, available at https://www.nsd.ru/en/publications/news/media-about-us/nsd-makes-it-possible-to-maintain-financial-privacy-in-blockchain-use-2017-10-17_181400/?sphrase_id=25181.

44 SWIFT, *SWIFT launches DLT e-Voting PoC*, (March 6, 2019), available at https://www.swift.com/news-events/press-releases/swift-launches-dlt-e-voting-poc

45 Finextra, *ADX showcases blockchain voting at AGMs*, (October 9, 2017), available at https://www.finextra.com/pressarticle/71057/adx-showcases-blockchain-voting-at-agms; Coindesk, *Abu Dhabi Stock Exchange Launches Blockchain Voting Service*, (October 17, 2016, 12:52 pm), available at https://www.coindesk.com/abu-dhabi-exchange-blockchain-voting.

46 Gulf News, *ADX hosts six AGMs using blockchain technology* (May 31, 2017, 6:19 pm), available at https://gulfnews.com/business/markets/adx-hosts-six-agms-using-blockchain-technology-1.2036438.

					companies listed on the Exchange free of charge.[47]
Broadridge, J.P. Morgan, Northern Trust and Banco Santander	March 23, 2018.	Pilot	Unknown.	Voting at Santander's AGM.[48]	One-fifth of the shareholder votes were cast on the DLT.
Broadridge, ICJ, and Tokyo SE	2019	DLT PoC.	Quorum DLT.	Blockchain-based proxy voting in Japan.[49]	
Broadridge	2019	Proxy voting solution for distribution of meeting notices to retail.	Unknown.	No.	Electronic distribution and voting through several means. Fulfilment of disclosure obligations required by

47 Abu Dhabi Securities Exchange, *Abu Dhabi Securities Exchange (ADX) to provide free of charge remote e-voting for Annual General Meetings of listed companies* (March 21, 2020), available at https://www.adx.ae/English/pages/NewsDetails.aspx?viewid=20200322140015

48 Broadridge, *Santander and Broadridge Complete a First Practical use of Blockchain for Investor Voting at an Annual General Meeting* (May 17, 2018), available at https://www.broadridge.com/press-release/2018/santander-and-broadridge-completed-practical-use-of-blockchain.

49 Broadridge, *ICJ and Broadridge collaborated to design and execute a blockchain-based proxy voting process for the Japanese market, with a pilot mirroring the reconciliation and vote delivery process using DLT* (January 14, 2019), available at https://www.broadridge.com/intl/press-release/2019/icj-and-broadridge-execute-the-proxy-voting-process.

		shareholders and voting.[50]			the Shareholders Rights Directive II to intermediaries.
Broadridge	2018	Obtainment of patent No. 9,967,238 from the U.S. Patent and Trademark Office for applying blockchain to proxy voting and repo agreements.	Unknown.	Yes.	This achievement is defined as a milestone for Broadridge's business.[51]

[50] See Broadridge, *World's-Largest Financial Institutions Utilizing Broadridge to Solve New Obligations Under European Shareholder Rights Directive (SRD II)* ((December 4, 2019), available at https://www.broadridge.com/intl/press-release/2019/broadridge-to-solve-new-obligations-under-european-srd.

[51] See Broadridge, *Broadridge Secures Industry-Leading Blockchain Patent for Proxy Processing and Repo Agreements*, (May 10, 2018), at: https://www.broadridge.com/press-release/2018/broadridge-secures-industry-leading-blockchain-patent. With respect to the repo agreements, in October 2017 Broadridge successfully completed a pilot of blockchain-based bilateral repo solution together with Natixis and Société Générale; please, see Broadridge, *Broadridge Successfully Completes Pilot of Blockchain-Based Bilateral Repo Solution*, (October 17, 2017), available at https://www.broadridge.com/press-release/2017/broadridge-successfully-completes-pilot-of-blockchain-based-bilateral-repo-solution.

BitFlyer[52]	2020	Shareholders virtual voting solution for annual meetings.	Blockchain-based app (bVote) to allow fair voting at virtual shareholders meetings.	No.	
Nasdaq and Strate (Pty) Ltd (South African CSD)[53]	2017	The PoC established in the Estonian pilot.	Unknown.	No.	
AST Financial and NuArca	2017	Scaled pilot[54]	The proxy voting network utilizes Hyperledger Fabric and will be deployed as a cloud service'. The	Yes, and it will launch in March 2018.	Yes, indicating it was a successful pilot also in terms of speed and scale.

[52] See Cointelegraph, *BitFlyer Blockchain Reveals Voting App for Virtual Shareholders Meetings*, (June 11, 2020), available at https://cointelegraph.com/news/bitflyer-blockchain-reveals-voting-app-for-virtual-shareholders-meetings.

[53] See Nasdaq, *Nasdaq to Deliver Blockchain E-Voting Solution to Strate*, (November 22, 2017), available at http://ir.nasdaq.com/news-releases/news-release-details/nasdaq-deliver-blockchain-e-voting-solution-strate.

[54] See Business Wire, *AST Completes Successful Pilot of Blockchain-based Solution for Proxy Voting, Processing at Volumes Simulating the Largest Proxy Campaigns*, (December 13, 2017, 9:05 am), available at https://www.businesswire.com/news/home/20171213005230/en/AST-Completes-Successful-Pilot-Blockchain-based-Solution-Proxy; and Asset Servicing Times, *Blockchain Proxy Voting Pilot Proves Solution's Scalability*, (December 15, 2017), available at http://www.assetservicingtimes.com/assetservicesnews/article.php?article_id=7842.

			project is called "TransactChain".		
American Stock Transfer & Trust Company, LLC (AST)[55]	2020		ProxyIQ, a blockchain-based platform for proxy campaign management, tabulation, reporting and predictive analytics for the mutual fund industry.	No.	
KAS Bank and Atos Origin[56]	2018	Prototype	Voteroom app via the Ethereum network as a basis.	Yes, at the AGM held on April 25, 2018.	The next step would have been for the app to be available to listed companies for purchase and free for

[55] AST, *AST Launches ProxyIQ™ to Provide Unmatched Speed, Accuracy and Cost-Effectiveness in Mutual Fund Proxy Campaign Analytics and Management*, (February 26, 2020), available at https://www.astfinancial.com/us-en/news-events/news-room/news/ast-s-mutual-fund-proxy-campaign-platform-proxyiq-recognized-as-a-2020-benzinga-fintech-awards-finalist/.

[56] Caceis Investor Services, *Blockchain Technology Simplifies Voting Rights*, (April 6, 2018) available at https://www.caceis.kasbank.com/en/about-us/news/2018/blockchain-technology-simplifies-voting-rights.

					shareholders to use. Such step has not been taken yet.

12.4.2. Blockchain possible goals

Were a permissioned blockchain structure to apply to corporate elections, the shareholders, as beneficial owners, would be provided with as many as tokens as the number representing their voting power: the "votecoins".[57] To register their preferences, voters could then transmit those tokens to the public addresses on the blockchain, to which only themselves and their proxy agents would have access through a private key.

Such a system would ensure greater speed and transparency of the cast ballots, and the accuracy of blockchain voting may enable beneficial owners to cast more easily their votes and feel themselves more involved in the corporate governance.[58]

Moreover, finally implementing blockchain to the voting process would solve the frequent empty-voting problems. Blockchain share registration would be capable of providing both transparency and early warning of the rearrangement of voting rights prior to any elections, in order to have a clear picture of the most up-to-date ownership structure of the corporation. Accordingly, borrowing shares in the stock lending market, with voting rights transferred to the borrower until he/she returns the shares, would be immediately transparent to

---

57 Yermack, *supra* note 11, at 23.

58 For a different point of view on this issue, see Park Bramhall, *Blockchain will not solve the proxy voting problem*, (July 31, 2019), available at http://clsbluesky.law.columbia.edu/2019/07/31/blockchain-will-not-solve-the-proxy-voting-problem/. In the article, the author stresses that, regardless of the implementation of the blockchain technology, end-to-end vote confirmations are already possible under the existing proxy voting system, stating the DTCC's Direct Registration System Service has enabled investors to avoid holding their securities in street name since 1996. However, he deems investors are not willing to directly hold their own tokens and still prefer to hold them in "street name" – because of the complexity of blockchains' functioning, where the loss of private keys associated with a particular token would result in the loss of that token.

the other stakeholders, and regulators who could, respectively, counteract the acquisition of votes by an empty voter, and potentially enjoin the voting of the shares.[59]

With a view to stepping forward along the blockchain implementation, adopting laws and regulations will be paramount in assisting and supporting such a change. Law is often required to catch up with business innovations to regulate what has already been invented. In this regard, for achieving the blockchain target, the U.S. states would be supposed to enact a legal framework for digital identity management of share transactions. Adopting a legal framework could mitigate some of the intrinsic risks of blockchain and provide the proxy voting platforms with the right level of security and privacy. Should states be able to enact some legislation, "*the effect of the "blockchain revolution" on the corporate governance of public companies will be optimized, and proxy voting as we know it will finally be changed for the better*."[60]

12.5. Hurdles for Blockchain Implementation

Implementing the blockchain technology has not been equally perceived by everyone. Besides its endorsers, who are trying to scale-up their projects, other market players are also aware of the potential adverse consequences that may impact their own activities.

In that regard, blockchain would clash with the interests of those who are concerned with disclosing their own identities to the corporation in which they either participate or are willing to invest. Under the Securities and Stock Exchange (SEC) rules, beneficial owners may prohibit their intermediaries to disclose information regarding their identity to the issuer (*i.e.*, objecting beneficial owners or OBOs). As such, the company cannot reach out to the OBOs directly.[61]

---

59 Yermack, *supra* note 11, at 23.

60 Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 Berkeley Tech. L. J. 487 (2018).

61 For an overview of the OBO/NOBO ownership distinctions and the relevant consequences, Alan L. Beller and Janet Fisher, *The OBO/NOBO Distinction in Beneficial Ownership: Implications for Shareholder Communications and Voting*, (February 2010), available at https://www.cii.org/files/publications/white_papers/02_18_10_obo_nobo_distinction_white_paper.pdf.

This is certainly the case of activist investors and raiders,[62] whose investing strategy is mainly based on the surprise effect. By not authorizing their intermediaries to disclose their own identities and share position to the market, it is easier for them to catch issuers' managers off guard, and unable to promptly adopt defensive mechanisms. In particular, the mentioned investors act frequently under the 5% threshold to avoid the disclosure requirements with the SEC.[63] However, should activists go beyond the 5% threshold, they can still benefit from a 10-day grace period prior to being required to publicly file the information. In this window of time, they can "*furiously buy every share* [they] *can*".[64]

In this respect, blockchain could create better information equality among market investors, making shareholders activism more difficult and less cost-efficient. Shareholder activists – like hedge funds – are eager to buy stakes in companies with a view of putting pressure on the current management and getting higher dividends. Their investing strategy has not always been deemed detrimental to the targeted issuers: for instance, activists have been committed to raising the share price, and holding the management more accountable for their actions.[65]

---

62 Yermack, *supra* note 11, at 19-20.

63 It is worth recalling that, under Section 13D of the SEC rules commonly referred as "beneficial ownership report", those who solely or collectively acquire beneficial ownership of more than 5% (significant ownership) of a voting class of a company's equity securities registered under Section 12 of the Act, are required to file the Section 13D form with the SEC, unless they qualify as passive investors and are consequently eligible for the less burdensome Section 13G form. Therefore, all active investors, intending those interested in influencing or exercising control over the issuer, are required to disclose more information relating to their goals (*e.g.*, changing the composition of the board, paying out excess cash, rescinding takeover defenses, or seeking the sale of the firm).

64 Interview with David Yermack, the Albert Fingerhut Professor of Finance and Business Transformation at New York University Stern School of Business, in connection with a course of three stand-alone lectures at the Stigler Center on the potential implications of blockchain technology for the future of corporate governance. The entire lecture is available at https://promarket.org/blockchains-corporate-finance-blockchain-market-shareholder-activists-might-play-much-less-role/.

65 David Yermack, *Shareholder Voting and Corporate Governance*, (March 17, 2010), available at https://pdfs.semanticscholar.org/3283/6fda4e5c90acf7655f8d5abe6e11e2e9dbf1.pdf. In this article, the

Hence, blockchain would basically prevent activists from pursuing their silent strategy, and their moves would be visible from the very first trade. This will obviously render shareholder activism more cumbersome as the management, once aware of the imminent takeover threat, could trigger any available defensive measures: *inter alia*, poison pills, seeking a white knight, and setting up staggered boards.[66]

Overall, it is likely that the costs borne by shareholder activists will have a significant adverse impact on their strategy, resulting in lowering the number of those players.

In addition to activist investors, clearinghouses and custodians may look at the blockchain voting and clearing initiative as detrimental to themselves.[67] Although blockchain implementation would result in savings ranging from fifteen to thirty-five billion USD for issuers and end-investors, such savings will likely come at the expense of the above-mentioned entities that will be replaced by the distributed ledger technology.[68] Such intermediary actors, whose business is fundamental in connection with the voting process, are not willing to enable blockchain technology to dismantle their thriving activities. Should it happen, it would be hard for them to find a new role in an ever more automated market. Although some intermediaries have proceeded with exploring blockchain technology, many of them are unlikely to accept such a sudden change.[69]

In the recent past, CEOs of the most prominent U.S. investment banks seemed to have taken a stand against the implementation of blockchain in their business, which contributed to slowing down the

---

author states that "[m]ost activists have relatively short time horizons, generally seeking to pressure firms into immediate governance reforms but not seeking full operating control."

66 Yermack, *supra* note 52, where the author maintains that making the shareholder registry as transparent as possible, may constitute a form of takeover defense.

67 Wonnie Song, *Bullish on Blockchain: Examining Delaware-s Approach to Distributed Ledger Technology in Corporate Governance Law and beyond*, 8 Harv. Bus. L. Rev. Online 9 (2017-2018).

68 Bain & Co., *Blockchain in Financial Markets: How to Gain an Edge*, at 4-5 (February 9, 2017), available at https://www.bain.com/insights/blockchain-in-financial-markets-how-to-gain-an-edge/.

69 Bain & Co., *supra* note 56.

spread of blockchain across the market.[70] Yet, some executives have changed their minds, and now look at blockchain as a more powerful device.[71]

Nonetheless, in spite of wider openness toward blockchain, replacing the current multi-party proxy system is a long way to go, and it is not predictable yet how long it will take.

12.6. Conclusions

The described "state of the art" testifies the recent efforts made by firms and stock-exchanges in developing PoCs and prototypes, some of which were eventually put in practice. Those entities are now faced with a difficult challenge: scaling up their business to enhance the amounts of investors involved. Additionally, all market players – regulators, issuers, shareholders, financial intermediaries, and auditors – should act in concert and cooperate to make what has been invented so far more standardized and financial consumer-friendly.

Over the last three years, many U.S. States have experienced an increasing interest in blockchain by enacting bills regarding blockchain regulation. It is worth mentioning Bill No. H.B. 101 enacted by the Legislature of the State of Wyoming, which (i) authorizes the use of a network address to identify corporation's shareholder; (ii) authorizes corporations to accept shareholder votes if signed by a network signature that corresponds to a network address; and (iii) specifies requirements for use of electronic networks or databases. Further, Bill No. A08792 enacted by the New York Assembly is of importance , as it directs the state board of elections to study and evaluate the use of blockchain technology to protect voter records and election results.[72]

---

[70] Jamie Dimon, JP Morgan Chase CEO, and Lloyd Blankfein, former Goldman Sachs CEO, opposed blockchain and, in general, embracing crypto currencies. See CB Insights, *How Blockchain Could Disrupt Banking*, (December 12, 2018), available at https://www.cbinsights.com/research/blockchain-disrupting-banking/.

[71] Jamie Dimon, after not endorsing blockchain technology in a first moment, took a step toward blockchain. See Matt Egan, *Jamie Dimon hated bitcoin. Now JPMorgan is getting ahead of the crypto revolution*, February 15, 2019, available at https://www.cnn.com/2019/02/15/investing/jpmorgan-bitcoin-crypto-jamie-dimon/index.html.

[72] For a more thorough analysis of all legislative initiatives regarding blockchain, see Heather Morton, *Blockchain State Legislation*, (March 28, 2019), available at

Even Vice Chancellor J. Travis Laster, in his 2016 keynote speech, remarked the importance of the blockchain technology. He pointed out that blockchain could represent the solution of "*the problems with the voting and stockholding infrastructure of U.S. securities markets*". He also recognized that applying distributed ledger technologies to corporate voting will result in "*better accuracy, greater transparency, and superior efficiency for settling securities trades and voting in corporate elections*".[73]

Still recently, the European Parliament has proposed an e-voting blockchain platform that "*could speed up, simplify and reduce the cost of elections, and might lead to higher voter turnouts and the development of stronger democracies*."[74]

Given the latest legislative developments and corporate projects, it is likely that the general tendency would be toward an increasingly implementation of the blockchain permissioned systems in connection with shareholders voting. Blockchain technology, in its permissioned form, may be able to solve the current inefficiencies affecting shareholders voting: the "chain", according to a consensus mechanism, can store any information in a verifiable and immutable way.

---

http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx. A relevant data is the significant number of laws already enacted by Wyoming (13). As stated by Caitlin Lon, member of the Wyoming Blockchain Task Force and former Chairman and President of Symbiont, Wyoming is becoming the "Delaware of digital asset law"; it holds a comprehensive legal framework that enables blockchain technology to thrive.

73 J. Travis Laster, Del. Ch., *The Block Chain Plunger: Using Technology to Clean Up Proxy Plumbing and Take Back the Vote*, Keynote Speech for the Council of Institutional Investors (Sept. 29, 2016), available at https://www.cii.org/files/09_29_16_laster_remarks.pdf. See also Jack Markell, former Governor, State of Delaware, *Consensus 2016 Keynote Presentation: Introducing the Delaware Blockchain Initiative* (May 2, 2016), available at https://www.youtube.com/watch?v=-mgxEhIvSTY, where he announced the official public launch of the "Delaware Blockchain Initiative."

74 See Boucher P. (2016) What if blockchain technology revolutionized voting? Unpublished manuscript, European Parliament. In this article, the author describes two ways to develop blockchain-enabled e-voting: 1) creating a brand-new blockchain system; or 2) piggybacking a well-established blockchain system.

13. Oblio e diritto: brevi note giurisprudenziali

Marco Rizzuti

In un breve scritto di qualche tempo fa[1] avevamo avuto occasione di esprimere alcune prime considerazioni in ordine all'effettivo impatto che il riconoscimento europeo del cosiddetto diritto all'oblio, nella celeberrima sentenza *Google Spain*[2] e quindi nelle *Guidelines* dell'*Article 29 Data Protection Working Party*[3], avesse avuto sulla giurisprudenza interna. L'impressione era che, a fronte di un, forse già sin troppo entusiastico, riconoscimento interno emerso negli anni immediatamente precedenti[4], la riflessione suscitata dagli interventi europei avesse

---

1 M. RIZZUTI, *Il diritto e l'oblio*, in *Corriere giuridico*, 2016, 8/9, pp. 1077-1082.

2 Il riferimento è a Corte UE 13 maggio 2014, C-131/12, su cui si vedano SCORZA, *Corte di giustizia e diritto all'oblio: una sentenza che non convince*, in *Corriere giuridico*, 2014, 12, p. 1473; G. RESTA, V. ZENO ZENCOVICH, *Il diritto all'oblio dopo la sentenza Google Spain*, Roma, 2015; FLORIDI e altri, *The Advisory Council to Google on the Right to be Forgotten*, in www.google.com.; S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars interpretandi*, 2017, 1, pp. 67-80.

3 Si allude alle *Guidelines* adottate il 26 novembre 2014 dalle Autorità per la tutela della Privacy di tutti i Paesi europei riunite per l'appunto nel cosiddetto *Article 29 Data Protection Working Party*.

4 Nella dottrina in tema di oblio precedente alle sentenze che qui si vanno a discutere si possono vedere, senza pretese di completezza: T. AULETTA, *Diritto alla riservatezza e "droit a l'oubli"*, in G. ALPA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, p. 127 ss.; G.B. Ferri, *Diritto all'informazione e diritto all'oblio, in Rivista di diritto civile.*, 1990, 801 ss.; G. GIACOBBE, *Diritto all'oblio*, in *Atti del convegno di Urbino 17 maggio 1997*, a cura di E. GABRIELLI, Napoli, 1999, p. 30 ss.; MORELLI, *Oblio (diritto all')*, in *Enciclopedia del diritto, Aggiornamento*, VI, Milano, 2002, p. 848 ss.; MEZZANOTTE, *Diritto all'oblio vs. diritto alla memoria: il moderno sviluppo della privacy*, in *Diritto pubblico comparato ed europeo*, 2002, p. 1604 ss.; NIGER, *Il diritto all'oblio*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato*, Padova, 2007, 59 ss.; MEZZANOTTE, *Il diritto all'oblio: contributo allo studio della privacy storica*, Napoli, 2009; S. AMATO, *Il diritto all'oblio*, in ID., CRISTOFARI, RACITI, *Biometria. I codici a barre del corpo*, Torino, 2013, p.

semmai indotto a (ri)scoprire i limiti di tale diritto ed i necessari bilanciamenti con ulteriori posizioni giuridiche di carattere fondamentale. Così, nelle prime decisioni di merito che a tale elaborazione sovranazionale facevano riferimento, il limite rappresentato dal ruolo di rilievo pubblico del richiedente l'oblio veniva ravvisato nell'iscrizione di un soggetto all'albo degli avvocati[5], mentre quello della valenza storica di fatti particolarmente gravi veniva opposto ad un ex terrorista[6]: decisioni entrambe particolarmente significative in quanto solo pochissimi anni prima quelli che si sarebbero potuti considerare i *leading cases* della giurisprudenza di legittimità interna erano pervenuti ad esiti sostanzialmente opposti[7]. Uno sviluppo, insomma, in direzione

---

103 ss.; Pizzetti, *Il caso del diritto all'oblio*, Torino, 2013; J.R. De Verda, *Breves reflexiones sobre el llamado derecho al olvido*, in *Actualidad Jurídica Iberoamericana*, 2014, 1, pp. 29-34; V. Putortì, *Internet, diritto all'oblio e tutela dell'identità della persona*, in V. Barsotti (a cura di), *Libertà di informazione, nuovi mezzi di comunicazione e tutela dei diritti*, Santarcangelo di Romagna, 2015, p. 157 ss.

5 Trib. Roma, Sez. I, 3 dicembre 2015, in *Corriere giuridico*, 2016, 8/9, p. 1072, rigettava la richiesta di deindicizzazione con riferimento al coinvolgimento dell'attore in indagini penali che non avevano portato ad alcuna sentenza. Nella specie rilevava anche l'estrema brevità del tempo trascorso, ma a noi interessa soprattutto l'esplicito richiamo al criterio di cui al n. 2 delle menzionate *Guidelines* circa il ruolo del soccombente nella vita pubblica anche solo in quanto iscritto all'albo forense.

6 Garante per la protezione dei dati personali, provvedimento 31 marzo 2016, n. 152, in *Corriere giuridico*, 2016, 8/9, p. 1074, escludeva la possibilità di esercitare il diritto all'oblio con riguardo alla posizione di un soggetto che, in quanto appartenente ad una formazione terroristica di destra, si era reso protagonista di determinate vicende di particolare importanza storica.

7 Per il primo profilo si allude a Cass. 5 marzo 2012, n. 5525, in cui un esponente dell'allora P.S.I., indagato per corruzione ed arrestato, ma poi prosciolto e candidato *in pectore* ad una tornata elettorale, aveva ottenuto che fosse imposto al *Corriere della Sera* di predisporre un meccanismo idoneo a segnalare, nell'archivio informatico che rendeva tuttora accessibile *online* la notizia del suo arresto, anche il successivo sviluppo a lui favorevole della vicenda: invero il ruolo pubblico del soggetto sembra incomparabilmente maggior di quello del mero iscritto all'albo professionale del successivo caso… Per il secondo profilo si allude invece a Cass. 26 giugno 2013, n. 16111, in cui un ex appartenente alla formazione terroristica Prima Linea, che aveva già scontato la relativa pena, ha ottenuto la condanna di un quotidiano locale comasco al risarcimento dei danni derivatigli dalla ripubblicazione di notizie inerenti a tali trascorsi, in ordine ai quali egli invocava appunto il diritto all'oblio, mentre nel successivo caso vagliato dal Garante è stata assunta una decisione diametralmente opposta con riguardo alle notizie circolanti su *internet* a proposito di un neofascista di spicco: naturalmente tale evoluzione ci sembra giustificabile soprattutto in considerazione dei nuovi orientamenti europei, e non certo in ragione di una differente valutazione dei due opposti estremismi.

ben diversa da quello, oramai risalente, che in materia di *privacy* aveva visto i nostri giudici costruire un nuovo diritto ancora inesistente nell'ordinamento interno tramite una delle prime operazioni di diretta applicazione dei principi di un ordinamento sovranazionale[8].

Il menzionato *trend* verso il ridimensionamento del "*right to be forgotten*" ci sembrava, e ci sembra, da valutare in termini positivi. Occorre invero tener presente come questa nuova incarnazione dell'antichissimo sforzo di imporre con strumenti giuridici l'oblio a fronte di quelle tecnologie[9] che di volta in volta sembrino minacciare una perennità delle informazioni, o quantomeno la sua apparenza[10], abbia

---

8 Si allude al celebre caso *Soraya* (Cass. 27 maggio 1975, n. 2129), in cui nel riconoscere alla ripudiata imperatrice di Persia il risarcimento dei danni cagionati dalla diffusione delle notizie sulle vicende intime che a tale ripudio avevano condotto, si era fatta diretta applicazione dell'art. 8 CEDU.

9 Per il profilo antropologico si possono vedere: D. BATTAGLIA, *At Play in the Fields (and Borders) of the Imaginary: Melanesian Transformations of Forgetting*, in *Cultural Anthropology*, 1993, pp. 430-442; A. ASSMANN, *Formen des Vergessens*, Göttingen 2016; F. CIMATTI, *La fabbrica del ricordo*, Bologna 2020. Al paradigma delle leggi sull'oblio finalizzate a placare gli odi civili si possono ricondurre, nei secoli, i casi del divieto di "*μνησικακεῖν*"dopo la cacciata dei Trenta Tiranni, la proposta di "*αμνηστία*" formulata da Cicerone dopo il cesaricidio, il divieto di "*renouveler la mèmoire*" imposto da Enrico IV di Francia, ed il *Pacto del Olvido* che nella Spagna postfranchista è durato sino alla *Ley de Memoria Històrica* del 26 dicembre 2007. Sono poi numerosissime le vicende storico-giuridiche attinenti al tentativo di dominare oblio e memoria ordinando la distruzione di statue (J. ASSMANN, *Das kulturelle Gedächtnis: Schrift, Erinnerung und politische Identität in frühen Hochkulturen*, München 1992; E. VARNER, *Mutilation and Transformation: Damnatio Memoriae and Roman Imperial Portraiture*, Boston 2004; L. SANFILIPPO-A. RIGON (eds.), *Condannare all'oblio: pratiche della Damnatio Memoriae nel Medioevo*, Ascoli Piceno 2010; N.N. MAY (ed.), *Iconoclasm and Text Destruction in the Ancient Near East and Beyond*, Chicago, 2012) o successivamente il rogo di libri (cfr. R. KNUTH, *Burning Books and Leveling Libraries: Extremist Violence and Cultural Destruction*, Westport 2006; L.X. POLASTRON, *Livres en feu. Histoire de la destruction sans fin des bibliothèques*, Paris 2004; P. BATTISTA, *Libri al rogo. La cultura e la guerra all'intolleranza*, Milan 2019). Ed anche ai nostri tempi comparabili battaglie culturali attorno alle tecnologicamente più antiche forme di preservazione della memoria sono tutt'altro che irrilevanti: basti pensare all'iconoclastia islamista (cfr. V. DOMENICI, *Contro la bellezza*, Milano, Sperling & Kupfer, 2015; P. VEYNE, *Palmyre, l'irremplaçable trésor*, Paris, 2015; P. BRUSASCO, *Dentro la devastazione. L'ISIS contro l'arte di Siria e Iraq*, Milano, 2018) o all'odierno fenomeno della cosiddetta *cancel culture* (si veda il numero dedicato di *Limes*, 8/20, *È la storia bellezza*).

10 Che l'informatica abbia sempre tali potenzialità si potrebbe, d'altronde, fondatamente mettere in dubbio: la leggibilità futura di quanto memorizzato su supporti elettronici è, infatti, molto più incerta di quella dei libri cartacei, data l'altissima velocità di obsolescenza delle nuove tecnologie in discorso (cfr. L. RUSSO, *La rivoluzione*

dato vita, beninteso secondo percorsi diversi nelle varie esperienze giuridiche[11], ad un costrutto peculiarissimo, inquadrabile come un diritto alla cancellazione di informazioni non diffamatorie né false né riservate ed in origine pubblicate in maniera pienamente lecite, ma oggi non più coerenti con l'identità dell'interessato. Il facile abuso di un meccanismo del genere rischia invero di pregiudicare pesantemente la libertà informativa altrui e di conseguenza, soprattutto in quei casi magari quantitativamente non numerosissimi ma più suscettibili di pervenire all'attenzione di un giudice per la rilevanza degli interessi in gioco[12], emergerà prepotentemente la necessità di un ragionevole bilanciamento[13].

Un bilanciamento cui, come evidenziato dai casi prima ricordati, si

---

dimenticata, Milano, 2001, p. 433, nt. 8). Invero, a tutti sarà capitato di incontrare enormi difficoltà pratiche nel tentativo di accedere ai dati memorizzati su CD-ROM anche solo di pochi anni fa, o ai *files* redatti con versioni di un *software* non più compatibili con quella aggiornata, mentre accedendo ad una biblioteca o ad un archivio storico o ad un museo si possono leggere volumi centenari ed iscrizioni millenarie.

11 Per un ampio ed aggiornato panorama comparatistico si veda F. Werro (ed.), *The Right To Be Forgotten. A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia*, Cham 2020. Proprio negli ultimi anni alla giurisprudenza interna di non pochi Paesi si sono presentati casi eclatanti e discussi, come quello di Paul Termann in Germania e quello di Aida Curi in Brasile.

12 Invero, secondo i dati resi noti da Google, la stragrande maggioranza delle richieste di esercizio del diritto all'oblio, pervenute alla società californiana dopo la sentenza europea del 2014, provenivano da cittadini comuni e non da personaggi di rilievo pubblico (cfr. Del Ninno, *Gli scenari applicativi pratici del c.d. "diritto all'oblio"*, in www.dirittoegiustizia.it). Non è però un caso se le vicende processuali interne hanno riguardato ben altre problematiche, in quanto l'interesse che spinge ad affrontare gli oneri di un percorso giudiziario molto spesso ha una natura di carattere politico o economico molto più significativa di quella attinente all'eventuale eliminazione, per stare agli esempi che più spesso vengono proposti, di un'immagine "postata" in gioventù, quando la stessa poteva sembrare spiritosa e non ancora ridicola, oppure di qualche menzione del proprio nome in siti privi di ogni rilevanza pubblica. Rispetto a tali vicende sembrano, in effetti, molto più congrue le procedure interne ai gestori dei motori di ricerca che sono state implementate all'indomani della pronunzia europea, o al limite quelle esperibili in sede amministrativa presso le autorità preposte alla protezione dei dati personali. D'altra parte, rispetto alle vicende più "serie", quantitativamente meno numerose, ma che hanno maggiori probabilità di arrivare in sede giudiziaria, bisognerà, invece, tenere presente come la pretesa all'oblio incontri quegli importanti limiti che stiamo mettendo in luce.

13 Sulla clausola generale della ragionevolezza si veda, per tutti, G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015.

perviene anche e soprattutto grazie ad una distinzione tra piani diversi: altro è riconoscere che un soggetto abbia già scontato ogni sanzione civile e penale con riferimento a determinate vicende, e che nulla si possa pertanto da lui pretendere, ma altro sarebbe dover accettare ogni sua pretesa di imporre ai terzi un silenzio informativo al riguardo. Analogamente, del resto, in un altro ramo dell'ordinamento, certo differente ma anch'esso segnato da una recente dialettica tra oblio e conoscenza che si va ribilanciando a favore della seconda, si tende sempre più ad ammettere che riconoscere in determinate ipotesi il diritto del genitore biologico a non instaurare relazioni giuridiche familiari col nato non può escludere anche il diritto di quest'ultimo ad un accesso al mero dato informativo circa le proprie origini genetiche[14]. Ed al contrario, ma coerentemente, in un ancora diverso ambito del diritto delle relazioni personali, con riferimento cioè al mutamento del nome in caso di cambiamento di genere, un ulteriore tipologia di oblio è stata riconosciuta in maniera piena, mancando qui un effettivo controinteresse da bilanciare[15].

---

[14] Com'è noto, Corte cost. 22 novembre 2013, n. 278, in *Corriere giuridico*, 2014, 4, p. 471 con nota di T. Auletta, collocandosi sulla scia di CEDU, 25 settembre 2012, *Godelli c. Italie*, ric. 33783/09, ha imposto al legislatore di istituire un procedimento che consenta al figlio di richiedere che la partoriente sia riservatamente interpellata in ordine all'eventuale sua volontà di revocare l'anonimato, procedimento che è stato poi, nonostante la totale inerzia legislativa, elaborato in via pretoria e finalmente consacrato da Cass., S.U., 25 gennaio 2017, n. 1946. Frattanto, Corte cost. 10 giugno 2014, n. 162, in *Corriere giuridico*, 2014, 8-9, p. 1062 con nota di G. Ferrando, nel dichiarare l'illegittimità del divieto della fecondazione eterologa, ha osservato che in tal modo non viene a determinarsi un vuoto normativo, in quanto i diversi profili del fenomeno possono già trovare la loro disciplina in altre fonti, fra cui appunto la citata Corte cost. n. 278 del 2013 per quanto attiene al diritto alla conoscenza delle origini, da riconoscere dunque in qualche forma pure a fronte di questa diversa ipotesi di anonimato. La netta distinzione tra il profilo della impossibile costituzione dello *status* in caso di parto in anonimato e quello della mera conoscenza delle origini è chiaramente messa in luce da Trib. Milano, 14 ottobre 2015, in www.ilcaso.it. D'altra parte, una recentissima decisione (Cass., 22 settembre 2020, n. 19824) ha invece ritenuto che dopo la morte della partoriente anonima, evento ritenuto tale da estinguere la meritevolezza di tutela dell'anonimato, anche un'azione per la dichiarazione giudiziale della maternità potrebbe essere ammissibile.

[15] Il riferimento è alla recente Cass., 17 febbraio 2020, n. 3877, in cui si è chiarito che la persona *transgender* non è tenuta ad adottare la forma adattata al nuovo genere del prenome precedentemente utilizzato, ma può adottarne uno nuovo così da conseguire un totale oblio della precedente identità. Ci sembra infatti che si ottenga in tal modo una piena realizzazione della personalità del soggetto senza ledere gli interessi di chicchessia.

Riterremmo che l'approccio sin qui delineato abbia trovato nei successivi sviluppi a livello europeo ulteriori importanti conferme[16], specie quando quella che era stata un'elaborazione giudiziaria e di prassi ha trovato la propria consolidazione anche e soprattutto nella normativa che il nuovo regolamento sulla protezione dei dati personali ha dedicato sia al "*right to be forgotten*" sia ai suoi limiti[17]. In un caso italiano giunto all'attenzione dei supremi giudici del Lussemburgo si è

---

16 Ci concentriamo in questa sede sull'ordinamento dell'Unione Europea, ma anche dalla Corte di Strasburgo arrivano indicazioni nel senso del necessario bilanciamento del diritto all'oblio in favore della libertà giornalistica e storica: cfr. CEDU, 28 giugno 2018, *M.L. et W.W. c. Allemagne*, ric. 60798/10 e 65599/10.

17 Il riferimento è all'art. 17 del Regolamento UE 2016/679 del 27 aprile 2016, il cosiddetto *General Data Protection Regulation* o *GDPR*, di cui si riporta di seguito il testo: "*1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims*". Si possono vedere al riguardo, anche per ulteriori riferimenti: D. Barbierato, *Osservazioni sul diritto all'oblio e la (mancata) novità del regolamento UE 2016/679 sulla protezione dei dati personali*, in *Responsabilità civile e previdenza*, 2017, 6, p. 2100 ss.; A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio*, in *Nuove leggi civili commentate*, 2017, 2, p. 410 ss.; R. Senigaglia, *Reg.*

nettamente respinta la pretesa, non a caso elaborata proprio nel nostro ambiente giuridico così propenso ad impostazioni estensive in punto di diritto all'oblio, mirante di farlo valere contro le risultanze dei pubblici registri, col rischio evidente di snaturarne completamente la funzione[18]. Ed ancor più di recente un nuovo caso *Google* ha offerto agli stessi eurogiudici l'occasione di esplicitare, a fondamento della propria motivazione, la natura non assoluta e la necessità di bilanciamento del diritto all'oblio. Nella specie si trattava di escludere l'esistenza di un obbligo giuridico del motore di ricerca a procedere alla deindicizzazione su tutte le versioni nazionali, così evidentemente depotenziando assai la portata concreta del pur riconosciuto oblio[19]. Ma il profilo probabilmente più significativo della decisione si coglie nel confronto con un'altra quasi coeva pronunzia europea che invece, avendo riguardo alla tutela contro informazioni diffamatorie illecita-

UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale, in *Nuove leggi civili commentate*, 2017, 5, p. 1023 ss.; F. Di Ciommo, *Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (eds.), *I dati personali nel diritto europeo*, Torino, 2019, pp. 353-396; M. Rizzuti, *GDPR and The Right to Be Forgotten*, in *European Journal of Privacy Law & Technologies, Special Issue*, 2020, p. 105 ss.

18 Il riferimento è a CGUE, C-398/15, *Camera di Commercio Industria Artigianato e Agricoltura di Lecce v Salvatore Manni*, 9 marzo 2017. Si vedano in proposito A. Verdesca, I. Stellato, *Diritto all'oblio e pubblicità commerciale: un bilanciamento invertito*, in *Corriere giuridico*, 2018, 8-9, 1125.

19 Ci riferiamo a due sentenze "gemelle": CGUE, Case C-507/17, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, 24 settembre 2019, e CGUE, Case C-136/17, *GC e a. v Commission nationale de l'informatique et des libertés (CNIL)*, 24 settembre 2019. Il passaggio motivazionale decisivo è il seguente: "*the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights*", e di conseguenza "*there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject… to carry out such a dereferencing on all the versions of its search engine*" Si vedano al riguardo, da differenti prospettive: M. Astone, *Il diritto all'oblio on line alla prova dei limiti territoriali*, in *Europa e Diritto Privato*, 2020, 1, p. 223 ss.; G. Calabrese, *Bilanciamento ed estensione territoriale del diritto alla deindicizzazione*, in *Nuova giurisprudenza civile commentata*, 2020, 4, p. 794 ss.; M. Crisafulli, *Per la CGUE la deindicizzazione sui motori di ricerca non può essere "globale"*, in *Jus Civile*, 2020, 4, p. 1178 ss.; W. Lamik, *Advancement of the right to be forgotten – analysis of the judgment of the Court of Justice of the European Union of 24 September 2019 in the case of Google LLC versus Commission Nationale de l'Informatique et des Libertés (CNIL) – C-507/17*, in *European Journal of Privacy Law & Technologies, Special Issue*, 2020, p. 113 ss.

mente pubblicate, è arrivata a riconoscere un blocco globale dell'accesso all'informazione[20]. E non si tratta a nostro avviso di schizofrenia giudiziale né di un contrasto che debba essere risolto col superamento di una delle due posizioni, bensì di un riconoscimento, implicito ma invero chiarissimo, della differenza di grado assiologico fra le posizioni in discorso, con una superiorità gerarchica della tutela dell'onore e della reputazione, questi sì diritti assoluti, ed una ben minore rilevanza per il diritto all'oblio di informazioni lecitamente pubblicate, relativamente riconosciuto purché contenuto e bilanciato.

Quanto alla giurisprudenza italiana più recente, ci esimeremo in questa sede da una rassegna completa[21], ma riteniamo necessario esplicitare qualche valutazione critica con riferimento ad una recente pronunzia, e non tanto per l'esito concreto cui è pervenuta quanto per un passaggio del suo *iter* motivazionale che sembra denunciare come non vi sia, a nostro avviso, ancora piena chiarezza sulle problematiche qui in esame. La sentenza attiene in particolare all'imposizione dell'anonimizzazione dei dati relativi ai protagonisti della ricostruzione giornalistica di un fatto di cronaca nera di qualche decennio fa, ed i supremi giudici motivano in tal senso ritenendo che nell'ipotesi non operi la tutela del diritto di cronaca e della libertà di informazione ex art. 21 Cost., in quanto non di cronaca ma di mera ricostruzione storica si tratterebbe, per l'appunto in ragione del tempo trascorso[22]. A prescindere dall'esito in concreto, è quest'ultimo il profilo della motivazione che non riesce a convincerci: la ricerca storica dovrebbe, infatti, godere semmai di una protezione costituzionale ancora più forte, quella della libertà della scienza cui l'art. 33 Cost. non prescrive nemmeno i limiti cui il predetto art. 21 sottopone invece la più generica

---

20 Si allude a CGUE, Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, 3 ottobre 2019.

21 Possiamo comunque ricordare alcune recenti pronunzie in linea con l'approccio ispirato alla necessità del bilanciamento e che, a differenza di quelle di merito prima richiamate, possono fondarsi direttamente sulla citata norma dell'art. 17 GDPR: Cass. 27 marzo 2020, n. 7559, e Cass. 19 maggio 2020, n. 9147.

22 Il riferimento è a Cass., S.U., 22 luglio 2019, 19681, in *Foro italiano*, 2019, 10, I, 3071. Si vedano al riguardo anche i commenti di V. Cuffaro, *Una decisione assennata sul diritto all'oblio*, in *Corriere giuridico*, 2019, 10, p. 1189, e di M. Mezzanotte, *Il diritto all'oblio secondo le Sezioni unite: cerbero o chimera?*, in *Giurisprudenza Costituzionale*, 2020, 1, p. 349 ss.

libertà informativa[23].

L'osservazione critica ci serve però soprattutto per ribadire come i limiti da contrapporre al diritto all'oblio avrebbero invero fondamentali radici anche al livello apicale dell'ordinamento interno, e che i ricordati sviluppi europei ne consentono la riscoperta più che l'invenzione. Ci sembra insomma fondamentale evitare che il nuovo (ma in realtà nuove sono piuttosto le tecnologie cui oggi lo riferiamo) diritto all'oblio finisca per pregiudicarne altri, forse da più tempo radicati nella tradizione liberale, come appunto la libertà dell'informazione e della scienza, ma non per questo meno importanti, dato che della stessa sono stati anzi fondativi. Oltretutto sul piano della costruzione di nuovi diritti non ci sembrerebbe affatto peregrino collocare specularmente al "*right to be forgotten*" anche un vero e proprio diritto alla memoria storica[24], comparabile a quello già ricordato alla memoria

---

[23] Com'è noto, il limite del buon costume, previsto per la generica manifestazione del pensiero dall'art. 21 Cost., non vale invece per l'arte e per la scienza ai sensi dell'art. 33 Cost.

[24] Nella recente esperienza di molti ordinamenti non mancano leggi sulla memoria, cui non sembrerebbe azzardato attribuire non solo il rilievo amministrativo che attiene all'organizzazione di eventi commemorativi, ma anche una valenza personalistica, che si sostanzi nel riconoscimento in capo agli interessati, i superstiti ed i loro discendenti, di un diritto alla memoria, tale da rappresentare una forma di compensazione che, rovesciando i passati tentativi di imporre l'oblio su queste vicende, surroghi o si affianchi a quelle di carattere risarcitorio, che nella gran parte dei casi sono difficilmente praticabili, o comunque tardive e sempre inadeguate rispetto alla gravità del torto subito. Per la legislazione italiana si vedano: la l. 20 luglio 2000, n. 211, che ha istituito il Giorno della Memoria della *Shoah*; la l. 30 marzo 2004, n. 92, che ha istituito il Giorno del Ricordo delle Foibe e dell'Esodo; la l. 4 maggio 2007, n. 56, che ha istituito una Giornata della Memoria delle Vittime del Terrorismo; la l. 21 marzo 2016, n. 45, che ha istituito la Giornata Nazionale in Memoria delle Vittime dell'Immigrazione; la l. 8 marzo 2017, n. 20, che ha istituito la Giornata Nazionale in Memoria delle Vittime della Mafia. Quanto ad esperienze di altri Paesi si possono considerare: i numerosi riconoscimenti giuridici della memoria della *Shoah* nella maggior parte dei Paesi del mondo (per tutti, si veda la risoluzione dell'Assemblea Generale delle Nazioni Unite del 1° novembre 2005, n. 60/7); quello relativo allo *Holodomor* sovietico (risoluzione del Parlamento Europeo del 23 ottobre 2008) e ad altri crimini del Comunismo (risoluzione del Parlamento Europeo del 19 settembre 2019); quelli, spesso tuttora fonti di tensioni internazionali con la Turchia, relativamente al *Medz Yeghern* armeno (ad esempio, la *loi 29 janvier 2001, n. 70*, in Francia, e la risoluzione del *Bundestag* del 2 giugno 2016, in Germania) ed alle meno note coeve vicende del *Seyfo* assiro e della *Katastrophè* grecoasiatica (su entrambe la mozione del *Riksdag* svedese dell'11 marzo 2010); gli ancora isolati riconoscimenti, da parte di Paesi oggi in aperto conflitto con la Russia, del *Sürgünlik* dei tatari crimeani (risoluzione della

identitaria personale, ed in fondo consistente per l'appunto in un diritto alla ricerca della verità, di quel concetto cioè che gli antichi esprimevano, com'è ben noto, proprio come la negazione dell'oblio[25].

Rada ucraina del 12 novembre 2015) e della pulizia etnica del popolo circasso (risoluzione del Parlamento georgiano del 21 maggio 2011); la sostituzione in numerosi Stati americani delle celebrazioni in onore di Colombo con altre dedicate invece alla memoria del genocidio degli amerindi (ad esempio, con il decreto 10 ottobre 2002, n. 2028, nel Venezuela chavista). Non di rado queste vicende si inseriscono in vere e proprie "guerre delle memoria", con riconoscimenti contrapposti: in Francia abbiamo ad esempio sia la *loi 21 mai 2001, n. 434*, sulla memoria della Tratta degli Schiavi come crimine contro l'umanità, sia la *loi 23 février 2005, n. 158*, sulla memoria del ruolo positivo della presenza francese oltremare. In altri casi è invece la riconciliazione nazionale che passa proprio da uno scambio fra la rinunzia ad ogni pretesa punitiva e la promozione di meccanismi istituzionali volti a far piena luce sul passato ed a mantenerne vivo il ricordo, come nella ben nota vicenda della *Truth and Reconciliation Commission* istituita in Sudafrica da Mandela, e che trova vari paragoni anche in ulteriori Paesi, sebbene non certo nel nostro. Nella letteratura non solo giuridica si possono vedere, da differenti prospettive, P.B. Hayner, *Unspeakable Truths: Facing Challenge of Truth Commissions*, New York, 2010; D. Rieff, *In Praise of Forgetting: Historical Memory and Its Ironies*, New Haven 2016; E. Sjöberg, *The Making of the Greek Genocide: Contested Memories of the Ottoman Greek Catastrophe*, New York 2017; M. Bianca (ed.), *Memoria versus oblio*, Torino, 2019; V. Pisanty, *I guardiani della memoria e il ritorno delle destre xenofobe*, Firenze-Milano, 2020; M. Flores, *Cattiva memoria. Perché è difficile fare i conti con la storia*, Bologna 2020; P. Caroli, *Il potere di non punire. Uno studio sull'amnistia Togliatti*, Napoli, 2020; P. Mieli, *La terapia dell'oblio. Contro gli eccessi della memoria*, Milano, 2020.

[25] Basterà ricordare che verità in greco è *ἀλήθεια* da alfa privativo più *Λήθη*, la personificazione dell'oblio (una delle temibili figlie di Eris, e quindi nipoti della nera Notte a sua volta figlia del Caos, secondo Esiodo, *Teogonia*, vv. 225-226), ma anche che la contrapposta personificazione della memoria è *Μνημοσύνη* (cfr. G. Pugliese Carratelli, *Tra Cadmo e Orfeo. Contributi alla storia civile e religiosa dei Greci d'Occidente*, Bologna, 1990, p. 410), che è madre delle Muse (*Μοῦσαι* da *Μόνσαι* con la medesima radice *μεν-μαν* del nome della loro madre e di parole latine quali *mens* o *meminisse*), e quindi anche di Clio, la Musa della storia (Esiodo, *Teogonia*, vv. 53-79). Nella letteratura contemporanea si vedano F. D'Agostini, M. Ferrera, *La verità al potere. Sei diritti aletici*, Torino, 2019, ma anche e soprattutto M. Kundera, *Il libro del riso e dell'oblio*, trad. it., Milano, 2000, p. 14, dove fa dire ad un personaggio che "*la lotta dell'uomo contro il potere è la lotta della memoria contro l'oblio*".

14. Regole di trasparenza e rapporti tra imprese nei mercati digitali: il Regolamento (UE) 2019/1150 sull'intermediazione *online* e i motori di ricerca

Federico Ruggeri

14.1. Economia delle piattaforme ed esigenze regolatorie

Nei più diversi contesti delle vendite a distanza, l'affermazione del ruolo degli intermediari della rete è un dato che può ormai dirsi acquisito. Il numero di imprese che scelgono di rivolgersi a un modello di *business* incentrato su piattaforme digitali è notevolmente aumentato negli ultimi anni e il fenomeno non sembra affatto destinato ad arrestarsi[1].

Non è dunque un caso che, oggi, il riferimento alla c.d. economia delle piattaforme sia globalmente diffuso nella letteratura come nel linguaggio dei legislatori, proprio a riconoscerne il ruolo centrale e strategico per lo sviluppo dell'impresa, oltre che del sistema economico nel suo complesso. In particolare per la capacità delle piattaforme di connettere le parti di un contratto per l'acquisto di un bene o per la prestazione di un servizio, fungendo allo stesso tempo quale luogo

[1] C. Busch, H. Schulte-Nölke, A. Wiewiórowska-Domagalska, F. Zoll, *The Rise of the Platform Economy: A New Challenge for EU Consumer Law?*, in *EuCML*, 1, 2016, p. 3.

(virtuale)[2] e soggetto (reale) che permette l'incontro delle rispettive volontà[3]. Con elementi di utilità per entrambe le categorie di utenti coinvolte nello scambio commerciale[4], in forza dei quali le ragioni sottostanti il successo dei modelli di digitalizzazione delle vendite trovano una spiegazione ragionevole sotto il profilo economico: la riduzione dei costi di transazione. Da un lato, infatti, l'utente-consumatore beneficia dell'esistenza di un'unica vetrina *online* che propone una varietà di prodotti – almeno in potenza – incredibilmente ampia, di cui è comodamente possibile confrontare caratteristiche e prezzi, nonché acquisire informazioni da parte di quei precedenti acquirenti che ivi abbiano altresì condiviso la propria, personale, esperienza di consumo, attraverso una valutazione o una recensione dei beni o servizi acquistati. Dall'altro, il posizionamento di un'impresa all'interno di una piazza virtuale crea nuove opportunità di vendita, in quanto consente di raggiungere un pubblico altrimenti difficilmente accessibile, almeno nella stessa ampiezza, tanto *offline* quanto attraverso un canale privato sul *web*[5]. E in questo modo trova compimento quell'effetto c.d. di rete in base al quale l'incremento della domanda dei servizi di intermediazione *online* da parte degli utenti-consumatori accresce il valore di mercato e reputazionale della piattaforma, coinvolgendo di riflesso un numero crescente di utenti-venditori, e viceversa. Un aumento diret-

---

2 Sulle peculiarità delle reti telematiche come spazi «svuota[ti] di *storicità* e *territorialità*», si veda già N. Irti, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, 2, 1998, pp. 347 ss.

3 M. Cantero Gamito, *Regulation.com. Self-Regulation and Contract Governance in the Platform Economy: A Research Agenda*, in *EJLS*, 2017, p. 55. Per un inquadramento del modello di mercato delle piattaforme digitali, si veda M. Colangelo, V. Zeno-Zencovich, *La intermediazione* on-line *e la disciplina della concorrenza: i servizi di viaggio, soggiorno e svago*, in questa *Rivista*, 1, 2015, pp. 43 ss.

4 Con riferimento agli scambi del commercio elettronico, si richiamano, in particolare, R. Clarizia, *Informatica e conclusione del contratto*, Giuffrè, Milano, 1985; G. Finocchiaro, *I contratti informatici*, in F. Galgano (diretto da), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, vol. XXII, Cedam, Padova, 1997; C.M. Bianca, *I contratti digitali*, in *Studium Iuris*, 1998, pp. 1035 ss.; F. Delfini, *Contratto telematico e commercio elettronico*, Giuffrè, Milano, 2002; E. Tosi, *Il contratto virtuale. Procedimenti formativi e forme negoziali tra tipicità e atipicità*, Giuffrè, Milano, 2005.

5 C. Busch, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, in A. De Franceschi, R. Schulze (a cura di), *Digital Revolution – New Challenges for Law*, C.H. Beck, Monaco, 2019, p. 58.

tamente proporzionale, in sostanza, cui consegue per ciascuna categoria di utenti il beneficio della contestuale presenza di propri pari nel medesimo spazio della rete, utile a trasmettere quella fiducia necessaria ad incentivarne, a monte, l'approdo stesso ai mercati digitali. Ma di cui è in realtà il titolare della piattaforma a trarre il maggior vantaggio[6], soprattutto in termini di dipendenza: dei consumatori, tendenzialmente portati a preferire mercati diffusamente conosciuti e capaci di soddisfare le più svariate esigenze di consumo; e dei venditori, rispetto a quella piattaforma che sia divenuta lo strumento principale per la conclusione dei propri affari.

Con riferimento a questi ultimi, si è di recente assistito a un significativo intervento normativo ad opera del legislatore europeo, orientato all'innovazione e al ravvicinamento del diritto privato degli Stati membri[7].

A fronte di un'avanzata disciplina in materia di contratti dei consumatori[8], la posizione dei soggetti di *business* era in effetti rimasta estranea, ancora negli ultimi anni, alle attenzioni del regolatore del mercato unico. Sicché la condizione di *platform dependency* evolveva come per natura nell'approfittamento del proprio ruolo di parte forte di un rapporto evidentemente asimmetrico, attraverso comportamenti

---

6 B. MARTENS, *An Economic Policy Perspective on Online Platforms*, in *JRC Working Papers on Digital Economy*, 2016, p. 10.

7 G. CAPALDO, *Armonizzazione della disciplina del contratto e attività della Commissione europea*, in G. VETTORI (a cura di), *Codice del consumo. Commentario*, Cedam, Padova, 2007, p. 619, evidenzia in particolare quanto la definizione di un apparato comune di regole in materia contrattuale sia di primaria importanza per la progressiva costruzione del mercato unico. Doveroso il richiamo all'insegnamento di G. BENEDETTI, *La categoria generale del contratto*, in *Il diritto comune dei contratti e degli atti unilaterali tra vivi a contenuto patrimoniale*, Jovene, Napoli, 1997, pp. 104 ss., che, nell'affermare il valore euristico della categoria generale del contratto in funzione di politica del diritto ed epistemologica, sostiene convintamente l'opportunità di tendere ad una disciplina uniforme.

8 Si vedano, in particolare, V. ZENO-ZENCOVICH, *La tutela del consumatore nel commercio elettronico*, in questa *Rivista*, 3, 2000, pp. 447 ss.; F. BRAVO, A.M. GAMBINO, F. TOZZI, *I contratti telematici e il commercio elettronico*, in G. ALPA (a cura di), *I diritti dei consumatori*, Giappichelli, Torino, 2009, pp. 599 ss.; S. SICA, A.G. PARISI, *La tutela del consumatore nel contratto* online, in A.M. GAMBINO (a cura di), *Rimedi e tecniche di protezione del consumatore*, Giappichelli, Torino, 2011, pp. 29 ss.; E. BATTELLI, *Riflessioni sui procedimenti di formazione dei contratti telematici e sulla sottoscrizione* online *delle clausole vessatorie*, in *Rass. dir. civ.*, 4, 2014, pp. 1035 ss.; M.P. PIGNALOSA, *Contratti a distanza e recesso del consumatore*, Giuffrè, Milano, 2016.

unilaterali, imprevedibili, iniqui. Si pensi in particolare alla modifica senza preavviso delle condizioni contrattuali; alla cancellazione di beni o servizi dalle vetrine virtuali; all'improvvisa sospensione o eliminazione di un *account*; alla mancanza di trasparenza nelle regole di determinazione del posizionamento o di accesso ai dati; alla previsione di clausole che proibiscono la vendita di beni e servizi su altri canali distributivi e a prezzi più bassi; nonché alla concorrenza praticata direttamente dai fornitori di quei servizi di intermediazione che consentono di accedere a un mercato digitale. Rischi, questi, tutt'altro che eventuali nelle dinamiche della rete, che le imprese si trovano a fronteggiare ormai da tempo, pur in mancanza di strumenti adeguatamente efficaci[9].

In tale contesto si colloca dunque il nuovo Regolamento (UE) 2019/1150 (di seguito, il Regolamento)[10], che rappresenta in definitiva il primo tentativo di regolazione dei rapporti commerciali tra imprese e piattaforme digitali, nonché il frutto di un lungo *iter* di lavoro condotto in seno alle istituzioni europee[11].

Si tratta, a volerne anticipare le principali caratteristiche, di un intervento legislativo fortemente innovativo, che mira alla creazione di un sistema degli scambi commerciali fondato su criteri di equità, prevedibilità, sostenibilità e sicurezza, per la prima volta rivolgendosi non ai consumatori, ma alle imprese quali nuovi soggetti deboli nell'economia delle piattaforme. Con il fine ultimo di garantire il corretto ed efficiente funzionamento del mercato interno nel suo complesso[12], e

---

9 Esaustivo sul punto il documento redatto da Ecorys per la Commissione europea "Business-to-Business relations in the online platform environment" nel 2017.

10 Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione *online*.

11 Già nella Comunicazione COM(2015) 192 def. "Strategia per il mercato unico digitale in Europa" e, a seguire, in quella COM(2016) 288 def. "Le piattaforme *online* e il mercato unico digitale. Opportunità e sfide per l'Europa" la Commissione europea manifestava l'urgenza di un intervento regolatorio delle piattaforme digitali, in considerazione del loro crescente potere di mercato e contrattuale verso i propri clienti e, in particolare, nei confronti delle piccole e medie imprese (PMI).

12 Allo stesso modo della disciplina a tutela del consumatore. Cfr. sul punto, A. Gentili, *La «nullità di protezione»*, in *Eur. dir. priv.*, 1, 2011, pp. 77 ss., che sostiene come in questo contesto si miri all'efficienza e alla «giustezza» del contratto non solo a livello individuale, ma, più ampiamente, a livello di mercato.

dunque, di riflesso, anche a tutela dei destinatari finali delle offerte di consumo[13]; nonché di impedire un'eventuale frammentazione normativa tra gli Stati membri nella disciplina di un settore tanto rilevante oltre che in continuo sviluppo.

14.2. L'ambito di applicazione

Come specificato dall'art. 1, § 2, del Regolamento, la nuova normativa di derivazione europea è rivolta ai c.d. servizi di intermediazione *online* e ai motori di ricerca *online*.

Per questi ultimi possono comprensibilmente intendersi quei servizi digitali che consentono agli utenti di formulare domande al fine di effettuare ricerche (es. Google o Bing)[14], in particolare su siti *web* e applicazioni di offerta di beni e servizi ai consumatori. Il riferimento ai servizi di intermediazione appare invero più articolato in quanto concerne «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»[15], che faciliti gli utenti commerciali[16] nell'offerta di beni e servizi ai consumatori e che costituisca l'oggetto del contratto concluso da tali utenti commerciali con il fornitore dei servizi di rete. Relazione negoziale, questa, del tutto distinta e indipendente da quella che lega la piattaforma e i consumatori-utenti della stessa, sulla quale

---

13 La crescita del numero di imprese attive nei mercati digitali, attesa in seguito all'implementazione di un sistema fondato sui principi di fiducia, prevedibilità e certezza del diritto, dovrebbe influire positivamente sulla concorrenza e incrementare, la qualità dell'offerta di beni e servizi ai consumatori, anche a prezzi inferiori (Commissione europea, MEMO/18/3373).

14 Il Considerando 13 del Regolamento pone l'accento sulla neutralità di tale definizione sotto il profilo tecnologico, in particolare alla luce della rapidità con cui lo sviluppo tecnologico introduce nel mercato innovativi strumenti di fruizione dei servizi di intermediazione. Il riferimento espresso è dunque alle c.d. richieste vocali (si pensi ai dispositivi Google Home), ma non può escludersi che in un prossimo futuro saranno altresì disponibili nuove tecnologie, ad esempio di realtà aumentata, comunque riconducibili all'ampia categoria individuata dal Regolamento.

15 Art. 1, § 1, lett. b), della Direttiva (UE) 2015/1535.

16 L'"utente commerciale" è definito come «un privato che agisce nell'ambito delle proprie attività commerciali o professionali o una persona giuridica che offre beni o servizi ai consumatori tramite servizi di intermediazione online per fini legati alla sua attività commerciale, imprenditoriale, artigianale o professionale» (art. 2, n. 1), del Regolamento).

trova peraltro concretamente luogo l'offerta – e l'acquisto – dei beni e dei servizi proposti dagli utenti commerciali.

I fornitori dei servizi di intermediazione *online* ai sensi del Regolamento si individuano dunque innanzitutto nei mercati del commercio elettronico[17], i c.d. *online marketplace*, di cui Amazon costituisce indubbiamente l'esempio più noto. Ma anche nei portali di prenotazione alberghiera o di vendita di pacchetti turistici (es. Booking o Expedia); negli *store* di applicazioni digitali, ovvero, su tutti, Google Play e App Store; nonché nei *social network* le cui funzioni permettono lo svolgimento di attività di offerta di beni e servizi, come il *marketplace* di Facebook o l'opzione "*shopping*" di Instagram, o nei siti di comparazione di prezzi e proposte (es. Skyscanner, Tripadvisor o Trivago).

In generale, la loro individuazione appare peraltro prescindere dall'eventualità sia che il consumatore che fruisce delle relative piattaforme di acquisto esegua pagamenti in denaro, sia che le transazioni ivi realizzate siano concluse anche parzialmente *offline*. Inoltre, in applicazione del principio di neutralità della rete, è irrilevante quale sia la tecnologia impiegata per la fornitura dei servizi di intermediazione, potendovi rientrare anche i più moderni dispositivi di assistenza vocale. Ma non anche i servizi di pagamento *online* (es. Paypal), considerati al più quali servizi ausiliari per la fornitura di beni e servizi e, pertanto, esclusi; così come gli strumenti e gli scambi di pubblicità *online* (es. DoubleClick) «che non sono forniti con l'obiettivo di agevolare l'avvio di transazioni dirette e che non implicano una relazione contrattuale coi consumatori»[18]; nonché, di regola, le piattaforme digitali di intermediazione tra pari (c.d. *peer-to-peer*)[19] e i servizi rivolti alle sole

---

17 G. Pica, (voce) *Commercio telematico*, in *Dig. disc. priv. (sez. civ.)*, *Agg.*, II, Utet, Torino 2003, suggerisce invero l'utilizzo del termine "commercio telematico", in quanto «lo strumento immediato di trasmissione delle informazioni e delle rispettive volontà delle parti è la telematica, ed è la dimensione telematica a rappresentare lo «spazio» tecnologico entro cui si attuano i rapporti intersoggettivi di commercio; l'elettronica rappresenta piuttosto la sottostante tecnologia di gestione delle forze elettriche che si utilizzano nell'informatica e nella telematica».

18 Art. 1, § 3, del Regolamento.

19 Si noti tuttavia che applicare tale esclusione in modo generalizzato e acritico rappresenterebbe un abbaglio, occorrendo considerare come molte piattaforme *peer-to-peer* siano potenzialmente idonee ad essere ricondotte alla nozione di intermediario descritta dal Regolamento. In questo senso, Airbnb costituisce certamente un esempio di piattaforma che, seppur proponendosi quale strumento di intermediazione tra pari, di frequente si presta a funzionare in presenza di situazioni di asimmetria tra

relazioni tra aziende, in considerazione del mancato coinvolgimento finale dei consumatori.

In ogni caso, l'efficacia del Regolamento presenta una portata sostanzialmente globale, non rilevando in alcun modo quale sia il luogo di stabilimento o di residenza del fornitore dei servizi di intermediazione o dei motori di ricerca *online*, né quale sia il diritto altrimenti applicabile, purché (i) i relativi utenti abbiano sede in uno Stato membro e (ii) i consumatori cui l'offerta di beni o servizi è rivolta si trovino nel territorio dell'Unione europea[20]. Condizioni, queste ultime, da intendersi in senso cumulativo e che, ove rispettate, permettono di estendere l'applicazione della normativa europea oltre i confini del mercato unico, peraltro coerentemente al fenomeno della fornitura di servizi digitali che, per sua natura, appare inadatto ad essere relegato entro determinati limiti spaziali.

14.3. I termini e le condizioni: definizione e mutamento

L'art. 3 del Regolamento definisce i requisiti di trasparenza sulla cui base un fornitore di servizi di intermediazione *online* è chiamato a determinare i termini e le condizioni dello schema contrattuale cui gli utenti commerciali interessati si limiteranno ad aderire.

È infatti il fornitore che, almeno di regola, si occupa di predefinirne unilateralmente la struttura e il contenuto. E in ciò si spiega l'esigenza, avvertita dal legislatore europeo anche in un'ottica di (auspicabile) uniformazione, di individuare alcuni specifici elementi di garanzia della posizione degli utenti commerciali, che in questo contesto rappresentano la parte debole del rapporto contrattuale. Con l'obiettivo, dunque, di applicare tali requisiti in modo quanto più efficace ed estensivo possibile, si prevede che la determinazione circa l'unilatera-

l'utente-fornitore del servizio e l'utente-fruitore dello stesso; in particolare in tutti quei casi in cui l'offerta a breve termine di un alloggio acquista i connotati di un'attività a carattere professionale e non (più) meramente occasionale. Appare a tal fine possibile richiamare la figura del c.d. *prosumer*, ovvero di quel consumatore che ricopre al tempo stesso il ruolo di produttore di beni o fornitore di servizi, su cui cfr. A. Quarta, *Il diritto dei consumatori ai tempi della* peer economy*. Prestatori di servizi e* prosumers*: primi spunti*, in *Eur. dir. priv.*, 2, 2017, pp. 667 ss.

[20] Il Considerando 9 del Regolamento specifica come non sia necessario, ai fini di tale valutazione, che essi risiedano in uno Stato membro né che ne abbiano la cittadinanza.

lità della definizione dei termini e delle condizioni debba essere effettuata caso per caso, in base a una valutazione complessiva, che non tenga esclusivamente conto della dimensione delle parti interessate o dell'eventualità che si sia svolta una qualsiasi forma, anche soltanto parziale, di negoziazione.

Il primo requisito richiesto dal Regolamento consiste nella redazione dei termini e delle condizioni in un linguaggio semplice e comprensibile, dovendosi in ogni caso evitare l'utilizzo di frasi o parole fuorvianti, vaghe e non dettagliate[21]. Tale garanzia di accessibilità al testo, utile ad assicurare un ragionevole grado di prevedibilità sugli aspetti più importanti della relazione contrattuale, costituisce invero una pregevole innovazione nell'ambito della regolazione dei rapporti tra imprese a livello europeo, essendo stata finora impiegata nella sola dimensione consumeristica[22].

Termini e condizioni devono poi essere facilmente reperibili per gli utenti commerciali, già nel corso della fase precontrattuale[23]. Al fine di poterne ragionevolmente prevedere l'applicazione, essi devono altresì specificare in modo chiaro le ragioni giustificative di un'eventuale decisione del fornitore di sospendere, cessare o limitare, anche solo parzialmente, la prestazione dei servizi di intermediazione. Ancora, devono indicare i potenziali canali aggiuntivi di distribuzione e programmi affiliati di cui il fornitore potrebbe avvalersi per commercializzare i beni e i servizi offerti dagli utenti commerciali[24], così da

---

21 Si noti d'altra parte la mancanza di un'apposita indicazione dedicata alla lingua di elaborazione del testo contrattuale, in ciò avendo verosimilmente prevalso, dal punto di vista del legislatore europeo, l'intenzione di evitare un eccessivo, e probabilmente sproporzionato, aggravio delle prestazioni cui il fornitore è tenuto ad adempiere. Una particolare attenzione alla necessaria conoscenza della lingua di redazione dei termini e delle condizioni contrattuali trova invece espresso riscontro con riferimento ai requisiti di nomina dei mediatori *ex* art. 12, § 2, lett. c), del Regolamento.

22 In tema, si rinvia *ex multis* a E. Battelli, Interpretatio contra proferentem *e trasparenza contrattuale*, in *Contr. impr.*, 1, 2017, pp. 194 ss.

23 In termini generali su tali questioni si richiamano gli studi di C. Scognamiglio, *Principi generali e disciplina speciale nell'interpretazione dei contratti dei consumatori*, in *Riv. dir. comm.*, I, 1997, pp. 947 ss.; A. Genovese, *L'interpretazione dei contratti standard*, Giuffrè, Milano, 2008, pp. 157 ss.

24 Da intendersi in modo neutro da un punto di vista tecnologico e che potrebbero includere, ad esempio, altri siti *web* o altre applicazioni digitali da cui i consumatori possano acquistare i beni o i servizi offerti dagli utenti commerciali.

individuare possibili luoghi e destinatari di una stessa offerta. Da ultimo, si richiede che vi siano altresì incluse le informazioni necessarie a definire i margini e i limiti di incidenza del vincolo contrattuale sulla titolarità e sul controllo dei diritti di proprietà intellettuale vantati dagli utenti commerciali, ad esempio con riferimento all'utilizzo di loghi, marchi o denominazioni commerciali.

Ai cinque requisiti generali di trasparenza appena richiamati occorre accostare gli ulteriori tre di cui al successivo art. 8, rubricato "Clausole contrattuali specifiche", che avrebbero l'espressa funzione di assicurare «che le relazioni contrattuali tra i fornitori di servizi di intermediazione *online* e gli utenti commerciali siano condotte in buona fede e con correttezza». In particolare, la necessità di garantire prevedibilità e trasparenza dell'agire dei fornitori importa che questi non possano imporre modifiche dei termini e delle condizioni aventi effetto retroattivo, se non quando discendano dall'esigenza di adeguarsi a un obbligo normativo o regolamentare ovvero laddove attribuiscano un vantaggio agli utenti commerciali. E, ancora, che vengano indicate le informazioni necessarie a conoscere delle condizioni di risoluzione del contratto, le quali debbono risultare proporzionate e non indebitamente difficili da attuare; nonché dei contenuti di carattere informativo, forniti o generati da un utente commerciale nell'utilizzo dei servizi di intermediazione *online*, che il fornitore intenda conservare cessato il rapporto contrattuale per poter eventualmente continuare ad avervi accesso.

Il mancato adeguamento dei termini e delle condizioni ai requisiti generali imposti dalla normativa ora in vigore ne comporta la nullità, anche solamente parziale, come disciplinato dall'art. 3, § 3, del Regolamento[25]. Forma di invalidità, questa, che non sembra tuttavia poter trovare applicazione rispetto alle previsioni dell'art. 8. E la mancanza di un espresso riferimento in tal senso lascia dunque aperta la risposta

[25] Il Considerando 20 del Regolamento precisa che «i termini e le condizioni non conformi dovrebbero essere nulli, vale a dire che si dovrebbero considerare come mai esistiti, con effetti *erga omnes* ed *ex tunc*. Ciò dovrebbe tuttavia riguardare solo le disposizioni specifiche dei termini e delle condizioni che non sono conformi. Le disposizioni rimanenti dovrebbero restare valide e applicabili, nella misura in cui possono essere dissociate da quelle non conformi».

sulla reale volontà del legislatore europeo di incidere sulla validità del contratto[26].

D'altra parte, lo stesso art. 3, § 3, del Regolamento estende invece la sanzione della nullità alle modifiche dei termini e delle condizioni che non intervengano in conformità a quanto previsto dal secondo paragrafo di tale articolo. Coerentemente all'obbligo di assicurare che il contratto sia facilmente reperibile in ogni fase del rapporto commerciale, si richiede innanzitutto che qualsiasi variazione del testo negoziale che non sia meramente redazionale, ma che ne alteri il contenuto o il significato, sia previamente notificata agli utenti commerciali tramite un supporto durevole e con un preavviso di non meno di quindici giorni e il cui termine risulti ragionevole e proporzionato alle circostanze del caso concreto. In ciò rilevando la natura e la portata delle modifiche, nonché la loro incidenza sulle attività degli utenti commerciali. In particolare, la concessione di un tempo superiore a quindici giorni apparirebbe dunque indispensabile in tutti quei casi in cui le modifiche proposte dai fornitori dei servizi di intermediazione *online* imponessero agli utenti commerciali di effettuare degli adeguamenti di tipo tecnico o commerciale – ad esempio con riferimento all'accesso alla piattaforma digitale o ai beni o servizi tramite essa offerti – necessari per una conveniente prosecuzione del rapporto contrattuale.

Anche in tal senso si comprende allora la ragione per cui, al momento della notificazione della proposta di modifica, è previsto che sorga in capo all'utente commerciale il diritto di risolvere il contratto entro i successivi quindici giorni, purché non trovi applicazione un termine inferiore, come eventualmente disposto dal diritto civile nazionale.

Gli utenti commerciali possono peraltro decidere di rinunciare al termine di preavviso tanto in modo espresso, mediante una dichiarazione scritta, quanto implicitamente attraverso un comportamento inequivocabile, ad esempio ravvisabile nell'offerta di nuovi beni o servizi sulla piattaforma del fornitore. Ciò, tuttavia, a patto che il termine in questione non ecceda i quindici giorni, in tal caso presumendosi che il compimento di una qualsiasi azione positiva di fruizione dei servizi di intermediazione sia meramente funzionale ad evitare un'interruzione

---

[26] Si veda, *amplius*, A. Gentili, E. Battelli, *Le patologie del contratto telematico*, in E. Tosi (a cura di), *La tutela dei consumatori in internet e nel commercio elettronico*, Giuffrè, Milano, 2012, pp. 371 ss.

eccessivamente prolungata dell'attività commerciale svolta sul *market-place* e, in quanto tale, di per sé non idonea a configurare una forma di rinuncia tacita al preavviso.

Da ultimo, l'art. 3 del Regolamento prevede che, a prescindere da una manifestazione di volontà da parte dell'utente commerciale, il termine di preavviso non trovi applicazione laddove il fornitore dei servizi di intermediazione sia improvvisamente tenuto, in forza di un obbligo legale o regolamentare, ad implementare in tempi rapidi la modifica dei termini o delle condizioni contrattuali. Né qualora le modifiche siano eccezionalmente necessarie a fronteggiare «un pericolo imprevisto e imminente connesso alla difesa dei servizi di intermediazione *online*, dei suoi consumatori o di altri utenti commerciali da frodi, *malware*, *spam*, violazione dei dati o rischi per la sicurezza informatica» (art. 3, § 4, lett. b), del Regolamento).

14.4. I provvedimenti di limitazione, sospensione e cessazione dei servizi di intermediazione

Il legislatore europeo ha posto particolare attenzione alla prassi, alquanto diffusa nei contratti con le piattaforme digitali[27], di limitare, sospendere ovvero cessare definitivamente la fornitura dei servizi di intermediazione *online*. Pratiche, queste, generalmente attuabili in qualsiasi momento e a prescindere dalla sussistenza di un giustificato motivo, in forza di una corrispondente previsione contrattuale imposta in via unilaterale.

Se già si è detto del relativo obbligo di trasparenza previsto a tal fine, l'art. 4 del Regolamento determina alcuni requisiti procedurali che permettono la definizione di una più compiuta disciplina di tali specifiche vicende della relazione contrattuale.

In capo al fornitore la norma introduce infatti un vero e proprio dovere di motivazione della decisione di limitare, sospendere o cessare la prestazione dei propri servizi, da trasmettere all'utente commerciale interessato mediante un adeguato supporto durevole. A tal fine è pertanto chiamato a fare apposito riferimento ai fatti o alle circostanze su

---

[27] Cfr. il già richiamato documento "Business-to-Business relations in the online platform environment" (*supra* nt. 9).

cui la decisione si fonda, nonché, per verificarne la coerenza, alle ragioni descritte nel contratto ai sensi dell'art. 3, § 1, lett. c), del Regolamento.

In tal senso, non si vuole certamente negare che il fornitore possa vantare motivi ragionevoli a fondamento del proprio provvedimento – provvisorio o definitivo che sia –, ma risulta cruciale tutelare l'interesse dell'utente commerciale quale parte debole del rapporto a non essere arbitrariamente estromesso dall'utilizzo della piattaforma. Ciò soprattutto in considerazione delle conseguenze negative che da tale scelta possono facilmente discendere in ordine all'esercizio della propria attività commerciale, a garanzia della necessaria prevedibilità dell'agire della controparte.

Alla luce di quanto disposto dal terzo paragrafo dell'art. 4, la comunicazione delle suddette motivazioni costituirebbe inoltre il presupposto per l'avvio del procedimento interno di gestione dei reclami di cui all'art. 11 del Regolamento, volto ad una composizione amichevole della controversia. In questo contesto, all'utente commerciale deve infatti essere offerta l'opportunità di chiarire i fatti e le circostanze addotte a fondamento della decisione del fornitore, il quale potrebbe di conseguenza ritenere di reintegrarlo nell'utilizzo dei servizi della piattaforma, riconoscendo ad esempio di aver compiuto una valutazione sbagliata o, nel caso in cui il provvedimento derivasse da una violazione dei termini e delle condizioni da parte dell'utente commerciale, che quest'ultimo non fosse in mala fede e che vi abbia rimediato in un modo ritenuto soddisfacente.

Quanto al momento in cui provvedere alla trasmissione delle motivazioni, il Regolamento distingue sostanzialmente in base alla severità della sanzione. La decisione di limitare[28] o sospendere la fornitura dei servizi di intermediazione *online* utili all'offerta dei beni o dei servizi da parte di un utente commerciale viene dunque comunicata «preventivamente o al momento in cui la limitazione o la sospensione prende effetto» (art. 4, § 1, del Regolamento); mentre quella relativa alla completa cessazione dalla prestazione dei servizi di intermediazione *online*, cui consegue la soppressione dei dati forniti per l'utilizzo degli

[28] La limitazione appare per esempio realizzabile attraverso forme di oscuramento o di retrocessione nel posizionamento dei beni o dei servizi offerti da un determinato utente commerciale.

stessi da parte dell'utente commerciale coinvolto, richiede espressamente un preavviso di almeno trenta giorni. Tale determinazione si spiegherebbe proprio in ragione delle significative ripercussioni che la scelta del fornitore può avere non solo in relazione all'offerta di beni e servizi ai consumatori, ma anche sulla concreta capacità dell'utente commerciale di esercitare i diritti complessivamente riconosciuti dal Regolamento. La comunicazione deve pertanto garantire un margine di tempo minimo e certo, da rispettarsi necessariamente prima che la decisione del fornitore possa effettivamente spiegare i suoi effetti. Ciononostante, la norma prevede anche delle precise ipotesi in cui il termine non trova applicazione, ovvero: a) quando il fornitore è tenuto ad adempiere a un obbligo normativo o regolamentare che gli impone la cessazione della fornitura di tutti i suoi servizi nei confronti di un determinato utente commerciale, in modo tale da non permetterne il rispetto; b) quando la terminazione consegue all'esercizio del diritto di recesso a norma del diritto nazionale, purché sulla base delle circostanze del caso di specie e della valutazione degli interessi di entrambe le parti non emerga che possa ragionevolmente proseguirsi il rapporto contrattuale fino al termine convenuto o fino alla scadenza di un termine di preavviso; c) laddove il fornitore possa dimostrare una ripetuta violazione da parte dell'utente commerciale dei termini e delle condizioni contrattuali[29].

Si evince dunque come la cessazione completa della fornitura dei servizi di intermediazione rappresenti la decisione più severa che la piattaforma possa prendere nei confronti dell'utente commerciale, in ciò apparendo opportuno che tale scelta entri in gioco soltanto laddove non appaia utilmente possibile intervenire tramite provvedimenti meno rigorosi, in applicazione del principio di proporzionalità[30]. Un progressivo inasprimento, in sostanza, delle scelte in tal senso prati-

---

[29] In generale, il Considerando 23 del Regolamento prospetta che tali eccezioni possano rilevare «in particolare in relazione a contenuti illeciti o inappropriati, alla sicurezza di un bene o servizio, a contraffazioni, frodi, *malware*, *spam*, violazione di dati, altri rischi per la cibersicurezza o all'adeguatezza del bene o servizio per i minori».

[30] Sull'affermazione della proporzionalità quale principio generale del diritto europeo dei contratti, si veda C. CAUFFMAN, *The Principle of Proportionality and European Contract Law*, in J. RUTGERS, P. SIRENA (a cura di), *Rules and Principles in European Contract Law*, Intersentia, Cambridge, 2015, pp. 69 ss.

cate dai fornitori, affinché, se ragionevolmente e tecnicamente possibile, esse vengano in primo luogo dirette verso singole categorie di beni o servizi; e tendano a un esito più grave soltanto ove sia effettivamente inevitabile procedere altrimenti.

La disciplina così delineata per le ipotesi di limitazione, sospensione o cessazione dei servizi di intermediazione *online* non risponde tuttavia ad alcuni interrogativi tutt'altro che irrilevanti. E in particolare a quali siano le conseguenze dell'eventuale violazione dell'obbligo di motivazione; o del mancato rispetto delle regole di proporzionalità. L'art. 15, § 2, del Regolamento si limita invero a puntualizzare che a qualsiasi violazione dello stesso debbano far fronte le misure «efficaci, proporzionate e dissuasive» previste dai singoli ordinamenti nazionali. Appare dunque possibile ritenere che in questi casi il provvedimento del fornitore non possa che produrre meri effetti materiali, giuridicamente non rilevanti, e che l'utente commerciale possa piuttosto vantare un diritto al risarcimento del danno da responsabilità contrattuale, nel nostro ordinamento *ex* art. 1218 c.c.

14.5. I criteri di posizionamento

Il tema del posizionamento, spesso indicato anche con il termine inglese di *ranking*, dei beni e dei servizi offerti ai consumatori attraverso piattaforme digitali rappresenta un aspetto cruciale delle relazioni P2B (*Platform-to-Business*).

La disposizione di ciascun prodotto presente su un *marketplace* ha un'incidenza determinante nelle scelte di acquisto di ciascun utente-consumatore e, di riflesso, sul successo commerciale dell'utente-venditore di beni e servizi *online*. E lo stesso può dirsi anche dei siti *web* di vendita di beni o servizi, che appaiono sulle pagine dei motori di ricerca. In genere, gli utenti della rete tendono infatti a preferire, a parità di caratteristiche, i prodotti o i siti che trovano per primi, più in alto, più evidenti[31].

Ne discende evidentemente il forte interesse degli utenti commerciali ad evitare che tale aspetto del rapporto contrattuale con le piattaforme digitali sia trattato secondo criteri arbitrari, in quanto tali del

---

31 Cfr. C. Busch, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, *cit.*, p. 67.

tutto imprevedibili o incomprensibili. In questo senso, tuttavia, occorre pure rilevare che il posizionamento delle offerte degli utenti commerciali avviene di regola per il tramite di meccanismi algoritmici, il cui funzionamento potrebbe plausibilmente essere oggetto di segreto commerciale da parte del fornitore dei servizi di intermediazione.

Attraverso l'art. 5 del Regolamento il legislatore europeo è dunque intervenuto a disciplinare alcune regole in materia di *ranking* dei prodotti e dei siti *web*, seguendo una logica di bilanciamento tra interessi fondamentalmente contrapposti. Da un lato, quello degli utenti commerciali al rispetto dei principi di trasparenza e prevedibilità anche con riferimento al loro posizionamento sulle pagine di piattaforme e motori di ricerca; dall'altro, quello dei fornitori a mantenere segrete determinate informazioni di cui dispongono in modo esclusivo, caratterizzate perché non generalmente note ad altri e solo in quanto tali idonee ad attribuire al loro detentore uno specifico vantaggio economico[32].

In tal senso si prevede innanzitutto che i fornitori dei servizi di intermediazione *online* debbano indicare, tra i termini e le condizioni contrattuali, i principali parametri che determinano la formazione del *ranking* di quanto sia oggetto delle ricerche degli utenti della piattaforma, nonché, tra i diversi parametri individuati, i motivi della maggiore rilevanza, ovvero la c.d. importanza relativa, di alcuni rispetto ad altri. Non ogni parametro ha infatti pari valore nella determinazione del posizionamento di un prodotto ed è pertanto opportuno che gli utenti commerciali conoscano l'incidenza di ciascuno di essi nel relativo processo decisionale. Rilevano così fattori quali le caratteristiche dei beni o dei servizi offerti ai consumatori, ovvero la loro presentazione tanto nelle immagini quanto nelle parole.

Allo stesso modo, sorge in capo ai fornitori di motori di ricerca *online* il dovere di rendere facilmente e pubblicamente accessibile, attraverso un linguaggio semplice e comprensibile e regolari aggiornamenti, la descrizione dei criteri di ordinamento dei siti *web* risultanti

---

[32] Si tratta dei requisiti costitutivi dei segreti commerciali, indicati dall'art. 98 c.p.i. come da ultimo riformato dal d. lgs. 11 maggio 2018, n. 63 in recepimento della Direttiva *Trade Secrets*, su cui si veda C. GALLI, *L'attuazione italiana della Direttiva europea sui* Trade Secrets *tra continuità nella disciplina sostanziale e deviazioni rispetto al testo della Direttiva*, in *Contr. impr./Europa*, 1, 2018 pp. 25 ss., nonché, in particolare, M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, in *AIDA. Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 27, 2018, pp. 199 ss.

dalla ricerca in rete degli utenti-consumatori, nonché, anche in questo caso, l'importanza relativa di ognuno di essi[33]. In particolare, potrebbero rilevare a tal fine le caratteristiche grafiche del sito, ad esempio quelle relative alla visualizzazione dello stesso tramite dispositivi mobili, o dei beni o servizi tramite esso illustrati e offerti sul mercato.

I rispettivi fornitori dovrebbero altresì informare circa la possibilità – se prevista – per gli utenti commerciali e per i titolari dei siti Internet di influire sul risultato relativo al proprio posizionamento attraverso la corresponsione di un corrispettivo. Il quale può trovare esecuzione sia attraverso il pagamento di un prezzo per il solo o principale scopo di migliorare la propria posizione attuale, sia in forma indiretta, ad esempio accettando di sottostare a vincoli ulteriori come l'utilizzo di particolari servizi accessori proposti dal fornitore.

Si è già osservato come la chiarezza espositiva nell'adempimento di tali prescrizioni da parte dei fornitori costituisca un aspetto di cruciale importanza. Tale richiesta non si estende tuttavia, per espressa previsione del sesto paragrafo dell'art. 5, al punto di imporre loro di rivelare nel dettaglio il funzionamento degli algoritmi utilizzati per la determinazione del posizionamento. Si è anche detto, infatti, di come il proposito di assicurare un certo grado di prevedibilità dei comportamenti dei fornitori incontri un limite insuperabile proprio nella corrispondente tutela dei loro interessi commerciali, perciò riconoscendosi idonea al rispetto delle previsioni dell'art. 5 del Regolamento una descrizione generale dei parametri di posizionamento tale da consentire a utenti commerciali e titolari di siti *web* di comprendere i meccanismi di formazione del *ranking* e di confrontare le pratiche seguite dai diversi fornitori di servizi di intermediazione e motori di ricerca. E lo strumento attraverso cui operare tale bilanciamento viene dunque

---

[33] Il fatto che tra i fornitori dei motori di ricerca e gli utenti titolari dei siti *web* non intercorra un vincolo contrattuale determina che la descrizione in questione debba essere posta a disposizione del pubblico sullo stesso motore di ricerca, in modo da poterne agevolmente avere visione. Sul punto, il Considerando 26 del Regolamento evidenzia inoltre che laddove una modifica del *ranking* di un sito ovvero la sua rimozione dalle pagine del motore di ricerca consegua a una segnalazione proveniente da un soggetto terzo, il titolare del sito stesso debba avere la possibilità di analizzarne il contenuto su un'apposita banca dati *online* pubblicamente accessibile. Ciò si spiega evidentemente in funzione della necessità di proteggere l'interessato, da un lato, e dissuadere i terzi, dall'altro, da un potenziale abuso dello strumento delle segnalazioni.

espressamente individuato nella disciplina relativa alla tutela del segreto industriale, ormai armonizzata nell'intera Unione europea attraverso la Direttiva (UE) 2016/943[34], nonché alla luce degli orientamenti espressi dalla Commissione europea nelle apposite linee guida recentemente pubblicate[35].

14.6. Sul duplice ruolo delle piattaforme: dall'intermediazione alla concorrenza

Spesso i fornitori dei servizi di intermediazione *online* non si limitano ad eseguire la prestazione dovuta nei confronti della controparte contrattuale, ovvero gli utenti commerciali, ponendosi direttamente o tramite imprese collegate in concorrenza con essi. In particolare, offrendo beni e servizi ai consumatori tramite quegli stessi servizi che costituiscono oggetto del contratto con tutti gli utenti commerciali operativi sul proprio *marketplace*.

Tale generale consapevolezza ha spinto il legislatore europeo a regolare tramite l'imposizione di specifici obblighi di trasparenza l'eventualità che le piattaforme ricoprano questo duplice ruolo di prestatori di servizi e, al tempo stesso, di concorrenti del complesso degli utenti commerciali. Ciò in considerazione delle evidenti distorsioni che tale comportamento può ragionevolmente realizzare nel sistema della (leale) concorrenza tra i soggetti del mercato. Circostanza che sarebbe peraltro di difficile riconoscimento da parte dei consumatori, e perciò idonea a limitare la loro effettiva libertà di scelta nella ricerca e nell'acquisto di beni o servizi. Basti pensare al potere di controllo esercitato dalle piattaforme quali strumenti di raccolta e di elaborazione dei dati utili a profilare le preferenze dei consumatori, tanto singolarmente quanto nel loro complesso, ad esempio mettendo in evidenza i prodotti più acquistati in un certo periodo di tempo. Non apparendo in questo modo del tutto peregrina l'ipotesi che il fornitore dei servizi di intermediazione approfitti della posizione privilegiata in cui si trova per favorire la vendita dei propri prodotti, come di quelli di utenti

---

[34] Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio dell'8 giugno 2016 sulla protezione del *know-how* riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti.

[35] Comunicazione della Commissione (2020/C 424/01) "Orientamenti sulla trasparenza del posizionamento a norma del Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio" dell'8 dicembre 2020.

commerciali da esso stesso controllati, grazie a determinati vantaggi tecnici o economici per l'offerta di beni e servizi di contro negati agli utenti concorrenti[36].

L'art. 7 del Regolamento interviene dunque per prevenire tale scenario, a tutela non solo degli utenti commerciali che ne verrebbero coinvolti, ma del funzionamento del mercato nel suo complesso[37]. Al fornitore dei servizi di intermediazione *online* si impone così di agire secondo trasparenza, dovendo includere nei termini e nelle condizioni contrattuali un'apposita descrizione relativa agli eventuali trattamenti differenziati riservati o riservabili ai beni o ai servizi offerti ai consumatori sia in via diretta che attraverso utenti commerciali controllati. Misure particolari, di vantaggio per chi possa usufruirne, relative all'accesso a dati personali e non personali, ai criteri di posizionamento, all'uso di servizi, funzionalità o interfacce tecniche in rapporto di connessione o complementarietà con i servizi principali del fornitore, anche avverso il pagamento di un corrispettivo.

Nella stessa ottica, la norma prevede corrispondenti obblighi di trasparenza anche con riferimento ai fornitori di motori di ricerca *online*, per l'eventualità in cui si pongano in una posizione di concorrenza diretta o indiretta con i titolari dei siti *web* utenti dei loro servizi sulla rete.

Connessa alla (potenziale) duplice veste delle piattaforme di intermediazione è anche la previsione di cui all'art. 6 del Regolamento, rubricato "Prodotti e servizi accessori". Tale norma dispone infatti un ulteriore obbligo di trasparenza, relativo in questo caso a quei beni e servizi qualificabili, appunto, come accessori, ovvero il cui funzionamento o la cui esecuzione dipendono tipicamente da un altro specifico bene o servizio, cui sono direttamente collegati. Costituiscono oggetto

---

36 Si guardi ad esempio alle indagini avviate dalla Commissione europea nei confronti di Amazon, e in particolare ai procedimenti AT.40462 del 17 luglio 2019 e AT.40703 del 10 novembre 2020, per verificare l'effettiva sussistenza di trattamenti di favore per la vendita dei prodotti propri o di utenti commerciali controllati, in contrasto con la disciplina europea in materia di concorrenza *ex* artt. 101 e 102 TFUE.

37 Preme evidenziare come il Regolamento rappresenti complessivamente un nuovo strumento della più ampia strategia di regolazione predisposta dalla Commissione europea, che trova il proprio spazio accanto alla già esistente disciplina in materia di concorrenza, di per sé ritenuta ormai non sufficientemente adeguata a far fronte all'affermazione di un sistema di mercato *platform oriented* e di modelli di *business* fondati sull'utilizzo dei dati. Cfr. C. Busch, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, *cit.*, pp. 59-60.

di offerta al consumatore in quella fase immediatamente precedente il completamento della transazione relativa all'acquisto principale, a sua possibile, ma non indispensabile, integrazione. Tra i beni, per esempio, quelli utili ad aggiornare o a personalizzare uno specifico prodotto; tra i servizi, quello di riparazione di un bene o anche prodotti finanziari specifici come l'assicurazione per il noleggio di un'automobile da parte di un turista[38].

Resterebbero in sostanza esclusi da tale disciplina tutti quei beni o servizi venduti in aggiunta a quanto costituisca oggetto principale dell'acquisto, ma al contempo in mancanza di un qualsiasi elemento di complementarietà.

Ebbene, l'offerta di beni e servizi accessori è ammissibile in quanto i termini e le condizioni contrattuali contengano una descrizione riferita non solo alle loro caratteristiche, ma anche al soggetto concretamente deputato a provvedere in tal senso. Il quale potrebbe risultare lo stesso fornitore dei servizi di intermediazione *online*, come anche un soggetto terzo o – purché sia espressamente indicato a quali condizioni – un utente commerciale della piattaforma.

14.7. L'accesso ai dati

Il valore dei dati nell'economia delle piattaforme si individua come è noto nella conoscenza delle preferenze e dei consumi degli utenti

[38] Il comparto turistico risulta particolarmente interessato dall'offerta ai consumatori-viaggiatori di prestazioni accessorie integrative, come ad esempio l'acquisto di un biglietto aereo o di un soggiorno alberghiero, da ultimo avvalorato anche con la Direttiva (UE) 2015/2302 relativa ai pacchetti turistici e ai servizi turistici collegati. Si veda sul punto A. FINESSI, *La responsabilità del professionista nella nuova disciplina dei contratti di viaggio*, in *NLCC*, 6, 2018, pp. 1307 ss., che si sofferma peraltro sull'avvenuta attuazione della normativa europea con il d. lgs. 21 maggio 2018, n. 62. In materia di servizi turistici, già G. CAPALDO, *Commento* sub *artt. 82-84*, in G. VETTORI (a cura di), *Codice del consumo. Commentario*, *cit.*, pp. 687 ss. Per un approfondimento in tema di *ancillary revenues* tramite la prestazione di servizi accessori, cfr. V. IAIA, *La tutela della concorrenza nell'ambito del trasporto aereo: il caso Ryanair c. Lastminute*, in *Cammino diritto*, 9, 2020.

della rete, che al giorno d'oggi costituisce probabilmente la più importante fonte e il principale strumento per essere altamente competitivi sul mercato[39].

Il fatto che la prestazione di servizi di intermediazione *online* permetta di accumulare e controllare enormi quantità di informazioni non poteva dunque non essere oggetto di specifica attenzione da parte del legislatore europeo.

L'art. 9 del Regolamento richiede che i fornitori di tali servizi assicurino agli utenti commerciali una chiara descrizione circa la portata, la natura e le condizioni di accesso ai dati generati tramite la piattaforma, oltre che del loro utilizzo, da parte degli stessi contraenti ovvero di terzi[40]. Indicazioni, anche generiche, che siano utili a comprendere se e come sia possibile servirsi di tali informazioni per incrementare il livello di qualità della propria proposta commerciale nel suo complesso. Ma anche a sapere se il fornitore condivide i dati generati dagli utenti commerciali nell'utilizzo dei servizi di intermediazione con soggetti terzi, in particolar modo laddove ciò avvenga per scopi non inerenti al corretto funzionamento dei servizi di intermediazione. Dovendosi altresì indicare, in tale ultimo caso, lo scopo effettivo della condivisione e le possibilità a disposizione degli utenti commerciali per evitarla.

In generale, la norma interessa tutti quei dati, personali e non personali, generati o forniti da ogni utente della piattaforma, con riferimento a tutte le attività di offerta, ricerca o acquisto che su essa trovano compimento. Per esempio le valutazioni e le recensioni di clienti e acquirenti, indubbiamente utili per orientare l'andamento della propria attività commerciale[41]. Ma anche i loro contatti, indirizzo di posta elettronica o numero telefonico, indispensabili per instaurare un rapporto

---

39 Per una lettura del fenomeno dei dati secondo le categorie del diritto civile si veda, in particolare, V. Zeno-Zencovich, G. Giannone Codiglione, *Ten Legal Perspectives on the "Big Data Revolution"*, in *Conc. merc.*, 1, 2016, pp. 29 ss.

40 Ulteriore requisito di trasparenza contrattuale imposto dalla nuova disciplina europea, in quanto non si riconosce in capo agli utenti commerciali un più generale diritto di accesso ai dati. Cfr. C. Busch, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, *cit.*, p. 70.

41 Le valutazioni e le recensioni pubblicate in rete dai consumatori di un certo bene o servizio compongono il c.d. capitale reputazionale delle piattaforme digitali. Le prime si caratterizzano per l'indicazione di un punteggio sulla base della scala pro-

diretto, che non necessiti dell'intermediazione della piattaforma, così come per la promozione di nuove offerte di vendita o per altre comunicazioni necessarie alla prestazione di un servizio.

Appare quindi con evidenza come la possibilità di accedere a tali informazioni costituisca il fondamento di notevoli opportunità per l'attività commerciale del beneficiario; nonché come, di contro, la mancata autorizzazione ponga invece dei limiti probabilmente insormontabili e decisivi per il suo svolgimento. In ogni caso, la previsione di apposite misure di trasparenza a regolare un aspetto tanto delicato della relazione tra la piattaforma e i suoi utenti commerciali pare essenziale, anche nell'ottica di sostenere una maggiore condivisione dei dati, di informazioni che rappresentano una fonte inesauribile di innovazione e crescita del mercato nel suo complesso. Ciò, chiaramente, nei limiti del rispetto dell'esistente quadro normativo europeo in materia, costituito dal Regolamento (UE) 2016/679 [42], dalla Direttiva (UE) 2016/680[43] e dalla Direttiva 2002/58/CE[44], opportunamente richiamati dallo stesso art. 9 in commento.

posta dal *marketplace*; le seconde per la disponibilità di una casella di testo ove elaborare un proprio commento. Fattore che risulta particolarmente rilevante sotto il profilo della portabilità, ovvero del trasferimento in massa di tali informazioni da una piattaforma all'altra, su cui cfr. C. BUSCH, *Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, Intersentia, Cambridge, 2016, pp. 223-243. Per un'interessante riflessione in materia di sistemi reputazionali, si veda G. SMORTO, *Reputazione, fiducia e mercati*, in *Eur. dir. priv.*, 1, 2016, pp. 199 ss.

42 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

43 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

44 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche).

14.8. Le c.d. *parity clauses*

Ai sensi dell'art. 10 del Regolamento, qualsiasi limitazione alla capacità degli utenti commerciali di offrire beni e servizi tramite altri mezzi di distribuzione e a condizioni diverse rispetto a quelle previste sulla piattaforma di un fornitore di servizi di intermediazione *online*, deve essere espressamente indicata, motivata e resa facilmente accessibile al pubblico. Si tratta delle c.d. *parity clauses*, anche note come *best-price* o *most-favored-nation* (MFN) *clauses*, volte ad assicurarsi che la propria vetrina virtuale proponga prezzi almeno pari, se non anche inferiori, rispetto a quelli indicati da soggetti concorrenti[45]. Con quel che evidentemente ne consegue in termini di capacità attrattiva degli utenti-consumatori, in particolare quando la propria proposta di vendita risulta maggiormente conveniente rispetto ad altre, e di loro fidelizzazione alla piattaforma.

Tali clausole possono avere una portata più o meno ampia, potendosi parlare di *wide parity clauses* quando si nega la capacità degli utenti commerciali di offrire i propri prodotti, a prezzi più economici, su altre piattaforme concorrenti e sul proprio sito Internet; nonché di *narrow parity clauses* quando la limitazione concerne soltanto l'offerta tramite le proprie pagine *web* e non anche i concorrenti diretti del fornitore controparte contrattuale. Appare immediatamente intuibile come la previsione di siffatte clausole ponga degli interrogativi sul funzionamento del sistema concorrenziale, soprattutto in relazione alle concrete possibilità per nuovi operatori di entrare ovvero di espandersi all'interno di un mercato rilevante[46].

Tuttavia il Regolamento, sfuggendo qualsiasi considerazione in merito alla loro capacità distorsiva della concorrenza, si limita a formulare il relativo requisito di trasparenza. E sembra però inevitabile chiedersi quanto, ed eventualmente come, tale previsione contrattuale possa in concreto giovare agli utenti commerciali: a loro tutela sarebbe stato probabilmente più efficace prevedere un vero e proprio divieto di tali clausole, come peraltro già previsto da alcuni provvedimenti di

---

45 A tal fine, si considerano "soggetti concorrenti" sia gli altri *marketplace* presenti sulla rete che il sito *web* privato del singolo utente commerciale.

46 Sul punto si veda M. Colangelo, *Parity Clauses and Competition Law in Digital Marketplaces: The Case of Online Hotel Booking*, in *JECL&Pract.*, 2017, pp. 3 ss.

carattere nazionale all'interno dell'Unione europea[47]. In tal senso, il secondo paragrafo dell'art. 10 lascia quantomeno impregiudicate le limitazioni a clausole di questo tipo ad opera sia del diritto degli Stati membri che del diritto europeo.

14.9. Il sistema interno di gestione dei reclami e la mediazione

Il legislatore europeo completa il quadro delle regole di equità e trasparenza dei rapporti con le piattaforme digitali con alcune disposizioni dedicate alla risoluzione delle controversie tramite la gestione interna dei reclami e il procedimento di mediazione.

È infatti apparso necessario intervenire su un sistema che, allo stato, non salvaguardava la posizione degli utenti commerciali con la previsione di strumenti di ricorso accessibili ed efficaci, in mancanza di adeguati meccanismi di gestione dei reclami ovvero di soggetti specializzati a dirimere questioni sorte nell'ambito di questo specifico rapporto contrattuale. Ciò, peraltro, non impedendo in alcun momento – prima, durante e anche a conclusione del procedimento stragiudiziale – di esercitare il diritto di adire la competente autorità giudiziaria.

L'art. 11 del Regolamento impone dunque ai fornitori di strutturare dei sistemi interni[48] di gestione dei reclami per garantire agli utenti commerciali, anche quando destinatari dei provvedimenti di limitazione, sospensione o cessazione dei servizi (v. *supra* § 4), l'accesso gratuito e non difficilmente praticabile a possibilità di ricorso immediate,

---

47 In particolare, l'art. 1, comma 166, l. 4 agosto 2017, n. 124 (Legge annuale per il mercato e la concorrenza) per cui «[è] nullo ogni patto con il quale l'impresa turistico-ricettiva si obbliga a non praticare alla clientela finale, con qualsiasi modalità e qualsiasi strumento, prezzi, termini e ogni altra condizione che siano migliorativi rispetto a quelli praticati dalla stessa impresa per il tramite di soggetti terzi, indipendentemente dalla legge regolatrice del contratto». Similmente, in Francia, l'art. 133 della *Loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques*, nota come Legge Macron, prevede che le clausole di questo tipo debbano essere considerate come non scritte.

48 Il Considerando 39 del Regolamento precisa che l'utilizzo di tale termine non dovrebbe essere inteso come un impedimento a delegare tale attività «a un fornitore di servizi esterno o a un'altra struttura aziendale», a condizione che il soggetto prescelto garantisca pienamente la conformità del sistema di gestione adottato ai requisiti del Regolamento.

idonee ed efficaci al raggiungimento di un accordo. Da conseguire peraltro entro «un lasso di tempo ragionevole», naturalmente sulla base dell'importanza e della complessità di ogni singolo reclamo.

Organizzato in funzione del rispetto dei principi di trasparenza e di parità di trattamento a parità di situazione, il sistema concerne in particolare i reclami proposti per: a) la presunta inadempienza degli obblighi che il Regolamento dispone in capo ai fornitori di servizi di intermediazione *online*; b) problemi di natura tecnica nella fornitura dei servizi agli utenti commerciali; c) l'adozione da parte del fornitore di misure o comportamenti connessi allo svolgimento della propria prestazione. In ciascuna di queste ipotesi si richiede peraltro che l'utente commerciale intenzionato a proporre reclamo ne abbia subìto le relative conseguenze.

Tutte le informazioni relative all'accesso alla procedura, nonché al suo svolgimento, devono essere esplicitate nei termini e nelle condizioni del contratto. Si deve garantire che la trattazione dei reclami avvenga in modo rapido ed efficace, pur senza sacrificare la qualità dell'indagine e al fine di risolvere adeguatamente le questioni insorte. E che l'esito del processo venga comunicato direttamente al reclamante adoperando un linguaggio semplice e comprensibile.

Del funzionamento e dell'efficacia del proprio sistema interno di gestione dei reclami viene poi data conoscenza diffusa tramite la pubblicazione, con verifica e aggiornamento a cadenza almeno annuale, di informazioni rilevanti, come il numero totale e le categorie di reclami presentati dagli utenti commerciali, i tempi mediamente necessari al trattamento, i dati aggregati relativi agli esiti. La *ratio* di tale disposizione appare ancora una volta ravvisabile nell'opportunità di assicurare agli utenti commerciali interessati uno strumento di prevedibilità dell'agire della controparte contrattuale, in applicazione del principio di trasparenza. In questo modo, si rendono infatti conoscibili alcuni aspetti particolarmente importanti per chi abbia intenzione di impegnarsi convenzionalmente con un determinato fornitore, come le principali problematiche insorte in questa tipologia di rapporti o le possibilità di risolverle in tempi rapidi e in modo effettivo.

La previsione di un sistema interno di gestione dei reclami costituisce indubbiamente un passaggio importante verso l'equità e la trasparenza procedurale nei rapporti tra piattaforme e utenti commerciali; tuttavia, non può non riscontrarsi come il Regolamento resti in verità piuttosto vago su sul contenuto, in particolare, di questa equità. Anche

in considerazione della tipologia di atto adottato dal legislatore europeo, sarebbe stato forse maggiormente opportuno incidere con più convinzione introducendo requisiti più precisi, ad esempio in relazione alla durata massima del procedimento di reclamo o alla maggior tutela degli utenti commerciali da comportamenti imprevedibili o sproporzionati dei fornitori dei servizi di intermediazione[49].

D'altra parte, il Regolamento individua nella mediazione un'ulteriore alternativa stragiudiziale per la risoluzione delle controversie relative alla fornitura dei servizi di intermediazione *online*, altresì comprendendo quei reclami che non sia stato possibile risolvere ai sensi del precedente art. 11. Perciò consolidandosi notevolmente il quadro delle tutele irrinunciabili che l'ordinamento europeo pone a disposizione dei soggetti del mercato.

A tal fine, l'art. 12 del Regolamento esige che il fornitore indichi nel contratto almeno due mediatori con cui sia disposto ad impegnarsi nel caso in cui ne occorresse l'intervento. Non esclude per ciò soltanto la possibilità nel caso concreto di designare uno o più soggetti diversi, anche in accordo con l'utente commerciale di volta in volta coinvolto. Purché, nel complesso, il fornitore si impegni a promuoverne ed agevolarne il processo, il cui avvio rimane in ogni caso vincolato alla comune volontà delle parti interessate e, come detto, non impedisce di procedere in sede giudiziale. Anche in tal senso, i fornitori devono mettere a disposizione degli utenti commerciali che lo richiedano le informazioni sul funzionamento e sull'efficacia della mediazione relativamente alle loro attività.

Il successivo art. 13 invita peraltro la Commissione europea, in sinergia con gli Stati membri, a sostenere l'istituzione di veri e propri organismi di mediazione specializzati, con riferimento ai settori specifici di azione degli utenti commerciali tramite piattaforme digitali e anche in considerazione della natura transfrontaliera dei servizi di intermediazione *online*, proprio nell'ottica di accrescere la generale fiducia degli operatori di questi mercati nei processi di mediazione e, di riflesso, di aumentare le probabilità di successo, rapido e soddisfacente, di questi meccanismi di giustizia alternativa.

---

[49] C. Busch, *The P2B Regulation (EU) 2019/1150: Towards a "Procedural Turn" in EU Platform Regulation?*, in *EuCML*, 4, 2020, p. 134.

Ai fini previsti dal Regolamento, sono incaricati come mediatori quei soggetti che: diano garanzia di imparzialità e indipendenza; prestino i loro servizi a prezzi sostenibili dagli utenti commerciali della piattaforma, nonché nella lingua di redazione dei termini e delle condizioni; siano facilmente raggiungibili, fisicamente nel luogo di stabilimento o di residenza dell'utente commerciale oppure virtualmente mediante strumentazione telematica, non costituendo impedimento *ex se* l'ipotesi in cui i servizi di mediazione siano prestati da un luogo esterno all'Unione europea; garantiscano un lavoro puntuale, efficace ed efficiente, anche in considerazione delle proprie conoscenze specifiche in materia di rapporti commerciali tra imprese.

Quanto al procedimento di mediazione, la norma rimarca la necessità che le parti si comportino secondo buona fede nell'esperimento di ciascun tentativo di composizione della controversia. Ma il Considerando 42 del Regolamento ammette anche che il fornitore non sia sempre tenuto ad impegnarsi in tale procedimento, in particolare laddove la relativa richiesta provenga da un utente commerciale di cui un precedente mediatore abbia accertato, sulla stessa questione, un agire contrario alle regole di buona fede ovvero con cui ripetuti tentativi di mediazione già esperiti non abbiano avuto successo. Così cercando di prevenire qualsiasi situazione di abuso del sistema da parte degli utenti commerciali cui lo strumento è rivolto. Ciò anche in quanto la norma prevede che siano i fornitori dei servizi di intermediazione a sostenere una parte ragionevole dei costi totali di ciascun procedimento di mediazione, determinata in base alla proposta del mediatore, che è chiamato a tal fine a tener conto della fondatezza delle ragioni di ciascuna delle parti, del loro comportamento, nonché delle dimensioni e della capacità finanziaria di una parte rispetto all'altra.

Infine, in considerazione dei costi e degli oneri amministrativi che il fornitore si trova inevitabilmente a fronteggiare per l'implementazione tanto dei sistemi interni di gestione dei reclami quanto dei procedimenti di mediazione, il Regolamento esenta dagli obblighi di cui agli artt. 11 e 12 le piccole imprese, come definite dall'Allegato della Raccomandazione 2003/361/CE[50]. Con ciò restando naturalmente im-

[50] Ai sensi dell'art. 2 dell'Allegato è definita "piccola impresa" l'impresa che occupa meno di cinquanta persone e che realizza un fatturato annuo o un totale di bilancio annuo non superiore a dieci milioni di euro.

pregiudicato il diritto delle stesse di creare un sistema interno di gestione dei reclami e di indicare nel contratto i nominativi dei mediatori, su base volontaria, in modo conforme ai criteri stabiliti dal Regolamento.

Da ultimo, quanto all'ipotesi in cui il soggetto interessato non voglia procedere per via stragiudiziale, intendendo piuttosto adire il giudice nazionale competente, il Regolamento introduce all'art. 14 un'innovativa legittimazione ad agire in capo ad organizzazioni, associazioni o persone giuridiche pubbliche rappresentative di utenti commerciali, come anche di titolari dei siti *web* che appaiono sulle pagine dei motori di ricerca[51]. In conformità alla legge vigente nello Stato membro in cui l'azione è promossa, tali soggetti – che la norma chiede alla Commissione europea di individuare ed inserire in un apposito elenco da pubblicare, e aggiornare a scadenza semestrale, nella Gazzetta ufficiale dell'Unione europea – avrebbero dunque il diritto di rivolgersi all'autorità giudiziaria al fine di far cessare quella condotta dei fornitori che sia contraria agli obblighi imposti dal Regolamento. In particolare per quelle ipotesi in cui, per timore di ritorsioni, potrebbe addirittura apparire più conveniente una definitiva rinuncia all'azione. In questa chiave, la centralizzazione dei loro interessi potrebbe allora riuscire nell'intento di distogliere concretamente i fornitori dal portare avanti condotte lesive dei diritti degli utenti[52].

14.10. Osservazioni conclusive

Il Regolamento rappresenta un primo fondamentale tassello della strategia europea per la regolazione dell'economia delle piattaforme. In particolare attraverso la determinazione dei citati criteri di trasparenza, elaborati per qualificare quel peculiare rapporto tra piattaforme e utenti commerciali che l'attuale sistema di mercato, evidentemente proteso verso una conformazione sempre più *digital*, pone al centro di un dibattito nuovo. Un rapporto generalmente asimmetrico, di cui i fornitori dei servizi di intermediazione *online* rappresentano la parte

---

51 Purché le organizzazioni o associazioni siano costituite secondo il diritto di uno Stato membro, perseguano in via continuativa obiettivi di interesse comune, non abbiano scopo di lucro e siano indipendenti; oppure si tratti di organismi pubblici istituiti *ad hoc* (art. 14, §§ 3-5, del Regolamento).

52 C. BUSCH, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, *cit.*, p. 73.

che dispone di maggiore potere contrattuale, la parte le cui prestazioni si rendono indispensabili per restare competitivi e attrattivi sul mercato, la parte da cui inevitabilmente si finisce per dipendere. E rispetto alla quale occorreva pertanto definire degli adeguati strumenti di tutela[53].

A fronte di un numero effettivamente esiguo di piattaforme di intermediazione finalmente dirette e diffusamente note ai consumatori, le imprese che ne ricercano i servizi sono infatti milioni, per lo più trattandosi di realtà di modeste dimensioni[54]. Evidente, dunque, alla luce dell'importanza strategica e della crescita di questi soggetti nel mercato (tutt'altro che esclusivamente) europeo, l'opportunità di un intervento regolatorio a garanzia dei principi di equità e trasparenza nei rapporti P2B. Per trasmettere quel fondamentale fattore fiducia nell'utilizzo di tali meccanismi di offerta di beni e servizi agli utenti del *web*, nel tentativo di prevenire comportamenti unilaterali iniqui da parte degli intermediari.

Non resta dunque che interrogarsi su quale sia la portata, oltre che la concreta innovazione, del Regolamento. Definirlo limitato ad una generica fissazione di requisiti di trasparenza appare invero non del tutto appropriato. Nel complesso, infatti, il quadro normativo definito dal legislatore europeo sembra strutturare un vero proprio schema contrattuale, tipizzando il contenuto di clausole di cui si impone al tempo stesso la previsione: in ogni caso, alcune; sulla base di determinati presupposti, altre. Certo è che ognuna delle regole destinate dal Regolamento alla regolazione dei rapporti P2B intende preservare la

---

53 Per un utilizzo generalizzato della nozione di "asimmetria contrattuale", che ricomprende le diverse ipotesi in cui uno dei due contraenti deve essere considerato economicamente più debole, si vedano, *ex multis*, V. Roppo, *Contratto di diritto comune, contratto del consumatore, contratto con asimmetria di potere contrattuale: genesi e sviluppi di un nuovo paradigma*, in *Riv. dir. priv.*, 2001, pp. 769 ss. e in *Il contratto del duemila*, IV edizione, Giappichelli, Torino, 2020, pp. 69 ss.; C. Camardi, *Contratti di consumo e contratti tra imprese. Riflessioni sull'asimmetria contrattuale nei rapporti di scambio e nei rapporti reticolari*, in *Riv. crit. dir. priv.*, 4, 2005, pp. 549 ss.; E. Navarretta (a cura di), *Il diritto europeo dei contratti fra parte generale e norme di settore*, Giuffrè, Milano, 2008.

54 È infatti soprattutto con riferimento alle piccole e medie imprese (PMI) che le piattaforme rappresentano un'opportunità spesso irrinunciabile per accedere al mercato digitale, in considerazione delle maggiori possibilità di posizionamento dei propri prodotti e di conoscibilità su vasta scala.

posizione degli utenti commerciali dalle azioni imprevedibili o ingiustificate dei fornitori, contrastanti con i doveri, generalmente riconosciuti, di buona fede contrattuale.

Probabilmente il Regolamento si rivelerà presto insufficiente per perseguire tale ambizioso obiettivo, ma a colmarne le lacune e superarne le incertezze è atteso l'intervento delle corti, tanto a livello nazionale quanto, soprattutto, europeo. E sarà poi il legislatore europeo a doversi nuovamente occupare di tale categoria di rapporti, ad esempio operando opportune differenziazioni in base alle dimensioni e al potere di mercato delle piattaforme o alle diverse tipologie di offerte indirizzate ai consumatori[55], nonché disciplinando aspetti ulteriori, comunque connessi all'oggetto del Regolamento, come la portabilità dei dati reputazionali delle imprese.

Ciò anche alla luce di quanto emergerà dalle analisi effettuate dall'Osservatorio sull'economia delle piattaforme *online*, che sottoporrà pareri e relazioni alla Commissione europea come previsto dall'art. 18 del Regolamento[56]; nonché dalla prassi. Occorre infatti notare, da ultimo, come l'indeterminatezza che in taluni aspetti caratterizza l'attuale disciplina dei rapporti P2B potrà essere equilibrata anche ad opera degli stessi intermediari della rete, ovvero dei destinatari diretti dello schema regolatorio definito dal legislatore europeo. Soggetti regolamentati, dunque, e al tempo stesso in grado, a loro volta, di

---

55 Si pensi da ultimo alle proposte di Regolamento sui servizi e sui mercati digitali presentate dalla Commissione europea il 15 dicembre 2020 per rendere «i mercati digitali più equi e più aperti per tutti. Un *corpus* normativo per tutto il mercato unico promuoverà l'innovazione, la crescita e la competitività e fornirà agli utenti servizi *online* nuovi, migliori e affidabili» (Commissione europea, IP/20/2347).

56 L'Osservatorio è stato istituito dalla Commissione europea con la Decisione C(2018) 2393 def. proprio allo scopo di monitorare l'evoluzione e il funzionamento delle piattaforme digitali e permettere alle istituzioni europee di intervenire nei modi più opportuni a tutela del corretto funzionamento del mercato interno.

agire da regolatori[57]. Perciò apparendo, in sostanza, che il Regolamento costituisca uno strumento di regolazione di regolatori privati[58].

D'altronde, che le piattaforme non rappresentino semplicemente dei luoghi virtuali di connessione tra utenti-venditori e utenti-acquirenti, ma regolatori dei rapporti e delle transazioni che su di esse trovano spazio, risulta ormai indiscusso. Come è noto, infatti, gli intermediari tendono ad insidiarsi, attraverso i termini e le condizioni di utilizzo dei propri servizi, nelle relazioni contrattuali instaurate *online*; ad imporre apposite linee guida che dettano determinate regole comportamentali ai loro utenti; o a disporre dei meccanismi di pubblicazione delle valutazioni e delle recensioni dei consumatori[59]. Pertanto, se il disegno del legislatore europeo può dirsi effettivamente impostato, *de iure condito* i tempi non sembrano ancora maturi per poter esprimere considerazioni certe e definitive sull'efficacia delle nuove misure e sul loro grado di intervento sul potere regolatorio delle piattaforme digitali. La via della trasparenza è insomma sicuramente meno oscura, ma ancora poco nitida.

---

57 Ad esempio attraverso l'elaborazione di codici di condotta come previsto dall'art. 17 del Regolamento, dal quale emerge la consapevolezza del legislatore europeo della necessità che i fornitori di servizi di intermediazione *online* e di motori di ricerca manifestino attivamente di adeguarsi alla corretta applicazione del Regolamento, tenendo conto delle specificità dei diversi settori di offerta di beni e servizi ai consumatori.

58 Cfr. F. Cafaggi, *La responsabilità dei regolatori privati. Tra mercati finanziari e servizi professionali*, in *Merc. conc. reg.*, 1, 2006, pp. 9 ss.

59 C. Busch, *Self-Regulation and Regulatory Intermediation in the Platform Economy*, in M. Cantero Gamito e H. Micklitz (a cura di), *The Role of the EU in Transnational Legal Ordering: Standard, Contracts and Codes*, Elgar, 2019, pp. 115 ss.

15. Trasparenza e piattaforme *online* alla luce del Regolamento (UE) 2019/1150

Chiara Sartoris

15.1. Piattaforme digitali e nuove esigenze di protezione contrattuale: il Regolamento (UE) 2019/1150

Il 12 Luglio 2020 è entrato in vigore il nuovo Regolamento (UE) 2019/1150, con il quale l'U.E. intende promuovere l'equità e la trasparenza per gli utenti commerciali dei servizi di intermediazione *online*[1]. Tale Regolamento, che si inserisce nella *"Digital Single Market Strategy"* recentemente avviata, fa parte di un più ampio pacchetto di atti preordinati alla redazione del c.d. *"Digital Service Act"*, con l'obiettivo di dettare un quadro normativo comune in materia di transazioni commerciali *online*[2].

---

1 Cfr. TWIGG-FLESNER, *The EU's Proposals for Regulating B2B Relationships on Online Platforms Transparency, Fairness and Beond,* in *Jour. Eur. Cons. Mark Law*, 2018, p. 222 ss.; FRANZINA, *Promoting Fairness and Transparency for Business Users of Online Platforms: The role of Private International Law,* in PETRELLI (edited by), *Conflict of Laws in the Maze of Digital Platforms. Le droit international privé dans le labyrinthe des pleatformes digitales*, Zurich, 2018, p. 147 ss.; INGLESE, *La proposta di regolamento che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online: tanto tuonò che piovve,* in *Studi sull'integrazione europea*, 2019, 2, p. 463 ss.; PALMIERI, *Profili giuridici delle piattaforme digitali. La tutela degli utenti commerciali e dei titolari di siti web*, Torino, 2019; IAMICELI, *Online Platforms and the Digital Turn in EU Contract Law: Unfair Practices, Transparency and the (pierced) Veil of Digital Immunity*, in *European Review of Contract Law*, 2019, 4, p. 392 ss.; SMORTO, *La tutela del contraente debole nella platform economy dopo il Regolamento UE 2019/1150 e la Direttiva UE 2019/2161 (c.d. Omnibus),* in FALCE (a cura di), *Fairness e innovazione nel mercato digitale*, Torino, 2020, p. 49 ss.; BUSC , *The P2B Regulation (EU) 2019/1150: Towards a "procedural turn" in EU platform regulation?*, in *Journal of European Consumer and Market Law*, 2020, 4, p. 133 ss.

2 La Vicepresidente Esecutiva della Commissione Margrethe Vestager ha dichiarato: «The more than 10,000 online platforms in the EU are only one part of a broader

Il Regolamento (UE) 2019/1150 concretizza l'impegno dell'U.E. a disciplinare il fenomeno, sempre in crescita, dell'utilizzo di piattaforme digitali per la conclusione di affari commerciali o professionali[3]. Le piattaforme digitali sono spazi virtuali gestiti da soggetti che, professionalmente, forniscono o offrono di fornire servizi di intermediazione *online* a utenti commerciali, cioè a soggetti che svolgono un'attività commerciale, imprenditoriale, artigianale o professionale (art. 2, lett. 1), affinché possano offrire, a loro volta, beni o servizi ai propri consumatori. Di tale relazione multilaterale, però, il Regolamento disciplina un solo versante, cioè il contratto tra utente commerciale e fornitore di servizi di intermediazione *online* o di motori di ricerca (P2B)[4], ponendo

digital services ecosystem that derives innovations. Despite their role as an essential resource during the on-going health crisis, major issues of fairness and safety have to be addressed. The new rules will ban certain unfair practices such as unexplained account suspension, unclear terms and conditions; ensure greater transparency about ranking and provide new possibilities for resolving disputes and complaints». In considerazione di ciò, la *Digital Single Market Strategy*, in cui il presente provvedimento si inserisce, mira a rimuovere gli ostacoli alle attività online transfrontaliere allo specifico fine di creare condizioni favorevoli all'innovazione e massimizzare il potenziale di crescita dell'economia digitale.

[3] L'importanza della regolamentazione di tali rapporti contrattuali emerge già da un dato di ordine numerico. L'U.E. stima che un milione di imprese europee commerciano attraverso piattaforme digitali per favorire la conclusione di affari con i propri clienti e che circa il 60% dei consumi privati e il 30% dei consumi pubblici di beni e servizi connessi all'economia digitale sono realizzati attraverso l'uso di servizi di intermediazione *online*. E l'emergenza sanitaria di questi mesi non fa altro che rafforzare l'esigenza di regole chiare e precise per il loro corretto funzionamento. Cfr. Srnicek, *Platform Capitalism*, Cambridge, 2016; Lobel, *The Law of the Platform*, in *Minn. L. Rev*., 2016, n. 101, 87; Cohen, *Law for the Platform Economy*, 2017, in *U.C. Davis L. Rev*., 51, 133; RODRÍGUEZ DE LAS ERAS BALLELL, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU*, in *The Italian Law Journal*, 2017, 3, 1 ss.; Markou, *Consumer Protection, Automated Shopping Platforms and EU Law*, London, 2019; Ammannati, *Verso un diritto delle piattaforme digitali?*, in *www.federalismi.it*; Foltran, *Professionisti, consumatori e piattaforme online: la tutela delle parti deboli nei nuovi equilibri*, in *Rivista di diritto dei media*, 2019, 3, p. 162 ss.

[4] Ai sensi dell'art. 2, n. 2, del Regolamento per "servizi di intermediazione online" si intendono i servizi della società dell'informazione, cioè i servizi prestati dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario (cfr. art. 1, parag. 1, lett. b), della Direttiva (UE) 2015/1535 in materia di servizi della società dell'informazione), la cui finalità sia quella di consentire agli utenti commerciali di offrire beni o servizi ai consumatori, a prescindere da dove sono concluse le relative transazioni. Si pensi agli *e-commerce marketplaces*. Mentre, ai sensi dell'art. 2, n. 6, per "motore di ricerca" si intende un servizio digitale che consente all'utente di formulare domande al fine di effettuare ricerche sui siti *web*,

non pochi problemi, come si vedrà, in punto di coordinamento con la tutela dei consumatori.

La presente indagine intende approfondire le caratteristiche del rapporto contrattuale P2B per comprendere se il Regolamento (UE) 2019/1150 offra una tutela effettiva per gli utenti commerciali[5]. Invero, tale rapporto si connota per una strutturale asimmetria di posizioni[6], benché coinvolga – ed è questa la peculiarità – due soggetti che agiscono nell'esercizio della rispettiva attività professionale. Sicché, siamo in presenza di una relazione che costituisce sviluppo e, nel contempo, specificazione, dei contratti (asimmetrici) tra professionisti

---

sulla base di una interrogazione su qualsiasi tema, fornendo i risultati in cui possono essere reperite le informazioni relative al contenuto richiesto.

5 Sul principio di effettività: TROCKER, *Dal giusto processo all'effettività dei rimedi: l' "azione" nell'elaborazione della Corte europea dei diritti dell'uomo (Parte prima)*, in *Riv. trim. dir. proc. civ.*, 2007, n. 1, p. 35 ss.; ORIANI, *Il principio di effettività della tutela giurisdizionale*, Napoli, 2008; IRTI *Significato giuridico dell'effettività*, Napoli, 2009; MAK, *Rights and Remedies - Article 47 EUCFR and Effective Judicial Protection in European Private Law Matters,* in MICKLITZ (edited by), *Constitutionalization of European Private Law*, Oxford, 2014, p. 236 ss.; SAFIJAN e DÜSTERAUS , *A Union of Effective Judicial Protection: Addessing a Multi-leve Challenge through the Lens of Article 47 CFREU*, in *Yearbook of European Law*, vol. 33, n. 1, 2014, p. 3 ss.; PAGLIANTINI, *Diritto giurisprudenziale e principio di effettività*, in *Pers. e merc.*, 2015, 4, p. 112 ss.; VETTORI, *Contratto giusto e rimedi effettivi*, in *Pers. e merc.*, 2015, 1, p. 5 ss.; ID., voce *"Effettività delle tutele (diritto civile)"*, in *Enc. dir.*, Ann. X, Milano, 2017, p. 381 ss.; ID., *Il diritto a un rimedio effettivo nel diritto privato europeo*, in *Pers. e merc.*, 2017, 1, p. 15 ss.; IMBRUGLIA, *Effettività della tutela: una casistica*, in *Pers. e merc.*, 2016, 2, p. 62 ss.; NAVARRETTA, *Costituzione, Europa e diritto privato. Effettività e Drittwirkung ripensando la complessità giuridica*, Torino, 2017, p. 48 ss.; I. PAGNI, *Effettività della tutela giurisdizionale,* in *Enc. dir.*, Annali, X, Milano, 2017, p. 355 ss.; M. LIBERTINI, *Le nuove declinazioni del principio di effettività,* in *Eur. dir. priv.*, 2018, p. 1071 ss..

6 Sul concetto di "asimmetria": ROPPO, *Contratto di diritto comune, contratto del consumatore, contratto con asimmetria di potere contrattuale: genesi e sviluppi di un nuovo paradigma,* in *Riv. dir. priv.*, 2001, p. 769 ss.; ID., *Parte generale del contratto, contratti del consumatore e contratti asimmetrici (con postilla sul "terzo contratto")*, in ID., *Il contratto del duemila,* 2ª ed., Torino, p. 102 ss.; DE POLI, *Asimmetrie informative e rapporti contrattuali*, Padova, 2002; CAMARDI, *Contratti di consumo e contratti tra imprese. Riflessioni sull'asimmetria contrattuale nei rapporti di scambio e nei rapporti "reticolari"*, in *Riv. crit. dir. priv.*, 2005, p. 581 ss.; ZOPPINI, *Il contratto asimmetrico tra parte generale, contratti di impresa e disciplina della concorrenza,* in *Riv. dir. civ.*, 2008, I, p. 515 ss.; VETTORI, *Il contratto senza numeri e aggettivi. Oltre il consumatore e l'impresa debole,* in *Contr. e impr.*, 2012, p. 1190 ss.; BENEDETTI, voce *Contratto asimmetrico*, in *Enc. dir.*, Annali, V, Milano, 2012, p. 370 ss.; CIARELLA , *Contrattazione asimmetrica. Segmenti normativi e costruzione unitaria*, Milano, 2016; D'AMICO, *Giustizia contrattuale e contratti asimmetrici,* in *Eur. dir. priv.*, 2019, 1, p. 1 ss.

(B2B)[7], con la particolarità ulteriore di svolgersi in ambiente digitale. Ci pare che i gestori di piattaforme digitali dispongano di una posizione di forza per due ragioni essenziali: da un lato, essi entrano in possesso e controllano una grande quantità di dati che, grazie a sistemi algoritmici, consente loro di influenzare pesantemente la concorrenza; dall'altro lato, gli utenti commerciali stanno diventando sempre più dipendenti dalle piattaforme, perché permettono loro di raggiungere facilmente e in tempi rapidi un numero potenzialmente enorme di clienti[8]. Non solo. Il problema è che tale posizione di crescente forza economica e informativa sfocia spesso in condotte e pratiche scorrette dei fornitori di tali servizi. Si pensi all'imposizione di condizioni contrattuali sbilanciate o di loro modifiche ingiustificate senza che sia dato preavviso alla controparte; alla sospensione ingiustificata dell'*account* per l'accesso alla piattaforma degli utenti oppure all'esclusione degli

---

7 Il Regolamento (UE) 2019/1150 rappresenta la prima legge, a livello europeo, a disciplinare la posizione contrattuale dell'impresa nel rapporto con il fornitore di servizi di intermediazione *online.* Ma il nostro ordinamento, anche sulla spinta del diritto europeo, già conosce e regola rapporti contrattuali tra professionisti dotati di diversa forza contrattuale: in tema di condizioni generali di contratto gli artt. 1341 e 1342 c.c. dettano una regola di protezione applicabile anche ai professionisti, poiché prescinde dalla natura di impresa o di persona fisica della parte che se ne avvale; la legge n. 192/1998 in materia di subfornitura protegge il subfornitore contro il comportamento illecito della controparte integrante un abuso di dipendenza economica; la legge n. 27/2012 estende la protezione offerta dalla disciplina consumeristica anche alle piccole-medie imprese, assimilate ai consumatori nell'ambito di questa specifica materia. Cfr. Cian, *Contratti civili, contratti commerciali e contratti d'impresa: valore sistematico-ermeneutico delle classificazoni,* in *Riv. dir. civ.*, 2004, I, p. 849 ss.; Oppo, *I contratti d'impresa tra codice civile e legislazione speciale,* in *Riv. dir. civ.*, 2004, 847 ss.; Camardi, *Contratti di consumo e contratti tra imprese. Riflessioni sull'asimmetria contrattuale nei rapporti di scambio e nei rapporti "reticolari",* in *Riv. crit. dir. priv.*, 2005, p. 549 ss.; Falzea, *Il diritto europeo dei contratti d'impresa,* in *Riv. dir. civ.*, 2005, p. 6 ss.; Sirena, *La categoria dei contratti di impresa e il principio di buona fede,* in *Riv. dir. civ.*, 2006, II, p. 415 ss.; Maffeis, *Il contraente e la disparità di trattamento delle controparti,* in *Riv. dir. priv.*, 2006, p. 301 ss.; Villa, *Contratti asimmetrici tra imprese: profili generali di disciplina*, in AA.VV., *Il terzo contratto, l'abuso di potere contrattuale nei rapporti tra imprese,* a cura di Gitti e Villa, Bologna, 2008, 89; Franco, *Il terzo contratto: da ipotesi di studio a formula problematica. Profili ermeneutici e prospettive assiologhiche*, Padova, 2010.

8 Osserva Ammannati, *op. cit.*: «la crescente intermediazione di transazioni attraverso piattaforme *online* ha condotto ad una progressiva dipendenza del *business* dalle piattaforme che divengono simili a "*gatekeeper*" nei confronti di mercati e consumatori» in quanto il loro "potere" non si coglie tanto attraverso analisi economiche, quanto piuttosto «nel loro più generale ruolo di "controllori" dei flussi di informazioni e di dati».

utenti che si oppongono a particolari limitazioni di accesso (c.d *delisting);* o ancora alla mancanza di trasparenza con riguardo ad aspetti cruciali del rapporto, come le regole sul posizionamento nei motori di ricerca o sul trattamento di dati personali. Come è evidente, le illustrate prassi rischiano di nuocere allo sviluppo di singoli *marketplaces* e di compromettere la concorrenza sul mercato unico, danneggiando, in definitiva, non solo gli utenti commerciali, ma anche i consumatori, che rappresentano l'anello finale e maggiormente bisogno di protezione nella catena commerciale.

Al fine di prevenire tali storture, il Regolamento (UE) 2019/1150 detta una serie di regole e di obblighi a carico dei fornitori di servizi di intermediazione online o di motori di ricerca, funzionali ad assicurare la correttezza, l'equità e un'adeguata trasparenza sul funzionamento delle piattaforme (art. 1, parag. 1); nell'idea che una tale regolamentazione conduca benefici generalizzati, contribuendo anche a migliorare il benessere dei consumatori grazie alla maggiore possibilità di scelta di beni e servizi, nonché alla offerta di prezzi competitivi (considerando n. 1). In questa prospettiva, le nuove regole rappresentano indubbiamente un importante passo avanti nella evoluzione della disciplina contrattuale euro-unitaria poiché, per la prima volta, offrono una tutela *ad hoc* per i professionisti utenti di una piattaforma digitale[9]. Il presente contributo intende, dunque, analizzare i contenuti di tali regole e i rimedi attivabili in caso di violazione, evidenziando, però, talune criticità di fondo; con il proposito di avviare una riflessione non solo sulla effettività della tutela degli utenti commerciali, ma anche sui

---

[9] La posizione contrattuale dei professionisti nell'ambito del commercio elettronico è stata finora disciplinata dal d.lgs. n. 70/2003 in attuazione della Direttiva (CE) 2000/31 in materia di servizi della società dell'informazione nel mercato interno con particolare riferimento al mercato elettronico. Cfr. DE NOVA e DELFINI, *La direttiva sul commercio elettronico: prime considerazioni,* in *Riv. dir. priv.*, 2000, p. 693 ss.; DELFINI, *Commercio elettronico e servizi di investimento,* in *Contr.*, 2000, p. 716 ss.; LEOCANI, *La Direttiva UE sul commercio elettronico: cenni introduttivi, in Eur. dir. priv.*, 2000, p. 617 ss.; SANTAROSSA, *La direttiva europea sul commercio elettronico,* in *Contr. e impr./Eur.*, 2000, p. 852 ss.; COMANDÈ e SICA, *Il commercio elettronico. Profili giuridici*, Torino, 2001; BESSONE, *E-economy e commercio elettronico. Quale diritto per i tempi di internet?*, in *Dir. inf. e informatica*, 2002, p. 52 ss.; ZENO-ZENCOVIC , *Note critiche sulla nuova disciplina del commercio elettronico dettata dal D.lgs. 70/03,* in *Dir. inf. e informatica*, 2003, 3, p. 505 ss.; TOSI, *Commercio elettronico e servizi della società dell'informazione. Le regole giuridiche del mercato interno e comunitario. Commento al d.lgs. 9 aprile 2003, n. 70*, Milano, 2003; MANNA, *La disciplina del commercio elettronico*, Padova, 2005.

rapporti tra la disciplina a favore dei consumatori e le esigenze di protezione poste da tali nuove posizioni di "vulnerabilità" contrattuale.

15.2. La regola di trasparenza nei contratti di fornitura dei servizi di intermediazione *online*

Il Regolamento (UE) 2019/1150 si lascia apprezzare per aver introdotto un principio generale di trasparenza sulle regole di funzionamento della piattaforma digitale: le modalità di redazione dei termini e delle condizioni contrattuali, così come i contenuti essenziali del contratto P2B, sono disciplinati da norme volte a garantire il riequilibrio del *gap* informativo strutturalmente esistente tra le parti. Vediamo quali sono gli elementi chiave di tale impostazione.

Centrale è, innanzitutto, l'art. 3, che detta due regole generali concernenti il *drafting* di termini e condizioni contrattuali. Da un lato, è necessario che i termini e le condizioni unilateralmente imposti dal fornitore «*siano redatti in un linguaggio semplice e comprensibile*» (art. 3, lett. a)), cioè non devono risultare generici, fuorvianti, ambigui o privi di importanti dettagli sul contenuto contrattuale. Dall'altro lato, è necessario che tali termini e condizioni contrattuali «*siano facilmente reperibili dagli utenti commerciali in tutte le fasi del loro rapporto contrattuale con il fornitore (…)*», compresa la fase precontrattuale (art. 3, lett. b)). In tal modo, si vuole garantire non solo che l'utente commerciale sia a conoscenza, durante l'intera durata del rapporto contrattuale, delle condizioni di utilizzo del servizio di intermediazione *online*; ma anche che tale conoscenza sia caratterizzata da un ragionevole grado di certezza e di prevedibilità. Questi ultimi, infatti, sono due fattori chiave per l'organizzazione di qualunque attività imprenditoriale o professionale, a maggior ragione quando si progetta di trasferirla, in tutto o in parte, su piattaforma digitale.

Ma vi è di più. Oltre alle illustrate regole generali, il Regolamento definisce ulteriori e più dettagliati aspetti contenutistici del contratto, parimenti utili ad assicurare la trasparenza sul funzionamento della piattaforma digitale. Innanzitutto, lo stesso art. 3, lett. c-d), impone al fornitore di indicare le ragioni per le quali decida di sospendere, cessare o limitare la fornitura dei servizi di intermediazione online[10], così

[10] L'art. 4 regolamenta poi la procedura che il fornitore deve seguire per limitare, sospendere o cessare la fornitura dei servizi di intermediazione online a un determinato utente, prevedendo che la motivazione debba essere comunicata

come di trasmettere informazioni su eventuali canali di distribuzione aggiuntivi e potenziali programmi affiliati attraverso i quali rendere possibile la commercializzazione dei prodotti e dei servizi offerti dagli utenti.

Si pensi poi alla regolamentazione del c.d. *ranking* (art. 5). Per i soggetti che offrono beni e servizi sul mercato digitale è essenziale conoscere in anticipo quali sono i parametri in base ai quali ciascuna piattaforma determina il loro posizionamento e il posizionamento dei loro prodotti nello specifico *marketplace*[11]. La conoscibilità di tali aspetti ha un impatto centrale in quanto «*il modo in cui le offerte sono presentate ed elencate costituisce la variabile più rilevante per stabilire quali beni e servizi vengono scelti dai consumatori*»[12]. La trasparenza sui criteri di *ranking* è, quindi diretta a ridurre il margine di arbitrio dei fornitori e pone gli utenti nelle condizioni di poter valutare, prima di aderire al contratto, se sia conveniente attivare il servizio di intermediazione, tenendo conto sia di come le loro offerte sono ordinate e classificate sulla piattaforma, sia dell'eventuale costo per acquisire una posizione c.d. *premium.* Ciò che non emerge chiaramente dalla norma, tuttavia, è il grado di dettaglio in cui l'informazione sui parametri di *ranking* deve essere fornita, considerata anche la difficoltà di trovare un punto di equilibrio fra trasparenza e segreto commerciale (in particolare riguardo all'algoritmo per il calcolo dei fattori resi noti); i fornitori, infatti, sono tenuti a garantire la trasparenza su quei criteri solo nei limiti

usando un supporto durevole. Regole procedurali sono dettate anche per l'ipotesi di cessazione della fornitura del servizio.

[11] Con il termine "posizionamento" si fa riferimento «alla rilevanza relativa delle offerte degli utenti commerciali o alla rilevanza attribuita ai risultati della ricerca come presentati, organizzati o comunicati dai fornitori di servizi di intermediazione online o dai fornitori di motori di ricerca online, risultante dall'utilizzo di meccanismi algoritmici di ordinamento in sequenza, valutazione o recensione, dalla messa in evidenza visiva o da latri strumenti di messa in rilievo, o da una combinazione tra questi» (considerando n. 24).

[12] Così SMORTO, *op. cit.*, p. 66. Peraltro, la previsione in esame è in linea con quanto prevede l'art. 3, parag. 7, della Direttiva (UE) 2019/2161 (recante norme di modernizzazione della protezione del consumatore) che, nel modificare la Direttiva (CE) 2005/29 sulle pratiche commerciali sleali, introduce un art. 11 *bis* in cui si vieta che un professionista fornisca «risultati di ricerca in risposta a una ricerca online del consumatore senza che sia chiaramente indicato ogni eventuale annuncio pubblicitario a pagamento o pagamento specifico per ottenere una classificazione migliore dei prodotto all'interno di tali risultati».

in cui tali informazioni non violino le regole sul segreto commerciale (di cui alla Direttiva (UE) 2016/943).

A completare gli obbligo di *disclosure* del fornitore sono anche le regole dettate sui contenuti della *privacy policy* della piattaforma. L'art. 9 mira ad aumentare la trasparenza sulle regole di accesso ai dati (personali e non) forniti dagli utenti commerciali e dai consumatori per l'uso dei servizi, prescrivendo ai fornitori di inserire, all'interno di termini e condizioni, una descrizione relativa alle ipotesi di accesso tecnico e contrattuale (o alla mancanza di accesso) a tali dati, nonché alle eventuali condizioni di accesso e alle categorie di dati interessate. La disposizione, da leggere insieme ai principi del GDPR, regola, dunque, un profilo di assoluta rilevanza e attualità, costituendo oggi la trasparenza sulla *privacy policy* uno strumento indispensabile per professionisti/imprenditori per poter pianificare la loro strategia commerciale online[13].

A completare il quadro delle regole a tutela degli utenti commerciali va ricordato, infine, l'obbligo del fornitore di offrire informazioni su come i primi possano risolvere eventuali situazioni di conflitto con la piattaforma attraverso un sistema interno di gestione dei reclami. Ai sensi dell'art. 11, il funzionamento di tale sistema interno, di cui le piattaforme devono obbligatoriamente dotarsi, deve essere improntato a principi di trasparenza, parità di trattamento a parità di situazione e proporzionalità in base alla importanza e complessità dei reclami. Inoltre, tale meccanismo deve risultare facilmente accessibile e gratuito per gli utenti commerciali e avviene attraverso la presentazione di un reclamo, secondo regole che assicurino la celere e agile definizione della

---

[13] Si rinvia ai seguenti studi: Ren , *Beyond consent: improving data protection through consumer protecion law,* in *Internet Policy Review*, 2016, 5, p. 7 ss.; Albrect , *The EU's New Data Protection Law – ow A Directive Evolved Into a Regulation,* in *Computer Law Review International*, 2016, 2, p. 36 ss.; Metzger, *Data as Conuter-Performance: What Rights and Duties do Parties ave?,* in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2017, 8, p. 5 ss.; Giannone Codiglione, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione della privacy"*, in *Diritto dell'informazione e dell'informatica*, 2017, 2, p. 418 ss.; De Francesci , *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017; Luccini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori,* in *Contr. e impr.*, 2018, 1, p. 113 ss.; Tobani , *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento di massa dei dati personali*, Milano, 2018.

questione nel rispetto del diritto a un rimedio effettivo ed entro un termine ragionevole (cfr. art. 47 della Carta di Nizza)[14].

L'insieme delle regole sinteticamente richiamate dovrebbe contribuire a definire i contenuti del contratto di intermediazione online garantendo la trasparenza sui profili più rilevanti della relazione. Tali norme, tuttavia, talvolta difettano di dettagli operativi circa la procedura da seguire per garantire una efficace *compliance* allo *standard* di trasparenza richiesto (si pensi alle regole sull'accesso ai dati), altre volte non consentono di determinare il grado di precisione dei contenuti informativi da rendere, come con riguardo ai criteri di *ranking*. Manca, inoltre, una elencazione generale di pratiche scorrette o di termini/condizioni contrattuali vietati sul modello consumeristico. Occorre, dunque, interrogarsi sulla effettività della tutela garantita da tali norme, alla luce anche dei rimedi attivabili disposizione dell'utente.

15.3. I rimedi contrattuali a tutela degli utenti commerciali

Al fine di prevenire modifiche sfavorevoli e immotivate dei termini e delle condizioni contrattuali su cui l'utente ha prestato il consenso, l'art. 3, parag. 2, del Regolamento (UE) 2019/1150 prevede una prima tutela: il fornitore è tenuto a comunicare, su supporto durevole, qualunque cambiamento proposto dei termini e delle condizioni; non solo, ma le modifiche non possono essere attuate prima della scadenza di un termine di preavviso. A riguardo, si precisa che tale termine deve essere ragionevole e proporzionato alla natura e alla portata delle modifiche e non può avere durata inferiore a quindici giorni dalla data in cui il fornitore informa gli utenti delle modifiche stesse[15]. La previsione del termine di preavviso serve a consentire al professionista di

---

[14] I meccanismi interni di soluzione delle controversie comprendono, altresì, con la possibilità di indicare nel contratto due o più mediatori ai quali gli utenti commerciali possono rivolgersi per risolvere in via extragiudiziale eventuali controversie, compresi i reclami che non si riescano a risolvere mediante il sistema interno di gestione dei reclami di cui all'art. 11.

[15] L'art. 4, parag. 3 del Regolamento esclude l'obbligo del fornitore di rispettare il termine di preavviso al ricorrere di determinate situazioni: la necessità di adempiere un obbligo normativo o regolamentare che impone una immediata modifica dei termini e delle condizioni; la necessità di fronteggiare il verificarsi di un pericolo imprevisto e imminente connesso alla difesa dei servizi di intermediazione online e di tutti i suoi utenti contro frodi, *malware*, *spam*, ecc.

disporre del tempo necessario per adottare gli accorgimenti tecnici o commerciali necessari ad adattarsi alle modifiche delle condizioni contrattuali. La disposizione in esame appare interessante non soltanto perché regola la procedura da seguire per modificare il contenuto del contratto, ma anche perché fissa un primo strumento di tutela. In effetti, durante la pendenza del termine di preavviso, l'utente ha due possibilità: può decidere di rinunciare al termine mediante una dichiarazione scritta o un'azione chiara e affermativa (ad esempio, ai sensi dell'art. 3, parag. 2, tramite l'offerta di nuovi beni o servizi); oppure può risolvere il contratto con il fornitore.

Giova soffermare l'attenzione su tale rimedio. Poiché il Regolamento non indica chiaramente quale sia il *modus operandi*, è importante chiedersi se lo scioglimento del contratto possa essere realizzato in via stragiudiziale, mediante una semplice dichiarazione dell'utente pregiudicato dalle modifiche unilaterali realizzate in violazione dell'art. 3. Difatti, è opportuno ricordare come la risoluzione mediante dichiarazione sia uno strumento molto diffuso nella normativa euro-unitaria, in quanto reputato particolarmente agevole nelle sue modalità di esercizio. Di ciò possiamo trovare conferma, da ultimo, nell'art. 16 della Direttiva (UE) 2019/771, che riconosce al consumatore il diritto di risolvere il contratto di vendita di beni mediante una dichiarazione al venditore nella quale esprime la decisione di sciogliersi dal rapporto. Tale diritto a carattere stragiudiziale, che risulta sostanzialmente assimilabile a una forma di recesso unilaterale con funzione protettiva, offre una tecnica di scioglimento dal vincolo contrattuale molto agevole ed efficace. Sicché, il recepimento di tale disposizione nel nostro ordinamento rappresenterà un importante *step* nella definizione delle tutele attivabili dal consumatore[16], allineandolo agli Stati membri che già da tempo ammettono questa possibilità, come la Germania (con il *"gesetzsliche Rücktritt"* §§ 323 e 349 BGB)[17] e la Francia (con la *"rèsolution de*

---

[16] Il diritto di risoluzione stragiudiziale riconosciuto ora in via generale al consumatore avrà un significativo impatto sulla configurazione, nel nostro ordinamento, del rimedio risolutorio, nonché sul suo corretto inquadramento. Sia consentito rinviare a quanto osservato in Sartoris, *La risoluzione della vendita di beni di consumo nella dir. n. 771/2019 UE*, in *Nuova giur. civ. comm.*, 2020, 3, p. 706 ss.

[17] Cfr. Kaiser, *Die Rechtsfolgen des Rücktritts in der Schuldrechtsreform*, in *JZ*, 2001, p. 1057 ss.; Gaier, *Das Rücktritts (folgen)rect nach dem Schukderechtmodernisierungsgesetz*, in *WM*, 2002, p. 1 ss.; Koler , *Rücktrittsrechtilche Bereicherungshaftung*, in *JZ*, 2002, p. 682 ss.; Canaris, *La mancata attuazione del rapporto obbligatorio: profili generali. Il nuovo diritto delle Leistungsstorungen*, in *Riv. dir. civ.*, 2003, p. 21 ss.; Memmo, *Il nuovo modello*

contrat" dell'art. 138-2, co. 1, *code de la consommation*, o con l'art. 1226 del *code civil* che contempla in via generale la *"rèsolution par notification"*)[18].

Ebbene, si tratta di stabilire se le medesime considerazioni valgano anche per il diritto di risoluzione riconosciuto all'utente di una piattaforma digitale. La soluzione di tale quesito non ha una valenza solo teorica, ma anche pratica, oltre a rivestire un ruolo centrale per comprendere l'intensità con cui il legislatore europeo intende garantire la protezione dell'utente commerciale; il quale, pur non essendo un consumatore, presenta una posizione indubbiamente meritevole di considerazione e di tutela rispetto ai fornitori di servizi di intermediazione *online.* In conclusione, se si ragiona alla luce sia del dato sistematico testè ricordato, sia della *ratio* specifica del Regolamento, si dovrebbe concludere per il riconoscimento, anche a favore dell'utente commerciale, di una forma di recesso che avvicina la sua protezione a quella del consumatore.

Dubbi interpretativi si pongono anche rispetto all'altro rimedio contemplato dal Regolamento (UE) 2019/1150 per la violazione delle sue norme. In base all'art. 3, parag. 3, in caso di difformità dalle disposizioni dell'art. 3, parag. 1 oppure in caso di modifiche adottate in violazione delle disposizioni dell'art. 3, parag. 2, i termini e le condizioni sono *"nulli e privi di validità"* e, conseguentemente, non possono essere applicati al rapporto contrattuale. La norma in esame, nel prevedere la nullità, utilizza una espressione forse criticabile non solo in quanto tautologica, ma anche perché piuttosto scarna nella sua formulazione, non chiarendo né gli effetti né i i profili di disciplina di tale invalidità. Maggiori dettagli emergono dal considerando n. 20, ove si precisa che

---

tedesco della responsabilità per inadempimento delle obbligazioni, in *Contr. e impr.*, 2004, p. 797 ss.; DI MAJO, *Recesso e risoluzione del contratto nella riforma dello Schuldrecht: al di la` dell'inadempimento colpevole,* in *Eur. e dir. priv.*, 2004, p. 13 ss.; MARKENSIS, UNBERAT e JONSTON , *The German Law of Contract. A Comparative Treatise*, 2ª ed., Oxford-Portland, Oregon, 2006, 419 ss.; BARGELLI, *Dalla Schuldrechtmodernisierung all'attuazione della Direttiva 2011/83/Ue. Gli effetti del recesso nei contratti con il consumatore in Germania, in Annuario del contratto 2013*, diretto da D'ANGELO e ROPPO, Torino, 2014, p. 3 ss.

18 Cfr. ELMERIC , *Das Selbsthilferbot desfranzösichen Rechts und sein Einfluss auf Gesaltungs und Gestaltungsklargerechte*, Berlin, 1967; DE VINCELLES-BROUILLAUD, *Loi du 17 mars 204: novelles mesures protectrices du consommateur,* in *Dalloz*, 2014, 886 ss.: CANTEPIE e LATINA, *Le nouveau droit des obligations, Dalloz*, 2ª ed., 2018, n. 621, p. 621 ss.; GRANELLI, *Uno strumento (di dubbia efficacia) di risoluzione stragiudiziale: la diffida ad adempiere,* in *Pers. e merc.*, 2018, 1, p. 63 ss.

i termini e le condizioni non conformi «*si dovrebbero considerare come mai esistiti, con effetti* erga omnes *ed* ex tunc» allo specifico fine di tutelare gli utenti commerciali e, nel contempo, di garantire la certezza del diritto per entrambe le parti. Questo significa che la nullità in esame non colpisce l'intero contratto, bensì le sole «*disposizioni specifiche dei termini e delle condizioni che non sono conformi*», mentre «*le disposizioni rimanenti dovrebbero restare valide e applicabili, nella misura in cui possono essere dissociate da quelle non conformi*».

A nostro avviso, la nullità del contratto P2B merita di essere approfondita per almeno due aspetti, che, sicuramente, impegneranno gli interpreti in sede di applicazione del Regolamento (UE) 2019/1150. In primo luogo, è significativo che un regolamento qualifichi un rimedio in termini di "nullità". Probabilmente, tale presa di posizione va contestualizzata in relazione alla funzione propria del provvedimento in esame, che ha carattere generale ed è applicabile a tutti gli Stati membri senza bisogno dell'adozione di misure di recepimento. Sotto questo profilo, è chiaro che l'approccio del Regolamento (UE) 2019/1150 diverge profondamente da quello della Direttiva 1993/13/CE, che è un atto diretto a fissare obiettivi comuni da perseguire. Interessante è il raffronto con l'art. 6, che si limita a disporre che le clausole abusive «*non sono vincolanti per il consumatore*», senza definire il tipo di rimedio, la cui individuazione è rimessa agli Stati membri in sede di recepimento. Il legislatore italiano, dopo aver esitato a prendere posizione (come è noto, l'art. 1469 *quinquies* c.c. si esprimeva in termini di "inefficacia" delle clausole vessatorie), ha poi optato per la "nullità di protezione" dell'art. 36 cod. cons[19]. Ebbene, benché diversa la fonte di disciplina, ci pare che tanto nei contratti B2C, quanto nei contratti P2B, la tutela contro disposizioni contrattuali imposte unilateralmente dalla

[19] Gli studi sono innumerevoli: Alpa, *Per il recepimento della direttiva comunitaria sui contratti dei consumatori*, in *Contr.*, 1994, p. 115 ss.; Gentili, *L'inefficacia delle clausole abusive*, in *Riv. dir. civ.*, 1997, I, p. 412 ss.; Monticelli, *Dalla inefficacia delle clausole vessatorie alla nullità del contratto (Note a margine dell'art. 1469 quinquies, comma 1 e 3, c.c.)*, in *Rass. dir. civ.*, 1997, p. 565 ss.; Passagnoli, *Nullità speciali*, Milano, 1998; Id., *Commento all'art. 1469-quinquies, comma 1, 3 e 5*, in Vettori (a cura di), *Materiali e commenti sul nuovo diritto dei contratti*, Padova, 1999, p. 158 ss.; Scalisi, *Nullità e inefficacia nel sistema europeo dei contratti*, in *Eur. dir. priv.*, 2001, p. 507 ss.; Polidori, *Discipline della nullità e interessi protetti*, Napoli, 2001; Valle, *L'inefficacia delle clausole vessatorie*, Padova, 2004; Di Marzio, *Nullità di protezione, codice del consumo e contratti del* consumatore, in *Riv. dir. priv.*, 2005, p. 837 ss.; Girolami *La nullità di protezione nel sistema delle invalidità negoziali. Per una teoria moderna della nullità relativa*, Padova, 2008.

parte forte sia affidata a una nullità che opera in forma necessariamente parziale, al fine di garantire l'espulsione chirurgica delle sole disposizioni svantaggiose per il contraente tutelato e la conservazione della restante parte del contratto. In secondo luogo e conseguentemente, da un punto di vista funzionale, l'art. 3 del Regolamento (UE) 2019/1150 sembra offrire rimedio con finalità di protezione a favore dell'utente commerciale, come esplicitato dal considerando n. 20, benché dalla lettura di quest'ultimo emerga anche un ulteriore obiettivo, cioè la garanzia della certezza del diritto per entrambe le parti. Sicché, la nullità parziale necessaria, in questo specifico contesto, sembra tutelare l'utente nell'ottica più ampia di garantire la trasparenza del contratto attraverso l'eliminazione di qualsiasi disposizione in contrasto con il Regolamento. L'evidenziata ambiguità, o comunque, la doppia dimensione di interessi a cui viene attribuita rilevanza, sollevano poi dubbi circa le modalità operative del rimedio sotto il profilo della legittimazione ad agire. Non è chiaro se la nullità possa essere azionata dal solo utente commerciale, in linea con il rimedio consumeristico, o se, invece, la legittimazione sia aperta a chiunque abbia interesse. Né, tanto meno, è chiaro se, magari proprio in considerazione del duplice piano di interessi coinvolti, il giudice disponga di un potere di rilevazione officiosa della nullità analogo a quello che la Corte di Giustizia predica rispetto alle clausole abusive[20].

---

[20] In dottrina: MONTICELLI, *Nullità, legittimazione relativa e rilevabilità d'ufficio,* in *Riv. dir. priv.*, 2002, 4, p. 685 ss.; PAGLIANTINI, *La nullità di protezione tra rilevabilità d'ufficio e convalida,* in *Pers. e merc.*, 2009, 1, p. 28 ss.; ID., *La rilevabilità officiosa della nullità secondo il canone delle Sezioni Unite: "Eppur si muove"?,* in *Contr.*, 2012, 11, p. 869 ss.; ID., *La non vincolatività (delle clausole abusive) e l'interpretazione autentica della Corte di Giustizia,* in *Contr.*, 2017, 1, p. 11 ss.; ALESSI, *Clausole vessatorie, nullità di protezione e poteri del giudice: alcuni punti fermi dopo le sentenze Joros e Asbeek Brusse*, in *Jus civile*, 2013, 7, p. 388 ss.; ID., *Nullità di protezione e poteri del giudice tra Corte di Giustizia e Sezioni Unite della Corte di Cassazione,* in *Eur. dir. priv.*, 2014, 4, p. 1141 ss.. In giurisprudenza: Corte di Giustizia, 27 giugno 2000, cause riunite C-240/1998 a C-244/1998, *Océano Grupo Editorial e Salvat Editores*, in *Racc.,* I, p. 4941; Corte di Giustizia, 21 novembre 2002, causa C-473/2000, *Cofidis SA e Jean-Louis Fredout*, in *Racc.,* I, p. 10875; Corte di Giustizia, 26 ottobre 2006, causa C-168/2005, *Mostaza Claro*, in *Racc.,* I, 10421; Corte di Giustizia, 6 ottobre 2009, causa C-40/2008, *Asturcom Telecomunicaciones*, in *www.curia.europa.eu;* Corte di Giustizia, 4 giugno 2009, causa C-243/2008, *Pannon,* in *Racc.*, I, p. 4812; Corte di Giustizia, 14 giugno 2012, causa C-618/2010, *Banco Español de Crèdito,* in *www.curia.europa.eu*; Cass., Sez. Un., 4 settembre 2012, n. 14828, in *Nuova giur. civ. comm.*, 20112, I, p. 12 ss., con nota di SCOGNAMIGLIO, *Il giudice e le nullità: punti fermi e problemi aperti nella giurisprudenza della Corte di Cassazione*; Cass., Sez. Un., 12 dicembre 2014, nn. 26242-26243, in *Corr. giur.*, 2015, I,

15.4. Prime riflessioni sulla effettività della tutela e nuove sfide interpretative

Le regole illustrate rappresentano un importante punto di partenza per la tutela di una categoria di soggetti che, fino a ora, non godeva di considerazione specifica, men che meno in ambito digitale, nonostante possibili ipotesi di vulnerabilità. È altrettanto evidente, però, che il Regolamento (UE) 2019/1150 presenti alcune ambiguità di fondo, non essendo agevole l'esatta identificazione degli interessi tutelati, e tanto si ripercuote sia sulla definizione dei rimedi esperibili, sia sulla carenza delle relative regole operative. La tutela degli utenti commerciali, in caso di violazione degli obblighi di trasparenza del fornitore, sembra ispirarsi alla tutela del consumatore contro le clausole abusive; anzi, essa appare rafforzata dalla positivizzazione di un rimedio specifico e vincolante in modo omogeneo per tutti gli ordinamenti. La nullità, inoltre, operando retroattivamente e con efficacia *erga omnes*, produce effetti sia nello specifico rapporto negoziale, sia per tutti gli altri contratti predisposti dal fornitore con le medesime disposizioni censurate. Sicché, dietro tale nullità, ci pare di scorgere non solo uno strumento rimediale a favore del singolo utente leso, ma anche una vera e propria misura di deterrenza-sanzione nei confronti del fornitore responsabile. Ancor più significativa è poi la circostanza che la nullità sia legata all'inadempimento di obblighi di trasparenza, assimilati a una regola di validità. La distanza dal principio di separazione tra regole di comportamento/di validità appare evidente[21]. Da questo punto di vista, allora, il binomio in purezza instaurato fra trasparenza e nullità risulta denso di conseguenze anche rispetto a quel dibattito, legandosi, oltretutto, a quell'orientamento della giurisprudenza europea in tema di clausole abusive che sembra andare nella direzione di istituire una equazione

p. 70 ss., con nota di Carbone, *"Porte aperte" delle Sezioni Unite alla rilevabilità d'ufficio del giudice della nullità del contratto* e di Pagni, *Nullità del contratto – Il "sistema" delle impugnative negoziali dopo le Sezioni Unite*.

21 Cfr. D'Amico, *Regole di validità e regole di comportamento nella formazione del contratto,* in *Riv. dir. civ*., 2002, 1, p. 37 ss.; Meruzzi, *La responsabilità precontrattuale tra regole di validità e di condotta,* in *Contr. e impr*., 2006, 4-5, p. 944 ss.; Scoditti, *Regole di comportamento e regole di validità: i nuovi sviluppi della responsabilità precontrattuale,* in *Foro it*., 2007, 1, c. 2093; M. Ticozzi, *Violazione di obblighi informativi e sanzioni,* in *Contr*., 2007, p. 363 ss.; Vettori, *Regole di validità e di responsabilità di fronte alle Sezioni Unite. La buona fede come rimedio risarcitorio,* in *Obbl. e contr*., 2008, 2, p. 104 ss.

«*tra opacità informativa-inconsapevolezza del contrarre-nullità*»[22] da studiare attentamente nelle sue molteplici implicazioni.

A nostro avviso, giova osservare, tuttavia, che la meritevole esigenza di tutelare nuove forme di vulnerabilità tipiche dell'ambiente digitale si pone in termini ben diversi dalle istanze di protezione proprie dei contratti consumeristici. La posizione degli utenti commerciali ci appare meno svantaggiata di quella dei consumatori per l'ovvia considerazione che chi usufruisce di servizi di intermediazione *online* lo fa nell'esercizio della propria attività commerciale o professionale e, quindi, con piena consapevolezza e programmazione strategica delle scelte sulle modalità di offerta dei propri prodotti o servizi. Non a caso, spesso gli utenti si avvalgono di consulenti anche interni che forniscono loro il supporto necessario a valutare i rischi e i vantaggi connessi all'uso di una certa piattaforma e ad approntare la miglior strategia di vendita. Da questo angolo visuale, ci pare che il Regolamento fornisca uno *standard* minimo di regole di trasparenza e di equità, che richiedono poi di essere graduate dagli interpreti in relazione alle specifiche caratteristiche e competenze del singolo utente.

In ultimo, ci preme svolgere una considerazione di carattere più generale circa il grado di efficacia delle regole analizzate, poiché molteplici appaiono gli elementi di incompletezza. Ad esempio, il Regolamento non stabilisce quali obblighi informativi/di trasparenza debbano essere garantiti dalla piattaforma nel particolare caso in cui sia essa stessa a offrire beni o servizi direttamente agli utenti, dismettendo la veste di intermediario *online.* Allo stesso modo, non è chiaro quali siano gli obblighi da rispettare quando l'utente della piattaforma non sia un professionista, ma un privato che intende concludere transazioni con altri privati, secondo il modello sempre più diffuso della c.d. economia collaborativa (c.d. *sharing economy*)[23]. Sicché, da questi punti di vista, il Regolamento non appare in grado di disciplinare compiutamente e in modo unitario tutti i rapporti contrattuali coinvolti

---

[22] Così PAGLIANTINI, *La trasparenza consumeristica tra "dottrina" della Corte ed equivoci interpretativi,* in *Eur. dir. priv.*, 20193, p. 652.

[23] In tema di piattaforme collaborative v.: KATZ, *Regulating the Sharing Economy,* in *Barkeley Technology Law Journal*, 2015, p. 1067 ss.; MUSTACCI e SOMMA, *Il caso Uber. La sharing economy nel confronto tra common law e civil law*, Milano, 2016; QUARTA, *Il diritto dei consumatori ai tempi della peer economy. Prestatori di servizi e prosumers: primi spunti,* in *Eur. e dir. priv.*, 2017, p. 667 ss.; SMORTO, *Economia della condivisione e antropologia dello scambio,* in *Dir. pubbl. comparat. eur.*, 2017, p. 119 ss.; ATZOPULOS, *The Collaborative Economy and Eu Law Review*, Oxford, 2018.

nell'uso della piattaforma. Tale limitazione del *target* soggettivo ai rapporti P2B potrebbe rappresentare un punto di debolezza, contribuendo alla incertezza circa le regole applicabili al di fuori dei casi previsti[24]. Ci pare, invero, altrettanto criticabile che nel raggio di disciplina del Regolamento non rientrino neppure i consumatori che acquistano beni o servizi tramite piattaforma, pur essendo i destinatari finali dell'offerta. Al loro rapporto con il fornitore del servizio di intermediazione *online* si applica la normativa consumeristica esistente, che, ovviamente, non affronta i problemi specifici posti dalla contrattazione in ambiente digitale, salvo quanto ora previsto dalla Direttiva (UE) 2019/2161, il coordinamento con la quale non è chiarito[25], aumentando così il carattere frammentario della disciplina delle piattaforme.

Le sfide per l'interprete e per il legislatore appaiono, dunque, tutt'altro che esaurite. E in una visuale d'insieme, l'aspetto che dovrà essere approfondito in futuro ci pare sia ancora più profondo e di sistema. Se, da un lato, si impone la necessità di introdurre regole *ad hoc* per la tutela di nuove posizioni contrattuali, non essendo sufficiente una mera trasposizione di quelle dettate in materia consumersitica, dall'altro è opportuno riflettere sui confini, sempre più sfumati, della distinzione consumatore/professionista nell'ambito della contrattazione su piattaforma digitale.

---

24 Di questa opinione sono Rossi, *La sharing economy nel diritto internazionale*, Torino, 2019, p. 38-39; Inglese, *op. cit*., p. 466 ss.; Iamiceli, *op. cit*., p. 407 ss.

25 Cfr. Smorto, *La tutela del contraente debole nella platform economy dopo il Regolamento UE 2019/1150 e la Direttiva UE 2019/2161 (c.d. Omnibus)*, in Falce, (a cura di), *Fairness e innovazione nel mercato digitale*, Torino, 2020, p. 49 ss.; Loos, *The Modernization of European Consumer Law (Continued): More Meat on the Bone After All,* in *European Review of Private Law*, 2020, 2, p. 407 ss.; Tommasi, *The "New Deal" for Consumers: Towards More Effective Protection?*, *ivi*, p. 311 ss.

16. Il pagamento mediante dati personali

Shaira Thobani

16.1. Introduzione

È nota l'osservazione per cui i dati sono il nuovo petrolio. Come il petrolio, per essere fonte di utilità, i dati devono essere estratti e trattati. Quel che qui interessa è il profilo dell'estrazione, cioè della raccolta dei dati. Dove trovare i dati personali e come raccoglierli?

I dati possono essere acquisiti o direttamente presso l'interessato, o presso terze parti che già li detengono. L'avanzare delle nuove tecnologie, sempre più pervasive e invasive, ha comportato una maggiore facilità nella raccolta dei dati: in ragione del crescente utilizzo di dispositivi che tracciano gli utenti, gli individui lasciano dietro di sé (nella più parte dei casi inconsapevolmente) scie di dati, raccolti da chi gestisce tali dispositivi e da coloro che ad essi hanno accesso. Per raccogliere i dati una strategia è dunque quella di incentivare la fruizione di beni e servizi che, nell'essere utilizzati, in virtù della tecnologia adottata, registrano informazioni. L'altra strategia è invece quella di chiedere informazioni direttamente agli interessati. Le tipologie di dati raccolti sono diverse nei due casi: se ci si rivolge con una richiesta all'interessato, le informazioni sono filtrate da una sua valutazione e verbalizzazione; nell'altro caso, le informazioni raccolte riguardano i suoi comportamenti. La collaborazione richiesta per consentire la raccolta dei dati è dunque diversa nei due casi: mentre nel primo l'interessato deve collaborare attivamente comunicando egli stesso le informazioni, nel secondo la collaborazione è, per così dire, passiva, nel senso che è sufficiente che l'interessato usi un bene o servizio affinché i dati generati da tale comportamento siano suscettibili di registrazione.

In entrambi i casi, tuttavia, una forma di collaborazione è richiesta. In quest'ottica può essere letta la diffusione dell'offerta di beni e servizi il cui utilizzo comporta la raccolta di dati. Nel nostro ordinamento tale raccolta non è libera: come noto, la disciplina in materia di protezione dei dati personali consente il trattamento solo in presenza di una condizione legittimante. Tra queste vi è il consenso dell'interessato, che (pur costituendo una delle basi legittimanti il trattamento, posta dal legislatore sullo stesso piano delle altre) ha finito per assumere un ruolo preponderante. Si comprende allora la soluzione affermatasi nella prassi di legare in qualche modo l'offerta di beni e servizi alla prestazione del consenso al trattamento dei dati da parte degli utenti, condizionando l'una all'altra, al fine di assicurare che i dati registrati attraverso la fruizione dei beni e servizi offerti possano essere lecitamente trattati.

Le fattispecie sono varie. Innanzitutto, in particolar modo nel mondo online, si è affermato il business model di offrire beni e servizi senza prevedere un corrispettivo in denaro, ma, per l'appunto, chiedendo all'utente, come condizione per accedere alla prestazione, di acconsentire al trattamento dei propri dati: si tratta delle c.d. operazioni di *tying* (in cui il consenso viene "legato" a una prestazione)[1]. In altri casi la richiesta del consenso al trattamento è posta come condizione non per accedere a un bene o servizio, ma per fruire di sconti o agevolazioni ulteriori[2]. Più raramente si prevede una remunerazione diretta in denaro in favore di coloro che acconsentono al trattamento dei propri dati[3].

In tutti questi casi i dati sono, almeno di fatto, utilizzati come mezzo per accedere a una controprestazione (il bene o servizio, lo sconto, la somma di denaro). Si è parlato così di "pagamento" mediante dati personali, i quali, similmente al denaro, sembrano costituire uno

---

1 Si pensi a tutti i servizi online offerti "gratuitamente", come ad esempio caselle di posta elettronica, motori di ricerca, servizi di newsletter ecc.

2 Si pensi al caso delle tessere fedeltà o a quello delle scatole nere a fronte della cui installazione negli autoveicoli è prevista una riduzione del premio assicurativo. Su quest'ultimo caso, v. T. Pertot, *L'assicurazione auto con scatola nera. Sconti tariffari vs dati personali*, in *Oss. dir. civ. comm.*, 2018, 2, 529 ss.

3 Sembra avvicinarsi a un tale modello il caso (portato dal Garante italiano all'attenzione del Comitato europeo per la protezione dei dati personali) dell'app Weople, che promette agli iscritti una remunerazione in cambio della cessione dei propri dati personali.

strumento scambiato sul mercato per godere in cambio di beni, servizi o altre utilità[4].

Dal punto di vista del diritto, tale prassi può essere esaminata sotto due profili. Innanzitutto, e preliminarmente, ci si può chiedere se si tratti di una prassi lecita: è lecito il "pagamento" mediante dati personali? È lecito subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento dei dati personali? In secondo luogo, una volta tracciati i confini della liceità di tali operazioni, ci si può chiedere come le operazioni in questione siano disciplinate. In altre parole, come è regolato il mercato dei dati personali[5]?

16.2. Il pagamento mediante dati personali: liceità

La prima questione attiene, come si è detto, all'ammissibilità delle operazioni in cui i dati sono scambiati con una controprestazione e, dunque, alla liceità della subordinazione al consenso al trattamento dell'accesso a beni o servizi. La risposta in proposito offerta dal legislatore e dagli interpreti non è univoca.

---

[4] Sulla possibilità di considerare i dati personali (*rectius* il consenso al trattamento dei dati personali) come oggetto di una prestazione e sul conseguente nesso di corrispettività tra tale consenso e l'accesso al bene o servizio per cui il consenso è richiesto v. C. Langhanke, M. Schmidt-Kessel, *Consumer data as consideration*, in *Journal of European Consumer and Market Law*, 2015, 6, 218 ss.; A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 67 ss.; A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2017, 8, 1 ss.; G. Resta, V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 436 ss.; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, 160 ss.; V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf.*, 2018, 4-5, 689; A. De Franceschi, *Il "pagamento" mediante dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1381 ss.; V. Ricciuto, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 3, 642 ss.; R. Senigaglia, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2020, 2, 760 ss.

[5] Si fa riferimento al mercato per così dire primario dei dati, nel senso di mercato in cui sono gli interessati stessi a immettere i dati nei circuiti di circolazione. Diverso è invece il discorso con riguardo al mercato secondario dei dati, in cui i titolari del trattamento, una volta raccolti i dati, li fanno a loro volta circolare. In generale, sui problemi legati al mercato dei dati v. V. Zeno-Zencovich, *Do "Data Markets" Exist?*, in *Riv. dir. media*, 2019, 1, 22 ss.

Partiamo dal dato normativo. L'art. 7, par. 4 del regolamento 2016/679 (Regolamento generale sulla protezione dei dati, qui di seguito Regolamento) in tema di consenso al trattamento afferma che "[n]el valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".

Tale norma ci dice, innanzitutto, che non vi sono problemi di liceità se il trattamento dei dati personali è necessario all'esecuzione del contratto: è chiaro, ad esempio, che il venditore può subordinare la vendita online di un bene alla comunicazione, da parte dell'acquirente, dell'indirizzo (dato personale) cui inviare il bene. I problemi sorgono, invece, laddove il trattamento non sia necessario a prestare il bene o servizio richiesto: questo è il caso, ad esempio, del venditore di un bene che subordini la consegna al consenso dell'acquirente a ricevere email promozionali. Il Regolamento non vieta *tout court* tale operazione, ma afferma che si tratta di una circostanza da "tenere nella massima considerazione" nel valutare "se il consenso sia stato liberamente prestato".

La questione della liceità dello scambio di dati personali e servizi è dunque ricondotta al diverso tema della libertà del consenso al trattamento[6]. La domanda che ci si pone è la seguente: è libero il consenso se posto come condizione per accedere a un bene o servizio? Se la risposta è negativa (e, dunque, se il consenso non è da considerarsi libero), posto che la libertà è uno dei requisiti di validità del consenso al trattamento e dunque di liceità del trattamento stesso, il consenso al trattamento non potrà essere richiesto come condizione di fruizione di una prestazione e il trattamento che eventualmente ne segue sarà illecito. Ne deriva dunque un divieto delle operazioni di *tying*. La soluzione è di segno contrario se la risposta è positiva (se, dunque, il consenso è considerato libero).

Il Regolamento, come si è detto, non risolve univocamente la questione. Si noti che si tratta di una scelta non casuale: una versione precedente del regolamento poneva un divieto netto alle operazioni di

---

[6] Su tale requisito sia consentito il rimando alle riflessioni svolte in S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento dei diritti della personalità*, in *Europa dir. priv.*, 2016, 2, 513 ss.

tying[7], divieto poi stemperatosi nella versione attuale a seguito di un'attenta valutazione in sede legislativa degli interessi in gioco.

L'incertezza della prescrizione legislativa ha dato luogo a una divergenza di posizioni da parte degli interpreti. Da un lato vi è chi nega con fermezza l'ammissibilità della richiesta del consenso come condizione per l'accesso a beni o servizi, escludendo in tal modo la liceità della "cessione" dei dati da parte degli interessati per usufruire di una prestazione.

Questo è l'orientamento della nostra autorità garante per la protezione dei dati personali che, con una posizione sostenuta sin dalle prime pronunce sul tema, afferma che "non può definirsi 'libero', e risulta indebitamente necessitato, il consenso a ulteriori trattamenti di dati personali che l'interessato 'debba' prestare quale condizione per conseguire una prestazione richiesta"[8].

Si tratta di una posizione condivisa non solo da altre autorità garanti nazionali europee[9], ma anche dagli organi europei deputati alla protezione dei dati personali. Il Comitato europeo per la protezione dei dati personali, riprendendo quanto già in precedenza affermato dal

---

7 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Draft Report 17 December 2012*, 2012/0011(COD), amendment no 107, in cui il Parlamento proponeva di aggiungere il seguente paragrafo all'art. 7: "The execution of a contract or the prevision of a service may not be made conditional on the consent to the processing or use of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1)(b)".

8 Tale affermazione, applicata in maniera pressochè costante dal Garante fin dai suoi primi anni di attività, è contenuta anche in un provvedimento a carattere generale: v. le *Linee Guida in materia di attività promozionale e contrasto allo spam*, in Registro dei provvedimenti 4 luglio 2013, n. 330. Per una ricognizione dei provvedimenti sul punto, sia consentito il rimando a S. Thobani, *La libertà del consenso al trattamento dei dati personali*, cit., 532-538.

9 V. ad es. la posizione espressa dalla *Commission nationale informatique & libertés*, in *Projet de recommandation sur les modalités pratiques de recueil du consentement prévu par l'article 82 de la loi du 6 janvier 1978 modifiée, concernant les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur (recommandation «cookies et autres traceurs»)* del 14 gennaio 2020, art. 3. L'Information Commissioner's Office ha invece adottato una posizione più sfumata: mentre raccomanda "that organisations do not make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent cannot be sought separately", sottolinea al contempo che occorre considerare "whether there is a choice of other services and how fair it is to couple consent to marketing with subscribing to the service" (*Direct marketing guidance*, versione 2.3 del 6 marzo 2018, par. 66).

Gruppo Art. 29, afferma infatti che, tramite la citata previsione sulla libertà del consenso, il Regolamento "ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract"[10]. In quest'ottica, non sarebbe lecito condizionare una prestazione al consenso al trattamento in quanto in tal caso l'interessato non avrebbe una "real choice" se acconsentire o meno, in ragione della circostanza che in caso di rifiuto gli sarebbe precluso l'accesso al bene o servizio desiderato. Ne deriva, a contrario, la possibilità di chiedere lecitamente il consenso al trattamento se all'interessato vengono offerte due versioni equivalenti del medesimo servizio, l'una cui accedere prestando il consenso, l'altra usufruibile anche senza prestarlo: in questo caso, infatti, l'utente sarebbe realmente libero di scegliere se acconsentire o meno, in quanto manterrebbe in ogni caso la possibilità di accedere alla prestazione. Questo presuppone, chiaramente, che le due versioni siano equivalenti[11]. Se la versione che non prevede il trattamento richiede l'esborso

---

[10] Comitato europeo per la protezione dei dati personali, *Guidelines 5/2020 on consent under Regulation 679/2016*, versione 1.1 del 4 maggio 2020, par. 26. Il Comitato riprende sostanzialmente quanto già affermato dal Gruppo di Lavoro Art. 29 nelle *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 10 aprile 2018. Nello stesso senso v., in dottrina, J.P. Albrecht, *The EU's New Data Protection Law – How A Directive Evolved Into A Regulation*, in *Computer Law Review International*, 2, 2016, 36, il quale afferma categoricamente che "as a rule consent cannot be free if it is made a condition for the execution of a contract despite not being necessary for that purpose".

[11] Comitato europeo per la protezione dei dati personali, *Guidelines 5/2020*, cit., par. 37, secondo cui le prestazioni devono essere "genuinely equivalent". Lo stesso Gruppo di lavoro Art. 29 aveva in precedenza aperto a tale possibilità: v. Article 29 Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 aprile 2014, 47, il quale afferma che "[i]n the context where consumers signing up for 'free' online services actually 'pay for' these services by allowing the use of their personal data, it would also contribute towards a favourable assessment of the balance – or towards the finding that the consumer had a genuine freedom of choice, and therefore valid consent was provided under Article 7(a) – if the controller also offered an alternative version of its services, in which 'personal data' were not used for marketing purposes". V. anche la posizione espressa dal Garante europeo per la protezione dei dati, *Opinion 5/2016 Preliminary. EDPS Opinion in the review of the ePrivacy Directive (2002/58/EC)*, 22 luglio 2016, 15-16, secondo cui il fornitore del servizio deve "(i) either provide a choice whether or not to provide consent to processing data not necessary for the provision of the service without any detriment, (ii) or at least, make available a paying service at a reasonable price (without behavioural advertising and collection of data) as an alternative to the services paid by users' personal information".

di una somma di denaro sproporzionata rispetto alla prestazione offerta, non si potrebbe ritenere sussistente una "real choice"; diversamente, la previsione di un corrispettivo ragionevole non sembrerebbe inficiare la libertà di scelta dell'interessato.

Il Comitato esclude invece la sussistenza di una effettiva possibilità di scelta se sul mercato esistono prestazioni equivalenti offerte da altri operatori per la cui fruizione non è richiesto il consenso al trattamento dei dati[12]. Così, ad esempio, chi fornisce un servizio di posta elettronica chiedendo il consenso al trattamento come condizione per la registrazione non potrebbe invocare la liceità di tale operazione segnalando che sul mercato esistono altri fornitori di servizi email che non richiedono il consenso al trattamento.

Una soluzione diversa è stata invece proposta dalla nostra giurisprudenza di legittimità, secondo cui le operazioni di *tying* sono illecite "quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato"[13]. Il caso riguardava l'iscrizione ad una newsletter in tema di finanza, fisco, lavoro e diritto, per la quale era richiesto il consenso al trattamento dei dati per finalità promozionali. Come affermato dalla Corte, "nell'ipotesi di offerta di un generico servizio informativo" di tal fatta, "si tratta di informazioni agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio". La soluzione è dunque opposta a quella sposata dagli interpreti a livello europeo: per il nostro giudice di legittimità, se sul mercato esistono servizi equivalenti (in questo senso deve leggersi il richiamo alla "fungibilità") per cui non è richiesto il consenso al trattamento dei dati e se non si tratta di servizi irrinunciabili, allora è lecito condizionare l'offerta del bene o servizio al consenso al

---

12 Comitato europeo per la protezione dei dati personali, *Guidelines 5/2020*, cit. Per una critica a tale impostazione si rimanda a S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *RIv. dir. media*, 2019, 3, 142.

13 Cass. civ., 2 luglio 2018, n. 17278, in *Giur. it.*, 3, 2019, 530 ss. In dottrina, nel senso che il regolamento non pone un divieto assoluto alle operazioni di tying, v. S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, 55; A. Metzger, *Data as Counter-Performance*, cit., 5; E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. impr.*, 2018, 1, 113; G. Resta, V. Zeno-Zencovich, *Volontà e consenso*, cit., 432; C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. impr.*, 2020, 2, 883.

trattamento. Lo scopo è sempre quello preservare la possibilità di accedere a beni e servizi senza "cedere" i propri dati, ma è sufficiente a tal fine la presenza sul mercato di offerte di servizi analoghi che non prevedano il "pagamento" in dati personali.

A fronte di tali divergenze interpretative, torniamo alle previsioni del legislatore europeo. Come si è detto, la norma contenuta nel Regolamento non pone un divieto netto. Indizi legislativi per inquadrare meglio la questione possono cercarsi in altri corpi normativi, in particolare in alcune norme a tutela dei consumatori.

Interessanti indicazioni sono contenute nella disciplina relativa ai contratti di fornitura di servizi e contenuto digitale[14]. La proposta di direttiva inizialmente redatta faceva riferimento, con riguardo al proprio ambito di applicazione, ai "contratti in cui il fornitore fornisce contenuto digitale al consumatore, o si impegna a farlo, e in cambio del quale il consumatore corrisponde un prezzo oppure fornisce attivamente una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi dato"[15]. Il riferimento è chiaramente alle fattispecie che ci interessano, quelle, cioè, in cui i servizi sono "pagati" non in denaro ma in dati. A seguito dei rilievi mossi dal Garante europeo per la protezione dei dati personali che – in linea con la cennata interpretazione prevalente in sede europea – ha contestato la configurazione dei dati personali come una "mere commodity"[16], il legislatore europeo ha espunto dalla versione finale della direttiva qualunque richiamo ai dati come controprestazione, prevedendo semplicemente l'applicabilità della direttiva anche "nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore e il consumatore fornisce o si

---

[14] In proposito v. F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 2019, 1, 34 ss.; A. De Franceschi, *Il "pagamento" mediante dati personali*, cit., 1386 ss.; G. Resta, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679*, in A. D'Angelo, V. Roppo (a cura di), *Annuario del contratto 2018*, Torino, 2019, 125 ss. In generale, sulle questioni sollevate da tale direttiva, cfr. i contributi raccolti in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market*, Cambridge, 2016.

[15] Art. 3, par. 1 della Proposta di direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 9 dicembre 2015, COM(2015) 634.

[16] Garante europeo per la protezione dei dati personali, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for supply of digital content,* 14 marzo 2017.

impegna a fornire dati personali all'operatore economico" (art. 3, para. 1, direttiva UE 2019/770). A tale previsione si accompagna il riconoscimento che "la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce" (considerando n. 24). L'eliminazione del riferimento ai dati come controprestazione non ha però mutato la disciplina: la direttiva, nel delimitare il proprio campo di applicazione, contempla espressamente il caso in cui i dati sono scambiati con un bene o servizio, accostandolo a quello in cui i consumatori pagano un corrispettivo in denaro.

Da un lato le norme in materia di dati personali, pur senza vietarle del tutto, guardano con sospetto alle operazioni di *tying* (art. 7, par. 4, Regolamento); dall'altro, le norme in materia di consumatori contemplano tali operazioni senza metterne in discussione la liceità. Come coordinare tali corpi normativi? In realtà, il contrasto si stempera se si considerano i diversi campi di applicazione dei due corpi normativi. Il Regolamento ci dice quando si possono trattare lecitamente i dati; la direttiva, quali sono i rimedi a disposizione dei consumatori. In altre parole, la direttiva non prende posizione sulla liceità o meno della prassi in esame (questione che è il Regolamento ad affrontare), ma si limita a dire che ai consumatori che "pagano" tramite dati personali spettano rimedi analoghi a quelli a disposizione dei consumatori che pagano in denaro. A fronte della prassi dilagante di offrire servizi in cambio di dati, la direttiva ne prende atto e, senza interrogarsi sulla liceità di tali operazioni, si preoccupa unicamente di tutelare i consumatori.

Non vi è dunque contrasto tra i due corpi normativi; resta tuttavia il fatto che l'ipotesi patologica dell'uno costituisce quella fisiologica dell'altro.

In conclusione, è lecito il "pagamento" mediante dati personali? Come si è visto non ci sono risposte univoche. La tendenza in sede interpretativa europea sembra essere quella di un netto divieto, a cui non corrisponde tuttavia una analoga posizione da parte del legislatore europeo, che, come si è visto, da un lato (in sede di protezione dei dati personali) ha escluso un tale rigido divieto e, dall'altro (in sede di tutela dei consumatori), si è limitato a prendere atto della prassi.

16.3. Il pagamento mediante dati personali: disciplina

Tanto (non) chiarito sulla questione della liceità delle operazioni di "pagamento" mediante dati personali, vediamo ora i principali punti di disciplina.

Due sono i profili che si esamineranno. Innanzitutto, come si vedrà, una prima preoccupazione è quella di garantire che le operazioni in questioni siano condotte in maniera trasparente, a tutela della persona intesa sia come interessato (soggetto cui i dati si riferiscono) sia come consumatore. Un secondo profilo riguarda il nesso di corrispettività tra il consenso al trattamento, da un lato, e i beni e servizi offerti in cambio, dall'altro.

16.3.1. Trasparenza

La necessità che le operazioni in cui i dati sono scambiati con un bene o servizio siano condotte in maniera trasparente si ricava sia dalla normativa in materia di protezione di dati personali, sia da quella a tutela dei consumatori.

Per quanto riguarda la prima, il Regolamento (in continuità con la precedente direttiva), richiede che il consenso al trattamento sia informato e specifico (art. 4, n. 11). Si tratta di due facce della stessa medaglia: da un lato, la manifestazione del consenso deve essere preceduta da un'informazione che precisi in maniera puntuale, tra gli altri elementi, le finalità del trattamento. Dall'altro, il consenso deve essere espresso con riguardo a specifiche finalità. Quello che è un obbligo di condotta in capo a chi tratta i dati (informare l'interessato) si trasforma in un requisito di contenuto del consenso (che deve essere specifico), il quale copre solo i trattamenti di cui l'interessato è stato puntualmente informato.

L'interessato – che i dati siano raccolti da lui o presso terzi – deve infatti essere informato, per quel che qui interessa, in merito ai dati trattati, alle finalità del trattamento, ai soggetti che possono trattare i dati e alla eventuale sussistenza di processi decisionali automatizzati (artt. 13, 14). Il consenso è riferito al trattamento così delineato e deve essere prestato "per una o più specifiche finalità" (art. 6, par. 1, lett. a). L'interessato deve dunque essere portato a conoscenza del trattamento dei dati che lo riguardano e informato circa le caratteristiche e finalità dello stesso.

L'interessato deve inoltre essere informato in merito alla base giuridica del trattamento: gli si deve cioè comunicare se i dati sono trattati sulla base del suo consenso o in virtù di un'altra condizione legittimante. All'interessato occorre infatti specificare "se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione dei dati" (art. 3, par. 2, lett. e, Regolamento). Questo significa che, se il consenso al trattamento è richiesto come condizione per accedere a un bene o servizio, occorre chiarire all'interessato che la richiesta dei dati è frutto di una scelta del titolare (e non deriva invece da un obbligo legale) e che in mancanza di consenso l'interessato non potrà accedere al bene o servizio. Se si pongono in essere operazioni di *tying*, queste devono dunque essere condotte in maniera trasparente.

È interessante notare che a un analogo risultato si è giunti tramite l'applicazione della normativa a tutela dei consumatori, a ulteriore dimostrazione dell'intreccio dei due corpi normativi[17].

Nel nostro ordinamento interno, l'autorità garante della concorrenza e del mercato già da tempo sanziona, in quanto ingannevole, la pratica di pubblicizzare come gratuita l'offerta di beni o servizi per usufruire dei quali si richiede (non il pagamento di una somma di

[17] L'intreccio tra la tutela dei dati personali e la disciplina consumeristica è assai stretto nell'ordinamento statunitense, come segnala M. Graziadei, *Collusioni transatlantiche: consenso e contratto nel trattamento dei dati personali*, in F. Di Ciommo, O. Troiano (a cura di), *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, Piacenza, 2018, 367. Come si dirà subito nel testo, la raccolta non trasparente di dati è infatti sanzionata anche sotto il profilo delle pratiche commerciali scorrette: sul punto v. A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*, cit., 101 ss. Cfr. anche M. Rhoen, *Beyond consent: improving data protection through consumer protection law*, in *Internet Policy Review*, 5, 2016, 7-8 (il quale accenna anche alla possibilità di applicare le norme in materia di clausole vessatorie); N. van Eijk, C.J. Hoofnagle, E. Kannekens, *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, in *European Data Protection Law Review*, 3, 2017, 334, i quali svolgono l'analisi con riguardo sia all'ordinamento statunitense che a quello europeo; C. Goanta, S. Mulders, *'Move Fast and Break Things': Unfair Commercial Practices and Consent on Social Media*, in *Journal of European Consumer and Market Law*, 4, 2019, 141 ss. Sull'intreccio tra i diversi piani di tutela, dei consumatori da un lato, e degli interessati dall'altro, v. G. Resta, *Digital platforms and the law: contested issues*, in *Riv. dir. media*, 1, 2018, 245 ss.

denaro ma) il consenso al trattamento dei dati personali[18]. L'Autorità ha recentemente ribadito tale posizione, sanzionando come pratica commerciale ingannevole la condotta di non informare chiaramente gli utenti in fase di registrazione a un servizio delle finalità remunerative dello stesso e, anzi, di pubblicizzarne la "gratuità"[19]. Il giudice amministrativo ha confermato tale posizione, ritenendo "corretta la valutazione della Autorità circa l'idoneità della pratica a trarre in inganno il consumatore e a impedire la formazione di una scelta consapevole, omettendo di informarlo del valore economico di cui la società beneficia in conseguenza" dell'accesso al servizio (nel caso di specie, un social network)[20].

È interessante notare come in tali provvedimenti, al fine di affermare l'applicabilità della normativa a tutela del consumatore, si sia sentita la necessità di configurare il consenso al trattamento dei dati come "una vera e propria prestazione passiva"[21], e il dato personale come "possibile oggetto di compravendita": "[i]l fenomeno della patrimonializzazione del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio"[22]. Come accennato sopra, la normativa a protezione dei consumatori non si pronuncia tuttavia sulla liceità del "pagamento"

---

18 Provv. nn. 10276, 10277, 10278 e 10279, 20 dicembre 2001, in Boll. sett. AGCM n. 51-52, 7 gennaio 2002, 148-165.

19 AGCM, provv. *Facebook – condivisione dati con terzi*, 29 novembre 2018, n. 27432. L'Autorità ha anche sanzionato come pratica commerciale aggressiva quella di preselezionare l'opzione di condivisione dei dati prospettando agli utenti in caso di deselezione rilevanti limitazioni nella fruizione del servizio, maggiori rispetto a quelle effettivamente applicate. In quest'ultimo senso v. anche, oltre al provvedimento appena citato, AGCM, provv. *WhatsApp – Trasferimento dati a Facebook*, 11 maggio 2017, n. 26597, su cui v. G. Giannone Codiglione, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione della privacy"*, in *Dir. inf.*, 2, 2017, 418 ss.

20 TAR Lazio, 10 gennaio 2020, n. 260, in *Foro amm.*, 2020, 1, 99 ss., che ha sul punto confermato il provvedimento dell'AGCM *Facebook – condivisione dati con terzi*, cit. V. anche TAR Lazio, 11 aprile 2018, n. 5043, reperibile sul sito www.*dirittoegiustizia.it*.

21 AGCM, provv. 20 dicembre 2001, n. 10276, cit.

22 TAR Lazio, 10 gennaio 2020, n. 260, cit.

mediante dati personali, ma si limita a prenderne atto (riconoscendo esplicitamente il valore economico dei dati) e a predisporre mezzi di tutela per l'utente.

Tale è l'impostazione seguita anche in sede europea. La Commissione Europea ha infatti affermato che la violazione della normativa in materia di dati personali può rilevare ai fini della valutazione del carattere sleale di una pratica commerciale sotto il particolare profilo della trasparenza. Così, in ragione del "valore economico *de facto*" assunto dai dati personali, la pratica di non comunicare ai consumatori che i dati che questi ultimi sono tenuti a fornire per accedere al servizio saranno usati a fini commerciali "può essere considerata un'omissione ingannevole di informazioni rilevanti"[23].

Il risultato cui si giunge è dunque sempre quello della necessaria trasparenza delle operazioni in questione, richiesta talora per proteggere l'interessato, talaltra per tutelare il consumatore[24].

16.3.2. Corrispettività

Un secondo profilo riguarda il nesso di corrispettività che unisce la prestazione del consenso al trattamento dei dati al bene o servizio la cui erogazione è condizionata a tale consenso. Come si atteggia tale nesso e quali sono le conseguenze sul rapporto tra interessato/utente e fornitore del servizio?

Un primo piano della questione riguarda i rimedi a favore del consumatore. Come si è detto, la presa d'atto che vi è una corrispettività, almeno di fatto, tra consenso al trattamento, da un lato, e beni e servizi, dall'altro, ha condotto prima gli interpreti e poi il legislatore a riconoscere rimedi a favore dei consumatori in presenza (e in ragione) di tale corrispettività.

---

[23] Commissione europea, *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*, 25 maggio 2016, 28.

[24] Pare in proposito utile riportare quanto affermato in un passaggio del provvedimento del TAR Lazio 10 gennaio 2020, n. 260, cit., che ben esprime il diverso campo di applicazione dei due corpi normativi. Il giudice esclude il "rischio di un effetto plurisanzionatorio della medesima condotta (intesa come identico fatto storico) posta in essere dal professionista che gestisce il 'social network'", in quanto "[l]'oggetto di indagine da parte delle competenti autorità riguarda, infatti, condotte differenti dell'operatore, afferenti nel primo caso al corretto trattamento del dato personale ai fini dell'utilizzo della piattaforma e nel secondo caso alla chiarezza e completezza dell'informazione circa lo sfruttamento del dato ai fini commerciali".

In tale direzione si è mossa non solo la già richiamata direttiva 2019/770 sui contratti di fornitura di contenuto e servizi digitali, ma anche la direttiva 2019/2161 per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, che ha modificato la disciplina in materia di contratti conclusi a distanza e fuori dei locali commerciali[25]: entrambi gli interventi normativi sono volti ad estendere le tutele previste in favore dei consumatori sia che l'utente paghi un corrispettivo in denaro, sia che "paghi" in dati[26].

Al riguardo, in merito al nesso di corrispettività tra dati e servizi, possono farsi due notazioni.

Innanzitutto, per come è stato contemplato dalla disciplina in questione, si tratta di un nesso di corrispettività per così dire allentato.

La versione precedente (non adottata) della direttiva 2019/770 prevedeva che la stessa si applicasse solo nel caso in cui il consumatore fornisse "attivamente" i dati, con esclusione dei casi in cui "il fornitore raccoglie le informazioni, compresi i dati personali, quali l'indirizzo IP, o altre informazioni generate automaticamente, ad esempio le informazioni raccolte e trasmesse mediante un cookie, senza che il consumatore le fornisca attivamente, anche se accetta il cookie" (considerando n. 14). In altre parole, l'intento era quello di estendere la tutela consumeristica ai soli casi in cui fosse necessaria una collaborazione attiva dell'interessato/utente e, dunque, alle ipotesi in cui gli fosse

---

25 Che ha aggiunto il par. 1*bis* all'art. 3 della direttiva 2011/83/UE, ai sensi del quale "La presente direttiva si applica anche se il professionista fornisce o si impegna a fornire un contenuto digitale mediante un supporto non materiale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali ai professionisti, tranne i casi in cui i dati personali forniti dal consumatore siano trattati dal professionista esclusivamente ai fini della fornitura del contenuto digitale su supporto non materiale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui il professionista è soggetto, e questi non tratti tali dati per nessun altro scopo".

26 Si noti che tale estensione è stata prevista solo con riguardo alla fornitura di servizi o contenuti digitali: la direttiva 2019/771 relativa a determinati aspetti dei contratti di vendita di beni, si applica invece ai soli contratti di vendita tra consumatore e venditore, definiti come i contratti con cui "il venditore trasferisce o si impegna a trasferire al proprietà di beni al consumatore, e quest'ultimo ne paga o si impegna a pagarne il prezzo". Ai fini dell'interpretazione di tale norma, la mancata menzione dei casi in cui il consumatore acconsente al trattamento dei dati, presente invece negli altri testi normativi europei richiamati, conduce inevitabilmente a considerare il "prezzo" sinonimo di "corrispettivo in denaro".

richiesto di comunicare proprie informazioni (ad esempio, il nome in sede di registrazione) o di acconsentire al trattamento delle informazioni che avrebbe successivamente messo a disposizione del fornitore del servizio (ad esempio, le foto caricate su un social network)[27].

La versione finale della direttiva non prevede invece come requisito per la sua applicabilità che i dati siano forniti "attivamente", limitandosi a escludere dal proprio campo di applicazione, per quel che qui interessa, i casi in cui l'operatore economico raccolga solo metadati[28]. In tal modo, la disciplina consumeristica si allinea alla normativa in materia di protezione dei dati personali: come si è detto in apertura, il consenso al trattamento è necessario sia nel caso in cui i dati siano raccolti grazie a una comunicazione dell'interessato, sia nell'ipotesi in cui i dati si riferiscano a comportamenti da quest'ultimo posti in essere nell'utilizzo di beni o servizi, senza necessità di essere comunicati.

In altre parole, il nesso di corrispettività è considerato sussistente (al fine di applicare le tutele consumeristiche) tutte le volte in cui il consenso dell'interessato è necessario per trattare i dati, indipendentemente da una sua collaborazione attiva e da una sua effettiva consapevolezza in merito al trattamento. Non vi è invece corrispettività qualora i dati possano essere trattati anche senza il consenso dell'interessato (si pensi al caso in cui vi sia un legittimo interesse del titolare che giustifichi il trattamento)[29].

---

27 In senso critico rispetto a tale iniziale previsione v. A. De Franceschi, *La circolazione dei dati personali*, cit., 79-82; A. Metzger, *Data as Counter-Performance*, cit., 3; M. Narciso, *Gratuitous Digital Content Contracts in EU Consumer Law*, in *Journal of European Consumer and Market Law*, 2017, 203 s.; G. Resta, V. Zeno-Zencovich, *Volontà e consenso*, cit., 424.

28 Considerando n. 25. La direttiva non si applica altresì ai casi (che qui non interessano) in cui "il consumatore, senza aver concluso un contratto con l'operatore economico, è esposto a messaggi pubblicitari esclusivamente al fine di ottenere l'accesso ai contenuti digitali o a un servizio digitale". La direttiva lascia però agli Stati membri la possibilità di estendere anche ai casi esclusi la disciplina in questione.

29 Ci si può chiedere se vi sia corrispettività laddove all'utente sia offerta la possibilità di accedere al bene o servizio anche senza acconsentire al trattamento. Le norme sul campo di applicazione materiale delle direttive sopra richiamate non paiono, alla lettera, escluderlo, facendo riferimento al caso in cui il consumatore "fornisce o si impegna a fornire dati personali". Tale soluzione è però problematica. Si consideri infatti che, se il consenso al trattamento è facoltativo, il rapporto tra tale consenso e la fornitura del bene o servizio pare essere quello di mera contestualità, e non di corrispettività. In altre parole, in questo caso la fornitura del bene o servizio rappresenta una mera occasione per raccogliere dati, e non una condizione per poterli trattare: la sua configurazione come controprestazione è dunque dubbia.

Una seconda notazione riguarda le tipologie di rimedi previsti a tutela del consumatore.

Si è detto che scopo della normativa in questione è quello di estendere la protezione consumeristica ai casi in cui vi sia un "pagamento" mediante dati personali. Non vi è tuttavia una piena parificazione dei rimedi. In particolare, in caso di difetto di conformità del contenuto o servizio digitale, il rimedio della riduzione del prezzo è previsto solo qualora vi sia stato un pagamento in denaro (art. 14, par. 4, direttiva 2019/770)[30]. Potrebbe sembrare una previsione ovvia: può esservi restituzione in denaro, tramite la riduzione del prezzo, solo laddove una somma di denaro sia stata corrisposta. Si noti tuttavia che, a voler svolgere sino in fondo l'assunto del valore economico dei dati personali, si sarebbe potuto far riferimento a un meccanismo di quantificazione in denaro del valore dei dati al fine di ammettere anche in questo caso una parziale restituzione del "prezzo". Ma, anche nell'ottica del legislatore consumeristico che pur contempla l'ipotesi del "pagamento" mediante dati, i dati non sono denaro[31].

Tanto brevemente detto sui rimedi in favore del consumatore, un secondo piano della questione in merito alla corrispettività tra consenso al trattamento dei dati, da un alto, e beni o servizi, dall'altro, riguarda eventuali diritti e rimedi in favore del fornitore del servizio.

La corrispettività comporta la sussistenza di un nesso sinallagmatico tra le prestazioni (intese, qui, in senso atecnico). La disciplina a tutela dei consumatori si preoccupa di chiarire come tale sinallagma operi a favore del consumatore. Rimane invece da chiarire se e come esso possa operare in favore di chi fornisce il servizio.

---

30 Coerentemente con tale previsione, si richiede, ai fini dell'esercizio del diritto di recesso del consumatore, che il difetto di conformità non sia di lieve entità solo se vi è stato un prezzo in denaro (art. 14, par. 6).

31 E questo innanzitutto per la difficoltà di quantificarne il valore. Difatti, benchè il valore economico dei dati personali sia indubbio, seri dubbi permangono su quale sia il modo più accurato per misurarlo. V., ad esempio, lo studio effettuato dalla Organisation for Economic Co-Operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OEDC Digital Economy Papers No. 220, 2013. Sulle modalità di quantificazione del valore economico dei dati personali, v. anche G. Malgieri, B. Custers, *Pricing privacy – the right to know the value of your personal data*, in *Computer Law & Security Review*, 34, 2017, 294-297. Cfr. in proposito F.G. Viterbo, *Freedom of contract and the commercial value of personal data*, in *Contratto e impresa Europa*, 2, 2016, 606-607.

Innanzitutto, si tratta di analizzare se il nesso di corrispettività faccia sorgere profili di doverosità con riguardo alla posizione dell'interessato che acconsente al trattamento dei propri dati per accedere a un servizio. Così, ci si potrebbe chiedere se il fornitore disponga di rimedi (e quali) qualora, ad esempio, l'interessato fornisca informazioni false[32].

In secondo luogo, occorre interrogarsi sulla sorte del servizio fornito qualora l'interessato revochi il consenso al trattamento. In tal caso può il servizio essere interrotto? Il Regolamento prevede infatti il diritto dell'interessato "di revocare il proprio consenso in qualsiasi momento" (art. 7, par. 3), affermando anche che il consenso non è libero se l'interessato non può revocarlo "senza subire pregiudizio" (considerando n. 42). È chiaro che se si ritiene che le operazioni di *tying* siano di per sé illecite, allora, non potendo sussistere alcun lecito sinallagma, la revoca del consenso non potrà in alcun modo comportare l'interruzione del servizio: l'uno non dipende dall'altro, e, anzi, l'interruzione del servizio costituirebbe un "pregiudizio" volto a coartare indebitamente la volontà dell'interessato. Saremmo dunque in presenza di un sinallagma peculiare, per così dire, unidirezionale, in quanto darebbe luogo a tutele e rimedi nei confronti di una sola delle parti (il consumatore). Solo se, al contrario, si ritiene che vi siano margini di liceità per le operazioni di *tying*, allora, nella misura in cui si tratti di operazioni lecite, la revoca del consenso non può che comportare la cessazione del servizio. Se il sinallagma è lecito, esso opera normalmente in entrambe le direzioni.

16.4. Cenni conclusivi

La questione del "pagamento" mediante dati personali può essere guardata attraverso diverse lenti.

Innanzitutto, tramite lenti che ingrandiscano e consentano l'esame, da vicino, dei singoli rapporti in cui ha luogo uno scambio tra dati personali e servizi. In questa prospettiva le questioni riguardano la tutela del singolo interessato/consumatore e la sorte del singolo rapporto. Si noti, tuttavia, che, per quanto riguarda la tutela dell'interessato, chi intenda far cessare il trattamento dei propri dati potrà in ogni momento

[32] In proposito v. G. Resta, V. Zeno-Zencovich, *Volontà e consenso*, cit., 438 s.; A. De Franceschi, *Il "pagamento" mediante dati personali*, cit., 1405.

revocare il consenso, senza necessità di invocare l'illiceità delle operazioni di *tying*. Sul fronte della tutela del consumatore, chi ha acconsentito al trattamento dei dati per accedere a un servizio per la cui fruizione non gli viene richiesta altra prestazione, non necessariamente avrà interesse a far valere i rimedi previsti in suo favore chiedendo la risoluzione del (o recedendo dal) contratto. Peraltro, la difficoltà di quantificare il valore dei dati, unito alla considerazione che l'interessato ha pur goduto di un servizio, rischiano di rendere un esercizio complesso e sterile quello di interrogarsi sulle conseguenze in termini restitutori e risarcitori dell'illiceità delle operazioni in esame. Più in generale, gli interessati/consumatori nella maggior parte dei casi neppure si accorgeranno che i propri dati sono oggetto di trattamento (mentre saranno ben contenti di usufruire di servizi senza pagare un prezzo in denaro)[33].

L'importanza della questione in merito all'illiceità o meno delle operazioni in questione può forse meglio valutarsi adottando una lente che consenta di guardare al problema da lontano, in modo da apprezzarne la valenza collettiva. Scopo delle norme in materia di protezione dei dati personali che limitano le operazioni di *tying* è quello di limitare grosse concentrazioni di dati personali, il cui trattamento in massa genera rischi per la società nel suo complesso[34]. Scopo delle norme a protezione dei consumatori è la tutela, oltre che del singolo consumatore, del mercato[35]. In entrambi i casi le prescrizioni agiscono sul piano individuale per raggiungere risultati su quello collettivo.

---

33 Si tratta del c.d. paradosso della privacy, per cui gli interessati affermano di badare molto alla propria riservatezza, ma non pongono in essere alcun comportamento per tutelare i propri dati. In proposito v. A. Acquisti, J. Grossklags, *Privacy and Rationality in individual Decision Making*, in *IEEE Security & Privacy*, 2005, 3(1), 26; S. Kokolakis, *Privacy Attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*, in *Computers & Security*, 2017, 64, 122; L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *European Journal of Privacy Law & Technologies*, 2018, 1; N. Gerber, P. Gerber, M. Volkamer, *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior*, in *Computers & security*, 2018, 77, 226.

34 Valga, per tutti, il richiamo a S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 4, 585 ss.

35 Neppure si accenna qui alle interferenze con il diritto della concorrenza. In proposito, ci si limita a segnalare un'interessante pronuncia tedesca: OLG Düsseldorf, 26 August 2019, Case VI-Kart 1/19 (V).

Con questo non si intende negare l'importanza della prospettiva individuale: la massa di rapporti la cui disciplina è volta a tutelare (anche) interessi generali è pur sempre costituita da rapporti singoli. Le due prospettive non possono però essere esaminate disgiuntamente.

17. *Smart assistant* e dati personali: quali rischi per gli utenti?

Lavinia Vizzoni

17.1. Assistenti vocali, intelligenza artificiale e *Internet of Things*

Lo sviluppo delle tecnologie digitali applicate alla quotidianità ha condotto, negli ultimi anni, a una massiccia diffusione dei c.d. *smart assistant*. Si tratta di *software* che, grazie al c.d. *machine learning*, ossia a sistemi di apprendimento che utilizzano algoritmi di intelligenza artificiale, sono in grado di riconoscere il linguaggio naturale degli esseri umani e di interagire con gli stessi. Tale interazione può essere rivolta a soddisfare diversi tipi di richieste (ad esempio, fissare appuntamenti, impostare sveglie, *timer* e promemoria, riprodurre musica o notiziari, fornire previsioni meteo e di traffico) o a compiere determinate azioni, come accendere una luce, azionare un elettrodomestico o regolare la temperatura di un'abitazione.

Il loro costo contenuto, la frequente preinstallazione nei *device* e la semplicità di funzionamento ne hanno agevolato la diffusione e l'impiego. Gli assistenti in questione possono infatti essere installati in una pluralità di supporti: dagli *smart speaker* collocati all'interno delle abitazioni domestiche, ma anche di altri ambienti antropizzati, quali i luoghi di lavoro([1]), se non anche le automobili, ai *device* che portiamo fisicamente con noi, i c.d. *wearable*, sino ai dispositivi più diffusi come gli

---

[1] Con i conseguenti rilevanti interrogativi che si pongono in ordine alla sorveglianza dei lavoratori. Sulle intersezioni fra *data protection* e diritto del lavoro, v. precipuamente E. DAGNINO, *Tecnologie e controlli a distanza*, in *Dir. rel. ind.*, 2015, p. 988 ss. e STOLFA, *La tutela della privacy sul luogo di lavoro: gli orientamenti della Corte Europea dei Diritti dell'Uomo*, in *Lav. giur*, 2018, p. 530 ss.

smartphone, i *personal computer* e i *tablet*. In particolare, gli stessi si prestano anche ad agevolare lo svolgimento di attività quotidiane anche da parte di soggetti con autonomia ridotta.

Per fare questo, gli assistenti vocali raccolgono quasi ininterrottamente dati personali relativi sia all'utente diretto sia, più in generale, a coloro che si trovano nell'ambiente in cui gli stessi operano. Per di più, gli *smart assistant* si possono avvalere anche di soluzioni proprie del c.d. *Internet of Things* (*Iot*)[2], che offre la possibilità di sfruttare i vari oggetti, appunto, le "*things*" che incorporano i programmi di assistenza vocale "intelligente", per la raccolta di informazioni e l'attuazione di interventi finalizzati al miglioramento dei servizi offerti[3]. Gli *smart assistant* sono infatti capaci di "dialogare" con altri dispositivi ***IoT***, come *smartwatch*, *smart* TV, sistemi di controllo da remoto o di videosorveglianza; il che amplifica la possibilità di raccolta, incrocio dei dati e diffusione di informazioni personali.

Se in passato l'*Internet of Things* si collocava in una rete di sensori in grado di restituire informazioni mediante tecnologie di RFID (*Radio Frequency IDentification*)[4], con l'avvento del Web si è passati ad un contesto più evoluto, in grado di catturare quantitativi ben maggiori di informazioni attraverso la connessione dei dispositivi. Le applicazioni dell'*IoT* investono oggi molteplici settori, a partire dall'industria 4.0[5],

---

[2] Sulle applicazioni dell'*Iot*, con particolare riguardo proprio agli assistenti virtuali, cfr. le preoccupazioni espresse già da Ramaccioni *La protezione dei dati personali e il danno non patrimoniale. Studio sulla tutela della persona nella prospettiva risarcitoria*, Napoli, 2017, p. 16 ss. e p. 288 ss.

[3] Sulle potenzialità dell'*Iot* cfr. Santosuosso *Intelligenza artificiale e diritto*, Milano, 2020, 180 ss., il quale evidenzia come l'Internet delle cose sia al centro dell'interesse della politica economica dell'Unione Europea. In tale prospettiva, esso diviene punto focale per la digitalizzazione della società, nel contesto dell'implementazione delle tecnologie 5G e nel perseguimento del più ampio obiettivo della realizzazione del *digital single market*. Sugli sviluppi dell'*Iot* e sui relativi impatti in tema di trattamento dei dati personali, cfr. Tosi, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice* Privacy, in Id, (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, Milano, 2019, p. 36 ss.

[4] Cfr. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Milano, 2019, p. 1213.

[5] Nel contesto di quella che è una vera e propria *smart factory*, sono state sviluppate soluzioni che, per quanto futuristiche appaiano, sono già una realtà e vengono attualmente utilizzate in ambienti industriali tecnologicamente progrediti. Rientrano

e si raccordano sempre di più all'uso di piattaforme, che permettono di connettere e controllare esternamente i dispositivi, di memorizzare e analizzare i dati raccolti, di monitorare e comandare gli oggetti connessi[6].

Rispetto ai dati personali raccolti dagli assistenti *smart* connessi diventa inoltre oggi cruciale la nozione non solo di interconnessione, ma anche di interoperabilità fra i sistemi informatici[7]: la tendenza in atto è infatti quella dello sviluppo di multipiattaforme che puntano al controllo di oggetti *smart* di fornitori e marche diverse da un unico punto di contatto. Particolarmente significativo appare l'accordo di recente stretto tra Amazon, Apple e Google, in genere non propensi ad alleanze, per la creazione di un protocollo unitario per la casa connessa, grazie al quale tutti i dispositivi potranno essere controllati con Alexa, Siri e Google Assistant[8].

---

nel novero di siffatte soluzioni i dispositivi di robotica indossabile, quali gli esoscheletri per applicazioni industriali volti ad aumentare le capacità operative dei lavoratori che svolgono attività manuali e di movimentazione; o le *smart suit*, ossia tute realizzate anche tramite scansioni del corpo del lavoratore; così come le postazioni di lavoro auto-adattive, strutturate sulla base delle caratteristiche proprie di chi è chiamato ad utilizzare quelle postazioni, anche in termini di condizioni fisiche e di affaticamento. In proposito, v. l'analisi di GRECO, MANTELERO, *Industria 4.0, robotica e* privacy-by-design, in *Dir. informaz. informatica*, 2018, p. 883 ss.

6 In generale, sulle piattaforme *online*, v. DE FRANCESCHI, *La vendita di beni con elementi digitali*, Napoli, 2019, p. 19 ss. In proposito, cfr. anche C. BUSCH, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, in DE FRANCESCHI, SCHULZE (a cura di), *Digital Revolution – New Challenges for Law*, Baden-Baden, 2019, p. 57 ss.

7 Sulla interoperabilità v. RICCIO, PEZZA, *Portabilità dei dati personali e interoperabilità*, in CUFFARO, D'ORAZIO, RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 398 ss. Lo scritto (p. 404 s.) si sofferma sulla interoperabilità, in relazione all'effettività del diritto alla portabilità nel settore della telefonia mobile, evidenziando la positività del modello inglese che pone gli obblighi relativi a carico del precedente gestore. Cfr. anche BATTELLI, D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in TOSI (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, cit., p. 202 ss.

8 La notizia, datata 19 dicembre 2019, è tratta dal sito web www.corriere.it/tecnologia. Oltre ai citati Google, Amazon ed Apple, hanno aderito all'accordo in questione i produttori riuniti nella Zigbee Alliance, fra cui Ikea, Samsung SmartThings e Schneider Electric, a conferma del grande interesse che il mercato della domotica suscita. Il relativo protocollo sarà *open source* e tutti potranno realizzare prodotti compatibili con i tre noti assistenti vocali.

Lungo tale versante, sono destinate ad imporsi all'attenzione degli studiosi proprio le implicazioni legate alla sicurezza e all'interoperabilità di architetture *IoT*, che assumono sembianze sempre più capillari[9].

Da altra parte, l'implementazione dei programmi di assistenza vocale si lega strettamente ai progressi ottenuti nel campo dell'intelligenza artificiale. Lanciando ricerche vocali, l'utente inoltra segnali proprio ai sistemi di intelligenza artificiale utilizzati dagli *smart assistant*, che, tramite quegli *input* continuano a implementarsi così riuscendo a comprendere la domanda e a fornire risposte sempre migliori, riducendo progressivamente il margine di errore[10].

Più precisamente, l'intelligenza artificiale utilizza algoritmi sofisticati per ordinare enormi quantità di dati, tracciare schemi e fare previsioni: attività che sarebbero ripetitive e lunghe, se non praticamente impossibili, da eseguire manualmente. Le macchine "intelligenti" contribuiscono fortemente allo svolgimento di tali attività, avvalendosi anche della nota capacità di imparare da sé stesse, attraverso il c.d. *machine learning*, o addirittura di elaborare nuovi percorsi di apprendimento con il c.d. *deep learning*[11]. L'intelligenza artificiale pone però all'attenzione del giurista una serie di interrogativi che mettono alla prova le capacità di risposta dell'ordinamento giuridico e delle relative categorie concettuali[12]. Come osservato, l'idea che una macchina, per quanto ''intelligente'', possa assumere autonomamente decisioni che riverberano i loro effetti anche su diritti fondamentali della persona, suscita preoccupazione, e impone una riflessione approfondita che, in

---

9 Qualche risultato nella direzione della interoperabilità sembra stia arrivando da ONEM2M (http://www.onem2m.org/), un progetto congiunto di otto enti di standardizzazione mondiali, tra cui ETSI (Europa), ARIB (Giappone), CCIA (Cina), TIA (Nord America) e duecento partner, che si propone di definire degli standard di riferimento (*framework* di interlavoro) per la costruzione di piattaforme di servizio interoperanti.

10 V. D'Acquisto, Naldi, Big Data *e* Privacy by Design. *Anonimizzazione, Pseudonimizzazione, Sicurezza*, Torino, 2017, p. 9 ss.

11 Cfr. Crisci, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm*., 2018, p. 1787 ss.

12 V. Ruffolo, Gabrielli, *Introduzione*, in Id (a cura di), *Intelligenza artificiale e diritto,* in *Giur. it*., 2019, p. 1657 ss. Cfr. inoltre Zorzi Galgano, *Introduzione,* in Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, p. 15 ss.

prospettiva, coinvolge anche le decisioni di politica del diritto da assumere[13].

La vera sfida — che già si profila con una certa chiarezza — dei meccanismi che sfruttano, per il loro funzionamento, algoritmi di intelligenza artificiale, sarà quella di conseguire soluzioni che garantiscano, anche sul versante etico, di soddisfare i criteri di spiegabilità, robustezza, correttezza e tracciabilità[14]. Non a caso, dalla Commissione Europea sono di recente giunte Linee Guida per uno sviluppo etico dell'intelligenza artificiale: si tratta di un documento, dal valore programmatico, che detta indicazioni per uno sviluppo di un'intelligenza artificiale a misura di essere umano[15], da ultimo compendiate nel «Libro bianco sull'intelligenza artificiale — Un approccio europeo all'eccellenza e alla fiducia», datato 19 febbraio 2020.

A livello nazionale, è d'uopo quanto meno ricordare l'elaborazione dalle Proposte per una strategia italiana per l'intelligenza artificiale del Gruppo di esperti MISE[16], che, sulla stessa linea, indicano un percorso verso l'implementazione di un'intelligenza artificiale complementare — piuttosto che sostitutiva — all'intelligenza umana, tale da consentire di garantire il rispetto dei valori e dei principi fondamentali[17].

---

13 Cfr. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, p. 63 ss.

14 Sul bilanciamento, in chiave etica, fra diffusione di soluzioni tecnologiche avanzate e impatto sui diritti e le libertà della persona, cfr. WRIGHT, *A framework for the ethical impact assessment of information technology*, in *Ethics Inf. technol*., 2011, p. 199 ss.

15 Sono i risultati diffusi dall'*High Level Group on Artificial Intelligence* della Commissione europea, reperibili nel sito web www.ec.europa.eu. La Commissione stessa, nelle sue comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, ha diffuso la sua visione al riguardo, che sostiene un'AI «etica, sicura e all'avanguardia realizzata in Europa». Le linee guida della Commissione europea per un'intelligenza artificiale affidabile sono peraltro state aggiornate nel settembre 2019 dal centro studi del Parlamento europeo. Sul difficoltoso percorso orientato al pervenir ad un sistema europeo di *governance* dell'intelligenza artificiale, v. inoltre MAZZINI, *A system of governance for Artificial Intelligence through the lens of emerging intersections between AI and EU law*, in DE FRANCESCHI, SCHULZE (a cura di), *Digital Revolution – New Challenges for Law*, cit., p. 245 ss.

16 La prima versione delle Proposte per una strategia italiana per l'intelligenza artificiale è datata luglio 2019 ed è reperibile nel sito web del Ministero, www.mise.gov.it.

17 É tuttavia rilevante segnalare che la versione finale di tali Proposte, formulata nel corrente anno dal Gruppo di esperti di alto livello del MISE, esprime apertamente una visuale non del tutto collimante con le indicazioni provenienti dall'Europa. In particolare, nelle Proposte nazionali si fa riferimento alla circostanza per cui

17.2. I relativi vantaggi e rischi

Proprio lo sviluppo di algoritmi evoluti di intelligenza artificiale, unitamente all'interconnessione degli oggetti *smart*, ha consentito dunque di creare soluzioni parzialmente o totalmente autonome, le cui capacità di apprendimento e monitoraggio delle abitudini degli utenti crescono esponenzialmente, di pari passo al tentativo, sempre più preciso, di adattare il livello di servizio offerto sulla base delle richieste effettuate dagli individui stessi. E a sua volta, la proficua convergenza fra *IoT* e *AI* dipende dalla disponibilità di dati personali.

In questo contesto, l'attenzione particolare che può essere riservata agli assistenti vocali "intelligenti" deriva da una duplice ragione: lo stretto legame del loro funzionamento con i dati personali, posto che l'operatività del dispositivo abbisogna, anzi, è dichiaratamente funzionale alla raccolta delle informazioni dall'utilizzatore e dal suo ambiente esistenziale, nonché il loro elevato grado di pervasività rispetto alla vita degli utenti.

Soprattutto, considerazioni inerenti all'ingente quantitativo di dati personali raccolti ed elaborati dai *device*, e correlative perplessità, sono state avanzate con riguardo agli *home speaker*, che trovano collocazione proprio nella casa, luogo dell'*habitat* domestico nel quale si svolge la personalità umana, da difendere gelosamente dalle intrusioni esterne, tanto da elevarsi, nella sua accezione di domicilio, ad area inviolabile al pari della stessa libertà personale[18].

Come osservato, gli *home speaker* rappresentano una sorta di *alter ego*[19], se non dei veri e propri «maggiordomi» dei proprietari[20], che rac-

---

l'Unione Europea manifesterebbe una visione del fenomeno eccessivamente orientata in chiave industriale e poco attenta ai profili di sostenibilità dello sviluppo.

18 In sintesi, sul fondamentale rapporto di derivazione che lega il domicilio alla libertà personale, cfr. Scarlatti, *Libertà e inviolabilità del domicilio*, in *Diritto on line-Treccani*, 2016.

19 Cfr. Palmerini, *Dalle* smart cities *allo* scoring *del cittadino*, in *I Confini del Digitale. Nuovi scenari per la protezione dei dati*, Convegno per la Giornata europea della protezione dei dati personali 2019 - 29 gennaio, Roma, p. 17 ss., specie p. 23.

20 Sono le considerazioni di Pizzetti., *Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la* privacy, reperibile nel sito web www.*agendadigitale.eu*, 4 aprile 2018, secondo il quale gli assistenti digitali intelligenti sono paragonabili a «moderni maggiordomi dell'era digitale, ma, esattamente come i maggiordomi vittoriani, sanno tutto di ciò che accade nella casa e tutto registrano e ritrasmettono».

colgono dati non solo sulle proprie *performance*, quali prodotti, ma anche dati personali (scelte, preferenze, abitudini di consumo ...) degli utenti stessi; assistenti personali virtuali, dunque, che imparano a conoscere l'utente che interagisce con loro molto a fondo, e persino ad anticipare le relative richieste, eventualmente stipulando anche i relativi contratti[21].

Inoltre, gli assistenti vocali sono costantemente in attività grazie agli altri dispositivi ai quali sono connessi. Ciò può significare che, anche quando l'*assistant* non è in utilizzo, trasmette in continuazione ogni accadimento o variazione dell'ambiente che è in grado di percepire([22]), con la realizzazione di un'operazione continua di monitoraggio dei comportamenti e di profilazione degli individui([23]). In effetti, il rapporto vocale tra le persone e lo *speaker*, così cruciale negli assistenti, appunto, vocali, demandati a rispondere alle richieste dell'utente, è possibile in quanto l'apparecchio è dotato della capacità di ascolto non solo del comando che gli venga di volta in volta impartito, ma di tutto ciò che accade nell'ambiente circostante([24]). D'altronde, i dispositivi in questione hanno dimostrato di registrare indifferentemente tutte le conversazioni che avvengano all'interno dell'ambiente domestico, ivi comprese, dunque, quelle in cui partecipino terzi che potrebbero addirittura ignorare l'esistenza di tali *device* o il relativo funzionamento. Gli utenti, così come i terzi inconsapevoli, potrebbero persino attivare l'*assistant* inavvertitamente, con comandi vocali impartiti involontariamente: studi pratici hanno infatti svelato che molti *speaker* non solo si accendono per effetto della pronunzia delle parole convenzionali, bensì rispondono anche ad una serie di stimoli vocali ulteriori[25].

---

21 È quanto osservato da PALMERINI, *Dalle smart cities allo scoring del cittadino,* cit., p. 24.

22 V. ancora PIZZETTI, *Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la* privacy, cit.

23 In tema: PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, in CUFFARO, D'ORAZIO, RICCIUTO (a cura di), *I dati personali nel diritto europeo,* cit., p. 413 ss.

24 Nella scheda informativa dell'Autorità Garante per la protezione dei dati personali, su cui v. *infra*, par. 4, si fa espresso riferimento al fatto che «Quando è acceso ma non viene utilizzato, l'assistente digitale è in uno stato detto di *passive listening*, una sorta di "dormiveglia" da cui esce non appena sente la parola di attivazione che abbiamo scelto».

25 Soprattutto gli *home speaker* sembrano rispondere a molti più comandi vocali rispetto a quelle che sono le formule di accensione. Secondo quanto riportato dalla P*olicy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world* dello *European Consumer*

Il flusso di dati che i dispositivi generano è dunque costante e consistente: una situazione a cui fa, peraltro, da contraltare un profilo di particolare criticità, ossia la diffusa inconsapevolezza degli utenti[26], a maggior ragione particolarmente problematica proprio nei soggetti che da quelle soluzioni potrebbero trarre i vantaggi maggiori, ossia i soggetti più vulnerabili[27].

17.3. Assistenti vocali e trattamento dei dati personali

Già in siffatta esemplificazione si intravedono, a fianco delle molteplici opportunità, altrettanti rischi a carico dell'utente, soprattutto sul versante del trattamento dei dati personali[28]. Non è senza significato che ogni *Big Player* della Rete abbia creato un proprio *smart assistant*, strumento diretto per operare la profilazione dell'utente (i noti

Consultative Group, datata 16 maggio 2018, p. 13: «In 2017, the Federation of German Consumer Organisations (vzbv) analysed the voice-controlled personal assistant 'Amazon Echo' and found that the device was recording far more conversation than the user intended as it reacted not only to the activating code word 'Alexa' but also to similar words. The same has been found to be true for Google Assistant». Ancora, nella *Policy* si legge (p. 9): «Practical testing by the Digital Market Watch project of German consumer association has demonstrated that Google's Home Assistant that is supposed to be activated with the words 'OK Google' also awakens when conversations contain 'OK Kuchen' - meaning "OK cake" in German - and 'OK gut' – meaning 'OK fine'. The unwanted activation of the home assistant system entails that more private conversations are being transmitted and processed by Google than intended. Similar results were obtained for Amazon's Alexa».

26 A proposito dell'inconsapevolezza dell'utente v. Mantelero, *Data protection, e-ticketing, and intelligent systems for public transport*, in *International Data Privacy Law*, 2015, p. 309 ss.

27 Fra questi, i minori. In proposito, cfr. le preoccupazioni espresse da Palmerini, *Dalle smart cities allo scoring del cittadino*, cit., p. 25. Sulla vulnerabilità della posizione dei minori in merito al trattamento dei loro dati personali operato anche da oggetti *smart*, v. inoltre Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019, specie p. 5 ss. e p. 57 ss.

28 Sulle profonde trasformazioni legislative vissute dal settore, *in primis* legate all'entrata in vigore del Reg. Ue 679/2016, c.d. GDPR, v. in generale Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in Id (a cura di), L*a protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2017, p. 5 ss.

Siri di Apple, Alexa di Amazon, Cortana di Microsoft e Google Assistant di Google) e che proprio gli Internet Giants «are leading the pack ... with no clear competitor in sight»[29].

È in questa sede possibile soltanto accennare ai singoli profili che, dinanzi alla concreta operatività degli assistenti vocali intelligenti, svelano una particolare problematicità, senza poterli illustrare in dettaglio.

Già alcuni principi declamati dal Regolamento si attagliano con difficoltà a scenari tecnologicamente evoluti, come quello in esame, specialmente laddove — e questo può senz'altro accadere — il trattamento dei dati raccolti dagli assistenti vocali si traduca in un'attività di *Big data analytics*, ossia in un procedimento di raccolta e analisi di grandi volumi di dati (*Big Data*)(30). Fra questi, i tre principi tra loro strettamente connessi della minimizzazione dei dati trattati (art. 5, 1° c., lett. c) GDPR), della limitazione della loro conservazione (art. 5, 1° c., lett. e) GDPR) nonché della limitazione delle finalità del trattamento (art. 5, 1° c., lett. b) GDPR): non è infrequente che spesso si assista a raccolte di dati personali in notevoli quantità, sicuramente eccessive rispetto alle finalità del trattamento[31], con la frequente possibilità che questi vengano, peraltro, conservati oltre il necessario.

Di fronte a siffatto contesto, neppure l'anonimizzazione [32], anch'essa prevista dal Regolamento, e costituente una misura di pro-

---

[29] Lo riporta lo studio della Commissione europea, datato gennaio 2018, *The rise of Virtual Personal Assistants*, il cui testo è reperibile nel sito web www.ec.europa.eu.

[30] Particolarmente significative, in materia, due relazioni del Garante della privacy inglese (*Information Commissioner's Office*, ICO), *Big data, artificial intelligence, machine learning and data protection*, 2017, e *Anonymisation: managing data protection risk, code of practice*, 2012, reperibili entrambe sul sito web dell'Autorità.

[31] Sulla problematicità delle situazioni — quali quelle qui in considerazione — in cui le informazioni sono inferite dai dati, tale che la finalità del trattamento non è chiara fin dal principio, ma si va definendo con il trattamento stesso e dunque non può essere comunicata all'interessato, v. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in RUFFOLO, GABRIELLI, *Intelligenza artificiale e diritto*, cit., p. 1675.

[32] Sull'anonimizzazione in generale, e sulle incertezze relative al concetto di identificabilità dell'interessato, cfr. PELLECCHIA, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, p. 360 ss.

tezione dei dati personali, a sua volta coerente con il principio di minimizzazione, dimostra particolare efficacia[33]. Premesso che l'anonimato del dato è di per sé un parametro relativo, in quanto correlato alla collegabilità del dato all'interessato, che a sua volta dipende da circostanze specifiche (il soggetto che opera il collegamento, il contesto in cui questi opera, le modalità con le quali il trattamento è eseguito ...)[34], proprio rispetto a grandi volumi di dati raccolti da una pluralità di fonti, le pratiche di anonimizzazione risultano particolarmente inadatte, dal momento che l'incrocio di dati consente un'alta possibilità di re-identificazione dell'interessato[35], vanificando l'anonimato stesso.

Va inoltre tenuta in debita considerazione la circostanza per cui gli *speaker* intelligenti sono idonei a raccogliere e trattare non solo dati che costituiscono caratteristiche personali dell'utilizzatore (sesso, età, ecc.), ma anche informazioni che rientrano fra le categorie particolari *ex* art. 9 GDPR[36], come i dati sanitari (si pensi a uno *smart assistant* istruito per ricordare l'orario di assunzione di farmaci) e soprattutto i dati biometrici[37]. L'attivazione e/o operatività dello *speaker* stesso dipende infatti dal comando vocale; se poi lo *smart assistant* è dotato anche di videocamera lo stesso raccoglierà dati quali la conformazione

---

33 Specificamente sull'anonimizzazione e i rischi di re-identificazione nel contesto dell'*IoT* e dei *Big Data*, v. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., in Cuffaro, D'Orazio, Ricciuto (a cura di), *cit.*, p. 1222-23, Mantelero, *La* privacy *all'epoca dei* Big Data, *ivi*, p. 1190-91. Sulle difficoltà legate all'anonimizzazione nel contesto dei *Big Data* cfr. anche De Gregorio, Torino, Privacy, *protezione dei dati personali e* Big Data, in Tosi (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, cit., p. 474-5.

34 Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, cit., p. 1675.

35 Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, *cit.*, p. 1219.

36 De Gregorio, Torino, Privacy, *protezione dei dati personali e* Big Data, cit., p. 470-1 evidenziano per vero come perda di significato anche la distinzione fra dati personali e categorie particolari di dati, in merito alla *Big Data Analytics*, laddove quindi vengano raccolti e trattati grandi volumi di dati, e laddove vi sia la possibilità di inferire dati personali da dati rientranti nelle categorie particolari e viceversa.

37 Sui dati biometrici v. Pulice, *Sistemi di rilevazione di dati biometrici e* privacy, in *Lav. giur.*, 2009, p. 994 ss., e, da ultimo, le riflessioni di R. Ducato, *I dati biometrici*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 1285 ss. (sulla loro definizione e collocazione normativa, prima e dopo l'avvento del GDPR, cfr. in particolare p. 1294).

dell'iride e le espressioni del volto, dalle quali ricavare persino stati emozionali, e sarà in ogni caso capace di geolocalizzare l'utente.

Come noto, i dati biometrici sono una tipologia di dati personali connotata da peculiarità intrinseche, in cui si verifica quella sostanziale coincidenza fra persona e dato che rende il corpo del soggetto strumento per la sua identificazione, con le conseguenti possibili incidenze sull'identità stessa della persona(38). Inoltre, i dati biometrici sono atti a rivelare caratteristiche uniche del soggetto, tanto da essere i soli dati personali a consentire un'identificazione univoca della persona(39). Se in generale, le tecnologie biometriche apportano consistenti vantaggi pratici, poiché consentono il riconoscimento automatizzato dei soggetti e incentivano la semplificazione di una pluralità di procedure, anche nell'esercizio delle attività quotidiane[40], dall'altro lato, i rischi che si profilano per l'interessato, connessi ad un utilizzo illegittimo o inappropriato dei dati biometrici, divengono particolarmente consistenti[41]: dai pericoli connessi al furto di identità[42] ai rischi correlati all'idoneità, propria delle tecniche biometriche, di consentire rilevazioni a distanza degli interessati, o di rappresentare la base per trattamenti discriminatori[43].

Ove l'obiettivo prioritario degli *smart assistant* sia la profilazione dell'utente a fini commerciali, per l'invio in particolare di pubblicità comportamentale, il trattamento dei dati sanitari e biometrici apre poi scenari molto più delicati. Il rischio che si prospetta è legato alla presenza di *bias*, per tale intendendo quelle distorsioni che gravano le decisioni assunte da sistemi informatici automatizzati che «discriminano

---

38 Al riguardo, v. le riflessioni di BISI, *Il corpo come* password: *alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e dir.*, 2005, p. 3 ss.

39 Cfr. GRECO, MANTELERO, *Industria 4.0, robotica e* privacy-by-design, cit., p. 883 ss.

40 Per una ricognizione dei settori di operatività delle tecniche biometriche, cfr. DUCATO, *I dati biometrici*, cit., p. 1286.

41 DUCATO, *I dati biometrici*, cit., p. 1287.

42 V. BISI., *Il furto d'identità: panoramica attuale e prospettive giuridiche*, in *Ciberspazio e dir.*, 2004, p. 303 ss.

43 Sui rischi di discriminazione derivanti precipuamente dal trattamento di dati biometrici, che possono riguardare anche i lavoratori, v. PIERUCCI, *Videosorveglianza e biometria*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 1627 ss., eDE BERNART, *Art. 114, Garanzie in materia di controllo a distanza*, in CARAVÀ, SCIAUDONE (a cura di), *Il codice della privacy - Commento al d.lgs. 196/2003 e al d.lgs. 101/2018*, Pisa, 2019, p. 575 ss.

sistematicamente e ingiustamente certi individui o gruppi di individui a favore di altri», negando opportunità o generando risultati indesiderati per motivi irragionevoli o inappropriati[44]. La profilazione è espressamente definita dall'art. 4, par. 4 e regolata nell'art. 22 del GDPR, mentre il principio di non discriminazione non è sancito esplicitamente dal GDPR. Tuttavia, a parte la sua valenza di principio generale a fondamento delle carte europee[45], come puntualmente osservato, a partire dal considerando n. 71 dello stesso — laddove si stabilisce che è opportuno che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate che tengano conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impediscano tra l'altro effetti discriminatori — si ricava l'esistenza di ulteriore principio fondamentale, definito «latente» nella trama normativa, di «non discriminazione algoritmica», da riferirsi non solo alla profilazione, ma anche a qualsiasi altra forma di algoritmo predittivo[46]. Si tratta di una problematica complessa da risolvere, rispetto alla quale anche le soluzioni avanzate si moltiplicano. Da un lato si propone il ricorso all'intervento normativo atto a regolare i processi decisionali in cui siano coinvolti algoritmi. Questo implicherebbe un'estensione dell'oggetto della disciplina giuridica, che dovrà rivolgersi a entrambi i profili della decisione algoritmica: un profilo definito «interno», concernente il funzionamento dell'intelligenza artificiale, rispetto al quale occorrerà dettare regole volte ad evitare che il sistema possa generare decisioni discriminatorie; e un profilo definito «esterno» al funzionamento dell'intelligenza artificiale, relativo al peso che l'algoritmo esplica sulla decisione finale, e al possibile intervento umano in chiave mitigatrice e di controllo[47].

---

44 Così Friedman, Nissenbaum, *Bias in Computer Systems*, in *14 ACM Transactions on Information Systems*, 1996, p. 332 ss. Cathy O'Neil usa l'efficace espressione «Armi di distruzione matematica», che dà il titolo al suo scritto tradotto da Cavallini e edito nel 2016 da Bompiani.

45 Ci si può limitare in questa sede a citare il «Manuale di diritto europeo della non discriminazione» edito nel 2011 ad opera della Corte europea dei diritti dell'uomo e dell'Agenzia dell'Unione europea per i diritti fondamentali.

46 Simoncini, *L'algoritmo incostituzionale*, cit., p. 84 osserva ulteriormente come se anche l'algoritmo sia conoscibile e comprensibile, esso può essere di per sé discriminatorio e dunque incostituzionale.

47 Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, p. 202, e P. Zuddas, *Intelligenza artificiale e discriminazione*, *Consulta Online*, 16 marzo 2020, p. 11.

Dall'altro lato, vi è invece chi, partendo dal presupposto per cui non sia pensabile che gli sviluppatori degli algoritmi possano definire in maniera autoreferenziale e senza rischio di distorsioni i valori codificati negli algoritmi impiegati per governare la società, prospetta non un intervento legislativo, ma piuttosto l'adozione di un approccio partecipativo al processo di analisi del rischio, quale mezzo idoneo anche a consentire la piena attuazione del diritto dei consociati a prendere parte alle decisioni che li riguardano[48]. In tale ottica, si propone pertanto l'ampliamento della valutazione del rischio anche alla partecipazione di comitati di esperti o comitati etici, in grado di rappresentare le istanze sociali insite nelle soluzioni tecnologiche elaborate[49].

Quale che sia la soluzione preferibile, emerge con evidenza che il problema di fondo si traduce sul piano della programmazione e "*design*" dei modelli algoritmici e delle soluzioni tecnologiche che di quei modelli fanno applicazione.

17.4. Verso una concretizzazione della *privacy by design*: le recenti indicazioni del Garante

Dinanzi alle rilevate difficoltà, una soluzione "a monte" potrebbe essere di tipo "progettuale" e consistere nel compiere opportune scelte appunto di progettazione del programma di assistenza vocale. Così, esso dovrà essere strutturato ad esempio sulla minimizzazione dei dati raccolti, o sull'uso di tecniche di crittografia e/o pseudonimizzazione, per quanto possibile, nella trasmissione degli stessi all'*Internet Service Provider*; e ancora dovrà attivarsi solo quando riconosca l'apposito comando vocale dell'utente primario, escludendo dunque la raccolta e il trattamento di dati riguardanti altri soggetti [50] e dovrà consentire

---

48 MANTELERO, *La gestione del rischio nel GDPR, limiti e sfide nel contesto dei* Big Data *e delle applicazioni di* Artificial Intelligence, in MANTELERO, POLETTI (a cura di), *Regolare la tecnologia, il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna,* Pisa, 2018, p. 304.

49 MANTELERO, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review,* Volume 34, Issue 4, August 2018, p. 754 ss.

50 Con riguardo proprio ai *voice assistants* HOOFNAGLE, *Designing for Consent*, in *EuCML*, 2018, p. 167, ove si afferma che «[t]echnology may evolve to solve the prob-

all'utente la possibilità di programmare determinate modalità di funzionamento.

Si tratta di una direzione, quella incentrata sulla progettazione, incoraggiata anche dalla Scheda informativa diffusa dal Garante per la protezione dei dati personali nel marzo 2020, relativa proprio agli *smart assistant*[51]. Tale documento contiene alcune raccomandazioni, rivolte agli utenti, finalizzate ad un migliore utilizzo degli assistenti vocali. Alcune delle precauzioni formulate appaiono, per vero, assai semplicistiche e manifestano un eccessivo affidamento sulle capacità di discernimento dell'utilizzatore dello *speaker*. Fra queste «Informati sempre su come vengono trattati i tuoi dati» e «Non dire troppe cose allo *smart assistant*»: indicazioni che presumono la possibilità di conseguire un'informazione e una conoscenza di buon livello circa il funzionamento dello *speaker*, per vero raramente verosimili nell'utenza.

Altre raccomandazioni, invece, alludono, ben più significativamente, alle plurime modalità, in termini di operatività, dello *smart assistant* stesso. Fra esse «Decidi quali funzioni dell'assistente digitale mantenere attive[52]», «Disattiva l'assistente digitale quando non lo usi»: simili indicazioni presuppongono, oltre a un livello minimo di conoscenza da parte dell'utente, che l'assistente vocale offra concretamente la possibilità di impostare tali modalità determinando le relative opzioni.

L'adozione di una soluzione di tipo "progettuale", come è stata definita, consentirebbe l'immissione sul mercato di un prodotto o servizio che sia già stato testato non solo come efficiente (ad esempio sul versante energetico) e come sicuro[53], ma anche come conforme alla normativa, dal punto di vista dei trattamenti dei dati.

---

lem of the secondary user consent. For instance, Amazon already has "voice profiles" that could evolve to the point that Alexa will only "listen" to those it recognizes».

51 La scheda, datata 4 marzo 2020, è reperibile nel sito web dell'Autorità.

52 La scheda in questione fa espresso riferimento all'opportunità di disattivare funzioni particolarmente "invasive", quali l'invio di messaggi, la pubblicazione sui social o il compimento di acquisti *online*, ovvero, in alternativa, alla possibilità, sempre che sia contemplata dal programma, di inserire una *password* per autorizzare l'attivazione di simili funzioni solo su specifica richiesta dell'utente.

53 La disciplina della sicurezza generale dei prodotti è contenuta nella Direttiva 3 dicembre 2001, n. 95, attuata nel nostro ordinamento giuridico dal d.lgs. 21 maggio 2004, n. 172, poi confluito negli artt. 102 ss. cod. cons. In particolare, secondo il disposto dell'art. 104, comma 1, cod. cons., i produttori possono immettere sul mercato

Verrebbe così a concretizzarsi pienamente la *privacy by design*[54] di cui al GDPR stesso (art. 25); e la *data protection* acquisirebbe un ruolo autonomo appunto nel *design* — inteso come progettazione ma anche come applicazione di opportune *business policies* o strategie organizzative[55] — del programma/dispositivo. Da ciò deriverebbe anche un significativo incoraggiamento, in favore dei produttori, verso l'adozione di criteri di tipo proattivo, anziché reattivo, nell'ottica appunto di prevenire potenziali lesioni ai danni degli interessati[56].

17.5. L'analisi dei rischi e il sistema delle certificazioni

D'altronde, la *privacy by design* è un principio strettamente legato all'analisi del rischio, che a sua volta rappresenta un vero e proprio caposaldo del GDPR. Dal momento che spesso né i titolari né i responsabili del trattamento[57] posseggono però gli strumenti adeguati per operare questa analisi, come è stato proposto, si tratterebbe di traslare l'obbligo di effettuare l'analisi stessa, in modo che i rischi che derivano dai trattamenti operati, nel caso in esame dagli *smart assistant*, siano necessariamente e previamente valutati ad opera di terzi, in maniera sostanzialmente analoga a quanto già avviene in materia di sicurezza

---

soltanto prodotti sicuri. Con specifico riguardo al tema della sicurezza nel settore della robotica intelligente e degli algoritmi, v. GAMBINI, *Algoritmi e sicurezza*, in *Giur. it*., 2019, p. 1726 ss.

54 Sul rilievo della *privacy by design*, cfr. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, p. 211 ss., la quale, sebbene a proposito dei servizi *online*, evidenzia la necessità di adottare soluzioni — riconducibili proprio al paradigma della *privacy by design* — che, adottando un approccio «*user-centric*», rafforzino il potere decisionale dell'interessato, non valorizzato invece dalle soluzioni incentrate sul rilascio del consenso.

55 Cfr. GIOVANELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., p. 1236.

56 TOSI, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice* Privacy, cit., p. 40.

57 È pur vero che gli stessi soggetti del trattamento sono, in contesti tecnologicamente avanzati, di ardua individuazione, e la scansione operata dal GDPR dagli stessi possa apparire semplicistica. Sul punto, v. MANTELERO, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it.*, 2019, p. 2779. Pone in luce le relative difficoltà individuando una vera e propria concatenazione di trattamenti, PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., p. 44 ss. e p. 76-77.

dei prodotti[58]. Tali terzi potrebbero essere, come suggerito, le Autorità garanti stesse[59].

In questa prospettiva, si osserva che la valutazione del rischio si sposterebbe, almeno parzialmente e indirettamente, anche a carico del produttore/fornitore del servizio/prodotto *smart*, che verrebbe ad esempio ad essere gravato dell'obbligo di procurarsi idonea certificazione.

È, in effetti, altamente probabile (ed anche auspicabile) che nel contesto in questione un ruolo operativo importante venga assunto dalle certificazioni di cui agli artt. 42 ss. GDPR, ad oggi non ancora operanti nel nostro Paese, ma verso cui si sono ormai mossi i primi passi: la convenzione firmata in data 20 marzo 2019 tra Accredia e l'Autorità Garante, intervenuta subito dopo la pubblicazione del report finale della Commissione europea sui meccanismi di certificazione[60] ha impegnato i due soggetti ad uno scambio di informazioni sulle attività di accreditamento e sulle certificazioni previste dal GDPR. Nello specifico, ad Accredia è affidato il compito di attestare la competenza degli organismi in conformità alla norma UNI CEI EN ISO/IEC 17065, per la certificazione dei prodotti e servizi, e in base ai «requisiti aggiuntivi» che saranno individuati dal Garante a partire dalle Linee guida comuni elaborate dal Comitato europeo per la protezione dei dati personali. Sicuramente, il meccanismo delle certificazioni contribuirà all'identificazione dei rischi, nell'intento di individuare le migliori prassi per attenuare gli stessi e dovrebbe dunque prevenire la verificazione dei relativi danni.

Un'importanza significativa, su un piano distinto ma collaterale, è destinata ad essere assunta dalla normativa in tema di *cybersecurity*,

---

58 V. Mantelero, *Responsabilità e rischio nel Reg. Ue 2016/679*, cit., p. 149, e Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., p. 1225, che, nella stessa ottica, valorizza il ruolo della DPIA.

59 Cfr. Mantelero, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer law & security review*, 2014, p. 643 ss., sopr. p. 661 ss., che si pronuncia a favore della rivitalizzazione del modello autorizzatorio impiegato dalle prime generazioni di normative sui dati personali.

60 Cfr. il *Final report* della Commissione europea del febbraio 2019 *Data Protection Certification Mechanisms under Articles 42 and 43 of the General Data Protection Regulation* (GDPR) (EU) 2016/679 (*Study on*).

dopo l'approvazione della Direttiva 2016/1148 (c.d. direttiva NIS, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione). Anche se questa normativa riguarda un rischio diverso da quello della *Data Protection*, ossia il rischio dell'interruzione o dell'attacco *cyber* al servizio, nel caso del *Cloud computing* il rispetto di essa e l'acquisizione della certificazione europea di *cybersecurity* rafforzerà l'affidabilità del fornitore, specie quando questi si avvalga a sua volta di servizi (ad esempio di stoccaggio delle informazioni) forniti da ulteriori terzi[61]. Non vi è dubbio che gli *smart assistant* rientrino a pieno titolo in questo contesto.

In effetti, il GDPR ha inteso attribuire un ruolo fondamentale proprio agli strumenti di *soft law*[62]: codici di condotta e certificazioni *in primis*. Dall'art 42.1 GDPR risulta infatti evidente come agli Stati membri, alle autorità di controllo, al comitato e alla commissione, sia attribuito il compito di "incoraggiare", a livello di Unione Europea, meccanismi di certificazione della protezione dei dati allo scopo di dimostrare la conformità al Regolamento. L'istituzione di meccanismi di certificazione, sigilli e marchi di protezione dei dati rappresenta — o meglio, dovrà rappresentare — un importante strumento di autoregolamentazione privata anche nel settore della *data protection*. Come ulteriormente osservato su un piano più generale, con l'avvento del GDPR, il ruolo delle Autorità di controllo e vigilanza è profondamente mutato in direzione espansiva: esse, nel contesto della società digitale, non si limitano infatti alla mera vigilanza sul rispetto delle norme, bensì devono necessariamente svolgere anche un «ruolo proattivo»

---

61 V. in argomento VACIAGO, *L'attuazione della Direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi: i punti di contatto con il Regolamento UE 2016/679*, in CUFFARO, D'ORAZIO, RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 1147 ss., il quale osserva come in proposito assumerà un'importanza fondamentale l'applicazione del Regolamento volto a creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali, c.d. *Cybersecurity Act*, che idealmente si colloca dopo l'approvazione della Direttiva NIS del 2016. Il *Cybersecurity Act* mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali, oltre che a rafforzare il ruolo dell'ENISA. Esso è entrato in vigore il 27 giugno 2019. Sul tema, più in generale, v. inoltre CONTALDO, SALANDRI, *La disciplina della* cybersecurity *nell'Unione Europea*, in CONTALDO, MULA, *Cybersecurity Law*, Pisa, 2020, p. 1 ss.

62 La cui non vincolatività non è considerata tale da mettere a rischio quanto meno l'obiettivo dell'armonizzazione da RICCIO, PEZZA, *Certification Mechanism as a Tool for the Unification of the Data Protection European Law*, in *Medialaws*, 2018, p. 252.

nella direzione della protezione concreta dei diritti dei soggetti coinvolti[63]. Tale impianto appare perfettamente in linea proprio con l'esigenza che la protezione dei dati personali venga garantita fin dalla progettazione dei trattamenti, complessivamente intesa nell'accezione di predisposizione, ma anche applicazione di opportune strategie organizzative, conformemente alla tecnica della *privacy by design*.

Nell'assetto del Regolamento 2016/679, la centralità degli obblighi che gravano su titolare e responsabile del trattamento assegna alle certificazioni il ruolo non certo di produrre l'effetto di *discharge* di tali obblighi[64], ma piuttosto di agevolare nella dimostrazione della *compliance* alla normativa europea[65], al punto che le certificazioni vengono definite come veri e propri *accountability tools*[66]. Le certificazioni saranno rilasciate — una volta che il relativo meccanismo diverrà operativo — oltre che da autorità indipendenti, da organismi privati accreditati, chiamati a verificare la conformità del trattamento a criteri approvati alle autorità nazionali o dal Comitato europeo, nell'ottica, in questo secondo caso, di pervenire ad un vero e proprio «sigillo europeo per la protezione dei dati»[67]. Sicuramente, il meccanismo delle certificazioni contribuirà all'identificazione dei rischi, nell'intento di individuare le migliori prassi per attenuare gli stessi[68] e dovrebbe dunque prevenire la verificazione dei relativi danni.

---

63 Pizzetti, *Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in Mantelero, Poletti (a cura di), *Regolare la tecnologia*, cit., p. 78.

64 Come ribadito anche dalla versione definitiva dell'allegato 2 delle Linee guida sulla certificazione del Comitato europeo per la protezione dei dati, aggiornate al 4 giugno 2019.

65 V. Poletti, Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in Tosi (a cura di), Privacy *digitale*, cit., p. 376 ss.

66 Cfr. ancora Poletti, Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, *cit*., 379 e Riccio, Pezza, *Certification Mechanism as a Tool for the Unification of the Data Protection European Law, cit*., p. 256 ss.

67 Sileoni, *I codici di condotta e le funzioni di certificazione*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 924 e Poletti, Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, cit., p. 410.

68 Considerando n. 77 GDPR.

Nella direzione individuata, la nozione di sicurezza del servizio/prodotto da tenere a riferimento non sarebbe più la mera sicurezza informatica[69] o la sicurezza del solo processo di trattamento dei dati, ma, in un'ottica più ampia, la sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali della persona, che dall'operatività di quel servizio/prodotto possono essere compromessi[70]. L'analisi del rischio finirebbe in tal modo per "entrare" già dentro il prodotto o il servizio fornito all'utente, il quale non dovrebbe quindi preoccuparsi (sempre che sia in grado di farlo) di comprendere la reale incidenza del funzionamento del programma o dispositivo acquistato — nel caso qui considerato l'assistente vocale — sulla protezione dei propri dati personali.

---

69 TOSI, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice* Privacy, cit., p. 52, propone un approccio integrato che consideri sia le istanze della *privacy* che quelle della *cybersecurity*.

70 MANTELERO, *La gestione del rischio nel GDPR,* cit., p. 305.

Elenco autori/contributi

1. Attilio Altieri, *Assegnista di ricerca in Diritto commerciale presso l'Università degli Studi di Foggia*;

2. Giuseppina Capaldo, *Professoressa ordinaria in Istituzioni di diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

3. Lucio Casalini, *Dottore di ricerca in Diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

4. Ettore William Di Mauro, *Ricercatore in Diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

5. Andrea Maria Garofalo, *Ricercatore in Diritto privato presso l'Università Ca' Foscari di Venezia*;

6. Massimo Foglia, *Ricercatore in Diritto privato presso l'Università degli Studi di Bergamo*;

7. Daniele Imbruglia, *Ricercatore in Diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

8. Enzo Maria Incutti, *Dottorando in Diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

9. Laura Mancini, *Dottoranda in Diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

10. Salvatore Orlando, *Professore ordinario in Istituzioni di diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

11. Federico Pistelli, *Assegnista di ricerca in Diritto privato presso l'Università degli Studi Roma Tre*;

12. Eugenio Prosperi, *Dottorando in Diritto commerciale presso l'Università degli Studi di Roma, "La Sapienza"*;

13. Marco Rizzuti, *Ricercatore in Diritto privato presso l'Università degli Studi di Firenze*;

14. Federico Ruggeri, *Dottorando in Diritto privato presso l'Università degli Studi di Roma, "La Sapienza"*;

15. Chiara Sartoris, *Assegnista di ricerca in Diritto privato presso l'Università degli Studi di Firenze*;

16. Shaira Thobani, *Ricercatrice in Diritto privato presso Unitelma Sapienza*;

17. Lavinia Vizzoni, *Assegnista di ricerca in Diritto privato presso l'Università degli Studi di Siena*.

Il Comitato editoriale assicura una valutazione trasparente e indipendente delle opere sottoponendole in forma anonima a due valutatori, anch'essi anonimi. Per ulteriori dettagli si rinvia al sito: www.editricesapienza.it

Collana Materiali e documenti

Per informazioni sui precedenti volumi in collana, consultare il sito:
www.editricesapienza.it

60. CNDSS 2019
Atti della IV Conferenza Nazionale delle Dottorande e dei Dottorandi in Scienze Sociali
a cura di Giovanni Brancato, Gabriella D'Ambrosio, Erika De Marchis, Raffaella Gallo, Melissa Stolfi, Marta Tedesco

61. INDUSTRIA, ITALIA
Ce la faremo se saremo intraprendenti
a cura di Riccardo Gallo

62. Sistema bibliotecario Sapienza 2012-2020
a cura di Giovanni Solimine ed Ezio Tarantino

63. «Scrivere le cose d'Italia»
Storici e storie d'Italia tra umanesimo e controriforma
Elena Valeri

64. Lezioni di radiologia pediatrica
Mario Roggini

65. Il fascino dei minerali
Un mondo di forme e colori
Claudio Gambelli

66. Scritti di Alfonso Archi sulla religione degli Ittiti
a cura di Rita Francia, Valerio Pisaniello, Giulia Torri

67. La letteratura neogreca del xx secolo
Un caso europeo
Atti del convegno internazionale di Studi neogreci in onore di Paola Maria Minucci – Roma, 21-23 novembre 2018
a cura di Francesca Zaccone, Paschalis Efthymiou, Christos Bintoudis

68. La "realtà del disegno" nell'opera di Cesare Tacchi
Gaia Lisa Tacchi

69. Cesare Tacchi
Dalla "realtà dell'immagine" alla spiritualità della pittura, attraverso il progetto
a cura di Emanuela Chiavoni e Gaia Lisa Tacchi

70. Introduzione al neurodesign
L'applicazione delle neuroscienze agli studi di design
Fabio Babiloni, Loredana Di Lucchio, Marco Montanari, Alessio Paoletti, Davide Perrotta

71. Nascita e sviluppo dei Corsi di Laurea in Psicologia alla Sapienza
a cura di Maria Casagrande

72. La guarigione dopo "EVAR"
Aspetti clinici e metodologici
a cura di Maurizio Taurino

73. Past (Im)Perfect Continuous
Trans-Cultural Articulations of the Postmemory of WWII
edited by Alice Balestrino

74. Architetture per il restauro: l'anastilosi
a cura di Rossana Mancini, Roberta Maria Dal Mas, Maria Giovanna Putzu

75. Annuario 2021
Osservatorio Giuridico sulla Innovazione Digitale
Yearbook 2021
Juridical Observatory on Digital Innovation
a cura di Salvatore Orlando e Giuseppina Capaldo

Il volume contiene contributi di docenti e ricercatori di varie Università italiane su una pluralità di tematiche che sollecitano la riflessione circa la tenuta delle categorie tradizionali del diritto privato a cospetto delle trasformazioni dei modelli di relazione tra i privati recate dalle tecnologie digitali. Gli scritti sono maturati nel contesto delle attività di ricerca e seminariali promosse dall'Osservatorio Giuridico sulla Innovazione Digitale (OGID), costituito presso il Dipartimento di Diritto ed economia delle attività produttive dell'Università Sapienza di Roma.

I curatori dell'opera, **Salvatore Orlando** e **Giuseppina Capaldo**, sono professori ordinari di diritto privato presso il Dipartimento di Diritto ed economia delle attività produttive di Sapienza Università di Roma.

ISBN 978-88-9377-186-3

www.editricesapienza.it